Real Time Location System (RTLS)

Version 4.0

System Design Document

October 2014

Revision History

Date	Version	Description	Author
October 2014	4.0	Subsequent Submission to VA (NDR)	HP RTLS Team
August 2014	3.0	Subsequent Submission to VA	HP RTLS Team
November 2013	2.0	Subsequent Submission to VA	HP RTLS Team
October 2013	1.0	Initial Submission to VA	HP RTLS Team

Table of Contents

List of Figures

List of Tables

1 Introduction

The Department of Veterans Affairs (VA) is seeking an integrated, enterprise-wide solution for a Real Time Location System (RTLS) for VA. The RTLS will be used for the purpose of tracking equipment, supplies, and instruments, and may, in the future, be used for many other possible uses, including tracking staff, patients, paper documents, and other items. In addition, environmental monitoring such as humidity and temperature monitoring are required. Multiple tags and technologies will be needed for deployment (using existing wireless infrastructure, or wired infrastructure) to meet specifications and specialized needs.

The Veterans Health Administration (VHA) has a requirement to implement RTLS in all its facilities over the next several years. As currently envisioned, each VHA Veterans Integrated Service Network (VISN) or facility will have its own RTLS database that will be accessible via a single, standard user interface. The RTLS at each VISN or facility must also be capable of exchanging data with VA information systems (e.g., VistA) and with a single national information system, (the National Data Repository [NDR]), that will serve to aggregate and display RTLS data from all facility and/or VISN-level RTLS Databases (*design dependent*), and where analytics and business intelligence (BI) tools can be utilized to make enterprise-wide studies and decisions. The NDR, at a minimum, will need to be a database solution with open, flexible architecture that will house sophisticated business intelligence, predictive analytics, and reporting capabilities used for process improvement, business and financial analytics, workflow analysis and research analysis.

1.1 Purpose of this Document

The purpose of this document is to describe in sufficient detail how the proposed system is to be constructed. The System Design Document translates the Requirement Specifications into a document from which the system integrators and developers can create the actual system. It identifies the top-level system architecture, and identifies hardware, software, communication, and interface components. All information is provided to the extent that it is known.

1.2 Identification

This SDD applies to the integration of the RTLS within the VA environment. The RTLS includes RTLS infrastructure components, software, hardware, and tags deployed at local VA facilities, up through the NDR. RTLS will interface with numerous VA systems including multiple packages within VistA, and other VA owned third party systems. RTLS will confirm to the following standards:

1. RTLS shall comply with section 508 requirements as covered at http://www.section508.gov.
2. RTLS displays shall be HIPAA-compliant as covered at http://www.hhs.gov/ocr/privacy/ .
3. RTLS shall comply with the Federal Information Processing Standard (FIPS) 140-2. Information on FIPS can be found at http://www.itl.nist.gov/fipspubs/
4. RTLS shall comply with 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002." Information on FISMA can be found at http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
5. RTLS system will be compliant with all applicable healthcare Food and Drug Administration (FDA) Global Standard (GS1) global standards to include:
    a. Global Location Number (GLN).
    b. Global Trade Identification Number (GTIN) allocation rules
    c. Global Traceability Standards for Healthcare
    d. EPCglobal Pedigree Messaging Standard
    e. Global Data Synchronization Network (GDSN) Trade Item Extension: Healthcare.
    f. Automatic Identification and Data Capture (AIDC) Application Standard.

g. Automatic Identification and Data Capture (AIDC) Application Standards for Small Instruments.

Additional Information on the FDA GS1 Standard can be found at http://www.fda.gov/RegulatoryInformation/Guidances/ucm125505.htm

6. RTLS shall comply with EPC Global Tag Data Translation v1.4 http://www.gs1.org/sites/default/files/docs/tdt/tdt_1_4-standard-20090610.pdf
7. RTLS shall comply with EPC Global UHF Class 1 Gen 2 Standard v. 1.2.0 http://www.gs1.org/sites/default/files/docs/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf
8. RTLS shall comply with EPC Global Low Level Reader Protocol Standard v1.0.1 http://www.gs1.org/sites/default/files/docs/llrp/llrp_1_0_1-standard-20070813.pdf
9. RTLS shall comply with EPC Global Discovery Configuration & Initialization Standard v1.0 http://www.gs1.org/sites/default/files/docs/dci/dci_1_0-standard-20090610.pdf
10. RTLS shall comply with EPC Global Reader Management Standard v1.0.1 http://www.gs1.org/sites/default/files/docs/rm/rm_1_0_1-standard-20070531.pdf
11. RTLS shall comply with EPC Global EPC Information Services Standard v1.0.1 http://www.gs1.org/sites/default/files/docs/epcis/epcis_1_0_1-standard-20070921.pdf
12. RTLS shall comply with EPC Global Application Level Events Standard v1.1.1 http://www.gs1.org/sites/default/files/docs/ale/ale_1_1_1-standard-core-20090313.pdf http://www.gs1.org/sites/default/files/docs/ale/ale_1_1_1-standard-XMLandSOAPbindings-20090313.pdf
13. RTLS shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (http://www.cio.gov/documents/IPv6memofinal.pdf). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267, http://www.antd.nist.gov/usgv6/) and NIST SP 800 series applicable compliance, shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g., web, email, Domain Name Service (DNS), Internet Service Provider (ISP) services, etc.) shall support native IPv6 users, and all internal infrastructure and applications shall operate using native IPv6. To ensure interoperability, IPv4 will coexist during the transition to IPv6, and it is expected that VA will continue running IPv4 until it is phased out by 2015. By 2015, all computing, application and network resources must turn off IPv4 as a communication mechanism in VA, unless a waiver is obtained from the Office of the Principal Deputy Assistant Secretary for Information and Technology, Department of Veterans Affairs or the device/service runs in an enclave.
14. RTLS shall comply with the following Internal Organization of Standardizations (ISO):

RTLS

a. The RTLS shall be compliant with ISO/IEC Standards for RTLS: 24730-1, 2, 3, and 5.

Radio Frequency Identification (RFID)

a. The RTLS shall be compliant with the following ISO/IEC Standards; 1800:1,3-7, 1801, 15961:1-4, 15962:.1, 15963:.1, 24710, 24729:3,4, 24752, 24753, 29158.

Bar Codes

a. For systems that utilize barcodes, the system shall be compliant with the following ISO/IEC Standards for testing and quality control; 15960, 15415, 15416, 15421, 15423, and 24720. The system shall be compliant with the following ISO/IEC Standards for data carrying related to bar codes; 15417, 15424, 15438, 16022, 16023, 16388, 16390, 24724, 24728, and 24778.

Interoperability

a. The proposed RTLS aligns with industry standards for interoperability ISO/IEC 24730.

Security

a. The proposed RTLS aligns with industry standards for security ISO 15693.

Quality

a. The proposed RTLS aligns with industry standards for quality. ISO/IEC TR 18046-18047.

1.3 Scope

The following tables identify the scope of the RTLS procurement. The scope of the system is governed by the set of business needs that have been identified as part of the required functionality for the anticipated June 2012 award. The potential uses and benefits of this technology throughout VA are significant, and include improvement of quality of patient care, improved patient satisfaction, reduction of health care asset management costs, improvement of capacity/resource planning, improvement of employee and patient safety, as well as improvement of general asset management and inventory. Only those business needs that contain RTLS requirements are included in the Table 1 below.

Note: For further details, on which requirements are to be included in RTLS v1.0, see Overview of Significant Requirements.

Table 1: RTLS Scope Inclusions

Includes
BN 1: Adhere to the Enterprise-Level requirements within the Enterprise Requirements Repository (ERR).
BN 2: Procurement of a RTLS solution that will meet national VA requirements and support local needs to improve operational efficiency and the quality of Veteran care.
BN 3: This RTLS National Data Repository (NDR) application will have the ability to analyze data from multiple front-end RTLSs, as well as AEMS-MERS and other VistA packages.
BN 4: This RTLS National Data Repository (NDR) application will have the ability to generate reports from analyzed and aggregated data.
BN 5: All of the RTLS solution will track all equipment for purposes of conducting inventory, alert of theft, and finding the assets when needed.

The scope of this document covers the initial RTLS deployment, including 4 primary use cases that were identified by the RTLS Program Management Office (PMO) as providing the initial set of base use cases for procurement. These use cases include Asset Tracking, Cardiac Catheterization Lab supply tracking, Sterile Processing Service (SPS) workflow and instrument tracking, and Temperature Monitoring. Others will be added as future use cases are identified.

1.4 Relationship to Other Plans

The following functional requirements documents directly apply to this SDD:

- RTLS 20110208 Business Requirement Document version 2.3
- RTLS Requirement Specification Document version 1.1
- RTLS Use Cases (Note: TBA: Add link)

1.5 Methodology, Tools, and Techniques

Per ProPath recommendation, the technical details have been flushed out to this initial draft through conceptual design. Technical writing and Integrated Project Team (IPT) reviews will then provide a clean-up service on the documents way to Project Management Accountability System (PMAS) Review (as part of a packet of artifacts required to attain the Active state). From that review, changes will be implemented to further refine the accuracy of the document's technical content.

With the input of several program and project peers, the document will be ready for the Formal Review. Any feedback coming from this review will be implemented, as well. Any SDD change requests made during the development phase are then addressed as needed and changes captured throughout.

In addition, the RTLS program shall maintain a repository that contains all required artifacts (as defined in ProPath and the PMAS Guide section 3.1). The PMAS Artifact Central Repository (ACRe) will be a Microsoft Office SharePoint Server (MOSS) site created for all Office of Information and Technology (OIT) projects. The process for establishing a project artifact repository is in ProPath. PMAS projects will keep using their current organizational repositories until the new PMAS Artifact Central Repository is available.

1.6 Policies, Directives and Procedures

ProPath is the OIT-wide process management tool that assists in the execution of an Information Technology (IT) project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed. This document conforms to the ProPath template for the SDD and is required in the planning phase of a project. It is part of Determining Requirements which came after Developing the Project Management Plan. In ProPath 6.0 it is expected to come prior or at the same time as Developing the Project Management Plan.

PMAS mandates that all new VA IT projects/programs uses an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for Information and Technology, PMAS is a VA-wide initiative to better empower the Office of Information Technology (OIT) Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

Clinical data fetched from the source systems may contain Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 Code of Federal Regulations (CFR) Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the system shall be architected to protect PHI and ePHI.

1.7 Constraints

As with most nationwide deployments, the design of the RTLS is constrained by the requirements of numerous existing systems and other deployments that are taking place in the same time frame. The RTLS will be constrained to operate, to the maximum extent possible, utilizing the Wi-Fi infrastructure for location finding and tracking. The Wi-Fi deployment within the VA, and especially at the Veteran Affairs Medical Centers (VAMCs), is currently in progress and is planned to take several years to complete. Given this dependence on Wi-Fi, RTLS is schedule-constrained to be deployed to locations only after the Wi-Fi rollout to that location has occurred.

For locations that are not planned to receive Wi-Fi, (primarily Community-Based Outpatient Clinics – CBOCs) but where RTLS is desired, RTLS will utilize a nationally approved alternate technology that is designed to work with this package, but is now constrained by the desire to reduce the amount of infrastructure needed to deploy this alternate technology. Part of the Wi-Fi infrastructure is a Cisco Mobility Services Engine (MSE). To provide location data via the Wi-Fi network, the RTLS solution requires that each local facility (VAMC, CMOP, or CBOC) have an operating MSE.

Additionally, much of the source data for RTLS tagged items resides within existing VA systems, primarily VistA. This requires that the RTLS interface with these VA systems. Although the RTLS vendor will be the primary developer of these interfaces, some portion of the work will likely need to be done by VA staff. Given the numerous other projects ongoing within the VA that are planning to modify VistA, and the limited resources for development and testing within the VistA environment, the development of these RTLS-VistA interfaces may be constrained due to competing requirements for the same resources within the VA.

An additional constraint with regard to VistA data interfaces is VA's current move toward an "open source" model for VistA, and the associated need to define a "gold standard" version of VistA for conversion to open source. This may delay or preclude the ability to modify VistA in order to accommodate data interfaces to RTLS.

Another potential constraint is the desire of the VA to reduce the server infrastructure hosted and maintained at local facilities by moving to either regional VA data centers or to a national VA data center, or possibly even to a government-wide "cloud" data center. The VA is also in the midst of an initiative to maximize the amount of server virtualization at all locations.

With regard to supported web browsers, the expectation is that the RTLS system will be a web-based system with a large user base across the many VA facilities. Therefore, VA required that the software be able to run within the approved browsers used in the VA, without the need for custom plugins which would be difficult to manage on hundreds of thousands of computers.

Table 2 RTLS 1.0 Constraints

Req. ID	Requirement
DCS-010	The RTLS shall utilize VA enterprise software where possible.
DCS-020	VA Enterprise software includes: 1. Windows Server 2008 R2x64 2. Red Hat Enterprise Linux 6.5 3. Microsoft SQL Server 2012 4. IBM BigFix 5. Microsoft SCCM 2007 (System Center Configuration Manager) 6. Guidance EnCase 7. McAfee ePO (e-Policy Orchestrator) 8. McAfee VirusScan Enterprise V8.7 & HIPS V7.0 (Host Intrusion Prevention System)

Req. ID	Requirement
	9. SecureWave Sanctuary
DCS-030	The RTLS User Interfaces shall be compatible with Microsoft Windows XP SP3 Client Operating systems and newer.
DCS-040	The RTLS User Interfaces shall be compatible with Internet Explorer 7 or greater.
DCS-050	The RTLS browser and desktop configuration shall be in accordance with Federal Desktop Core Configuration (FDCC).
DCS-060	The RTLS browser configuration shall not require custom browser configuration.
DCS-070	RTLS shall utilize Wi-Fi as its primary location and wireless communication technology, except where otherwise approved by VA.
DCS-080	Data held within systems of record (such as VistA) shall, to the maximum extent possible, be pointed to by reference rather than stored by RTLS.

The NDR will be designed and developed with the following Constraints:

- Corporate Data Warehouse (CDW) Tools
    - Microsoft SQL Server 2012
    - Microsoft SharePoint 2013
    - Microsoft Hyper-V
    - TOAD Data Modeller
    - Embarcadero ER/Studio
    - SAS Analytics Pro
    - SAS Enterprise Miner
    - SAS Operation Research
    - SAS Access
    - SAS Connect
    - Tableau Desktop 8.2/Reader 8.1
    - ArcGIS v10
- VA Active Directory – the NDR will use existing and newly created active directory groups and service accounts authorized by National Data Systems (NDS) and administered by the Business Integrated Service Line – Office of Information and Technology (BISL-OI&T) and CDW.

1.8 Design Trade-offs

The conceptual design of the RTLS involves numerous tradeoffs, many of which are heavily design-dependent. The RTLS is primarily a Commercial off the Shelf (COTS) product. Each vendor makes design decisions within their own product domain. However, the SDD will highlight design decisions regarding any integrations or interfaces to VA property. Any design has tradeoffs, and the following outlines a number of the design tradeoffs involved with RTLS.

1.8.1 Open Architecture

Open architecture based on open standards can be more difficult to implement than closed, proprietary architecture. Designing for open architecture requires technology decisions that are not necessary if only the manufacturer will need access to the system’s underlying technology. The design trade off of an open architecture versus closed, proprietary technology was made to provide major benefits to VA due to its ability to support growth and insertion of new hardware or software as technology changes and new RTLS use cases are identified and implemented over time.

1.8.2 Server Placement

RTLSs are typically designed with a facility-centric view in mind. Typically, the server infrastructure is placed within the facility to receive and process location data and provide the web services typically used to track items and produce reports. As was mentioned in the previous section, the VA desires to move away from facility-based server infrastructure to a regional or national infrastructure for housing servers, whenever possible and practical. (It should be noted that the majority of VistA systems no longer physically reside in the local facility that they serve.)

Therefore, one tradeoff within RTLS is the placement of the RTLS server infrastructure that is supporting a facility. Since RTLS will be deployed to hundreds of locations, it would be beneficial to the VA to aggregate these servers in a few locations where they can be centrally managed and maintained. (This would be especially true if multiple RTLS instances can be run on a single virtual server, using VMware or similar, in keeping with VA's initiative to maximize server virtualization.) One issue with this approach is the requirements of the applications themselves. Certain applications, such as patient elopement and theft prevention, require very low latencies and quick response times. For these cases, it is possible that at least some server infrastructure may be needed at each facility where RTLS is installed.

1.8.3 RTLS Technology Selection

RTLS as a technology has matured over the years, with numerous vendors offering a plethora of different solutions working over different frequency bands. Given the multiple offerings from the vendors, one design tradeoff is in which technology to use. Wi-Fi is being widely deployed within the VA medical centers and presented a logical base technology for RTLS applications. Wi-Fi has been mandated as the backbone infrastructure to be used by default for all actively tagged applications in facilities that have, or are slated to get, ubiquitous Wi-Fi coverage. Areas requiring greater spatial resolution than can be provided with Wi-Fi alone will utilize a complementary technology, such as infra-red or ultrasound. Additionally, for certain areas where VA does not intend to install Wi-Fi (primarily short-term leased space for CBOCs) but where RTLS capabilities are needed, an alternate technology will need to be utilized. Since the primary driver for not installing Wi-Fi at such a location is the desire to avoid the costs associated with fixed infrastructure (e.g., wiring), the alternate RTLS technology should logically be one that does not require a significant amount of fixed infrastructure.

1.8.4 Data Location

The RTLS data will not be just for local (i.e. facility-level) use, but is intended to roll up, to be used for VISN-level, regional, and national reporting and analysis. The RTLS will generate large quantities of data per facility, which is compounded by the data obtained via interfaces to VA information systems, such as VistA. One tradeoff involves determining what data needs to be seen at each level in the hierarchy, and whether that data should be copied to both levels (i.e., local RTLS and NDR), or only a reference maintained at the national level with data retrieved from local servers when needed. Coupled with the server placement tradeoff, we see that this also involves a tradeoff in network utilization. The location and placement of servers, and the location and storage of data, and the method for accessing that data, all have impacts on the network.

1.8.5 Network and Database Design

The solution shall account for network utilization trade-offs in determining server location. The RTLS system will simplify and abbreviate data in transit without diminishing the meaning or the value that the data provides, thereby reducing bandwidth considerations. The data transfer shall take into account size, distance and time when operating across the VA nationwide network. Trade-offs in database design, location, frequency of updates, time and frequency of queries and cost all impacted System Architecture decisions. The solution should provide a flexible system architecture that can accommodate numerous interfaces at potentially multiple levels in the architecture.

The RTLS data itself will not be just for local use, but is intended to roll up to be used for VISN level, regional, and national reporting and analysis. The RTLS system itself shall generate large quantities of data per facility, which is compounded by the interfaces to local data maintained within the source VA systems. One tradeoff is what data needs to be seen at each level in the hierarchy, and whether that data should be copied to the multiple levels, or only a reference maintained and data retrieved when needed.

Coupled with the server placement tradeoff, VA sees that this also involves a tradeoff in network utilization. The location and placement of servers, and the location and storage of data, and the method for accessing that data, all have design impacts on the network.

1.8.6 Backup and Disaster Recovery

An issue closely related to data storage is the strategy for data backup and for disaster recovery (DR). Although it is anticipated that the RTLS servers will be designed in highly robust and fault-tolerant configuration, a geographically separate location for backup of data is still required. If primary RTLS servers need to be at local facilities, backup servers could be located at Regional Data Centers. If the primary RTLS servers are located at a Regional or National Data Center, the backup servers could be located at another Regional or National Data Center. Alternatively, it has been suggested that the NDR also serve as the backup for data from the RTLS servers. The trade-off here is that although this saves on the cost of separate backup servers, it implies that *all* RTLS data (as opposed to a relevant subset) must be transferred to the NDR and that the transfer must occur in real time (or near real time) as opposed to batch transfer during off-peak hours, as might otherwise be considered. Real time RTLS data transfer from the RTLS servers to the NDR may lead to contention for bandwidth on the VA Wide Area Network (WAN) during peak traffic hours, or may require adding WAN capacity to accommodate RTLS traffic.

1.8.7 Tag Agnosticism

Tying the system to proprietary tags from a single vendor would have presented fewer design challenges because the closed system would be more contained. However, the VA chose a tag-agnostic RTLS approach because it will provide VA more vendor options in the future. This will reduce the risk of vendor lock-in, thereby keeping VA's tag costs as low as possible. It will also allow VA to take advantages of advances in tag technology from various vendors quicker.

1.8.8 Active Tag Beaconing Frequency

Also relevant to the discussion of how to manage RTLS data is the frequency with which active tags will update their location (beaconing). Although more frequent beaconing yields finer, more granular data about movement of a tag, it also leads to shorter battery life and to greater amounts of data to process, store, and transmit across local and wide area networks (LAN and WAN). Careful consideration will be required in order to optimize the balance (trade-off) between granularity of movement data, and data storage and bandwidth requirements. (Note: It is anticipated that all active tags will operate in "beacon mode" only, and not create associations with the wireless network or be assigned IP addresses.)

1.8.9 Location Accuracy Tradeoffs

Read range accuracy refers to how far an RFID reader can accurately track and read data from a tag. That distance, of course, depends on whether the tag is active or passive and on the line of sight availability (for certain technologies like Infrared (IR)) between reader and tag. It is also highly dependent on the tag environment, including the asset to which the tag is attached, with liquids and metal presenting Radio

Frequency (RF) attenuation challenges. Each of the different RTLS applications have varying requirements for the required location accuracy, which influences the decisions regarding the type of tags and readers used, the method of affixing the tags and ultimately influences the location accuracy that will be achieved for that application.

1.8.10 Standards-based Message-oriented Integration

Proprietary point-to-point application interfaces are initially easier to implement because they avoid implementing integration message broker infrastructure to route messages between applications. However, point-to-point application interfaces contribute to spaghetti-interface chaos and to architecture brittleness instead of flexibility. The VA chose a more robust and agile integration approach to the RTLS overall system architecture. The technical solution includes a combination of the RTLS Enterprise Service Bus (ESB) and the Intelligent InSites Connector Framework because it will ease the challenges associated with integrating numerous disparate VA systems and their information models over the long run. This will help control interface maintenance costs and can also help manage the common information model that will form the basis for enhanced application information exchange. New applications need only map their information models to the canonical message model (CMM) to participate on the message-oriented service bus rather than building separate interfaces to multiple systems.

1.8.11 Unified User Interface

Providing a single unified user interface requires more up front planning than implementing a wider variety of interfaces in different parts of the enterprise, especially when these multiple interfaces come tightly with various packaged solutions. VA decided on a unified user interface because it will reduce user learning curve and make users more productive than having to log in and out of disparate user interfaces that function in different ways. This is especially true because RTLS needs to graphically represent the location of items in relation to facility floor plans.

An exception to the unified User Interface exists. Constituent niche systems (e.g., SPS) will likely have their own user interfaces, optimized for the niche use case. Those niche user interfaces can be utilized within the niche area for staff working only with the given niche use case.

1.8.12 Meta Data Management

Metadata has been identified as a key success factor in data warehouse projects. It captures the information necessary to extract, transform, and load data from source systems into the data warehouse, and afterwards to use and interpret the data warehouse contents. The NDR requires that all data be extracted from all COTS software databases and loaded into the CDW. In order to handle such a massive undertaking, the NDR will use metadata to drive its Extract Transform and Load (ETL) platform.

1.9 User Characteristics

VA intends the RTLS to be available for use by all staff, based on the application and level of need for interaction. The following table lists a number of the different types of users and describes how they are expected to use the RTLS. As more applications are added, the user base will grow.

Table 3 User Characteristics

User	Description
Logistics Staff	Currently responsible for entering new items into Automated Engineering Management System /Medical Equipment Reporting System (AEMS-MERS) and Generic Inventory Package (GIP) and distributing items from the warehouse to their destination. Most items that fall under the Asset

User	Description
	Management and Cardiac Catheterization Supply applications will be tagged and entered into the RTLS by these users.
Information Technology (IT) Staff, Clinical Engineering, Facilities Engineering	Responsible for performing yearly inventories of assets under their purview. RTLS will be used to automate the process to a large extent. (As with all other assets, IT assets will likely also be tagged and entered into AEMS-MERS by logistics staff.)
Clinical Staff (front line and supervisory)	For VHA, the clinical staff forms the primary front-end users of the RTLS. Depending on the application, these users will be using the system for finding a required piece of equipment, determining the levels of medical supplies, finding the location of patients and inventory, and performing workflow-related queries. They are also responsible for annual inventories.
Managers, Executive Staff, National Program Offices, etc.	Users at the VISN and enterprise levels are primarily interacting with the RTLS through the NDR. Users at this level are interested in determining the utilization rates of items, analyzing current business and workflow issues to make informed decisions on process improvements, and even using the data to analyze health outcomes (measuring hand washing rates and their impact on the spread of disease within a hospital for example). Facility-level executives will also have a need for this type of data, and may utilize the local RTLS or the NDR, depending on the level of complexity of the analysis.

VA has a large and diverse group of users with commensurately different skill levels and proficiencies with computer systems. Based on the application or task that needs to be executed, the RTLS shall present a user interface that can be easily understood and maneuvered by the typical user at the appropriate skill level and provides a graphical interface that allows them to quickly search for and find tagged items, create and share reports, and analyze workflows and utilization rates for overall efficiencies and improvements.

1.9.1 User Problem Statement

The user problem statement being looked at depends on the application being analyzed.

For asset tracking, there are several issues. The first problem is with the time and cost associated with performing yearly inventories. Typically multiple people need to search through multiple rooms scanning barcodes on assets to account for item locations. Of equal importance is the desire to reduce theft/misplacement of high value items. Using the RTLS, asset management is looking to significantly reduce the time and costs associated with performing yearly inventories, and reduce the costs associated with theft/misplacement/loss of equipment.

For clinical staff looking to locate assets, the problem is one of finding medical equipment when it is needed. The goal is to increase equipment utilization rates, (i.e. reduce the amount of "extra" equipment that is needed only because a certain percentage of equipment cannot easily be located) decrease equipment rental costs, and reduce time spent searching for available medical devices.

For Sterile Processing Service (SPS), the issue is with ensuring the sterilization and decontamination process is executed efficiently and without error and ensuring that reusable medical equipment is not used on a patient until it has been properly sterilized. Additionally, there is an issue with ensuring that all trays have the correct individual items on them, and equipment and instruments needed at the time of use are available.

For temperature monitoring, the users currently have to periodically check the temperatures in refrigerators / freezers/heaters and room locations at multiple times throughout the day, and manually record the results. A refrigerator malfunctioning can have significant costs associated with the items being stored. By introducing RTLS automated temperature monitoring, the user can now remotely track the status of the temperature-keeping devices in order to automatically maintain required log sheets and the RTLS can promptly provide alerts when such devices are not operating within their programmed temperature ranges.

For cardiac catheterization lab users, not being able to properly track the consumption of items affects multiple facets of their workflow. The ability to associate items, including ones on consignment, with a specific patient or procedure, is essential for proper billing and to ensure the availability of consumed items for subsequent procedures. Often items expire, and having the capability to send an alert to staff would provide the knowledge of when items are nearing or have reached their expiration dates. Real time notification to the user that an identical item to the one just removed, with a closer expiration date, exists in the smart cabinet, will cut down on costs associated with expired items.

RTLS users currently are provided with proprietary software that includes a VISN-level Business Intelligence tool. This VISN-level Business Intelligence tool has limited reporting features and lacks the customization of reports that VA desires. RTLS users need the ability to create custom predictive analytics and business intelligence reports across all of the deployed RTLS systems. With data limited to the VISN level, users are prohibited from seeing how one facility or VISN has streamlined workflows or increased asset utilization rates when compared to another facility or VISN. The NDR provides the ability to see an enterprise view of RTLS data. The NDR will provide local through national level reporting and information sharing through an enterprise database. VA will use the NDR analytics and business intelligence tools to provide enterprise reporting, perform enterprise wide studies, and support national decisions.

1.9.2 User Objectives

There are numerous objectives being sought for the RTLS. Broadly, the VA seeks a turnkey, integrated RTLS to be deployed nationwide, as well as the ability to aggregate the data on a national level. The purpose is to improve the efficiency of certain business processes in its hospitals, clinics, offices and cemeteries.

The goals for RTLS are to:

- Improve operational efficiency
- Decrease operational costs
- Maximize equipment utilization
- Increase clinical efficiencies and staff productivity
- Enhance VA’s ability to re-design processes, based on greater insight into the movement of patients, staff, and equipment.
- Reduce delays and improve patient care
- Minimize lost and misplaced items
- Improve the quality and safety of service from patient, physician, and institutional perspectives
- Provide medical centers with the real time capability to actively track all assets, significant medical supplies, staff, patients, and environmental conditions (e.g., temperature and humidity) through a common interface and reporting tool.
- Provide VISN-level and national-level reporting and information sharing through an enterprise database
- Improve patient and staff satisfaction

From the user perspective, at a high level they desire a capability that will decrease their workload, reducing the amount of time performing tedious or time-consuming tasks. VA leaders desire greater insight into business processes, in terms of when and where items and people move and how they interact with one another, so as to be able to optimize those business processes. Leadership also desires up-to-date information on where various assets are located, in case they should need to be quickly re-deployed during a time of emergency.

2 Background

2.1 Overview of the System

The Health Care Efficiency (HCE) Major Transformation Initiative is one of the Department of Veterans Affairs (VA) Secretary's key initiatives. The goal of the HCE initiative is to reduce operational costs and create more streamlined operations in targeted program areas to enhance program efficiency across the VA enterprise.

Under the HCE initiative, the Facility Automation sub-initiative identified areas where VA currently uses manual processes/data collection methods in healthcare delivery, and established the need to automate those processes/data collection methods using RTLS. RTLS is an umbrella term that includes multiple technologies for locating and tracking objects (e.g., assets, supplies, patients, etc.). It includes Wi-Fi based location finding using, active and passive RFID tags, reading of 1D and 2D barcodes for utilization reporting, Electrochemical/Electro-erosion markings on medical/surgical instrument for reprocessing workflows, and a number of other technologies.

The potential uses and benefits of this technology throughout VA are significant, and include improvement of quality of patient care, improved patient satisfaction, reduction of health care asset management costs, improvement of capacity/resource planning, improvement of employee and patient safety, as well as improvement of general asset management and inventory.

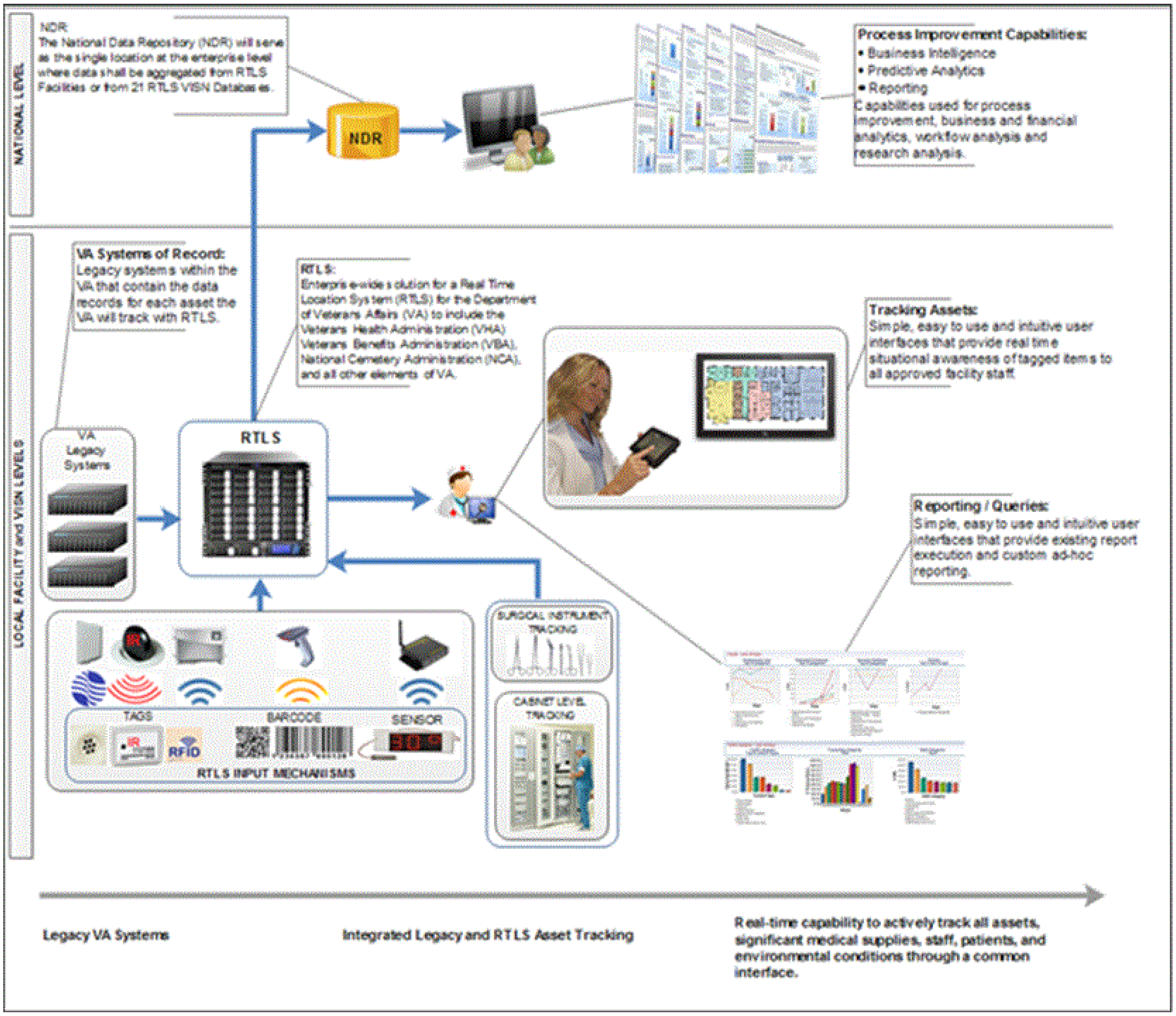
VA requires a turnkey, integrated, enterprise RTLS solution. The RTLS solution is composed of two major components - the RTLS and the NDR. The RTLS consists of the tags (active, passive, and barcodes), the databases associated with each deployment site that collect the data from the tags, and a Graphical User Interface (GUI) software application that allows users to interact with the RTLS data. An individual RTLS database may or may not be physically located at the deployment site. Additionally, an individual RTLS database may be specific to an individual facility or may be specific to an entire VISN. These configuration decisions will be made nationally and will be standardized across the enterprise.

The National Data Repository (NDR) is a data warehouse enclave within the CDW where all RTLS data will be stored. The NDR is where analytics and business intelligence tools can be utilized to provide enterprise reporting, perform enterprise wide studies, and support national decisions. NDR will provide local and national-level reporting and information sharing through an enterprise database.

The NDR will aggregate data from all individual RTLS databases to a central national database. The purpose of the RTLS solution is to improve the efficiency of targeted business processes in VA hospitals, clinics, and other facilities such as Consolidated Mail Outpatient Pharmacies (CMOP).

The following figures depict a system overview and a breakdown of the major components of RTLS and their purpose.

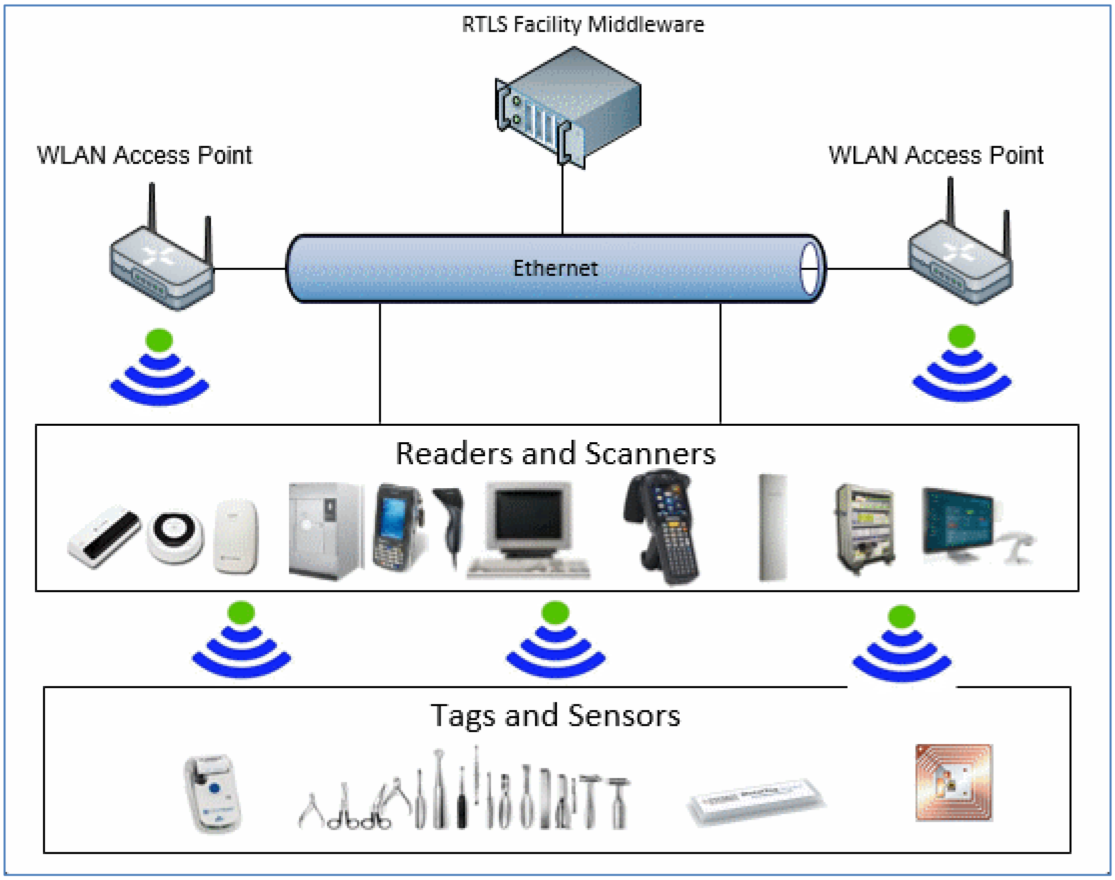
Figure 1: RTLS Overview



As shown in Figure 1, RTLS will receive data from existing VA Information Systems for most of the objects that RTLS is tracking. The RTLS shall provide spatial location information for each tagged item through RFID readers, Wi-Fi access points, location-enabled handheld wireless scanners, and barcode readers. The RTLS Middleware Server shall provide real time situational awareness of tagged items to all authorized users. It is important to note that if the overall RTLS solution includes use of existing or new niche systems (e.g., a specialized Instrument Tracking System or Temperature Monitoring System), which have their own databases, then the RTLS database at each deployment location MUST aggregate data from all of those niche systems. In this way, a user will be able to retrieve a holistic view of RTLS data for all assets without having to access multiple systems, and data from the niche systems can, if desired, interact with data from other niche systems and/or with the RTLS database at the site. Users will still be able to access and use the niche systems functionality directly, but the data will be made available to the integrated RTLS. (Note: this deployment-level aggregation of data is NOT to be confused with the NDR.)

A standard web- based reporting tool shall provide RTLS users with the ability to execute, create, save, edit and share both reports and returned data outputs. RTLS deployment-level (i.e., Facility- or VISN-level) Middleware Servers shall provide a data aggregation of both RTLS tagged object data and relevant imported VA Information and third-party Systems data to the NDR. At the NDR, sophisticated enterprise-level business intelligence, predictive analytics, and reporting capabilities are used for process improvement, business and financial analytics, workflow analysis, research analysis, and emergency management.

Figure 2: RTLS Components – Local Facility Level



As shown in **Figure 2**, a mix of RTLS trackable object data from Active and Passive RFID tags, barcodes, and sensors shall be sent to the RTLS Middleware/Application Server through both RTLS sensors and location-aware RFID and Barcode readers. Each reader shall have been authenticated and all tagged object data sent to the RTLS Middleware/Application Server.

In **Figure 3** below, the use of Wi-Fi-based technology with one add-on/complementary technology (802.11 with IR or 802.11 with Ultrasound, as examples) for the RTLS solution are being shown. The add-on technology will be required to help VA meet location proximity goals for applications where greater location accuracy (bed/bay-level as an example) is required than can be accomplished using Wi-Fi/802.11 alone.

A single, nationally standard alternate RTLS technology shall be implemented in facilities where the use of Wi-Fi is not technically or economically feasible, but where RTLS is desired.

Figure 3: National Facility-Level RTLS Deployments

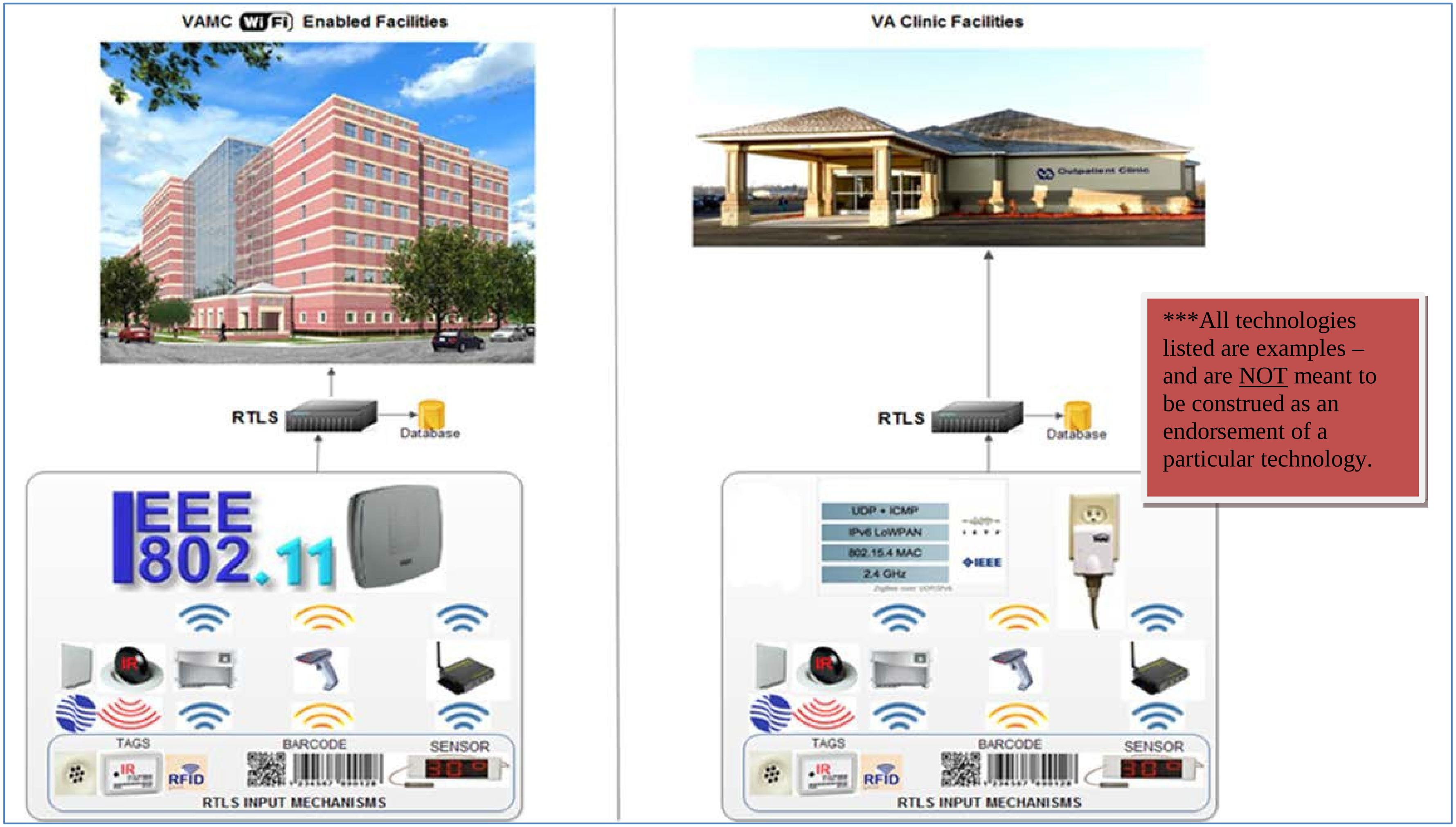
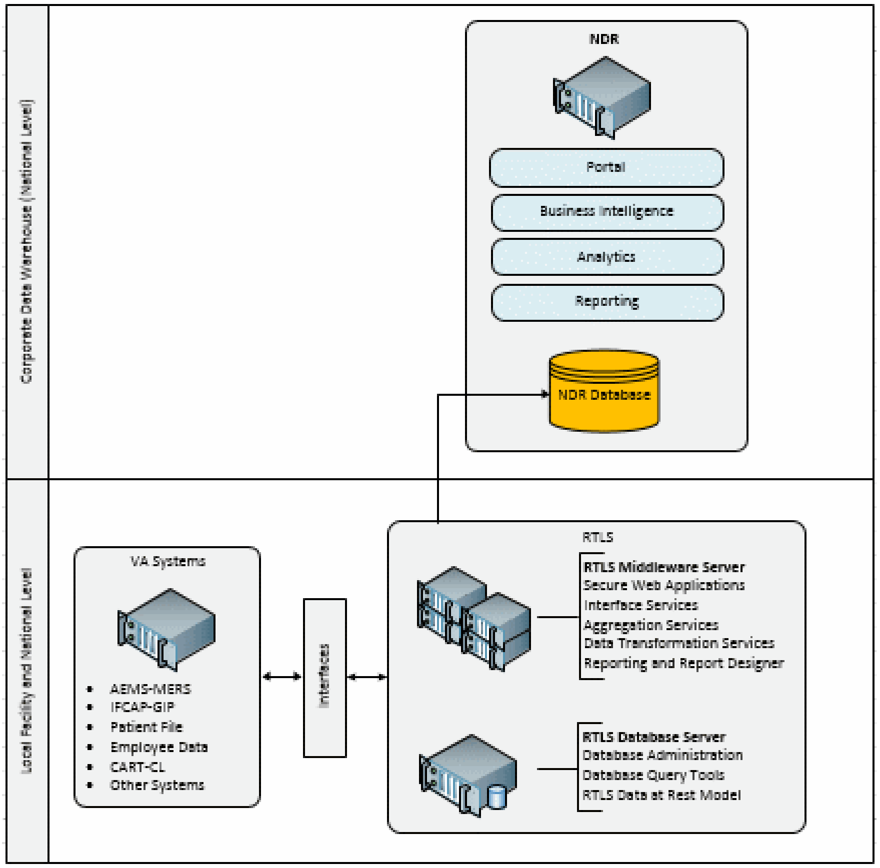


Figure 4: RTLS – Middleware & NDR Components



As shown in Figure 4, the RTLS Middleware/Application Server shall have a set of bidirectional and standards-based (e.g., open API - Application Programming Interface) interfaces to share data with VA Information Systems. Populating the RTLS with data that exist within VA Information System records shall streamline the RTLS integration to create the new RTLS item records.

The RTLS Middleware/Application Server shall contain at a minimum, the following applications to support the requirements:

- **Secure Web Applications** shall host GUI interactions between the RTLS applications and clients.
- **Interfaces Services** shall contain the individual Application Programming Interfaces (APIs) to the VA Information Systems that the RTLS applications utilize.
- **Aggregation Services** shall contain the logic and configuration GUI for sending all RTLS data to the NDR.
- **Data Transformation Services** shall provide data normalization between VA Legacy Systems data fields and the RTLS Data Model (RDM) shared across all RTLS installments.
- The **Reporting** and **Report Designer** shall provide a user-friendly database reporting tool with capability to create ad-hoc reports, execute, modify, save and share reports to users and groups with the appropriate access level at each of the RTLS installed facilities.

The National RTLS system will contain a Data Layer at the National Level (Data Warehouse with Business Intelligence functionality at VISN and Enterprise Levels). The following are components of the Data Layer:

- The **RTLS Database Server** shall incorporate information related to all RTLS Use Cases. Some of this information may be imported from other VA information systems through system interfaces, manually entered by facility personnel, or inputted by devices (e.g., RFID scanners/readers). The Database Server will provide an **Administrative and Query Tools** and contain a **RTLS data at rest**.
- The **NDR** shall host a web browser-based portal. The portal will bring information together from diverse data sources (data warehouse, data cubes, and data marts) in a uniform way. The NDR will have **Business Intelligence** tools that provide the capability to analyze business processes and workflows, determine the efficiency of the workflows, and to optimize them. NDR will have **Reporting** features that support Report Designing and Query capabilities for ad-hoc and predefined querying. The NDR shall include Predictive **Analytics** Tools for data mining and predictive modeling.

2.2 Overview of the Business Process

This section details the business practices that the RTLS will support. As additional applications are added in the future, additional business processes would be added to this section of the document. Table 4 provides a summary of the processes. See Appendix A (Section 10.7) for a legend that describes the shapes used in the RTLS Business Processes.

Table 4: Business Processes

ID	Name	Type	Owner	Description
001	Create Equipment	New	Logistics, IT, Clinical Engineering, Facilities Engineering, Sterile Processing Staff	Creates (check-ins) the equipment into the RTLS System
002	Retrieve Equipment Location	New	Logistics, IT, Clinical Engineering, Facilities Engineering, Sterile Processing Staff	Retrieves the current location of a tracked equipment asset in the RTLS System
003	Update Equipment Location	New	Logistics, IT, Clinical Engineering, Facilities Engineering, Sterile Processing Staff	Updates the current location of a tracked equipment asset in the RTLS System
004	Update Equipment Data	New	Logistics, IT, Clinical Engineering, Facilities Engineering, Sterile Processing Staff	Updates the underlying data (such as category) of a tracked equipment asset in the RTLS System.
005	Delete Equipment	New	Logistics, IT, Clinical Engineering, Facilities Engineering, Sterile Processing Staff	Decommissions a tracked equipment asset in the RTLS System
006	Create Catheterization Lab Consumables	New	Logistics, Clinical Staff	Create a new item (I.E: new consumable that has never been used) to a Smart Cabinet within the Catheterization Lab Procedure Rooms
007	Receive Catheterization Lab Consumable Inventory	New	Logistics, IT, Clinical Staff	Receive the inventory counts of items within a Catheterization Lab Procedure Room
008	Update Catheterization Lab Consumable Inventory	New	Logistics, Clinical Staff	Update the inventory counts of items within a Catheterization Lab Procedure Room (Add existing item to cabinet)
009	Update Catheterization Lab Consumable Data	New	Logistics, IT, Clinical Staff	Updates the underlying data (I.E: category) of a consumable item with a Catheterization Lab Procedure Room
010	Create Patient Encounter	New	Logistics, Clinical Staff	Create patient encounters in a Catheterization Lab

ID	Name	Type	Owner	Description
				Procedure Room (I.E: start time, staff, etc.)
011	Delete Catheterization Lab Consumable Item (End of Use)	New	Logistics, IT, Clinical Staff	Consumable item has either been installed in a patient or has been decommissioned.
012	Create Staff for Encounter	New	Clinical Staff	Adds a staff member to the RTLS Catheterization Lab System
013	Create Environmental Equipment Monitoring	New	Logistics, IT, Clinical, Sterile Processing Staff	Affix an environmental tag to an item
014	Create an Environmental Room Monitor	New	Logistics, IT, Clinical, Sterile Processing Staff	Affix an environmental tag to a room
015	Retrieve an Environmental reading	New	Logistics, IT, Clinical, Sterile Processing Staff	Retrieve an environmental reading on an item or room
016	Update an Environmental Monitor Status	New	Logistics, IT, Clinical, Sterile Processing	Updates the environmental reading on an item or a room
017	Delete an Environmental Room Monitor	New	Logistics, IT, Clinical, Sterile Processing Staff	Delete an environmental reading on a room
018	Delete Environmental Equipment Monitor	New	Logistics, IT, Clinical, Sterile Processing Staff	Delete an environmental reading on an item

Figure 5: 001Create Equipment Business Process

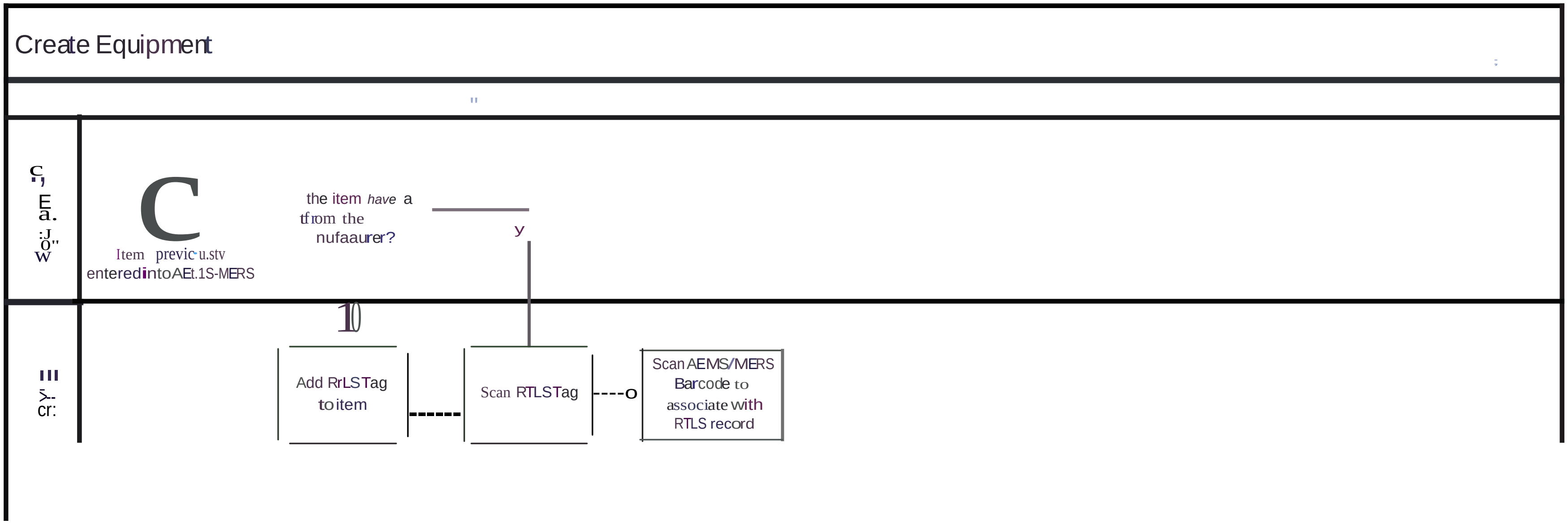


Figure 6: 002 Retrieve Equipment Location Business Process

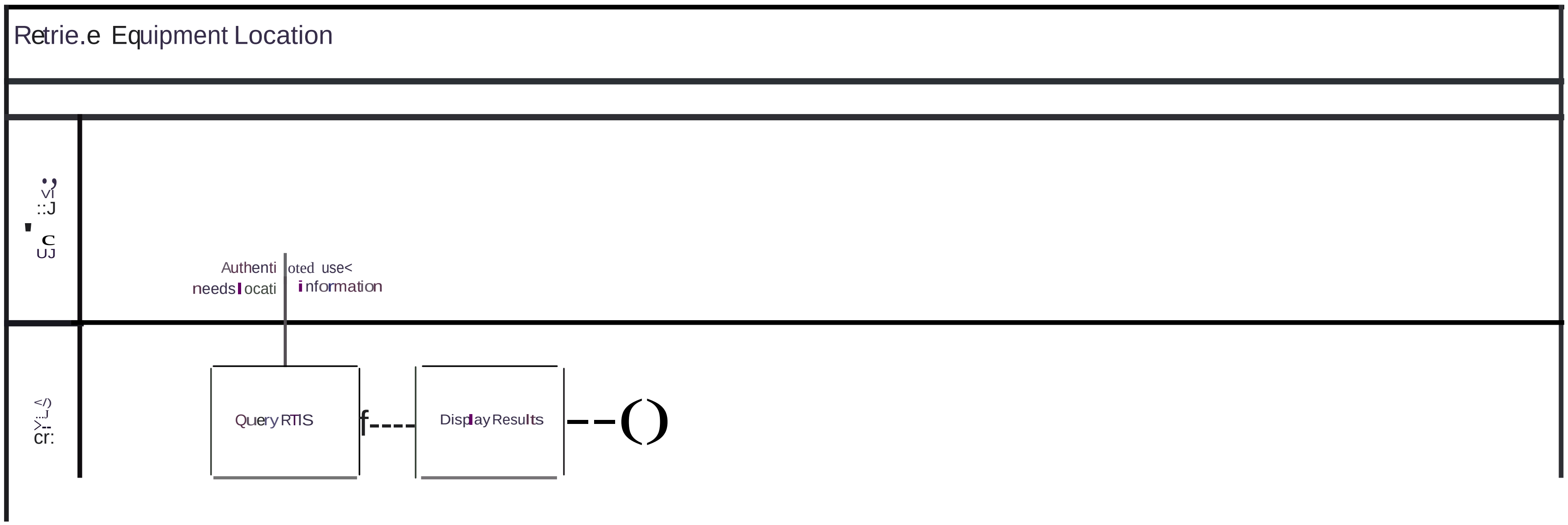


Figure 7:003 Update Equipment Location Business Process

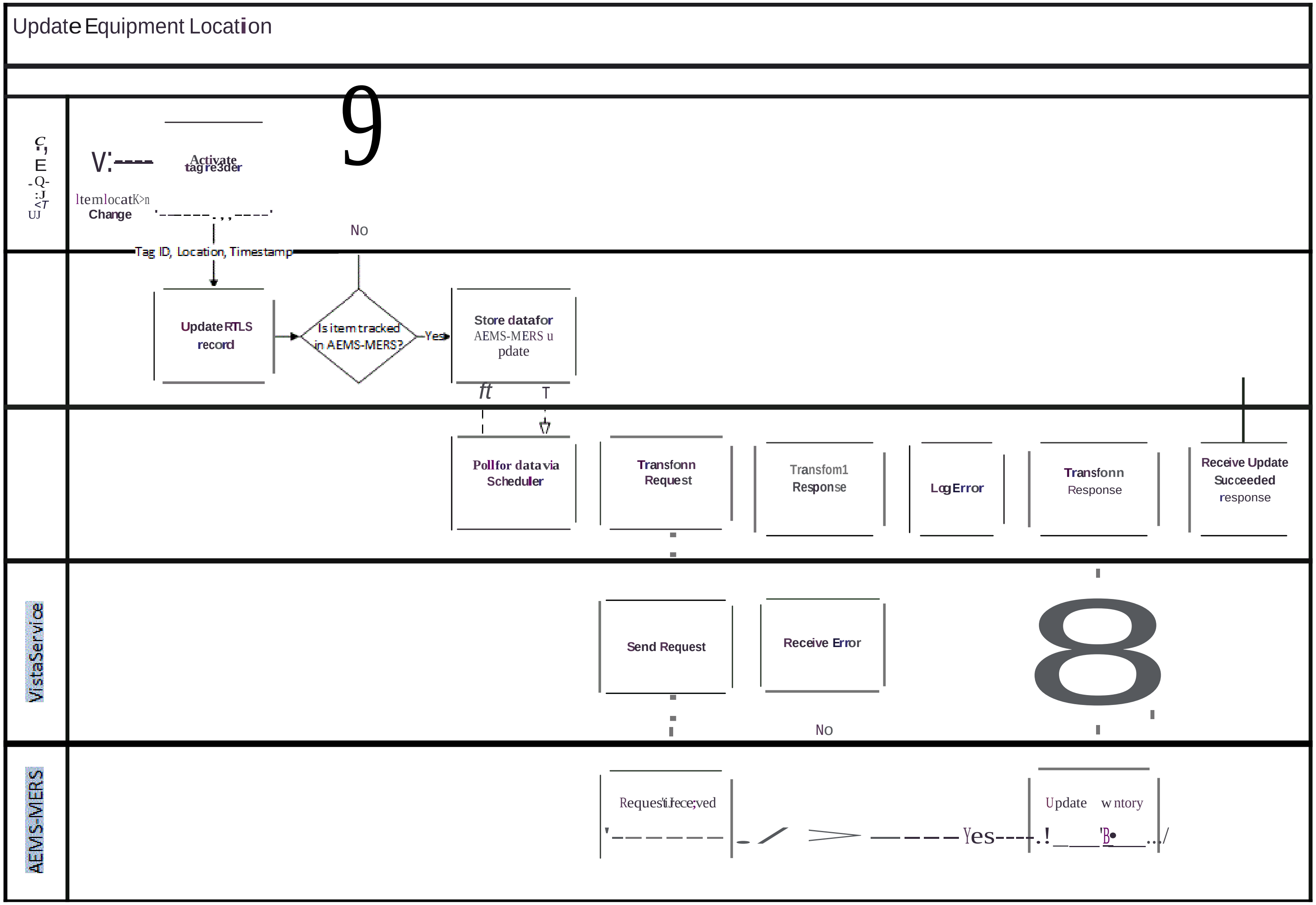


Figure 8:004 Update Equipment Data Business Process

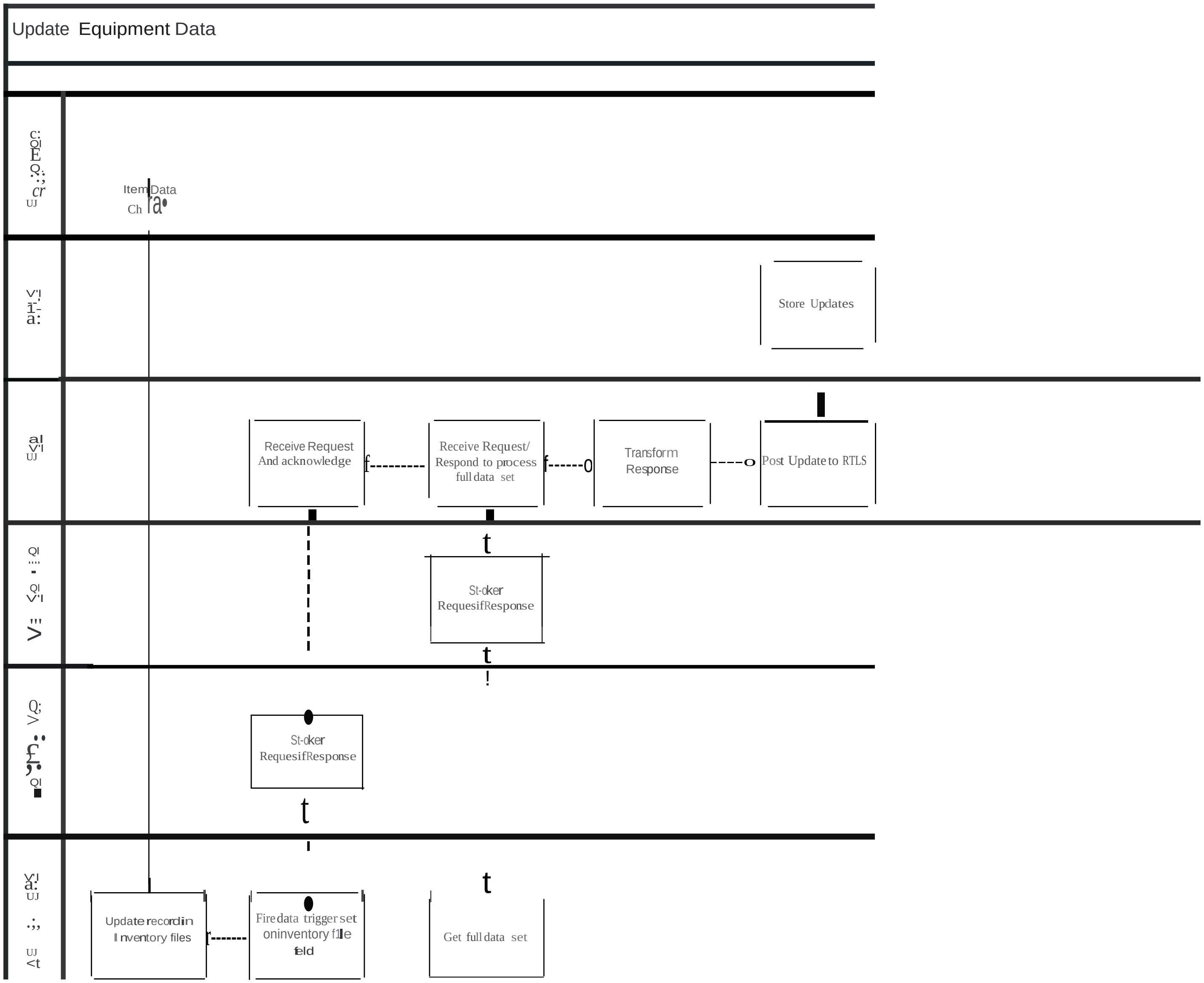


Figure 9:005 Delete Equipment Business Process

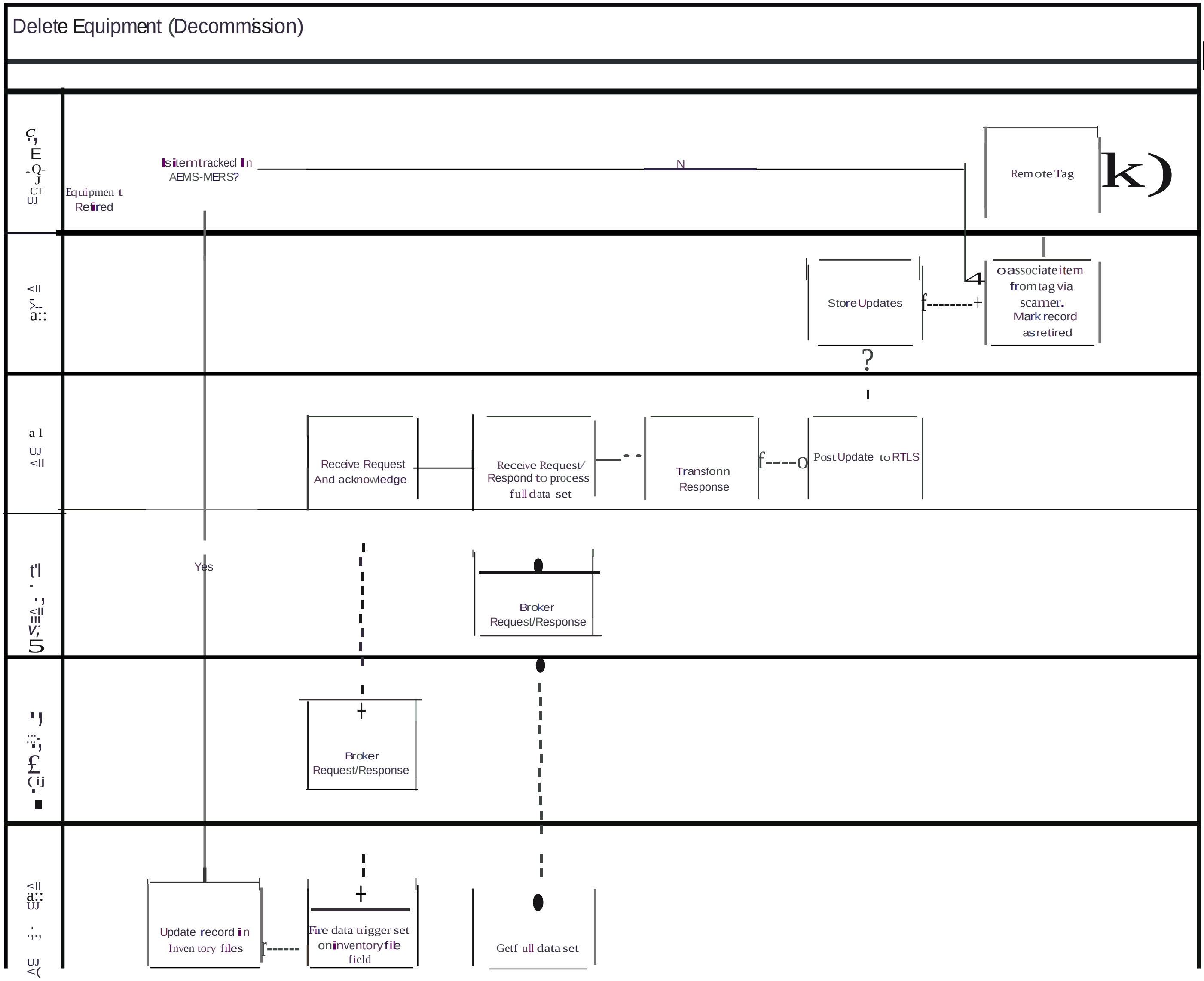


Figure 10:006 Create Catheterization Lab Consumables

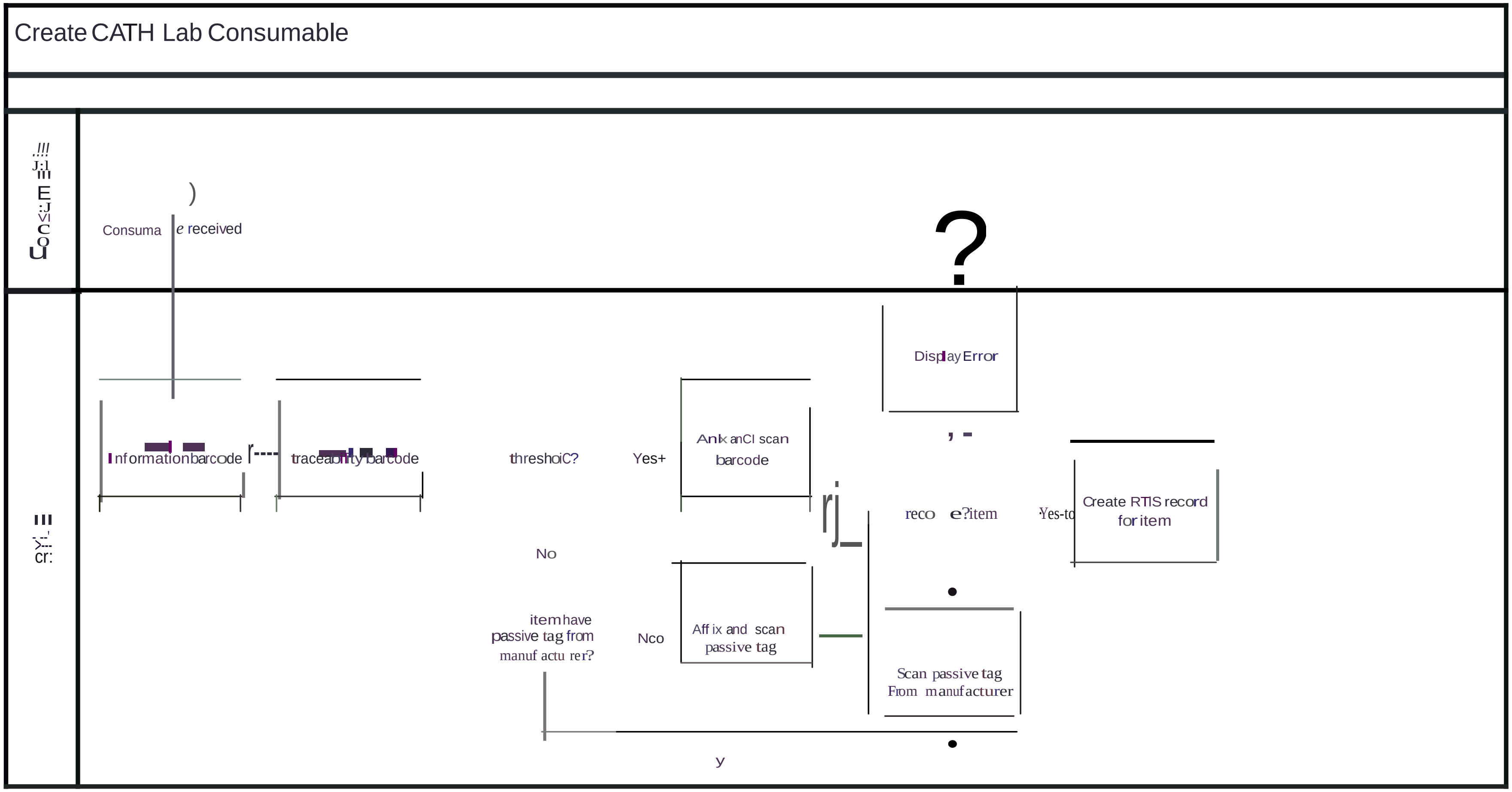


Figure 11:007 Receive Catheterization Lab Consumable Inventory

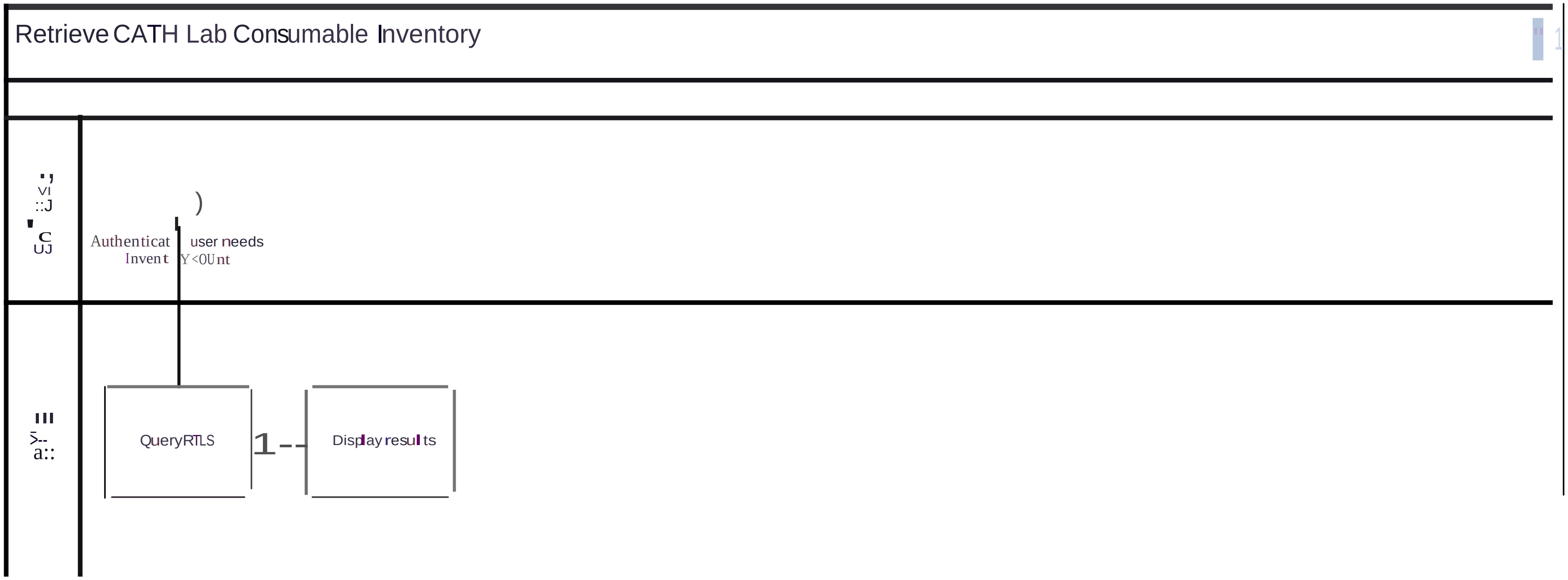


Figure 12:008 Update Catheterization Lab Consumable Inventory

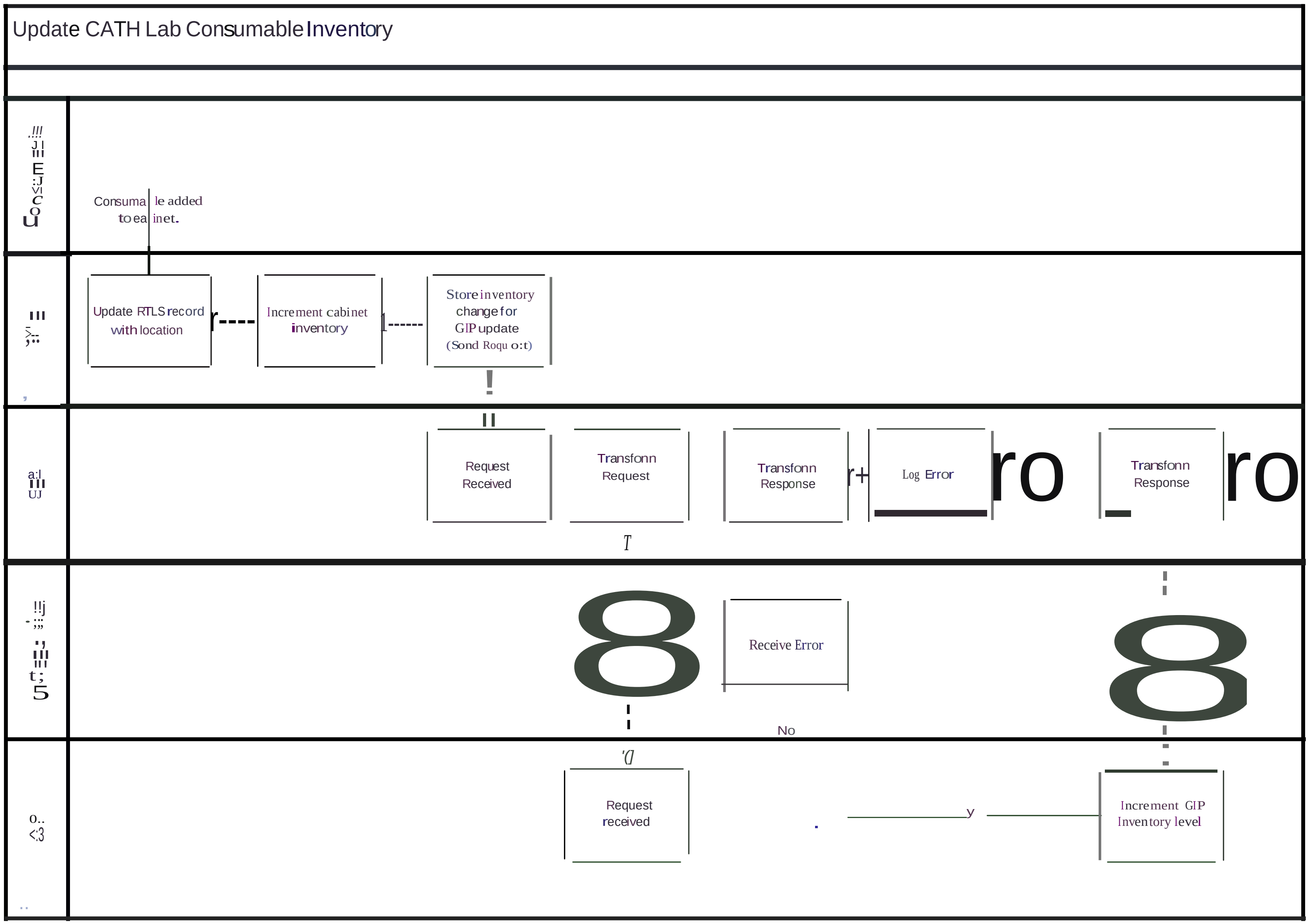


Figure 13:009 Update Catheterization Lab Consumable Data

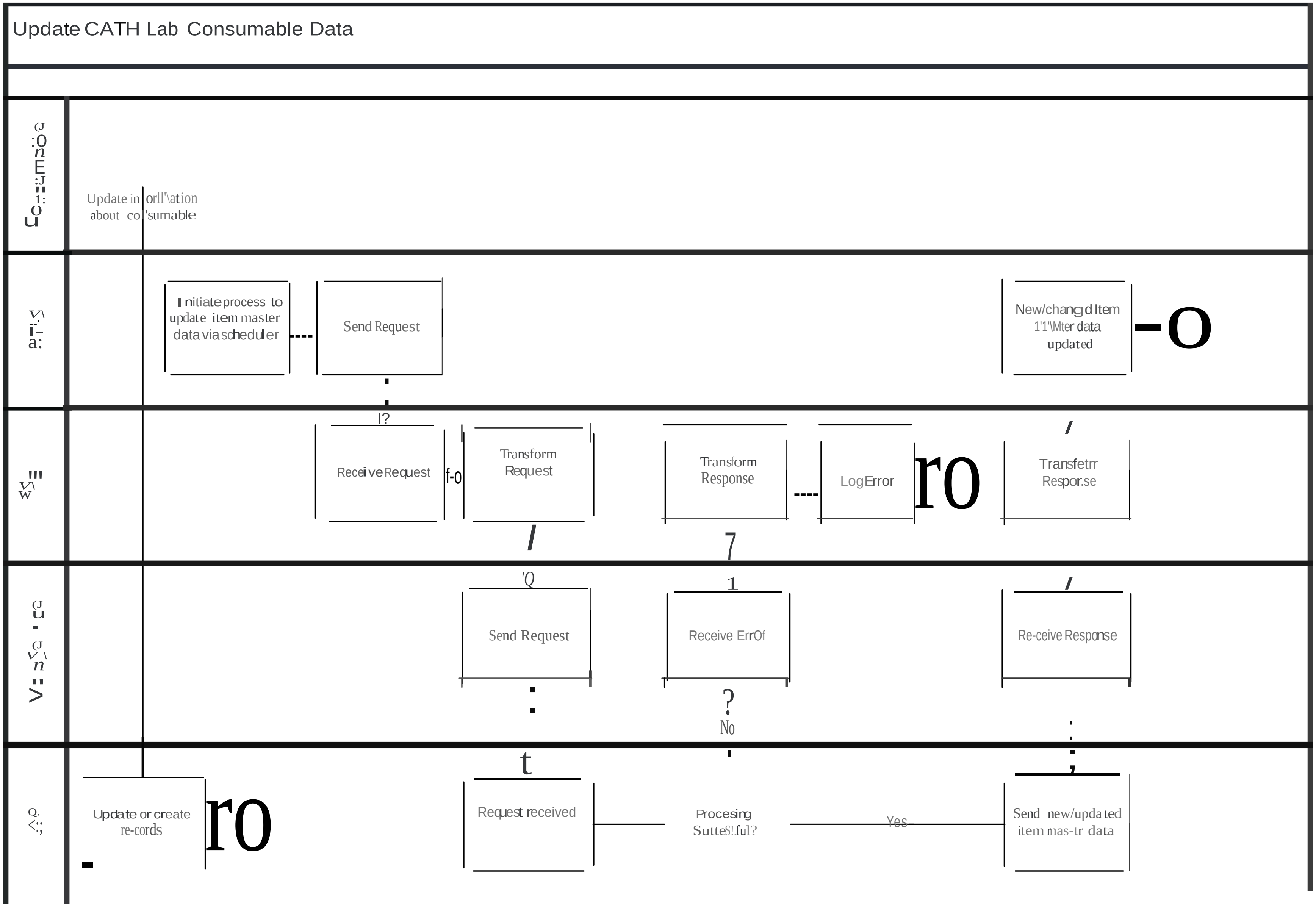


Figure 14: 010 Create Patient Encounter

Figure 15:011 Delete Catheterization Lab Consumable Item (End of Use)

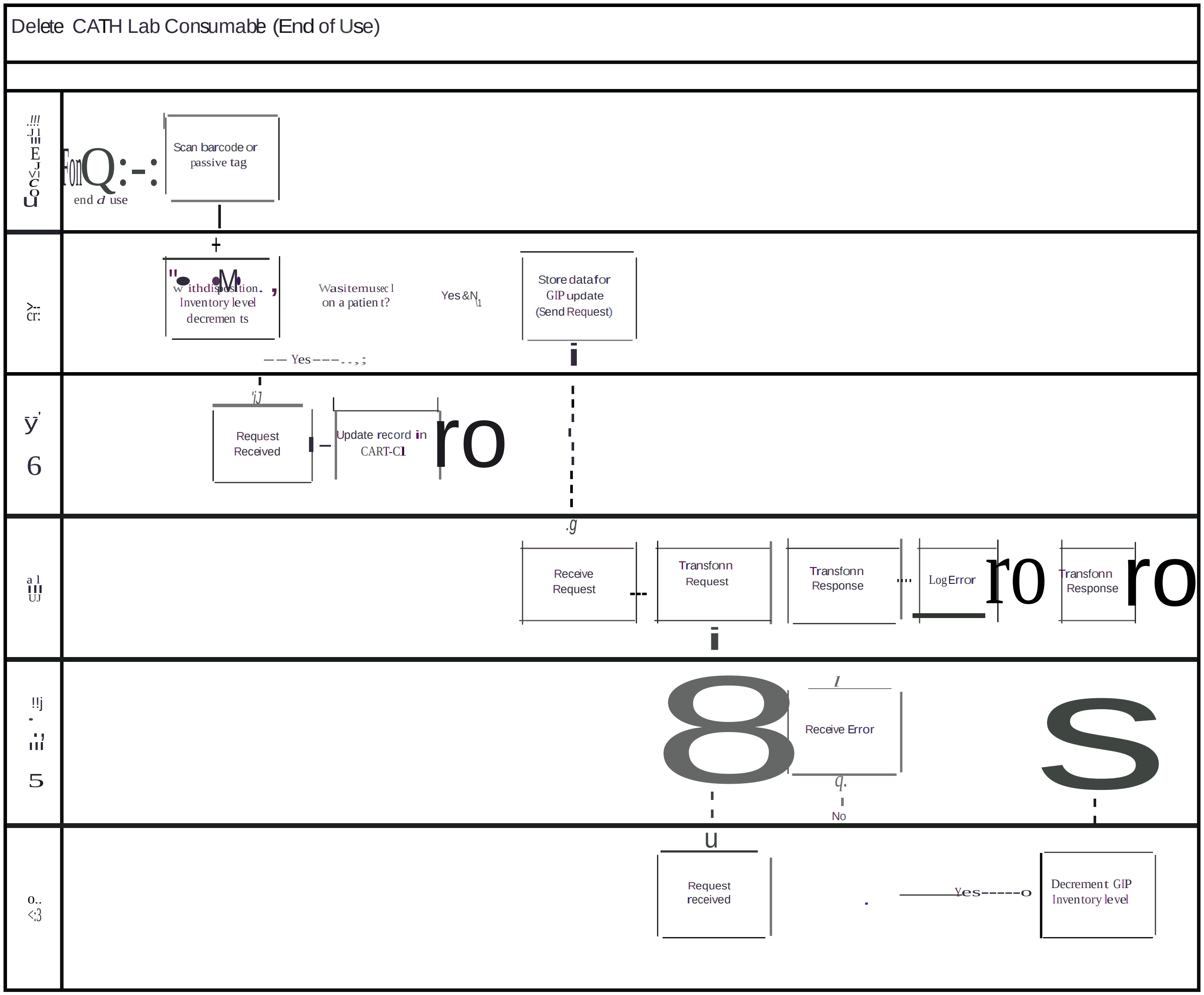


Figure 16: 012 Create Staff for Encounter

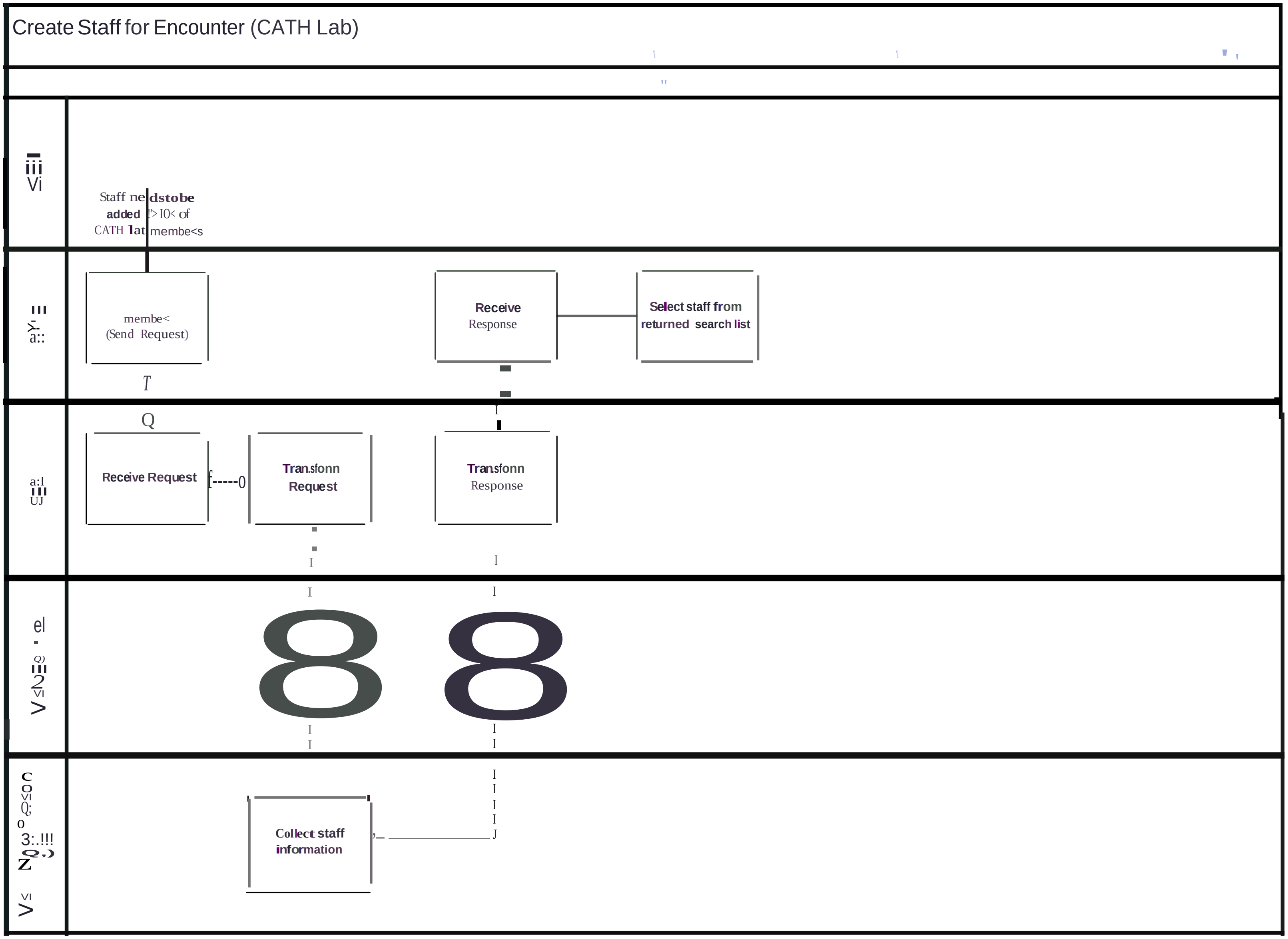


Figure 17:013 Create Environmental Equipment Monitoring

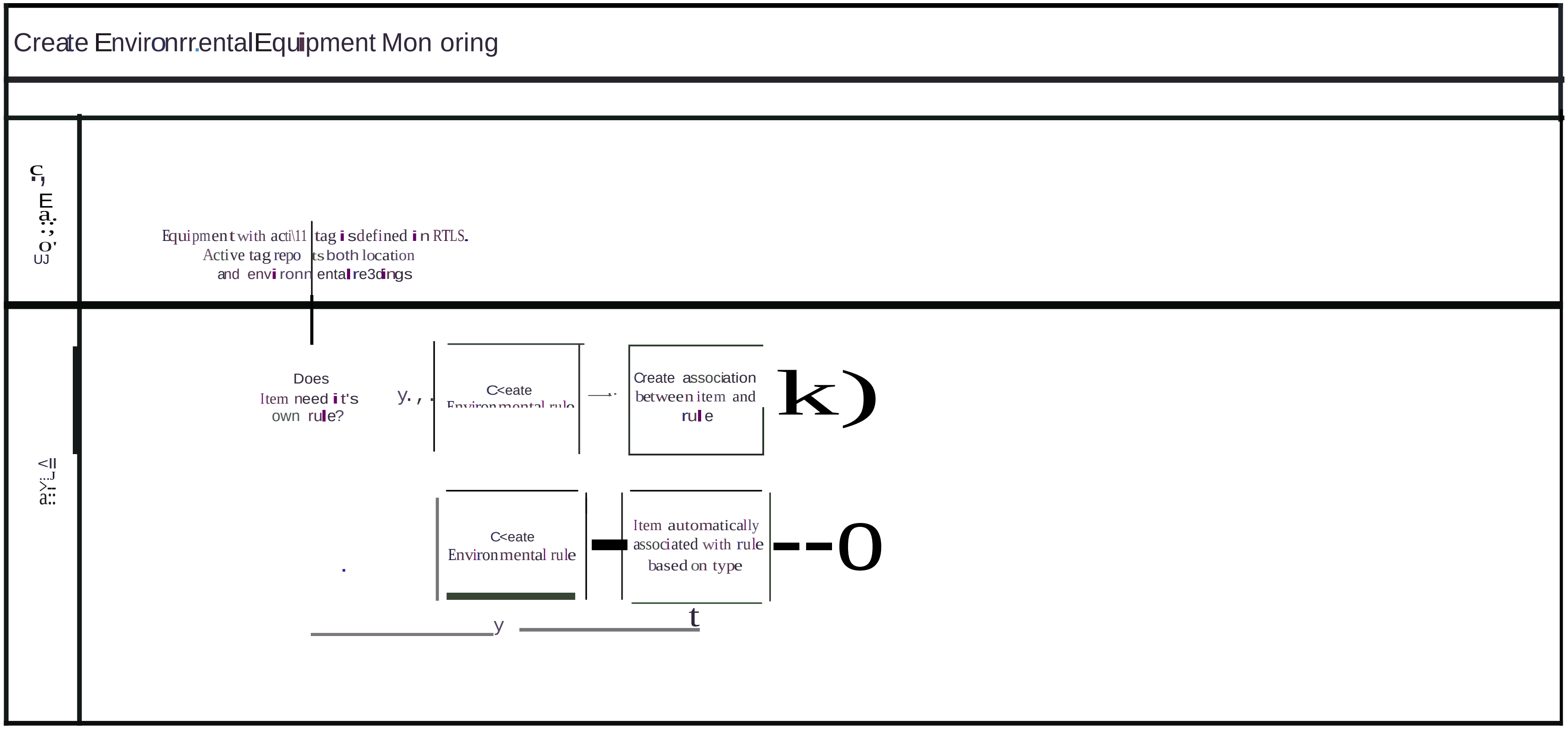


Figure 18:014 Create an EnvironmentalRoom Monitor

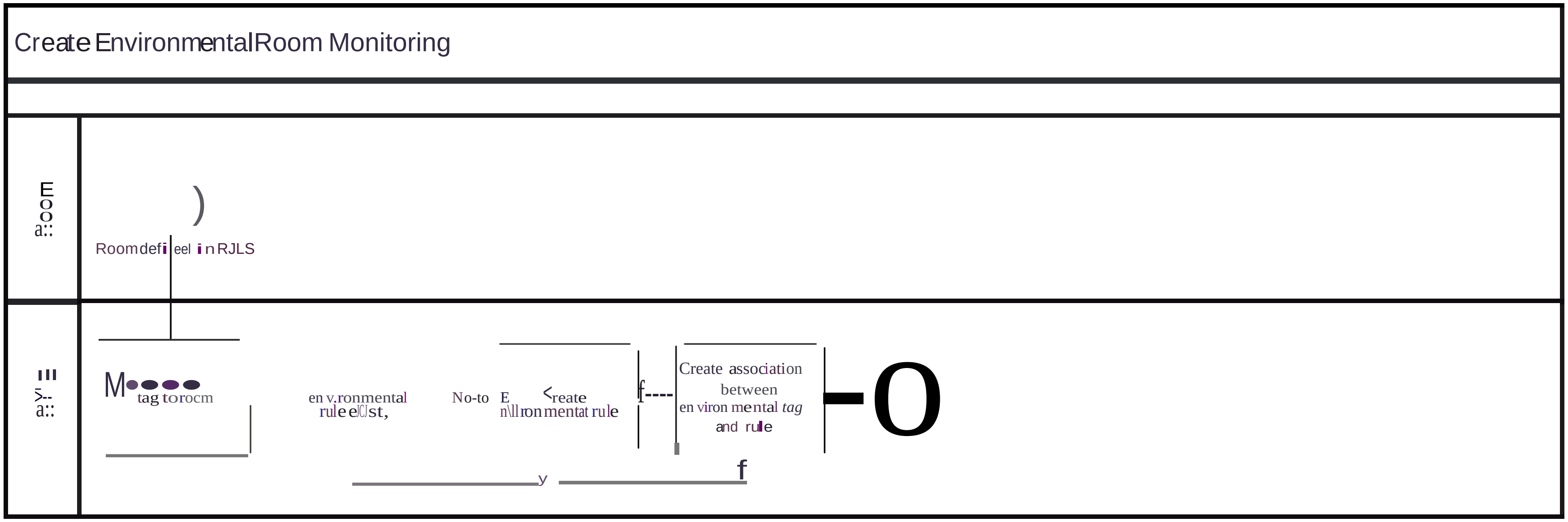


Figure 19:015 Retrieve an Environmental Reading

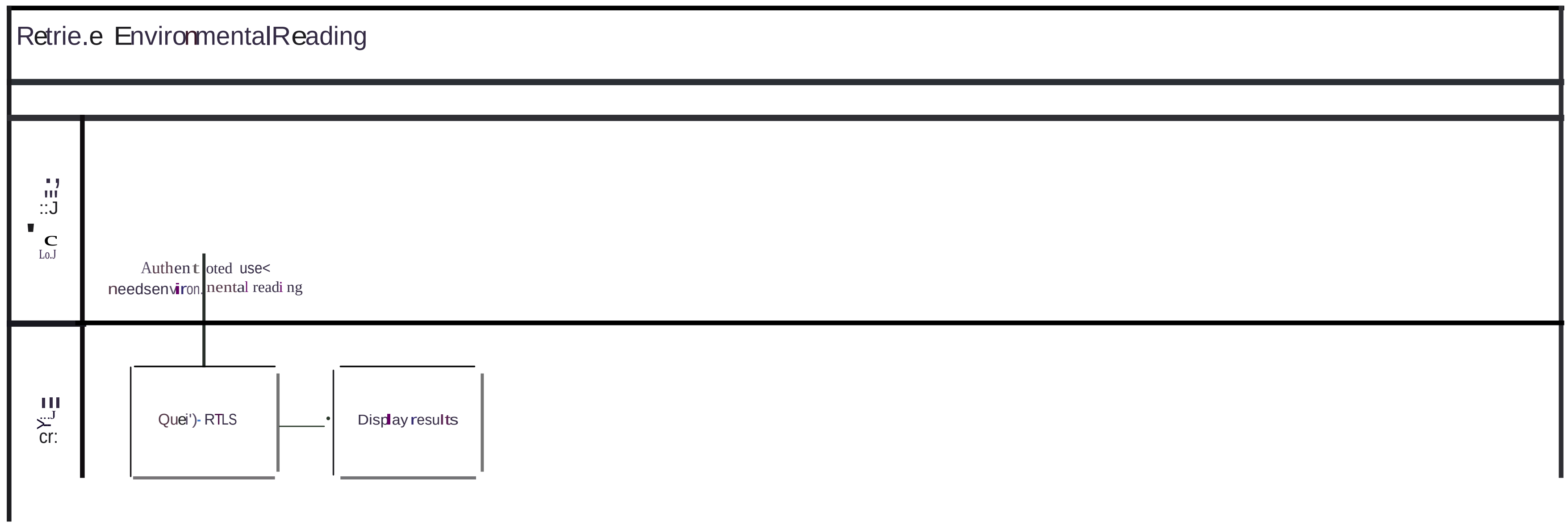


Figure 20:016 Update an Environm entalMonitor Status

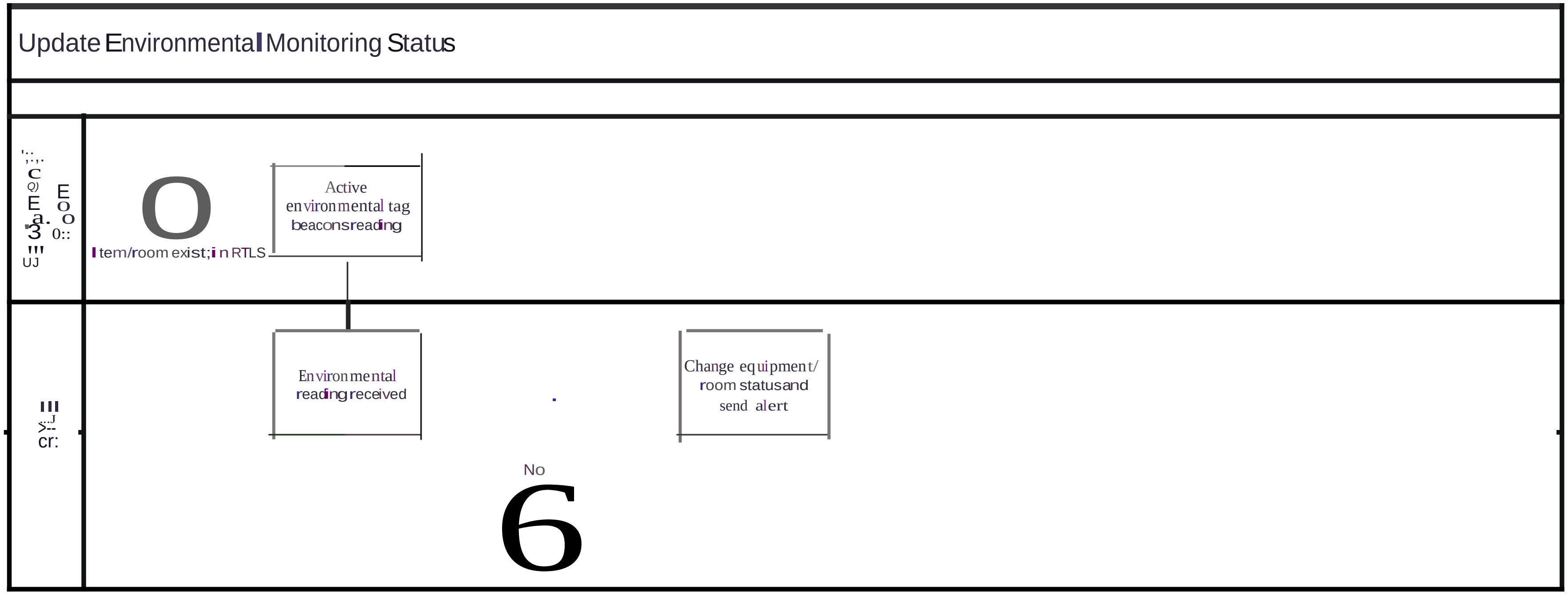


Figure 21:017 Delete an Environmental Equipment/Room Monitor

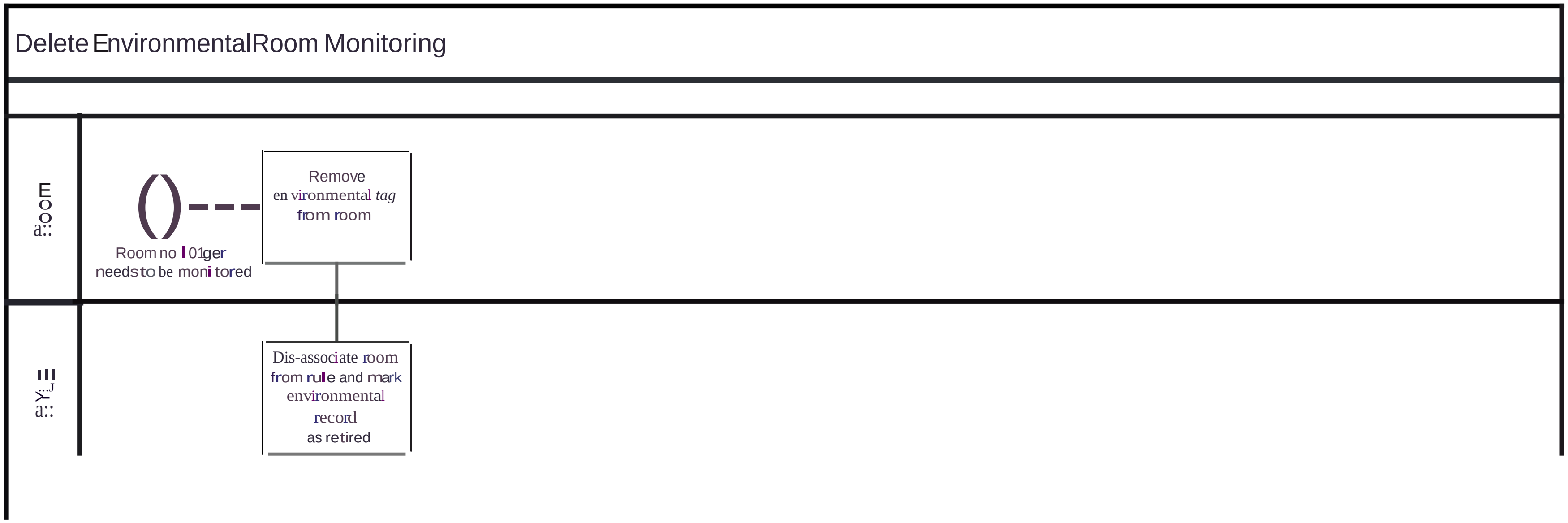
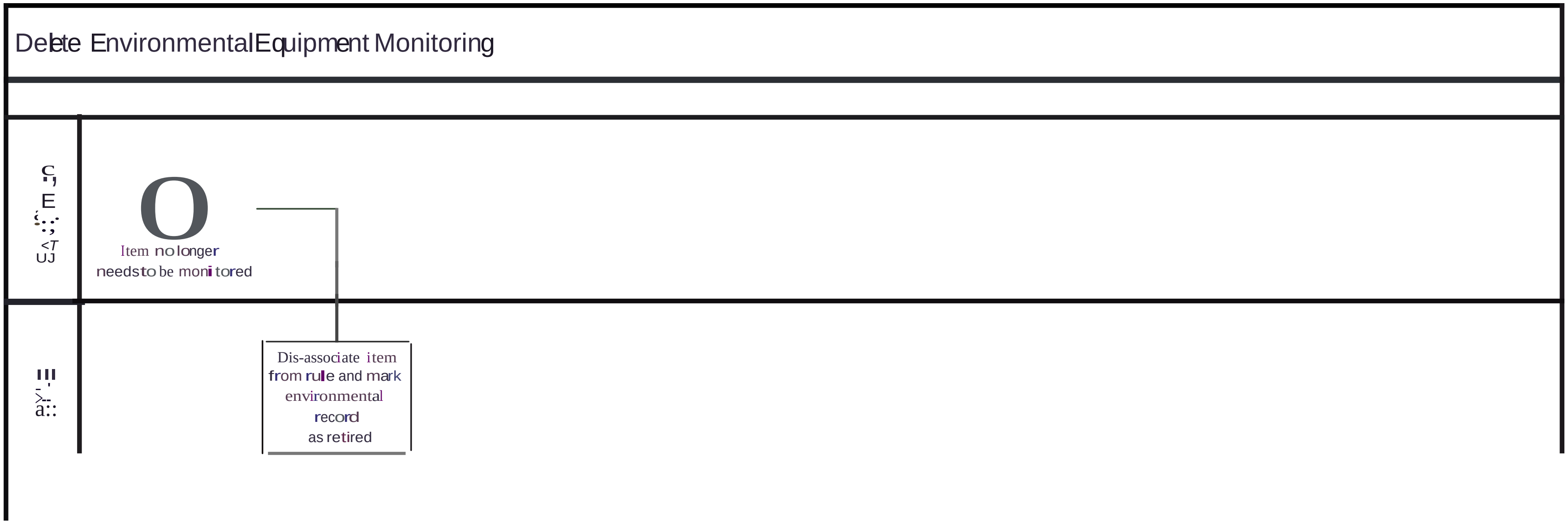


Figure 22:018 Delete EnvironmentalEquipment Monitor



2.3 Business Benefits

Implementation of the Real Time Location System v1.0 should provide the following business benefits.

General

- Improvement of quality of patient care
- Improvement of quality of patient satisfaction
- Positive return on investment (ROI)

Asset Tracking

- Improve Asset Utilization
- Eliminate excess inventory/leasing
- Improve maintenance process
- Loss and theft prevention

Operation Improvements

- Improve process through key assets visibility
- Eliminate bottlenecks
- Improve staff workflow
- Reduce errors
- Reduce delays
- Decrease operational costs

Safety and Security

- Track Employees or patients throughout the whole hospital Complex
- Panic Button alerts
- Man-down alerts
- Mustering and evacuations

2.4 Assumptions, and Constraints

This section describes the assumptions and constraints which are expected to impact the design of the RTLS. To date, assumptions are related primarily to the claims that RTLS is expected to seamlessly interface with other VA Systems, perform in all intended locations, and that RTLS traffic volume will not overwhelm these other VA Systems and the VA Wi-Fi network. These assumptions have led the VA design team to pay special attention to characteristics of the system which will support scalability as the use cases increase.

2.4.1 Design Assumptions

The following is a list of specific assumptions which will influence the design of the RTLS:

- This document will be considered a "living" document. In accordance with Agile processes, the document will change to accommodate changes to requirements, scope, and priorities as defined by VA.
- The RTLS solution will scale up and down to collect data from the 152 medical centers and 974 outpatient clinics nationwide, and CMOPS where RTLS is incrementally deployed. Deployment of the RTLS Systems will be incremental and not use a "big-bang" approach.

- RTLS shall co-exist with the VA Wi-Fi infrastructure and should leverage it to the maximum extent possible.
- All RTLS facilities can communicate via VA WAN.
- The active tagging solution within the RTLS System requires a physical Cisco MSE to be on the same premises as the active tags to meet the 10 millisecond network latency requirement.
- RTLS Tag can function in harsh environments unique to VA.
- Adequate AC power outlets exist in VA facilities to accommodate RTLS readers.
- Tags can be easily re-assigned via UID re-configuration.
- Standard set of default and configurable nomenclature exists for defining items/assets to be tagged.
- Line of sight RF coverage is acceptable at RTLS sites (VA Wi-Fi key requirement is wireless device links will be maintained within range of 3 access points at a minimum signal strength of -75 dBm).
- Server backup routines and replication are in place at VA facilities.
- RTLS will have servers in all facilities that uses RTLS to reduce network latency.
- The RTLS solution will interface with existing VA Active Directory infrastructure (Single Sign-On – SSO) to authenticate users and provide role based authorizations.
- Data will be encrypted for Personally Identifiable Information (PII).
- Certificates are in place for system-to-system data transfers aligning with FIPS-140.2 standards.
- RTLS COTS products have a relational database (DB), (e.g., Microsoft SQL Server or Oracle), to store RTLS data.
- The database schemas that make up the RTLS Data Model can be expanded to accommodate future use cases.
- The RTLS system will integrate with numerous VA and third-party systems to exchange data and for messaging.
- RTLS will interface with VistA.
- VistA can be updated to accommodate RTLS.
- VistA upgrade schedules are aligned with RTLS rollouts due to the use of COTS software and the existing RTLS work; interfaces to the existing VA Systems such as VistA and Clinical. Assessment, Reporting, and Tracking (CART-CL require custom development.
- All of the interfaces to VistA applications and data sources will use the web service framework already in place within VA. This framework uses VA's WebLogic application server to create a bidirectional data exchange between VistA and the client through a secure HTTPS connection. WebLogic is able to securely exchange information with VistA through the use of Remote Procedure Call (RPC). This secure connection is made through VistA-Link, a VA utility that uses Health Level (HL7) messaging to call RPCs and exchange information between VistA and remote systems.
- RTLS platform policy requires that all virtual machines, databases and servers in the RTLS solution be configured to synchronize with VA's Network Time Protocol (NTP) server so that the local time kept by each host platform is consistent nationwide.
- Software development processes will be consistent with the Institute of Electrical and Electronics Engineers (IEEE) standards, and the Software Engineering Institute (SEI), Capability Maturity Model, Level III or higher.
- The VA is moving its information systems toward designs that utilize a Service-Oriented Architecture (SOA). Therefore the design of the RTLS system will utilize SOA principles. These principles promote a separation of concerns which breaks down the RTLS into an optimal set of components that are loosely coupled and reusable, non-overlapping, suited for their intended purpose, aligned to business need, and interoperable.

- The NDR is an enclave within the CDW umbrella. The NDR solution will leverage existing CDW infrastructure, policies, procedures, guidelines, tools and resources to a maximum extent possible.
- Data transmitted from individual RTLS data stores to the NDR will be executed as efficiently as possible.

2.4.2 Design Constraints

The following is a list of unusual conditions or constraints which will limit the range of design choices that are available or impact the RTLS design choice to be made.

- Development tools and technologies shall be compliant with the VA Technical Reference Model (TRM).
- All application security cryptography modules/functions must be FIPS 140-2 certified
- Harsh environments to be encountered in SPS Use Case limiting tag life
- Small number of RFID tag manufacturers available for smart cabinet catheterization lab application
- Over the air protocol for active tags shall be Wi-Fi/802.11
- Must interoperate with legacy systems of record (e.g., VistA)
- No duplicate records allowed in RTLS and VA Systems DBs
- Limits based on time of day usage (peak use, dependency on limits of certain systems like VistA, network capacity/bandwidth)
- Some use cases (e.g., patient elopement) require low latency.
- Interoperability with legacy RTLS / Technology demonstration systems
- Web-based user interfaces required to maximum extent possible
- Reuse of VA enterprise-level software (Maximo, Microsoft Business Intelligence Stack, SAS, etc.)
- Virtualization for internal solutions
- Must use Microsoft Active Directory
- The RTLS User Interfaces shall be compatible with Microsoft Windows XP Client SP3 Operating systems and newer.
- The RTLS User Interfaces shall be compatible with Internet Explorer 7 or greater.
- The RTLS browser and desktop configuration shall be in accordance with Federal Desktop Core Configuration.
- The RTLS browser configuration shall not require custom browser configuration.
- For facilities equipped with Wi-Fi, RTLS shall utilize Wi-Fi as its primary location service.
- NDR will be developed, deployed, and operated in a similar administrative fashion as other enclaves within the VA CDW environment.
- Use of the VA CDW software. The following software is part of the CDW technology stack:
    - Microsoft Business Intelligence Stack
    - SAS (Analytics Pro, Enterprise Miner, Operation Research, Access, and Connect)
    - Microsoft SQL Server 2012
- RTLS will make use of VA's existing Microsoft SQL 2012 clusters and Oracle 11g RAC.

- The required use of this software disabled the RTLS solution to use Autonomy to handle unstructured data and Vertica to increase the data access speed.
- VA has a number of strategic initiatives designed to move towards an integrated Electronic Health Care program with the Department of Defense. The integrated Electronic Health Record (iEHR) is one initiative that is providing an Enterprise Service Bus (ESB). The RTLS ESB is based on common industry interoperability standards so the integration layer will be compatible with the iEHR ESB.
- The COTS RTLS software will not be modified for data extraction to the NDR.

2.5 Overview of the Significant Requirements

Significant requirements for the RTLS can be divided into several categories.

- Functional Requirements
- Operational Requirements
- Security of Privacy Requirements (Overview)
- Special Device Requirements
- Workload and Performance
- Technical Requirements
- System Criticality and High Availability

This section provides an overview of the major functions to be performed with the RTLS and the major requirements that drive the design described herein.

2.5.1 Overview of Significant Functional Requirements

The requirements specified below correspond to the **major** functional requirements defined in the RTLS Requirements Specification Document (RSD).

Table 5: Functional Requirements

Type	Synopsis
Tag Requirements	RFID Tags shall be the primary tool for implementing RTLS. The VA is interested in mainly two tag varieties: passive and active. All tags shall be standard COTS products and not require any vendor- or manufacturer-proprietary software, hardware, or firmware. The Contractor shall provide a variety of tags to fit a variety of assets with a variety of form factors. Tags shall be capable of being mounted and functioning on metal assets and in metal environments. Tags to be used in SPS need to withstand harsh environmental conditions, including cleaning and sterilization (liquid steam) in various techniques at temperatures up to 275 degrees Fahrenheit. Some tags shall be programmable to perform specific functions described here.
RTLS User Interface	RTLS shall have a browser-based user interface used to access the VISN level data for querying and reporting functionalities. The RTLS User Interface shall provide a feature to view other niche systems' user interfaces such as the SPS user interface. The RTLS User Interface will be configurable to generate reports, alarms, and alerts when user-set conditions are met. The Tool will function in accordance with user-specified workflows.

Type	Synopsis
Database Requirements	RTLS data shall be stored in a relational database (e.g., MS SQL or Oracle). Each RTLS facility or VISN database shall incorporate information on all tagged objects. Some of this information may be imported from other VA information systems through system interfaces, manually entered by facility personnel, or inputted by devices (e.g., scanners). The RTLS database solution shall provide up to date geo-location of each tagged object, open standards based connectivity, and tagged asset descriptive fields.
NDR Database Requirements	A data warehouse within the CDW shall serve as the single location at the enterprise level where an aggregation of RTLS Data from each RTLS-enabled facility will exist for reporting, analytics, business intelligence, and data mining functions (i.e., workflow analysis).
Interface Requirements	VA maintains numerous databases which may interface with the RTLS at the local, regional, and/or national level. In some instances, databases may be local within some facilities, and be regional in others. RTLS needs to provide a flexible system architecture that can accommodate numerous interfaces at potentially multiple levels in the architecture.
NDR Query Tool Requirements	The NDR Query Tools shall provide users access to all RTLS data holdings through both standardized and ad hoc queries. To maximize usage, the tool should have a simple, user-friendly and intuitive user interface. The user shall be able to access NDR reports and queries.
Reporting Requirements	A key component of the RTLS is the Reporting and Business Intelligence capability. The reporting functionality will provide insights into the business processes, workflows, and other relevant data at the local and national level in order that trends can be identified and observed and actionable recommendations can be made to improve business processes and reduce waste. The RSD lists numerous reporting requirements for the 4 initial use case: Catheterization Lab, Sterilization Process (SPS workflow), Asset Management, and Temperature Monitoring plus reporting requirements for Equipment Utilization, Clinical & Business Workflow, Nurse Call Integration, Patient Room/Bed Management, Contagious Disease Contact Tracking and Hand Sanitation Compliance, Lost and Stolen Equipment Detection, Instrument & Supplies Tracking, and Patient Elopement
NDR Analytics Tool Requirements	The NDR Analytics tool will support VA by providing comprehensive analytics and modeling capabilities. The NDR Analytics Tool will have an

Type	Synopsis
	intuitive, easy to use interface with which to build data sets for modeling. The tool will have the capability to execute workflow analysis in real-time, periodically, or on-demand across all RTLS data holdings.
GUI General Requirements GUI Mapping Requirements	RTLS shall employ a browser-based user interface to provide real time tag location/mapping data, alerts, temperature monitoring, and maintenance information as well as access to the querying and reporting functionalities. Accessibility to GUI features will be based on users' Role and Access levels. RTLS Alert Display refers to the computer monitor image depiction of the passive (user-initiated) reporting of system status, condition, or tag location.

2.5.2 Functional Workload and Functional Performance Requirements

The performance requirements for the facility based RTLS is a function of the facility.

With varied facility types and diverse facility specific requirements, the RTLS performance requirements are expected to be defined on a facility level. General latency requirements for user response times are outlined here.

The NDR's centralized, web-based nature and defined user base provides the ability to define the necessary performance requirements at this time.

- Approximate number of tags to be deployed:
    - VHA facility – average estimates is for 80,000 active and passive tags per facility. This will vary by facility and is for an initial deployment. It is expected that additional tags will be added over time.
    - CMOP facility – average estimate is for 3,000 active and passive tags per facility. This will vary by facility and is for an initial deployment. It is expected that additional tags will be added over time.

The RTLS system version 1.0 will undergo Systems Engineering and Design Review (SEDR) to be ratified.

NDR will comply with the following performance requirements:

- Pre-defined reports shall return results within one minute.
- Ad-Hoc reports shall return results within 10 minutes.
- Scheduled reports shall return results within 10 hours.

NDR will receive data from the various RTLS data stores. RTLS data stores exist at both the VISN Computer Room and Local Facilities. Based on information from the RTLS Enterprise Data Architecture, the following table shows an *estimate* of the number of data structures including the number of tables and columns that will be imported to the NDR from their transactional residency.

Table 6: RTLS Data Source Data Structures

Data Store Name	Location	Number of Tables	Number of Columns
Censis Censitrac	Local Facility	71	521
CenTrak GMS	VISN	12	521
Intelligent InSites Platform ODS	VISN	64	546
OATSystems OATxpress	VISN	117	1248
WaveMark EiRTLS	VISN	42	210

2.5.3 Operational Requirements

From our extensive experience with a variety of healthcare implementations, use cases, and RTLS technologies, we estimate the following typical updates in tag status:

- 30,000 active RTLS tags per VISN
- Tags attached to equipment provide updates approximately 80 times a day
- Tags attached to staff provide updates approximately 280 times a day
- Tags attached to patients provide updates approximately 100 times a day (with a large variance based on use case)
- 38 KB per day, per tracked item, in data growth in the VISN level
- Required Network bandwidth is a four 1GBps network connection to the network from the infrastructure in the data center and no more than two 1 GBps to the servers at the local facilities. It is important that all the servers have a high-capacity connection to support server-to-server communication.
- Expected bandwidth usage from server to server is 10Mbps up and down.
- Client browser traffic will consume a minimum of 2Mbps network bandwidth per 100 active browsers. Each browser has an active connection and is receiving data from the server even if the user is not actively browsing. Users that are actively browsing will consume more bandwidth but it is not significant.
- The NDR will be available 99% of the time between 7AM and 10PM, Monday through Friday Eastern Standard Time (EST).
- NDR will be initially capable of supporting a minimum of 100 concurrent users and able to scale up to at least 500 concurrent users.

For a sample VISN with approximately 135,000 active tags, 5,000 supplies, and 90 SPS workstations, we estimate approximately 80 Kilobytes per second of network traffic from each facility to the National Data Center. The strategy is to simplify and abbreviate the data in transit without diminishing the meaning or the value that the data provides, thereby reducing bandwidth considerations. We anticipate a nightly bulk data transfer (batch upload), per VISN, of approximately 1.6 GB.

In addition, the tables below show an estimate of network bandwidth expectations. At this time, it is difficult to gauge certain components as the payloads of the messages have not been finalized.

Table 7 (Actively Tagged Asset Network Data Rates) shows estimated network data rates for one actively tagged asset, one active tag reader, and the scheduled AEMS-MERS jobs running once daily. The columns in the Actively Tagged Asset Network Data Rates, Passively Tagged Asset Network Data Rates tables are defined as follows:

- Component – the name of the RTLS component that is consuming network bandwidth
- Packet Size (Bytes) – the number of bytes of data carried by a packet-switched network
- Packet Size (Kilobyte) - the number of Kilobytes of data carried by a packet-switched network
- Transactions per Day – the estimated number of transactions that the component will send over the network per day
- Transactions per second - the estimated number of transactions that the component will send over the network per second
- Devices – the number of devices installed at facility
- Data Rate (Kilobytes/sec) – is the amount of digital data that is moved from one place to another in a given time, measured in Kilobytes/sec
- Data Rate (Kilobits/sec) - is the amount of digital data that is moved from one place to another in a given time, measured in Kilobits/sec
- Flow – a description of how the data flows through the network and other components
- Local Traffic – indicates if the network traffic is local to the facility or uses the VA’s Wide Area Network (WAN) to communicate between facilities or data centers
- Notes – this is used to provide additional information about the data rate calculations

Table 7: Actively Tagged Asset Network Data Rates

local Facility (LAN)

Component	Packet Size (Bytes)	Packet Size (KiloByte)	Transactions per Day	Transactions per second	Devices	Data Rate (Kilobytes/sec)	Data Rate (KiloBits/sec)	Flow	Local Traffic	Notes
CenTrakActiveTags	12.0	0.01	400	0.00462963	1.0	0.00014	0.00109	From Active Tags (Local Facility) to Active Readers (Local Facility)	Yes	Devices Is the number of tags each local facility will have. Transactions Is the num of moves per asset (the frequency of moves on averaae an asset move is recorded 400 times a day). Data Rate=(Packet Size (Kilobyte) * Transactions per second * Devices) * 2.5 Each tag is read by 2.5 stars on average
CenTrak Active Readers	1450.0	1.42	28,800.00	0.333333333	1.0	o 4not	377604	Active Readers (Local Facility) to CenTrak Platform (Loca Facility)		Transact ons per day= 86400/3 (86400 seconds in a day) Stars read every 3 seconds. Devices is the number of readers per local facility (stars). Data Rate=Packet Size (Kilobyte) * Transa ions per second * Devices
CenTrak Platform	1450.0	1.42	28,800.00	0.333333333	1.0	0.47201	3.77604	CenTrak Platform (Local Facility) to InSites Connector Framework (Local Facility)	Yes	The calculation Is the same equation used to determine the active readers data rate.
					Total LAN Data Rate	0.94415	7.55317			This is the total data rate that is used at a local facility

Component	Packet Size (Bytes)	Packet Size (KiloByte)	Transactions per Day	Transactions per second	Devices	Data Rate (Kilobytes/sec)	Data Rate (KiloBits/sec)	Flow	Local Traffic	Notes
InSites Connector Framework	1228.8	1.20	10.00	0.000115741	1.0	0.00014	0.00111	Connector Framework (Local Facility) to InSites Platform (VISN/NOC)	No	aa:s divided by 10.10 is the averaa:e movement of a ta in a day. Realtime data i compared to data in cache. If asset has not moved the data is discarded
CenTrakGMS	1450.0	1.42	28,800.00	0.333333333	1.0	o 4not	3.77604	::; ; :: (LocalFacilty)to	No	The calculation is the same equation used to determine the CenTrak Platform data rate. To determine a VISN or NDC implementation, multiply this number by the number of facilities per VISN or belonging to the NDC
VistA (AEMS-MERS - Asset Details Update)	2048.0	2.0	10.0	0.000116	1.0	0.00023	0.00185	AEMS-MERS (Local Facility/Data Center) to InSites Platform (VISN/NDC) via VistAService and Mule ESB	No	This is a real time update when data is changed in VistA. The frequency of the updates is unknown (defaulted to 10 updates a day)
					Total WAN Data Rate	0.47238	3.77901			This is the total data rate that is used between a local facility and VISN Computer Center/NDC

local FaCility to/from VISN Computer Room/NDC (WAN) - Burst

Configurable Burst Traffic										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
IMtA I-OENS.-IERli - Equipment Movement)	1024.0	1.0	1.0	N/A	1.0	1.00000	8.00000	MuleESB (VISN/NDC) to InSites Platform (VISN/NDC) back through MuleESB (VISN/NDC) to VistAService to VistA (Local Facility/Data Center)	No	This is configurable traffic (defaulted to daily). This traffic is a burst job that runs on a configurable frequency. The devices column represents the number of actively tagged assets
				Total WAN Burst Data Rate		1.00000	8.00000			This is the total burst data rate that is used between a local facility and VISN Computer Center/NDC

An excel version of Table 7 can be found here: Actively Tagged Asset Network Data

Table 8 (Passively Tagged Asset Network Data Rates) shows estimated network data rates for one passively tagged asset, using one passive reader and the scheduled AEMS-MERS jobs running once daily. A description of the columns in the table is discussed prior to table 6.

Table 8: Passively Tagged Asset Network Data Rates

Passively Tagged Asset Tracking Network Data Rates										
Local Facility to VISN Computer Room/NDC (WAN)										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
Passive Readers	1024.0	1.00	2000	0.023148148	1.0	0.02315	0.18519	Tag Readers (Local Facility) to OATxpress (VISN/NDC)	No	Transactions are largely dependant on the opening of Egress points
VistA (AEMS-MERS - Asset Details Update)	2048.0	2.0	10.0	0.000116	1.0	0.00023	0.00185	AEMS-MERS (Local Facility/Data Center) to InSites Platform (VISN/NDC) via VistAService and Mule ESB	No	This is a real time update when data is changed in VistA. The frequency of the updates is unknown (defaulted to 10 updates a day)
					Total WAN Data Rate	**0.02338**	**0.18704**			**This is the total data rate that is used between a local facility and the VISN Computer Room/NDC**
VISN Computer Room/NDC (LAN)										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
OATxpress	2048.0	2.00	2000	0.023148148	1.0	0.04630	0.37037	OATxpress (VISN/NDC) to InSites Connector Framework (VISN/NDC)	Yes	Transactions are largely dependant on the opening of Egress points
OAT Enterprise Administrator	1024.0	1.00	288	0.003333333	1.0	0.00333	0.02667	OATxpress (VISN/NDC) to OAT Enterprise Administrator (VISN/NDC)	Yes	Transactions per day is that the data is sent every 5 minutes. 1440 minutes in a day/5 minutes = 288
InSites Connector Framework	1228.8	1.20	2000	0.023148148	1.0	0.02778	0.22222	Connector Framework (VISN/NDC) to InSites Platform (VISN/NDC)	Yes	
					Total LAN Data Rate	**0.07741**	**0.61926**			**This is the total data rate that is used at a VISN Computer Room/NDC**
Local Facility to/from VISN Computer Room/NDC (WAN) - Burst										
Configurable Burst Traffic										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
VistA (AEMS-MERS - Equipment Movement)	1024.0	1.0	1.0	N/A	1.0	1.00	8.00	MuleESB (VISN/NDC) to InSites Platform (VISN/NDC) back through MuleESB (VISN/NDC) to VistAService to VistA (Local Facility/Data Center)	No	This is configurable traffic (defaulted to daily). This traffic is a burst job that runs on a configurable frequency. The devices column represents the number of passively tagged assets
					Total WAN Burst Data Rate	**1.00000**	**8.00000**			**This is the total burst data rate that is used between a local facility and VISN Computer Center/NDC**

An excel version of Table 8 can be found here: Passively Tagged Asset Network Data

Table 9 (Instrument Sterilization Network Data Rates) shows estimated network data rates for one Censis Workstation. A description of the columns in the table is discussed prior to table 6.

Table 9: Instrument Sterilization Network Data Rates

Instrument Sterilization Network Data Rates										
Local Facility (LAN)										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
Censis Workstations	500.0	0.49	86400	1	1.0	0.48828	3.90625	Workstation (VAMC) to Censistrak Buffer Server (VAMC)	Yes	Transactions per day = 1 every second
Censis Censitrac	3072.0	3.00	86400	1	1.0	3.00000	24.00000	Censitrac Buffer Server (VAMC) to Connector Framework (VAMC)	Yes	Transactions per day = 1 every second
					Total LAN Data Rate	**3.48828**	**27.90625**			**This is the total data rate that is used at a local facility**
Local Facility to VISN Computer Room/NDC (WAN)										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
InSites Connector Framework	1228.8	1.20	86400	1	1.0	1.20000	9.60000	Connector Framework (VAMC) to InSites Platform (VISN/NDC)	No	Transactions per day = Censis Censitrac Transactions per day) * number of Workstations
					Total WAN Data Rate	**1.20000**	**9.60000**			**This is the total data rate that is used between a local facility and the VISN Computer Room/NDC**
Local Facility to Censis Cloud (WAN)										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
Censis Host Server	100	0.09765625	864	0.01	1.0	0.00098	0.00781	Censitrac Buffer Server (VAMC) to Censis Host Server (Cloud)	No	The host server receives data every 100 seconds from the Censitract
					Total WAN Data Rate	**0.00098**	**0.00781**			**This is the total data rate that is used between a local facility and the Censis Cloud**

Instrument Sterilization Networ

An excel version of Table 9 can be found here:

Table 10 (Catheterization Lab Network Data Rates) shows estimated network data rates for one WaveMark SmartCabinet, WaveMark Point of Use Station, one supply, one patient and the scheduled IFCAP-GIP jobs running once daily. A description of the columns in the table is discussed prior to table 6.

Table 10:Catheterization Lab Network Data Rates

Cathetenzat1on lab Network Data Rates										
aveMartcatheterizationLab(xPOS)	102400.	100.		1.15741E-OS	1.	0.0011	0.0092	POS(VAMC) toWaveMark Ena ine VIS NOC	No	Devices represent the number of xPOSat the VAMC. ranSKtionsis the number of tients 'da
WaveMark catheterization Lab (Smart cabinets)	102400.0	100.00	n	0.000833333	1.0	0.08333	0,66667	Smart cabinets (VAMC) to WaveMark Engine (VISN/NDC)	No	Devices represent the number of Smart cabinets at the VAMC Transactions = every 20 minutes a smart cabinet sends data (1440 minutes per day/20 minutes)
aveMark catheterization tab(xPOS -->Patient)	1024.	1.0[illegible]		1.15741E-OS	1.[illegible]	0.0000	0.0000	_waveMark xPOS(VAMC) to MuleESS (VISN/NDC) to VistASefvice VISN/NOC) to VistA (Local Facility/Data Center)and back to POSIV MC)	No	ransactions = number of patients Devices = number of xPOS
Employee (VistA)	100.0	0.10	10	0.0001157	1.0	0.00001	0.00009	WaveMark xPOS(VAMC) to WaveMark Engine (VISN/NDC) to MuleESB (VISN/NDC) to VistAService (VISN/NDC) to VistA (Local Facility/Data Center) and back to xPOS(VAMC)	No	Transactions – is the average of employee searches per day per xPOS (estimated 10per day) Devices = the number of xPOS
				Total WAN Data Rate		0.08451	0.67611			**This is the total data rate that is used between a local facility and the VISN Computer Room/NDC**

VISN Computer Room/NDC to Denver Data Center (Location of CART-CL) -WAN										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
WaveMark Engine (CART-CL)	10n o	3.00	1	1.15741E-05	1.0	0.00003	0.00028	WaveMark Engine (VISN/NDC) to CART-CL (Denver)	No	Transactions = Number of Patients * Number of xPOS Estimate 700 transactions Enterprise wide per day If calculating the number of transactions for NDC: tr,.onsacUo"s = number of patients • number of xPOS • nuombe"of VISNs implemented
				Total WAN Data Rat•		0.00003	0.00028			This is th• total data rat• that is us•d b.tw••n a local facility and the VISN Computer Room/NOC

LocalFac1llty to/from V SN Computer Room/NDC (WAN)- Burst										
	Packet Size (Bytes)	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	;; ;	**Local Traffic**	
FCAP-GIP (VistA) Item Master	ISO.O	0.1		N/A	1.0	0.1	1.1	WaveMark Engine (VISN/NOC) to MuleESB (VISN/NOC) to VistAService (VISN/NOC) to VistA (Local Facility/Data Center) (Defaulted to Daily)	No	This is configurable traffic (defaulted to daily). This taffic s a burst job that runs ona configurable frequency. The transactions column represents the number of supplies per VAMC. This number is an estimated number of supplies. One message contains all the supplies, the true packet size is 150 Bytes multiplied by the number of supplies (transactions).
IFCAP-GIP (VistA) On Handlink	100.0	0.1		N/A	1.0	0.09766	078125	waveMark Engine (VISN/NDC) to MuleESB (VISN/NDC) to VistAService (VISN/NDC) to VistA (local Fac lity/Data Center) (Defaulted to Daily]	No	This is configurable traffic (defaulted to daily). This traffic is a burst job that runs ona conf gurable frequency. The transactions column represents the number of supplies per VAMC. This number is an estimated number of supplies. One message contains all the supplies, the true packet size is 100 Bytes multipled by the number of supplies (transactions).
				Total WAN Burst Data Rate		0.24414	1.95313			This is the total burst data rate that is used **between a local facility and VISN Computer Center/NDC**

VISN Computer Room/NDC to/from WaveMark Cloud (WAN) - Burst										
Component	**Packet Size (Bytes)**	**Packet Size (KiloByte)**	**Transactions per Day**	**Transactions per second**	**Devices**	**Data Rate (Kilobytes/sec)**	**Data Rate (KiloBits/sec)**	**Flow**	**Local Traffic**	**Notes**
WaveMark Cloud (SFTP Logs)	52428800.0	51200.0	1	N/A	1.0	51200.00000	409600.00000	WaveMark Engine (VISN/NDC) to WaveMark Cloud	No	1 Transaction per install of WaveMark Engine
WaveMark Engine (SFTP Supplier catalog)	3072.0	3.0		N/A	1.0	3.00000	24.00000	WaveMark Cloud to WaveMark Engine (VISN/NDC)	No	1Transaction per install of WaveMark Eng ne
				Total WAN Burst Data Rate		51203.00000	409624.00000			This is the total burst data rate that is used between the VISN Computer Center/NOC and the WaveMark cloud

An excel version of Table 10 can be found here: Catheterization Lab Network Data Rates

The RTLS infrastructure will be in full compliance with the IT infrastructure standards. The RTLS will go through a SEDR process. This process will identify any issues with server utilization, hardware sizing, hard drive space, and failover. Once all these issues are addressed, the RTLS system will get a SEDR ratification.

The RTLS infrastructure will be in full compliance with the IT infrastructure standards. The RTLS will go through a SEDR process. This process will identify any issues with server utilization, hardware sizing, hard drive space, and failover. Once all these issues are addressed, the RTLS system will get a SEDR ratification.

The NDR will operate under the following requirements

- Pre-defined reports shall return results within one minute.
- Ad hoc reports shall return results within 10 minutes.
- Scheduled reports shall return results within 10 hours.

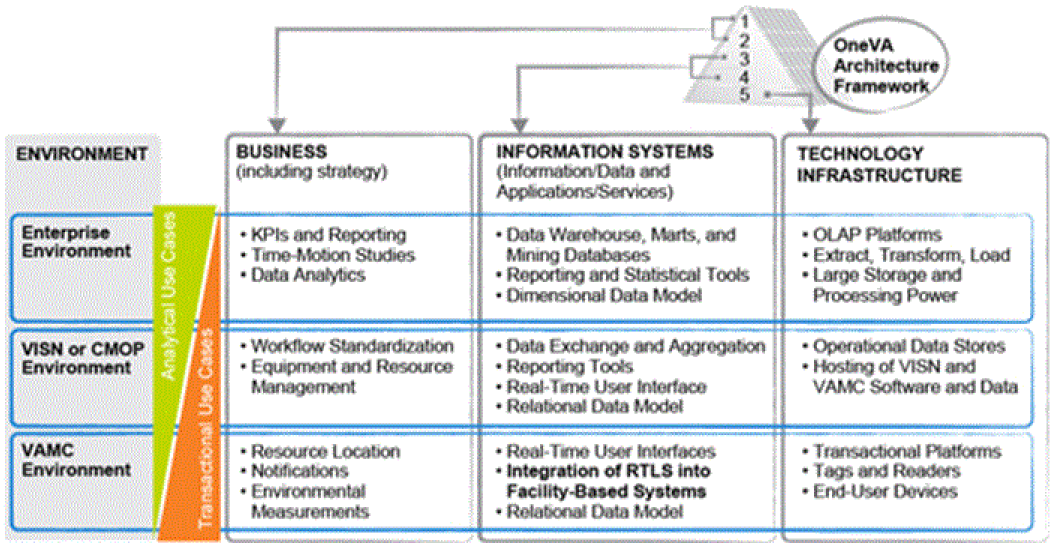
2.5.4 Overview of the Technical Requirements

The RTLS's compliance with the VA Enterprise Architecture and the One-VA Technical Reference Model will not be known until the COTS selection.

The RTLS System will be in full compliance of the One-VA Technical Reference Model and VA Enterprise Architecture. Any interface that is developed and deployed will be created by the VA-approved tools listed in the TRM.

The figure below illustrates how RTLS will utilize the VA Enterprise Architecture. This framework promotes completeness and integrity by recognizing the needs, inputs, and outputs of the Business, Information Systems, and Technology Infrastructure layers. Business needs and use cases guide the RTLS Data Model and workflow implementation within RTLS information systems. Looking at the figure vertically, VA enterprise analytics and reporting needs drive the type of data that must be processed, aggregated, and passed up to the VA national level from VISN and VAMC levels. The VISN-level environment focuses on RTLS data aggregation, operational reporting, workflow standardization and optimization, and resource utilization; the VAMC Level environment focuses on point-of-care transactions and real time decision support.

Figure 23: **RTLS Architectural Framework**



2.5.5 Overview of the Security or Privacy Requirements

The following section denotes the security and privacy requirements for the RTLS system.

For more information on the Security and Privacy Policies for the RTLS system, see Section 9. The RTLS System will go through the VA's Certification and Accreditation (C&A) process to obtain an authority to operate (ATO). RTLS including the NDR is designed to restrict access to Protected Health Information (PHI)/Personally Identifiable Information (PII) data to only authorized users of that data.

2.5.6 System Criticality and High Availability Requirements

RTLS and NDR are High Availability systems. The uptime, maintenance, and recovery requirements are detailed in the RSD.

RTLS has been designed with built-in redundancy and fault tolerance commensurate with a mission critical system where patient safety is at risk. The RTLS System will provide a process to make sure continuity of operations plan (COOP) and disaster recovery have been assessed within the design from VAMC systems up through the National Data Repository. These processes will include a COOP/DR Plan for the RTLS, including any architecture components placed in the VA National Data Centers. This plan will comprehensively address RTLS requirements for reliability/availability with a low-risk, cost-effective approach. The COOP/DR plan will protect all vital records from damage or destruction and provide continuous availability to them in compliance with standards such as the U.S. National Archives and Records Administration Code of Regulations, Subchapter B-Records Management. Our approach to creating the COOP/DR will be to work collaboratively with VA's OIT (formerly known as OI&T) Enterprise Systems Engineering Staff on the design of the COOP/DR and make sure that it adheres to all VA standards, including guidance from the OIT COOP Handbook 0320.1.

The NDR will adhere to existing CDW Disaster Recovery, backup and high availability polices. The NDR will follow guidance from the Office of Information and Technology Continuity of Operations handbook 0320.1 dated July 22, 2009.

2.5.7 Special Device Requirements

RTLS will utilize a variety of active and passive tags depending upon environmental operating conditions and limitations (e.g., tagged item size and form factor), usage, and user demands. The following table contains requirements for all types of RTLS RFID tags to be used.

Table 11: RTLS Tag Requirements

Req. ID	Requirement
H-T-001	The health status of tags shall be able to be dynamically monitored by the RTLS to ensure that all tags are functioning properly.
H-T-002	Active tags shall contain a battery voltage monitor circuit that will automatically 1. Indicate a visible alert (e.g., flashing on-tag LED – Light Emitting Diode) 2. Transmit alert to RTLS when battery life reaches a pre-defined low threshold level
H-T-003	If battery-powered tags are used, the power level shall be read using the readers.
H-T-004	Tag batteries shall be re-chargeable and/or easily replaceable by VA personnel using common standard tools.
H-T-005	Each active tag shall have tamper detection capabilities, to alert RTLS if it has been tampered with or removed from the object to which it was attached.
H-T-006	All tags shall be tamper resistant.
H-T-007	A tag's feature set shall not be compromised or diminished in any way by any standard, tamper-proof affixation option.
H-T-008	Tags shall be capable of operating in multiple environments, including but not limited to: high temperature and pressure (e.g., autoclave), sterile storage, liquids, oxygen rich, metallic, and indoor/outdoor.
H-T-009	Battery powered tags shall have a battery life of at least 3 years for a 10s beacon rate.
	Unique ID Number
H-T-010	RTLS tags (active, passive, 2D) shall come with a globally unique tag ID.
H-T-011	The RTLS solution shall ensure globally unique tag ID's across the entire VA system.
H-T-012	The unique identifier for the tag shall be physically located and visible on the tag in machine readable format (e.g., 2D barcode).
	RF Communications
H-T-013	Tags shall be able to communicate using any unlicensed Institute for Supply Management (ISM) bands and conform to all EPC (Engineering, Procurement, and Construction) Global and International Organization for Standards (ISO)/ International Electro-technical Commission (IEC) 18000 and 18000-6C series standards.
H-T-014	Tags shall be tested against and comply to RFID conformance test methods specified in ISO/IEC TR 18047-4:2004, Part 4: Test methods for air interface communications at 2.45 GHz
H-T-015	Tag reads shall occur within 5 milliseconds (or as defined by use case).
H-T-016	Quality of Service (QoS) protocols shall be utilized to prioritize certain use case applications and to avoid potential Wi-Fi network latency collisions.
H-T-017	Passive tag read range shall be 5 feet minimum in a 10 square foot room with 95% accuracy.
	RF Interference
H-T-018	RFID Tags shall not interfere with the VA facility's Wi-Fi network

Req. ID	Requirement
H-T-019	RFID Tags shall not interfere with any RF-susceptible system at the VA deployment site (e.g., patient telemetry, ultrasound).
H-T-020	Active tags shall comply with Federal Communications Commission (FCC) Code of Federal Regulations (CFR) 47 part 15.
	Tags with Sensors
H-T-021	The temperature monitoring solution shall include tags with the ability to be mounted in the interior of assets that have a closed container (e.g., fridge and freezers) without the use of an external probe and wire penetrating the insulation.
H-T-022	For tags with external temperature or humidity monitoring probes, the probes shall be NIST traceable and able to be calibrated.
H-T-023	Tags with sensors shall be configurable either in continuous or over-threshold logging modes
H-T-024	The environmental tag's sampling intervals shall be programmable from 8 seconds to 18 hours.
H-T-025	The environmental tag's temperature and humidity thresholds/alarms shall be programmable
H-T-026	Active tags with status indicator lights shall turn on when programmed sensor thresholds have been reached.
	Programmable Features
H-T-027	An active tag's internal configuration or status shall be programmable remotely via RF (over the air).
H-T-028	Active tags shall be configurable to have programmable beacon rates based on operational situations (e.g., tag will increase beacon rate when status changes from idle to in–motion enabled through a chokepoint trigger).
H-T-029	RTLs shall provide active tags that contain up to two (2) easily accessible alert buttons which enables critical/safety user information to be sent over the air and immediately displayed on RTLS monitors.
H-T-030	The active tag's operational mode shall be configurable and programmable.
H-T-031	Active tags shall have the capability to emit audible and/or visible alarms when the status of the tagged asset has changed (e.g., when a tagged asset or individual has departed a user-defined coverage area).
H-T-032	Tags shall have visible indicator or status and alert lights.
H-T-033	The operation of the tag indicator or status and alert lights shall be programmed to respond to sensors and readers or be triggered by an over the air command sent to the tag.
H-T-034	Some tags shall contain extended memory that enables specific information about the tagged item to be stored directly on the tag, allowing access in situations when an external database may not be available.
	Physical Design
H-T-040	Tags shall be capable of being mounted on metal and functioning in metal environments.
H-T-041	Tags shall be durable and properly sealed to guard against damage from exposure to liquids, dust, and debris.
H-T-042	Tags shall be able to be easily placed on patient ID bracelets and staff badges and be inconspicuous.
H-T-043	Each tag shall be reusable as defined in specific use cases.
H-T-044	Any adhesives used to mount tags shall be durable against delamination from exposure to chemical agents, liquid, dust, and debris (e.g., SPS processing).

Req. ID	Requirement
H-T-045	Tags shall be capable of transmitting and receiving without performance degradation when affixed to metal assets.
H-T-046	Tags shall be capable of being inserted and operating inside desktop computers, laptops, etc. The tags shall not interfere with the performance of these electronic assets to which they are affixed and the tags shall be able to operate without performance degradation in such potentially hostile electromagnetic interference environments.
	Size
H-T-050	Both active and passive tags shall have a small form factors so as not to interfere with the operation of the tagged equipment, does not affect usability, and shall be able to be attached in an unobtrusive location.
H-T-051	Tags shall have the ability to be attached to surgical instruments in a variety of sizes from 1 to 12 inches.
	Environmental
H-T-060	Tags intended for standard assets and personnel in normal indoor and outdoor environments shall be able to operate in temperature range of -25º C to 70º C (-13° F to 158° F) and withstand storage temperature range between -40 º C and 85º C (-40° F and 185° F).
H-T-061	Tags used for surgical and other sterilization devices shall be able to withstand cleaning and sterilization (liquid steam) in various techniques at temperatures of up to 275 degrees Fahrenheit for up to 30 minutes.
H-T-062	Tags shall be resistant to the disinfecting chemicals used to wipe down the surface of the assets and tags.
H-T-063	Tags shall be able to endure multiple cleaning protocols: 1. Low level disinfection (no claim for tuberculocidal activity) 2. Intermediate level disinfection (disinfectant with tuberculocidal activity) 3. High level disinfection (sterilant / disinfectant with sporicidal chemical - short contact time). 4. Sterilization (sterilant / disinfectant with sporicidal chemical - prolonged contact time).
H-T-064	Tags shall be resistant to high pressure fluids (e.g., water, steam, etc.).
H-T-065	Tags shall be able to operate in an oxygen rich environment and not ignite combustible gases.
H-T-066	Tags shall operate and be safe to use around electrical equipment that are known sources of interference.(e.g., plasma displays)
H-T-067	Tags shall withstand a reasonable amount of electrostatic discharge in accordance with industry standards.
H-T-068	Tags shall operate and be safe to use around large magnets (e.g., MRI equipment) or known sources of magnetic interference.
H-T-069	Tags shall be able to withstand shock and shear forces to the greatest extent possible.

There are two (2) types of RTLS readers/receivers/interrogators planned: fixed readers based in a set location (e.g., wall-mounted) and handheld/portable devices.

The table below contains interface and technical requirements for both fixed and handheld readers as well as for display monitors and printers used by RTLS.

Table 12: Fixed and Handheld Readers

Req. ID	Requirement
H-R-001	The RTLS shall be able to recognize both active and passive tags.
H-R-002	The RTLS infrastructure shall be flexible and expandable to accommodate any new physical additions or changes to the required coverage environment inside a facility.
H-R-003	The readers/receivers shall utilize or leverage the existing facility network (e.g., LAN Ethernet, Wi-Fi) to the maximum extent possible, and will be required to comply with VA security requirements.
H-R-004	All readers shall be able to read tag received signal strength indication (RSSI) and report those values to the RTLS. These values shall be able to be displayed on RTLS display monitors.
H-R-005	To avoid inaccurate and false tag reads, all readers (if not already a feature of tags) shall implement some type of read verification, such as a cyclic redundancy check (CRC).
	Fixed Readers
H-R-007	RTLS Readers shall be powered by a facility-provided standard 110V supply.
H-R-008	RTLS Readers/Receivers shall operate and communicate at an RF power level and frequency that does not interfere with any other device in VA facilities.
H-R-010	RTLS Readers shall be capable of functioning in a dense asset identification environment such as a warehouse storage room or clean utility room.
H-R-011	RTLS Readers shall be able to discretely identify all tagged items in such a location without any false positive or false negative identification’s.
H-R-012	The health status of RTLS Readers shall be able to be dynamically monitored by the RTLS and displayed on RTLS display monitors
H-R-013	Upon any RTLS Reader loss in tag connectivity (e.g., via a detection of RSSI falling below defined operational threshold for a user-settable time period), the tag shall display a visible alert (e.g., blinking LED) and RTLS shall be alerted.
H-R-014	Readers shall comply to UL Safety Standard 2043
	Handheld Readers
H-R-020	All fixed reader requirements mentioned previously in this section shall apply to the handheld readers.
H-R-021	Handheld RTLS passive tag readers/scanners shall have the capability to download and upload current (e.g., inventory) information from the RTLS database to better reconcile equipment assigned to various zones.
H-R-022	Handheld readers/scanners shall operate and communicate at an RF power level and frequency that does not interfere with any other devices in the medical center.
H-R-023	Handheld readers/scanners shall be able to communicate back to RTLS via the VA facility’s Wi-Fi (802.11) network.
H-R-024	Handheld reader/scanners shall have the capability to write/encode information onto passive tags.
H-R-025	Handheld reader/scanners shall have the capability to write/encode information onto to passive tags that are used with the Catheterization Lab RTLS Smart Cabinet.
H-R-026	RFID-enabled handheld readers/scanners shall be capable of optically reading 1D linear imaging and 2D area imaging barcodes.
	RF Communications

Req. ID	Requirement
H-R-027	Readers shall be able to communicate with tags using any unlicensed Institute for Supply Management (ISM) bands and conform to all EPC (Engineering, Procurement, and Construction), and ISO/IEC 18000 and 18000-6Cseries standards.
H-R-028	Readers shall be tested against and comply to RFID conformance test methods specified in ISO/IEC TR 18047-4:2004 , Part 4: Test methods for air interface communications at 2.45 GHz
	RF Interference
H-R-030	RTLS Readers shall neither operate within nor interfere with the active Medical Telemetry Frequency Range.
H-R-031	Readers shall comply with FCC Code of Federal Regulations 47 part 15: RADIO FREQUENCY DEVICES, specifically sections 15.225, 15.240, 15.245, 15.247, and 15.249.
H-R-032	Readers shall not interfere with the VA facility's Wi-Fi network
H-R-033	Readers shall not interfere with any RF-susceptible system at the VA deployment site (e.g., ultrasound)
	Environmental
H-R-035	Readers shall operate in normal indoor and outdoor environments at temperature range of -25º C to 70º C (-13° F to 158° F) and withstand storage temperature range between -40 º C and 85º C (-40° F and 185° F).
	RTLS Display Monitors
H-R-040	The RTLS shall provide the capability to display RTLS data to wall-mounted and desk display monitors in each ward or other locations as specified at the TO level.
H-R-041	RTLS shall provide display monitors with touch screen capability.
H-R-042	The size of the monitors will be determined at the Task Order level.
H-R-043	Displays shall not cause electromagnetic interference (e.g. plasma display).
H-R-044	Large, wall-mounted RTLS display monitors shall be HIPAA-compliant.

2.6 Legacy System Retirement

RTLS and NDR are neither replacing nor retiring any VA legacy system.

3 Conceptual Design

3.1 Conceptual Application Design

In this section, we provide diagrams that depict the context within which the RTLS System exists. The diagrams include:

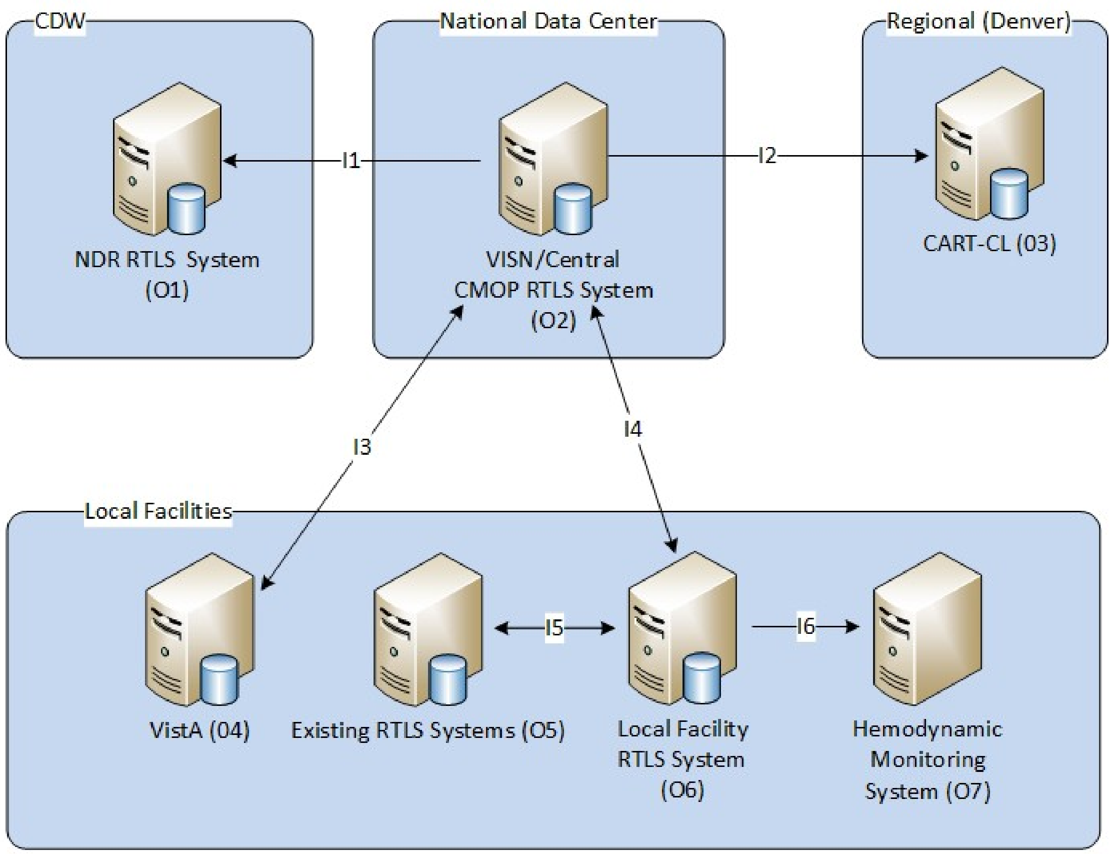
- Application Context
- High Level Application Design
- Conceptual Data Model
- Physical Hardware (VAMC, CMOP, VISN)
- NDR Physical Architecture
- Conceptual Network

- Conceptual Environments
- Conceptual Production String

3.1.1 Application Context

The following context diagram depicts the context in which RTLS and NDR will exist. This includes the RTLS system, NDR, as well as all currently known system/service the RTLS will need to interface with.

Figure 24: RTLS Application Context



Notes

- A local facility is considered to be a local VAMC, CBOC, or CMOP. A local facility may not have all the components drawn.

The following table describes each of the objects (systems) labeled (O1-O9) in the figure above. The columns in the Application Context Object Description table are defined as follows:

- ID – the label corresponds to the label in the diagram above
- Name – this is the name of the system
- Description – a brief explanation of the object
- Interface Name(s) – the name of the interface(s) that the system provides
- Interface System(s) – the system(s) that the object interfaces with

Table 13: Application Context Object Descriptions

Objects				
ID	**Name**	**Description**	**Interface Name(s)**	**Interface System(s)**
O1	NDR RTLS System	System that provides a sophisticated nationwide business intelligence, predictive analytics, and reporting purposes of all the VA RTLS systems.	• RTLS-NDR	• VISN/Central CMOP RTLS System
O2	VISN/Central CMOP RTLS System	RTLS System deployed on a per VISN/CMOP (1 instance of a CMOP) basis that provides real time reporting information on items, consumables, resources and business workflows. This system is used to aggregate all of the facility's assets and consumables into a VISN level data store.	• Intelligent Intelligent InSites Restful API Interface (https://[serverName]/api/2.0/rest/) • VistA-Service • WaveMark Integrator Connect API (https://[serverName]/wavemark/integratorconnect) • WMService • EmployeeFeed • EncounterLink	• NDR RTLS System • VistA • Local Facility RTLS System • CART-CL
O3	CART-CL	Cardiovascular Assessment Reporting and Tracking (CART) is a software application for standardized report generation, national Structured Query Language (SQL) data repository, and national quality improvement program for VA Catheterization labs. The application is integrated with VA's Computerized Patient Record System (CPRS) and Electronic Health Record (EHR) enabling providers to document care as part of routine clinical work. The application provides discrete data entry	CART_RTLS • RTLSSession • RTLSItem	• VISN/Central CMOP RTLS System

		(based on American College of Cardiology standards) with narrative text for customization.		
O4	VistA	VistA is a large suite of applications that include clinical, fiscal, quality management and administrative software.	VistA-Link	• VISN/Central CMOP RTLS System
O5	Existing RTLS Systems	These systems are the existing legacy RTLS systems that are in place throughout the various facilities.	N/A	• Local Facility RTLS System
O6	Local Facility RTLS System	System used in providing geo-location of items, consumables and resources at the local facility level. This system also includes the reprocessing of medical and surgical instruments. A local facility could be a VAMC, CBOC, or a CMOP.	• Intelligent InSites Restful API Interface • Bulk Streaming Protocol • Censis to Intelligent InSites Interface • BarcodeConnect • PatientConnect	• VISN/Central CMOP RTLS System • Hemodynamic Monitoring System • Existing RTLS Systems
O7	Hemodynamic Monitoring System	Hemodynamic monitoring systems that allow users (Nurses) the ability to monitor patient progress through real time procedure notes charting continually keeping clinical records up-to date. Many Hemodynamic Vendors exist in the VA today, each requiring its own interface.	N/A	• Local Facility RTLS System

The following table describes each of the external interfaces to the Office of Information Technology (OIT) labeled (I9) in the figure above. The columns in the Application Context External Interfaces Description table are defined as follows:

- ID – the label corresponds to the interface labelled in the diagram above
- Interface Name - the name of the interface that is exposed to the external system(s)
- Related Object - the name and label corresponds to the object in the diagram above that is providing the interface
- Input Messages – the format of the messages that get input to the interface
- Output Messages – the format of the messages that are output
- External Party – the external vendor(s) who use the provided interface

Table 14: Application Context External Interface Descriptions

Interfaces External to OIT					
ID	**Interface Name**	**Related Object**	**Input Messages**	**Output Messages**	**External Party**
I5	Intelligent InSites Data Connectors (custom data connectors are made for the various external parties)	Local Facility RTLS System (O10)	• UDP Stream • XML • HL7	XML	• Aeroscout • Ekahau • Sonitor • Versus

The following table describes each of the internal interfaces to the Office of Information Technology (OIT) labeled (I1-I8) in the figure above. The columns in the Application Context Internal Interfaces Description table are defined as follows:

- ID – the label corresponds to the interface labelled in the diagram above
- Interface Name - the name of the interface that is exposed to the internal system(s)
- Related Object - the name and label corresponds to the object in the diagram above that is providing the interface
- Input Messages – the format of the messages that get input to the interface
- Output Messages – the format of the messages that are output
- External Party – the external vendor(s) who use the provided interface

Table 15: Application Context Internal Interface Descriptions

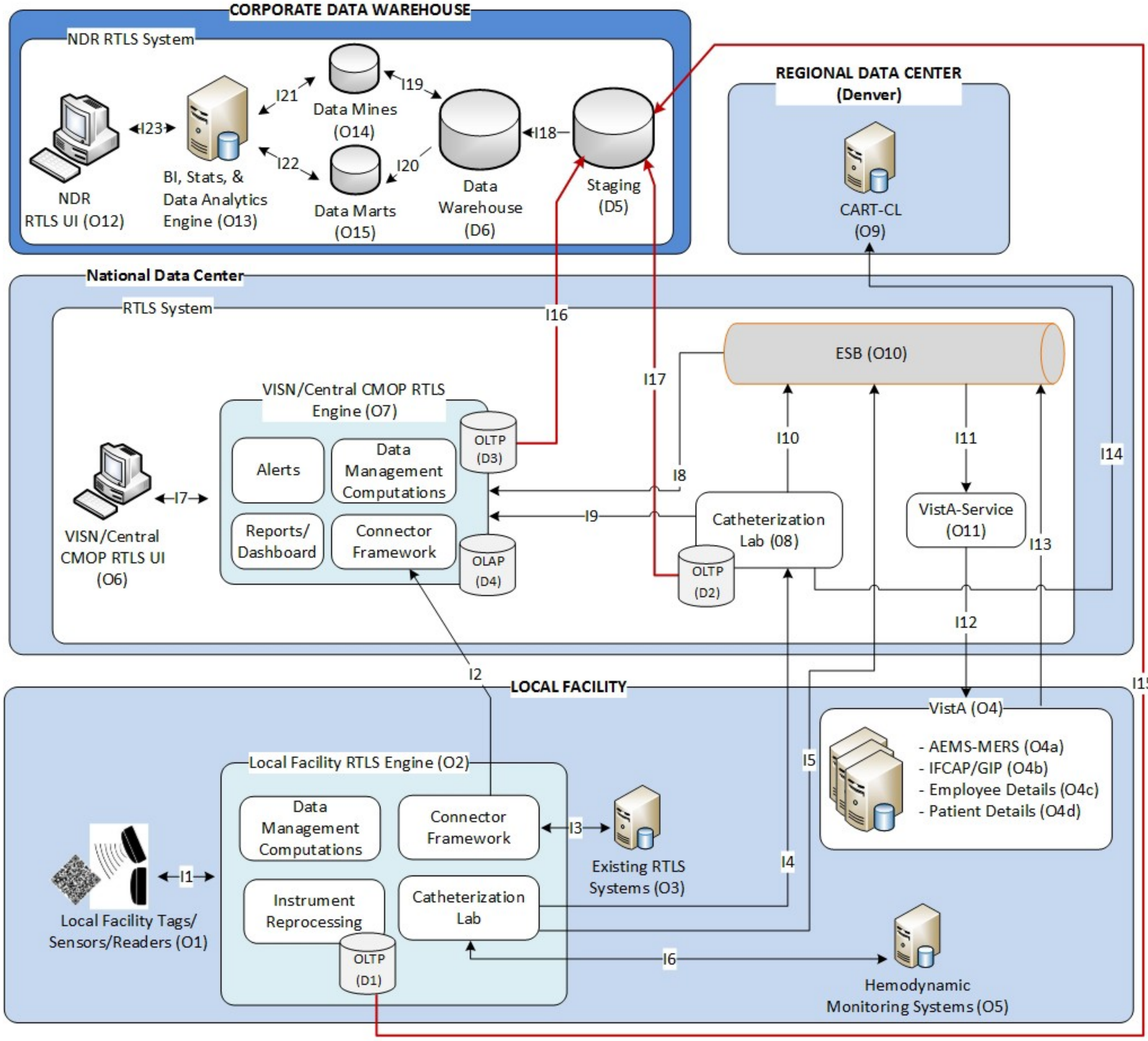
Interfaces Internal to OIT					
ID	**Interface Name**	**Related Object**	**Input Messages**	**Output Messages**	**Other CBP Party**
I1	RTLS-NDR	NDR RTLS System (O1)	File	File	
I2	EncounterLink	VISN/Central CMOP RTLS System (O2)	JDBC	JDBC	*None*
I3	VistA-Service (VistA-Link)	VISN/Central CMOP RTLS System (O2)	XML	XML	*None*
I4	• onHandLink • EmployeeLink	VISN/Central CMOP RTLS System (O2)	XML	XML	*None*

	• PatientConnect • WMService • InSites Restful API Interface				
I5	BarcodeConnect	Procedure Room Cath Lab RTLS System (O8)	Data Packets over HID or RS232	Data Packets over HID or RS232	*None*

3.1.2 High Level Application Design

The following High Level Application Design diagram is intended to identify the major components of the application and the relationships of the major application components to each other and to the surrounding applications.

Figure 25: High Level Application Design



Notes

- A local facility is considered to be a local VAMC, CBOC, or CMOP. A local facility may not have all the components drawn.

The following table describes each of the objects (O1 – O15) in the figure above. The columns in the Objects in the High Level Application Design table are defined as follows:

- Name - the name of the object that corresponds to the above diagram
- ID – the label corresponds to the interface labelled in the diagram above

- Description – a brief explanation of the object
- Service or Legacy Code – if the object is a Service or Legacy Code
- External Interface Name – the name of the interface(s) that the system provides within the RTLS System
- External Interface ID – the ID (corresponds to the above diagram) of the interface that the object interfaces outside of the RTLS system
- Internal Interface Name – the name of the interface(s) that the system provides within the RTLS System
- Internal Interface ID - the ID (corresponds to the above diagram) of the interface that the object interfaces within the RTLS system
- SDP Sections 1 & 2 – status of the object/interface. Valid values are:
    - Approved
    - Submitted
    - Being Developed
    - Future Development

Table 16: Objects in the High Level Application Design

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
Local Facility Tags/Sensors/Readers	O1	Transmits object sensory data (e.g., location data) to the Local RTLS Engine.	Service	N/A	N/A	N/A	N/A	Submitted
Local Facility RTLS Engine	O2	Engine used in providing sensory data (e.g., location) collection and monitoring of objects and resources at the VAMC, CBOC, or CMOP facility level. Provides a framework for connecting to various systems throughout the RTLS System.	Service	N/A	N/A	• Intelligent InSites RESTful API Interface - https://[Server Name]/api/2.0/rest/equipment.xml? • Bulk Streaming Protocol • BarcodeConnect • Censis-NDR Interface	I1, I3, I6, & I15	Submitted
Existing RTLS Systems	O3	These systems are the existing legacy RTLS systems that are	Legacy	TBA	TBA	N/A	I3	Approved

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
		in place throughout the various facilities (Aeroscout, Ekahau, Sonitor, Versus, etc.)						
VistA	O4	VistA is a large suite of applications that include clinical, fiscal, quality management and administrative software.	Legacy	N/A	N/A	N/A	I12	Submitted
AEMS-MERS	O4a	Automated Engineering Management System /Medical Equipment Reporting System (AEMS/MERS) is the Veterans Health Information Systems &	Legacy	N/A	N/A	• VIAA ENG ASSET MOVE • VIAA ENG GET DATA • VIAA ENG GET CATEGORY • VIAA ENG GET EQUIPMENT • VIAA ENG GET LOCATION	I12	Submitted

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
		Technology Architecture (VistA) equipment management system that resides locally.						
IFCAP/GIP	O4b	Generic Inventory Package (GIP) is a module of IFCAP that resides locally and manages the receipt, distribution, and maintenance of stock items received for the supply warehouse from outside vendors and distributed to primary inventory points.	Legacy	N/A	N/A	• VIAA GET INVENTORY POINT ITEMS • VIAA GET ITEM MASTER UPDATE • VIAA SET PAR LEVELS IN GIP • VIAA SET QUANTITY ON HAND	I12	Submitted
Employee Details	O4c	The VistA file containing identification information for	Legacy	N/A	N/A	• VIAA GET EMPLOYEE DATA	I12	Submitted

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
		all employees within the VA.						
Patient Details	O4d	The VistA file containing identification information for all patients.	Legacy	N/A	N/A	• VIAA GET PATIENT DATA	I12	Submitted
Hemodynamic Monitoring System	O5	Hemodynamic monitoring systems that allow users (Nurses) the ability to monitor patient progress through real time procedure notes charting continually keeping clinical records up-to date. Many Hemodynamic Vendors exist in the VA today, each requiring its own interface.	Service	N/A	N/A	• BarcodeConnect	I6	Approved
VISN/Central CMOP	O6	Role-based User Interface	Service	N/A	N/A	N/A	N/A	Being

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
RTLS UI		used to provide real time reporting information on objects, resources and business workflows at the VISN or VAMC, CBOC and CMOP level.						Submitted
VISN/Central CMOP RTLS Engine	O7	Engine used in providing real time reporting information on objects, resources and business workflows at the VISN/CMOP level.	Service	N/A	N/A	• Intelligent InSites Restful API Interface • Intelligent InSites-NDR Interface • OATSystems-NDR Interface • CenTrak-NDR Interface	I2, I7, I8, I9 & I16	Submitted
Catheterization Lab	O8	This system is used to aggregate the various systems in all of the local facility’s Catheterization	Service	N/A	N/A	• WMService • ControllerService • WaveMark - NDR Interface	I4, I10, I14 & I17	Submitted

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
		labs to keep track of consumables during a procedure						
CART-CL	O9	Cardiovascular Assessment Reporting and Tracking (CART) is a software application for standardized report generation, national SQL data repository, and national quality improvement program for VA Catheterization labs. The application is integrated with the VA's CPRS and EHR enabling providers to document care	Legacy	N/A	N/A	• EncounterLink	I14	Approved

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
		as part of routine clinical work. The application provides discrete data entry (based on American College of Cardiology standards) with narrative text for customization.						
ESB	O10	An enterprise service bus (ESB) is an integrated platform that provides fundamental interaction and communication services for complex software applications via an event driven and standards-based	Service	N/A	N/A	N/A	I5, I8, I10, I11, & I13	Submitted

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
		messaging engine, or bus, built with middleware infrastructure product technologies. The ESB platform is geared toward isolating the link between a service and transport channel and is used to fulfill service-oriented architecture requirements.						
VistA-Service (VistA-Link)	O11	VistA-Link is an transport adapter that provides communication to the VistA/M applications via a Web Service	Legacy	N/A	N/A	N/A	I11	Submitted
NDR RTLS UI	O12	User Interface that allows for customizable	Service	N/A	N/A	N/A	N/A	Being Developed

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
		dashboards to the end users to view critical business intelligence data.						
BI, Stats, Data Analytics Engine	O13	Engine that provides a sophisticated nationwide business intelligence, predictive analytics, and reporting purposes.	Service	N/A	N/A	*TBA*	I21 & I22	Being Developed
NDR Data Mines	O14	The NDR Data mines will provide a wide range of capabilities for exploring and analyzing data to help reveal patterns, opportunities, and information that can drive proactive,	Service	N/A	N/A	*TBA*	I19 & I21	Being Developed

Objects								
Name	**ID**	**Description**	**Service or Legacy Code**	**External Interface Name**	**External Interface ID**	**Internal Interface Name**	**Internal Interface ID**	**SDP Sections 1&2**
		evidence-based, and strategic decision-making.						
NDR Data Marts	O15	The NDR Data Marts are subsets of the NDR Data warehouse. This will allow users to manipulate data without effecting other users or data sets.	Service	N/A	N/A	*TBA*	I20 & I 22	Being Developed

The following table describes each of the data stores (D1 – D3) in the figure above. The columns in the Internal Data Stores in the High Level Application Design table are defined as follows:

- Name – the name of the data store that corresponds to the above diagram
- ID – the label corresponds to the data store labeled in the diagram above
- Data Stored – a description of the data being stored
- Steward – the name of the system/subsystem/service that manages the data
- Access – which create, read, update, and delete (CRUD) operations does this system do on the data store

Table 17: Internal Data Stores in the High Level Application Design

Internal Data Stores				
Name	**ID**	**Data Stored**	**Steward**	**Access**
Instrument Reprocessing OLTP	D1	Handles the storage and retrieval of surgical instrument inventory and tracking data. This data will be extracted and loaded into the NDR.	Instrument Reprocessing	Create/Read/Update/Delete (Soft deletes – no data is actual removed from the database) – by Censis Technologies Read – User access
VISN Catheterization Lab OLTP	D2	Collects, stores, and retrieves information from WaveMark's RFID Smart Cabinets and Point of Use Stations. The data stored in this data store allows for the efficient management of Catheterization Lab supplies. This data will be extracted and loaded into the NDR.	VISN Catheterization Lab	Create/Read/Update/Delete (Soft deletes – no data is actual removed from the database) – by WaveMark Read – User access
VISN/Central CMOP RTLS OLTP	D3	The data is aggregated from all the VAMC's and CBOC's RTLS systems belonging to the VISN or all the aggregated CMOPs. The bulk of the data is item and resource location that will be used for reporting and analysis. This data will be extracted and loaded into the NDR.	VISN/Central CMOP RTLS Engine	Create/Read/Update/Delete (Soft deletes – no data is actual removed from the database) – by Intelligent InSites System Read – User access
VISN/Central CMOP RTLS OLAP	D4	Business Intelligence is the reporting environment (Analytical Data Store) that contains a copy of the unstructured data from the VISN/Central CMOP RTLS	VISN/Central CMOP RTLS Engine	Create/Read/Update/Delete (Soft deletes – no data is actual removed from the database) – by Intelligent InSites System Read – User access

Internal Data Stores				
Name	**ID**	**Data Stored**	**Steward**	**Access**
		OLTP data store. This data store transforms unstructured data to structural data that will be used for reporting and analytical purposes.		
NDR Staging	D5	Data store used to aggregate data from all the VISNs and CMOPs. This data will be cleaned, transformed, and shipped to the data warehouse.	NDR Staging	Create/Read/Update/Delete
NDR Data Warehouse	D6	Enterprise wide data warehouse housing all RTLS data from all the locations including VISNs, VAMCs, CBOCs, and CMOPs	NDR Data Warehouse	Create/Read/Update/Delete

3.1.3 Application Locations

The following table identifies the potential locations that application components will be hosted. . The columns in the Application Locations table are defined as follows:

- Application Component – the name of the component
- Description – a brief explanation of the component
- Location at Which Component is Run – the facility where the component will be executed
- Type – the classification of component (Tag Layer, Presentation Layer, Service Layer, or Data Layer)

Table 18: Application Locations

Application Component	Description	Location at Which Component is Run	Type
Local Facility Tags/Sensors/Readers	Transmits object sensory data (e.g., location) to the Local Facility RTLS Connector Frameworks	Local RTLS Facility	Tag Layer
Local Facility RTLS Connector Framework	Provides system integration for RTLS data by utilizing adapters for various system to system communication (Enterprise Service Bus like features)	Local RTLS Facility	Service Layer
VISN/Central CMOP RTLS UI	Role-based User Interface used to provide real time reporting information on objects, resources and business workflows at the VISN/Central CMOP level.	VA National Data center	Presentation Logic
VISN/Central CMOP RTLS Engine	Engine used in providing real time reporting information on objects, resources and business workflows at the VISN/Central CMOP level.	VA National Data center	Service Layer
VISN/Central CMOP Data Warehouse	Aggregates CBOC/VAMC/CMOP RTLS data and sends to NDR	VA National Data center	Data Layer
NDR RTLS UI	User Interface that allows for customizable	VA Corporate Data	Presentation Logic

Application Component	Description	Location at Which Component is Run	Type
	dashboards to the end users to view critical business intelligence data.	Warehouse	
NDR BI, Stats, Data Analytics Engine	Engine that provides a sophisticated nationwide business intelligence, predictive analytics, and reporting purposes.	VA Corporate Data Warehouse	Service Layer
NDR Data Mines	The NDR Data mines will provide a wide range of capabilities for exploring and analyzing data to help reveal patterns, opportunities, and information that can drive proactive, evidence-based, and strategic decision making.	VA Corporate Data Warehouse	Data Layer
NDR Data Marts	The NDR Data Marts are subsets of the NDR Data warehouse. This will allow users to manipulate data without effecting other users or data sets.	VA Corporate Data Warehouse	Data Layer
NDR Staging	Data store used to aggregate data from all the VISN and CMOPs. This data will be cleaned, transformed and loaded in the NDR Data Warehouse.	VA Corporate Data Warehouse	Data Layer
NDR Data Warehouse	Enterprise wide data warehouse housing all RTLS data from all the locations including VISNs, VAMCs, CBOC, and CMOPs	VA Corporate Data Warehouse	Data Layer

3.1.4 Application Users

User access and authentication to the RTLS and its components shall be directly integrated with the existing VA Active Directory (AD) server. RTLS shall support the use of domain, organizational unit, group, and user hierarchy. Access to RTLS components shall be easily assigned to new user groups based on AD accounts through the configuration of assigning AD groups to RTLS features (e.g., screen views, reporting tool capabilities, database configuration, and work flow management). The following table describes the application users for the RTLS System. The columns in the Application Users table are defined as follows:

- Application Component – the name of the component
- Location – the location of the facility where the users will interact with the component
- User – the role of the user

Table 19: Application Users

Application Component	Location	User
Local Facility RTLS UI	VA National Data center	RTLS Administrator RTLS Groups & Users
Local Facility Tags/Sensors/Readers	Local RTLS Facility	RTLS Administrator RTLS Groups & Users RTLS Service Level
Local Facility RTLS Engine	Local RTLS Facility VA National Data center	RTLS Administrator RTLS Service Level
VISN/Central CMOP RTLS UI	VA National Data center	RTLS Administrator RTLS Groups & Users
VISN/ Central CMOP RTLS Engine	VA National Data center	RTLS Administrator RTLS Service Level
VISN/ Central CMOP RTLS Data Warehouse	VA National Data center	RTLS Administrator RTLS Service Level NDR Administrator
NDR RTLS UI	VA Corporate Data Warehouse	NDR System Administrator NDR Standard User NDR Power User NDR Data Steward
BI, Stats, Data Analytics Engine	VA Corporate Data Warehouse	NDR System Administrator NDR Standard User NDR Power User
NDR Data Mines	VA Corporate Data Warehouse	NDR System Administrator NDR Power User
NDR Data Marts	VA Corporate Data Warehouse	NDR System Administrator NDR Standard User NDR Power User NDR Data Steward
NDR Staging	VA Corporate Data Warehouse	NDR System Administrator NDR Data Steward

Application Component	Location	User
NDR Data Warehouse	VA Corporate Data Warehouse	NDR System Administrator NDR Power User NDR Data Steward

3.2 Conceptual Data Design

3.2.1 Project Conceptual Data Model

The RTLS Conceptual Data Model shown in the below Figure below represents data types associated with asset over its lifetime; incorporating four (4) asset subject areas: Asset Management, SPS, Cath-Lab, and Temperature Monitoring. The data model will allow new data fields and indices to be added without the need to change existing data elements and their functionalities. The conceptual data model in the below figure shows the entities and their relationships. A more detailed version of the data model is included in the Enterprise Data Architecture (EDA) document.

Figure 26: RTLS High Level Conceptual Data Model

3.2.2 Database Information

The following table identifies all databases that will be interfaced with for purposes of NDR rollup. The columns in the Database Inventory table are defined as follows:

- Database Name – the name of the database
- Description – a brief explanation of the database
- Type – the vendor and version of the underlying database
- Steward – the application or organization that manages and maintains the database

Table 20: Database Inventory

Database Name	Description	Type	Steward
RTLS Database	Each RTLS Middleware/Application Server responsible for tracking the up to date sensory data of any tagged object along with additional descriptive information acquired from other existing VA Systems that further define the tagged object.	Microsoft SQL Server 2012 & Oracle 11g	RTLS
RTLS Reporting (Business Intelligence) Database	This includes all the data from the real time database plus additional process data, including other sub-systems like Cath Lab. Each VISN/Central CMOP will have an instance of the RTLS Business Intelligence Database	MySQL & MonetDB	RTLS
RTLS NDR Staging Database	This includes an aggregation of the VISN level RTLS Databases including both transactional and analytical data stores.	Microsoft SQL Server 2012	NDR
NDR Database	A single national-level database/warehouse modeled and loaded from the RTLS NDR Staging database. This database could also contain additional information acquired from other existing VA Systems that further define the tagged objects.	Microsoft SQL Server 2012	NDR

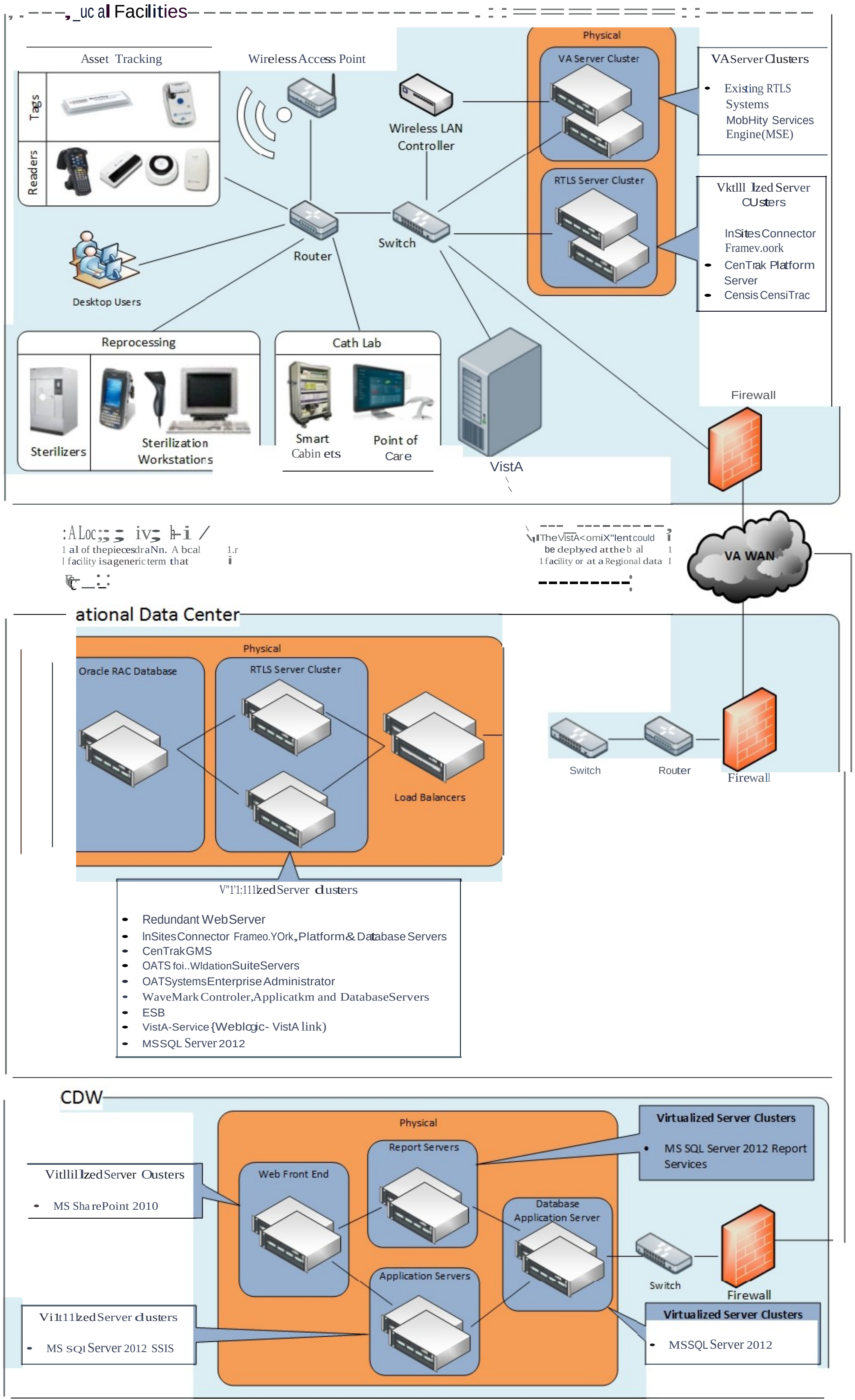
3.3 Conceptual Infrastructure Design

This section provides a very high level overview of the infrastructure that will be used to support RTLS System v1.0. Primary emphasis is on the environments that will be required and the locations at which they will be installed. Here, we will address any unique technology that is to be used, either to which this system will attach or which are part of this system.

The physical architecture, shown in the figure below, highlights several key elements of the solution. The figure below depicts what the logical information model looks like when implemented as a physical system, and it provides details on the vendor products and physical hardware implemented at the application and technology infrastructure layers. The NDR solution will leverage the CDW environment and existing technology resources. The physical architecture will provide scalability and capacity, as well as availability and reliability.

The below figure describes the server environment proposed to host the data behind this system and the software implemented to collect, manage, and process it.

Figure 27: Logical Hardware and Products



3.3.1 System Criticality and High Availability

Local Facility

The physical infrastructure at the Local Facility (VAMC, CBOC, or CMOP) will include VA provided switches, routers, firewalls, wireless access points, and MSE for the national RTLS installation. In addition two rack servers and a SAN storage will be installed to run the National RTLS software package. The RTLS System deployed at the local facility level will have seamless availability to the RTLS users by placing the servers in separated physical locations, and integrating a High Availability (HA) model. The model will include the use of heartbeat and performance metric monitoring technology to ensure uptime. To prevent outages, the RTLS System will use VMware failover and the installed SAN for high availability. If a piece of hardware within one of the rack servers or a software instance crashes, the instance(s) will fail over to the secondary server. The system is capable of caching real time data in the event the WAN is unavailable. The following table details the high availability strategy for each RTLS component at the local facility level.

Table 21: Local Facility High Availability Strategy

Component	High Availability Strategy
Censis CensiTrac	VMware failover across servers
CenTrak Platform Server	VMware failover across servers
Intelligent InSites Connector Framework	VMware failover across servers

National Data Center

The physical infrastructure at the national data center will include VA provided switches, routers, firewalls, load balancers, VMWare hosts, Oracle RAC servers and SAN storage for the national RTLS installation. The RTLS System servers which will include web, application and database servers will utilize clustering and redundant practices. Oracle Databases will use Oracle RAC and Microsoft SQL Server Databases will make use of the AITC High Availability cluster. High availability will be made through the use of load balancing, clustering across physical hosts, VMware failover and the use of the installed SAN storage device. The high availability strategy will prevent down time in the event of hardware or network failure. The RTLS servers will be monitored by heartbeat and performance metric software to ensure a high level of availability. The following table details the high availability strategy for each RTLS component at the data center level.

Table 22: Data Center High Availability Strategy

Component	High Availability Strategy
WaveMark EiRTLS	Load Balanced and Clustering across blades
WaveMark Controller	VMware Failover across blades

Component	High Availability Strategy
WaveMark Interface	VMware Failover across blades
WaveMark Monitor	Primary Only
WaveMark Oracle Database	Oracle RAC
Intelligent InSites Platform (Web)	Load Balanced and Clustering across blades
Intelligent InSites Platform (API)	VMware Failover across blades
Intelligent InSites Business Intelligence	VMware Failover across blades
Intelligent InSites Connector Framework	VMware Failover across blades
Intelligent InSites Transactional Database	HA Cluster
Intelligent InSites Business Intelligence Database	Primary Only
OATxpress	VMware Failover across blades
OAT Database	HA Cluster
OAT Enterprise Administrator	VMware Failover across blades
Mule ESB	Load Balanced and Clustering across blades
VistAServices (VistA Instances using Weblogic	Load Balanced and Clustering across blades
CenTrak GMS - Managed	VMware Failover across blades

Based on this physical architecture, RTLS will develop an independent COOP and/or Disaster Recovery Plan (DRP) to meet VA requirements.

NDR

The NDR will follow existing CDW COOP and DRPs. The NDR will be deployed on blade servers and SAN storage. The NDR servers which will include Microsoft SharePoint, Microsoft SQL Server Integration Services (SSIS) and MS SQL Server will utilize clustering and redundant practices. High availability will be made through the use of clustering across blade servers, VMware failover, and the use of the installed SAN storage device. The high availability strategy will prevent down time in the event of hardware or network failure. The NDR servers will be monitored by heartbeat and performance metric software to ensure a high level of availability. The NDR servers will back up to a secondary disk and to a tape which resides in a Disaster Recovery location.

3.3.2 Special Technology

As per section 2.5.7, RTLS is itself a special technology. The following table describes each of the special technology requirements needed for the RTLS system. The columns in the Special Technology Requirements table are defined as follows:

- Special Technology – the name of the technology
- Description – a brief explanation of the technology
- Notional Location – at what type of location will this technology be deployed
- TRM Status - is the technology in the Technical Reference Model

Table 23: Special Technology Requirements

Special Technology	Description	National Location	TRM Status
RTLS / RFID	Real Time Location System (RTLS) capable of tracking and identifying the location of objects in real time. The RTLS calculates accurate real time locations, environmental measurements, and provides a visual mapped representation of that object within its geographical defined environment using RFID passive tags, active tags and labels.	Each VA Facility installed with the RTLS solution.	TBD

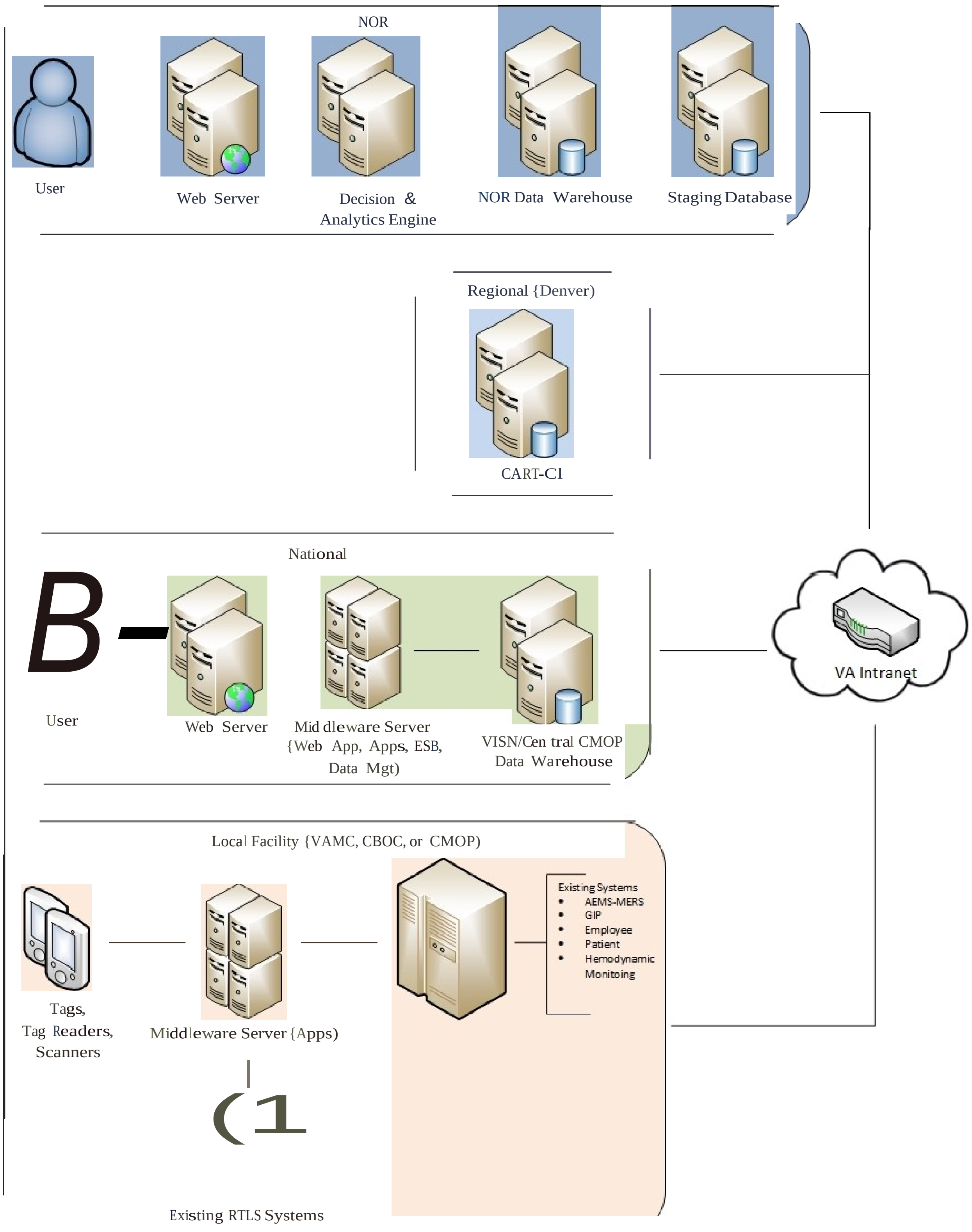
3.3.3 Conceptual Infrastructure Diagram

Location of Environments and External Interfaces

The figure below shows a conceptual view of the network that supports the RTL System. The RTLS users shall communicate directly with the National RTLS Middleware Server (per VISN/CMOP) for tracking objects, monitoring environmental measurements, performing workflows (reprocessing of medical/surgical instruments), performing queries and reporting capabilities through web-based GUIs running on an HTTPS Web Application Server. The Local Facility RTLS components shall interface with the National RTLS Middleware Server through the VA's WAN communication capabilities where the majority of the VA Legacy Systems reside. The national RTLS middleware server will communicate with a regional data center server (CART-CL) through the VA's WAN communication capabilities.

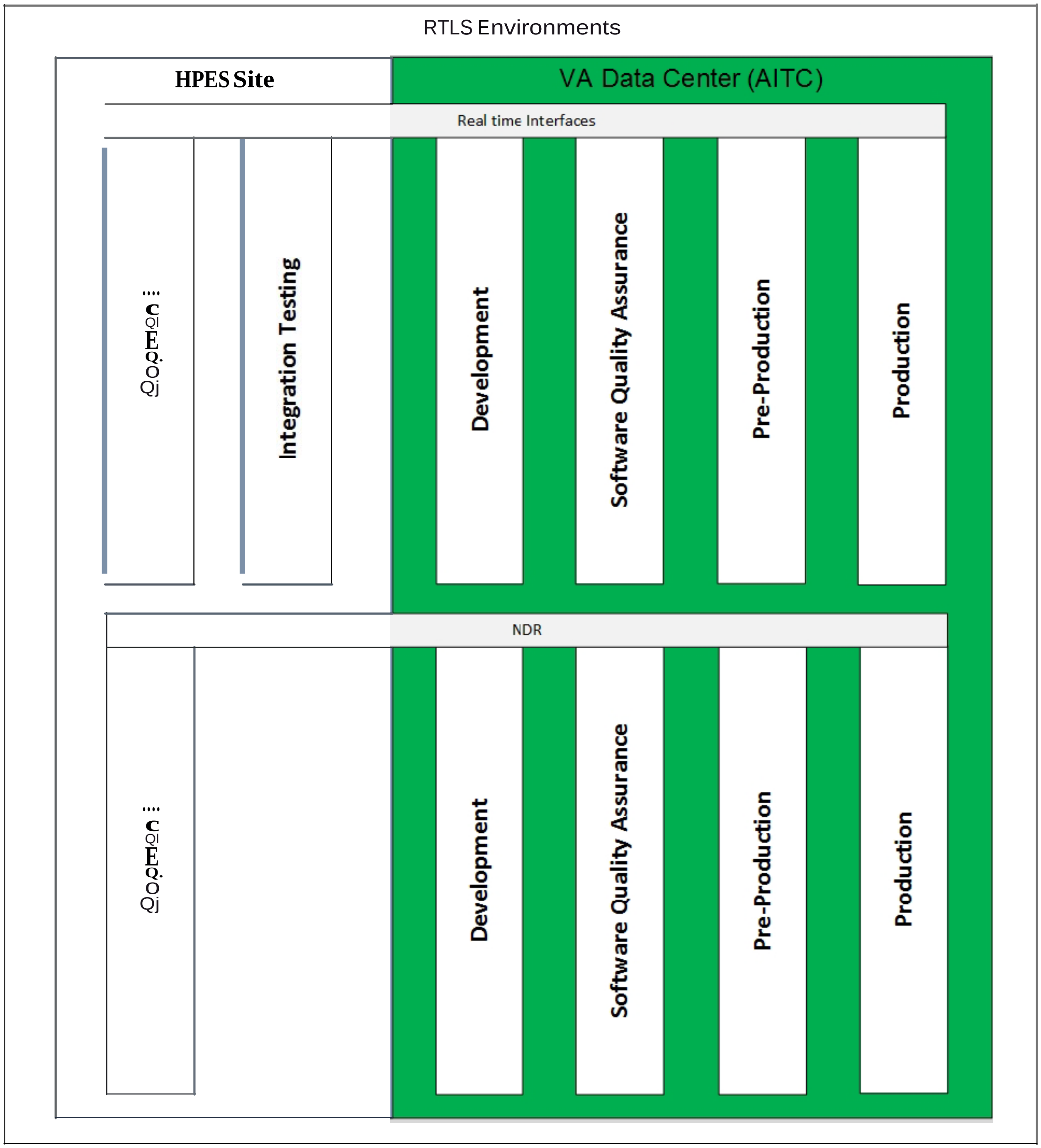
NDR Users shall communicate directly with the NDR Server for performing queries, reporting, business intelligence and analytic capabilities through a host of web-based GUIs running on an HTTPS Web Application Server. The VISN/Central CMOP RTLS Middleware Servers located at the NDC and the NDR Server shall communicate through the VA WAN for loading data into the NDR using ETL. The ETL will enable the NDR through a push-pull type interface to receive data for enterprise-type reporting across all the VA RTLS enabled locations.

Figure 28: RTLS Conceptual Network



This below figme depicts the environments that will be supported for RTLS, and the locations at which they will be installed.

Figure 29: **Conceptual Environments**



The following is a brief desctiption of each of the enviromnents in the above figure.

HPES Site

- Development: Environment used internally by developers to develop new software and enhancements to existing software.
- Integration Testing: Environment used internally by developers, quality assurance, and analysts to test new software and enhancements to existing software across the various integration points.

VA Data Center (AITC)

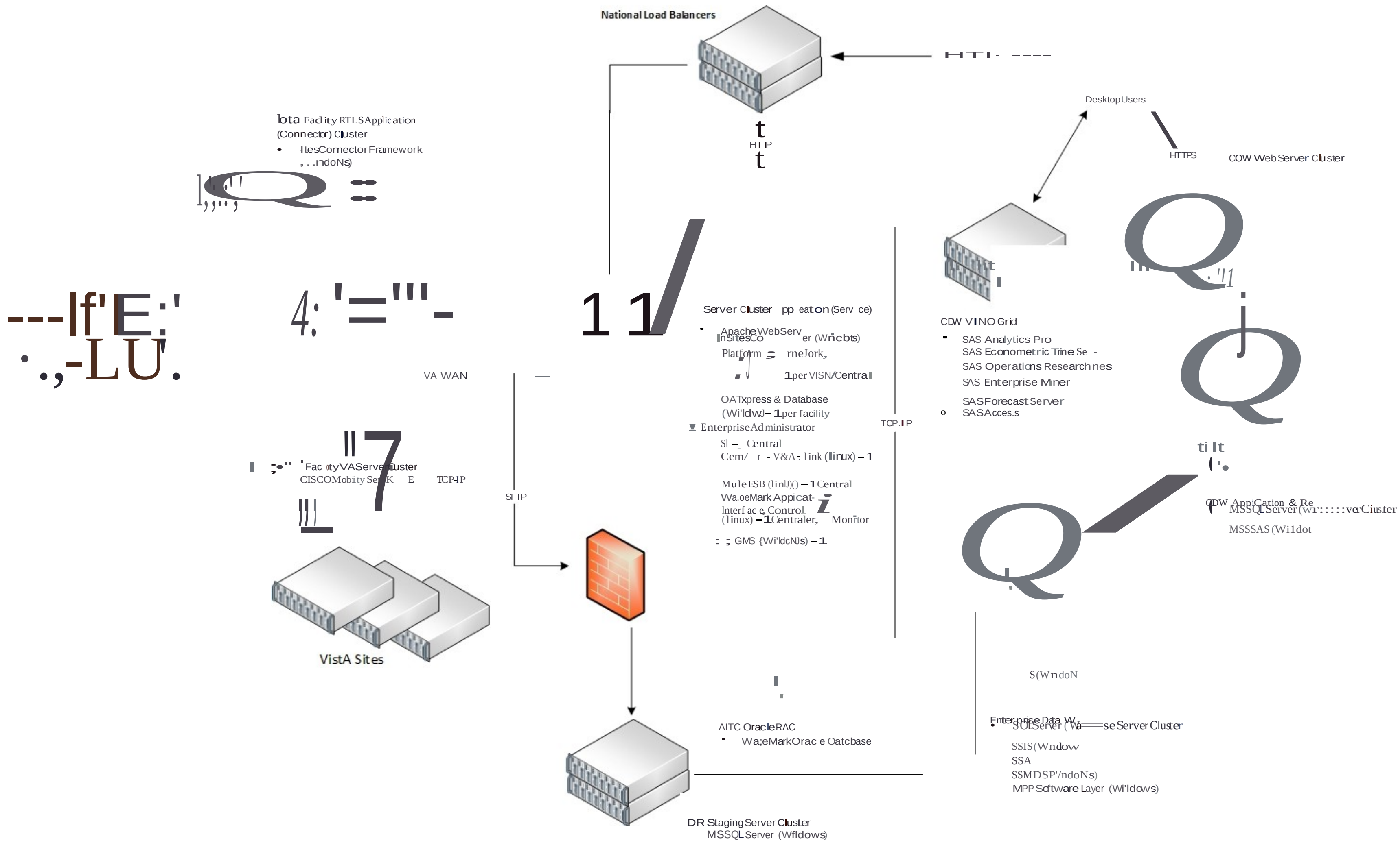
- Development: Environment used by developers to perform integration testing of the system.
- Software Quality Assurance: Environment used by Quality Assurance and VA Analysts to perform software quality assessments of the system.
- Pre-Production: Environment used to do initial field testing of the system under development.
- Production: Environment that hosts the full production system.

Note: The NDR Environment includes tools discussed in Section 6.2.5.2

Conceptual Production String Diagram

The following diagram (figure below) shows what a conceptual view of the Nation RTLS System Production String would look like.

Figure 30: Conceptual p reduction String



4 System Architecture

System Architecture is the model that defines structure, behavior, and views of the system. This section will cover the following architectures for the VA RTLS System:

- Hardware Architecture
- Software Architecture
- Communication Architecture

4.1 Hardware Architecture

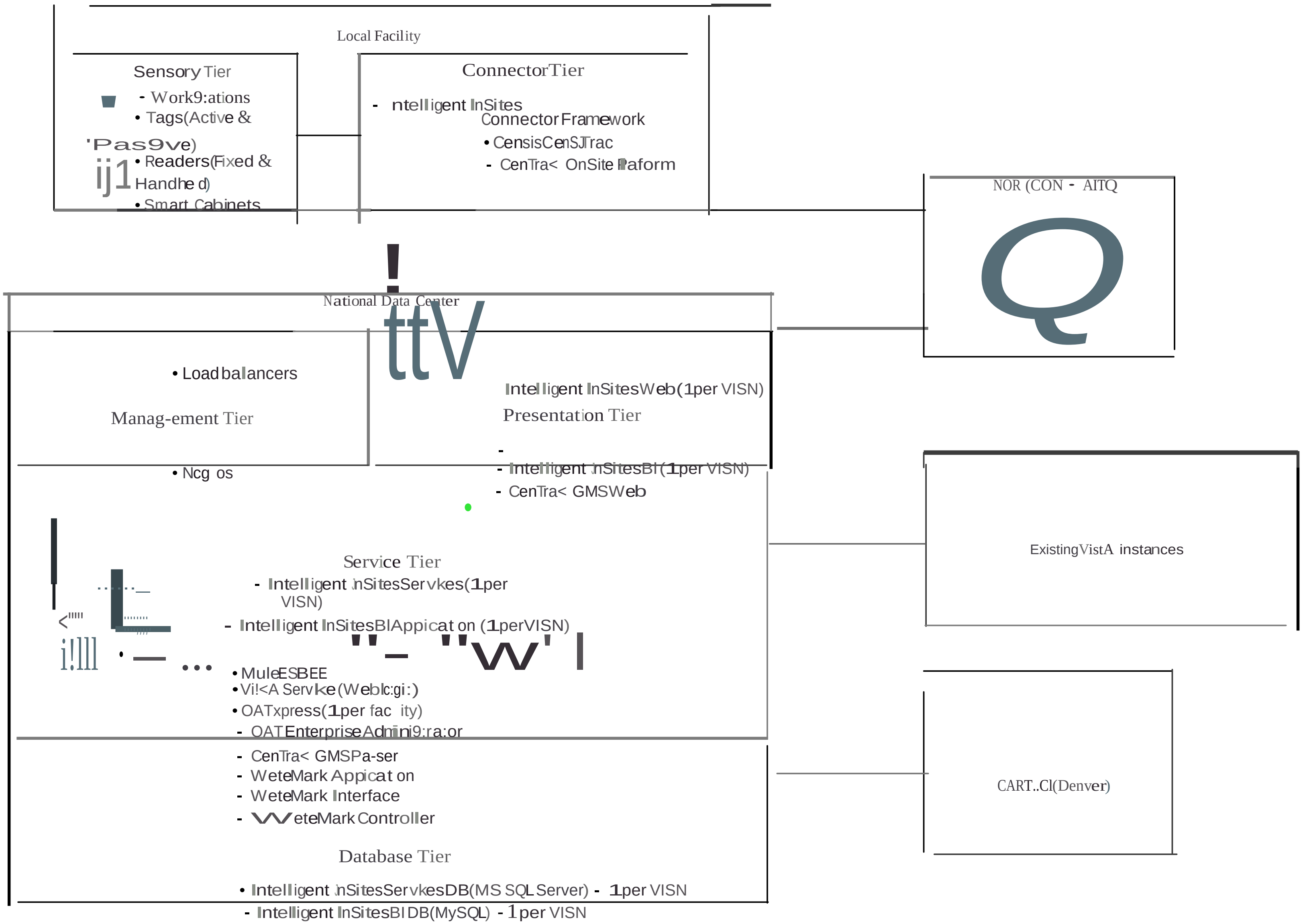
The To-Be hardware deployment will be Virtual Machine (VM)-based and deployed on a VMware "farm" at a National Data Center. The deployment consists of servers in a High Availability (HA) configuration, which provides load balancing and failover. These servers are aligned to a standard tier structure supporting the following tiers:

- Sensory Tier – input devices (readers, scanners, workstations, etc.)
- Connector Tier – provides interfaces for input devices to communicate with the Service Tier
- Presentation – browser-based User Interfaces
- Service Tier - 3rd Party and VA owned software/services used in the RTLS System. This tier provides integration middleware components
- Database Tier - data stores for various components in the Service tier
- Management Tier – provides management and monitoring of the system

All of the tier servers are running the VA's standard Red Hat Enterprise Linux and Windows operating systems. The table below describes the minimum required system components.

It is important to understand that more than production resources must be provisioned and supported. The VA RTLS System will have multiple environments (development, testing, pilot, production, etc.) The software releases of the product will advance through the normal sequence of development and testing environments. The physical support requirements for the product include providing physical resources (hardware, software, power, heating, cooling, etc.) for all of these environments.

Figure 31: RTLS Server Architecture



- CenTra< GMSDB (MSSQL Server)
- OATxpressDB (MSSQL Server – 1per fac ity
- W<weMark DB (Orac eEE RAC)

The following table describes each of the application components installed as part of the RTLS systems. The columns in the Deployment Components table are defined as follows:

- Application Name – the name of the application component that will be installed.
- Application Description – an explanation of the application component.
- Technology – the technologies (e.g., MS SQL Server 2008 R2) that the application component uses.
- Platform – the underlying operating system that the application component will be installed on.
- Devices used to C&A boundary traffic – any mechanism used for certification and accreditation for incoming traffic from the network boundary. A mechanism could be a VISN level firewall.
- Types of Access Controls Utilized (e.g., ACLs, VLANs) – a list of mechanisms used to control access to the application component.
- Ports – network ports required by the application component.
- Protocols/Services - network protocols and/or services required by the application component.
- Inbound (Y/N) – does the application component have network inbound traffic.
- Outbound (Yes/No, if "Yes" specify where) - does the application component have network outbound traffic, if the application component does have outbound traffic specify where the traffic is going to.

Table 24: Deployment Components

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
Intelligent InSites Connector Framework	The connector framework is a Windows server with a collection of tools for providing connectivity /integration to the Intelligent InSites Platform.	Mirth	Windows Server 2008 R2 (64 bit)	NDC and local facility Level Firewall	ACLs, VLANs	[redacted]	HTTPS	Y	Yes, Intelligent InSites Platform
		RabbitMQ	Windows Server 2008 R2 (64 bit)	NDC and local facility Level Firewall	ACLs, VLANs	[redacted]	TCP	Y	No
		Java jdk160_14_ R27.6.5-32	Windows Server 2008 R2 (64 bit)	NDC and local facility Level Firewall	N/A	[redacted]	N/A	N/A	N/A
Intelligent InSites Platform	Provides an User Interface, APIs and services that handles the creation, retrieval and updating of RTLS data (e.g., asset location)	MS SQL Server 2008	Windows Server 2008 R2 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	TCP	Y	Yes, JDBC, ODBC, and ETL processes
		Pentaho – admin console and Reporting	Windows Server 2008 R2 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTP, HTTPS	Y	Yes, User Community (Browsers)
		Java jdk160_14_ R27.6.5-32	Windows Server 2008 R2 (64 bit)	NDC and local facility Level Firewall	N/A	[redacted]	N/A	N/A	N/A

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
		JBoss 4.2.2	Windows Server 2008 R2 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTP, HTTPS	Y	Yes, User Community (Browsers)
							SNMP	Y	Yes, VA Account Users
							TCP	Y	Yes, server to server communicat ions
		Apache Web Server 2.2.3	Windows Server 2008 R2 (64 bit)	NDC and local facility Level Firewall	ACLs, VLANs		HTTP, HTTPS	Y	Yes, User Community (Brower)
		MonetDB	Windows Server 2008 R2 (64 bit)	NDC Level Firewall	ACLs, VLANs		JDBC MAPI	Y	No
		MySQL 5.5	Windows Server 2008 R2 (64 bit)	NDC Level Firewall	ACLs, VLANs		TCP	Y	Yes, JDBC, ODBC, and ETL processes

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
CenTrak OnSite Platform	The platform enables the use of existing Wi-Fi infrastructure to determine location through traditional RF triangulation. The platform also focuses on catastrophic events and operates when connection is lost to GMS-Managed.	Microsoft .Net Framework Version 3.5 (Paging Server)	Windows Server 2008 R2 (64 bit)	Local facility Level Firewall	N/A	[redacted]	TCP	Y	No
					N/A	[redacted]	UDP	N	Yes, Local Streaming - Client Location Server Status to Local Streaming client
		Microsoft .Net Framework Version 3.5 (Streaming Server)	Windows Server 2008 R2 (64 bit)	Local facility Level Firewall	N/A	[redacted]	TCP	N	Yes, PC - Paging Server - Streaming Server to Paging Server for command communication

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
					N/A	[redacted]	TCP	Y	Yes, PC - Streaming Server - Local Streaming client to Streaming server for command communication
					N/A	[redacted]	TCP	Y	Yes, PC - Streaming Server - Paging and Location server to Streaming server communication
					N/A	[redacted]	UDP	N	Yes, PC - Local Streaming - Client Local Streaming

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
					N/A	[redacted]	UDP	N	Yes, Intelligent InSites - Streaming 1
					N/A		UDP	N	Yes, Intelligent InSites - Streaming 2
					N/A		UDP	N	Yes, Intelligent InSites - Streaming 3
					N/A		UDP	N	Yes, Intelligent InSites - Streaming 4
					N/A		UDP	N	Yes, Intelligent InSites - Streaming 5
					N/A		UDP	N	Yes, PC - Local Streaming - Client Fast push button streaming

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
					N/A	[redacted]	UDP	N	Yes, PC - Local Streaming Client - Location Server Status to Local Streaming client
		Microsoft .Net Framework Version 3.5 (Location Server)	Windows Server 2008 R2 (64 bit)	Local facility Level Firewall	N/A		TCP	Y	No
					N/A		UDP	N	Yes, PC - Local Streaming Client - Location Server Status to Local Streaming client
		Microsoft	Windows	Local facility	N/A		HTTPS	Y	Yes, MSE

Application Name	**Application Description**	**Technology**	**Platform**	**Devices used to control C&A boundary traffic**	**Types of Access Controls Utilized (e.g., ACLs, VLANs)**	**Ports**	**Protocols/ Services**	**Inbound (Y/N)**	**Outbound (Yes/No, if "Y" specify where)**
		.Net Framework Version 3.5 (WiFi Connector)	Server 2008 R2 (64 bit)	Level Firewall	N/A	[redacted]	TCP	N	Yes, PC - Streaming Server - Wi-Fi Connector to Streaming server
CenTrak Global Monitoring System (GMS)	GMS monitors the health of all system components and maintain a reliable, high-performance RTLS infrastructure.	WEBDAV www.Viewtrac.com	Windows Server 2008 R2 (64 bit)	Local facility Level and CenTrak Firewall	N/A		TCP	Y	Yes, PC Server to GMS (Uploading of CenTrak GMS data from CenTrak Server to GMS server)
		Web Service www.Viewtrax.com	Windows Server 2008 R2 (64 bit)	Local facility Level and CenTrak Firewall	N/A		HTTP	Y	Yes, GMS Web service - Authentication and configuration from CenTrak Server to GMS server

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
WaveMark EiRTLS	EiRTLS collects information from WaveMark's RFID Smart Cabinets, Point of Use Stations, and various other data collection devices, and aggregates them to an enterprise visibility layer that allows for the efficient management of supplies in hospitals and other healthcare providers.	Weblogic v10.3.6	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTPS	Y	No
		Apache Web Server 2.2.3	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTP HTTPS	Y	Yes, User Community (browsers)
		JBoss 5.1.0 GA	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTPS	Y	Yes, User Community (browsers)
		Java jdk1.60_16	RHEL 6.5 (64 bit)	NDC Level Firewall	N/A	[redacted]	N/A	N/A	N/A
		Oracle 11g Database Enterprise Edition with RAC	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	TCP	Y	Yes, JDBC, ODBC, and ETL Processes
		PostgreSQL 8.1.21	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	TCP	Y	Yes, JDBC, ODBC, and ETL Processes
		MySQL Community Server 5.5.28	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	TCP	Y	Yes, JDBC, ODBC, and ETL Processes

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
		Splunk 5	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTP	Y	No
		Java jrockit-1.6.0_20-R28	RHEL 6.5 (64 bit)	NDC Level Firewall	N/A	[redacted]	N/A	N/A	N/A
		Zenoss 4	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTP TCP	N	No
WaveMark Point of Care (xPOS)	WaveMark's Point of Use Stations provides users with the ability to quickly and accurately capture product usage with the wave of the hand.	Java 1.6.0_33	openSUSE 11.0	VAMC Level Firewall	N/A	[redacted]	N/A	N/A	N/A
		MySQL V14.12 Distribution 5.0.51a	openSUSE 11.0	VAMC Level Firewall	N/A	[redacted]	TCP	N	No
WaveMark Smart Cabinet	RFID enabled SmartCabinet that provides automated inventory	Java 1.4.2_16-b06, headless (embedded)	Debian 3.1 Sarge (embedded)	VAMC Level Firewall	N/A	[redacted]	TCP	Y	N/A

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
	capture. Smart Cabinets run on a hardened, embedded single board computer (SBC).	MySQL 5.0.32-Debian_7etch1-log	Debian 3.1 Sarge (embedded)	VAMC Level Firewall	N/A	[redacted]	TCP	N	No
Censis Censitrac Buffer Server	Censitrac provides electronic instrument tracking and management. In addition, Censitrac	MS Internet Information Services (IIS) 7.5	Windows Server 2008R2 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTP, HTTPS	Y	No
		MS SQL Server 2008R2 Express	Windows Server 2008R2 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	TCP	Y	N/A

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
	provides automation and recordkeeping of for SPS terminals and Operating Room based flash sterilization. Censitrac is deployed at the local facility level.	Censis Buffer Agent	Windows Server 2008R2 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTP	N	Yes, User Community (Browsers)
Censis Host Server	The Host Server stores complete database for each VA facility. It provides backups and disaster recovery procedures.	MS IIS Web Server	Windows Server 2008R2 (64 bit)	Censis Firewall	Censis ACLs	[redacted]	HTTP	Y	No
		MS SQL Server	Windows Server 2008R2 (64 bit)	Censis Firewall	Censis ACLs	[redacted]	N/A	N/A	N/A

Application Name	**Application Description**	**Technology**	**Platform**	**Devices used to control C&A boundary traffic**	**Types of Access Controls Utilized (e.g., ACLs, VLANs)**	**Ports**	**Protocols/ Services**	**Inbound (Y/N)**	**Outbound (Yes/No, if "Y" specify where)**
OATSystems OATxpress	The OATxpress component is a RFID middleware for data capture and aggregation, device management and monitoring, EPC number and product management, and handles integrations with other business systems.	Apache Tomcat 7.0.32	Windows Server 2008R2 (64 bit)	NDC Firewall	ACLs, VLANs	[redacted]	HTTPS	Y	Yes, User Community (Browsers)
		Oracle Java 1.7.0_09	Windows Server 2008R2 (64 bit)	N/A	N/A		N/A	N/A	N/A
		MS SQL Server 2012	Windows Server 2008R2 (64 bit)	NDC Level	ACLs, VLANs		TCP	Y	N/A
OATSystems OAT Enterprise Manager	The OAT Enterprise Administrator manages all OATxpress servers within the enterprise. It provides a	Apache Tomcat 7.0.32	Windows Server 2008R2 (64 bit)	NDC Firewall	ACLs, VLANs		HTTPS	Y	Yes, User Community (Browsers)
		Oracle Java 1.7.0_09	Windows Server 2008R2 (64 bit)	N/A	N/A		N/A	N/A	N/A

Application Name	**Application Description**	**Technology**	**Platform**	**Devices used to control C&A boundary traffic**	**Types of Access Controls Utilized (e.g., ACLs, VLANs)**	**Ports**	**Protocols/ Services**	**Inbound (Y/N)**	**Outbound (Yes/No, if "Y" specify where)**
	single point to configure devices and scenarios. In addition it manages users and roles needed to access any server in the system.	MS SQL Server 2012	Windows Server 2008R2 (64 bit)	NDC Firewall	ACLs, VLANs	[redacted]	TCP	Y	N/A
ESB	An ESB is a set of rules and principles for integrating numerous applications together over a bus-like infrastructure.	MuleSoft ESB v3.3	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs		SFTP, HTTP, HTTPS	Y	Yes, Intelligent InSites Platform, WaveMark EiRTLS, WaveMark xPOS, VistA Service
		Java - Oracle/Sun jdk 1.7 Update 15	RHEL 6.5 (64 bit)	NDC Level Firewall	N/A		N/A	N/A	N/A

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
VistA Service	Vista-Service is an interface to VistA creating a uniform calling method for underlying MUMPS Remote Procedure Calls (RPCs). The RESTful web service methods provide a mechanism to encapsulate the VistA-Link calls into a standard format.	Weblogic v10.3.2	RHEL 6.5 (64 bit)	NDC Level Firewall	ACLs, VLANs	[redacted]	HTTPS	Y	Yes, Mule ESB
							HTTPS	Y	Yes, System Administrat ors
		Java - Oracle JRockit(R) (build R28.2.5-20-152429-1.6.0_37-20120927-1915-linux-x86_64)	RHEL 6.5 (64 bit)	NDC Level Firewall	N/A		N/A	N/A	N/A
		Vista-Link v1.6	RHEL 6.5 (64 bit)	NDC, local facility Level Firewall	VLANS		TCP-IP, HTTPS	Y	Yes, VistA
NDR ETL Engine	Custom Framework used to move RTLS data	MS SQL Server 2012	Windows Server 2008R2 (64 bit)	CDW Firewall	ACLs, VLANs		TCP	Y	N/A

Application Name	Application Description	Technology	Platform	Devices used to control C&A boundary traffic	Types of Access Controls Utilized (e.g., ACLs, VLANs)	Ports	Protocols/ Services	Inbound (Y/N)	Outbound (Yes/No, if "Y" specify where)
	from transactional source systems to the NDR.	MS SSIS	Windows Server 2008R2 (64 bit)	CDW Firewall	ACLs, VLANs	[redacted]	OLEDB ODBC	Y	Yes, Intelligent InSites Platform, WaveMark EiRTLS, OATxpress, Censis Censitrac, CenTrak GMS
		MS MDS including IIs	Windows Server 2008R2 (64 bit)	CDW Firewall	ACLs, VLANs	[redacted]	TCP HTTP	N	Yes, User Community (Browsers and Microsoft Excel)

4.2 Software Architecture

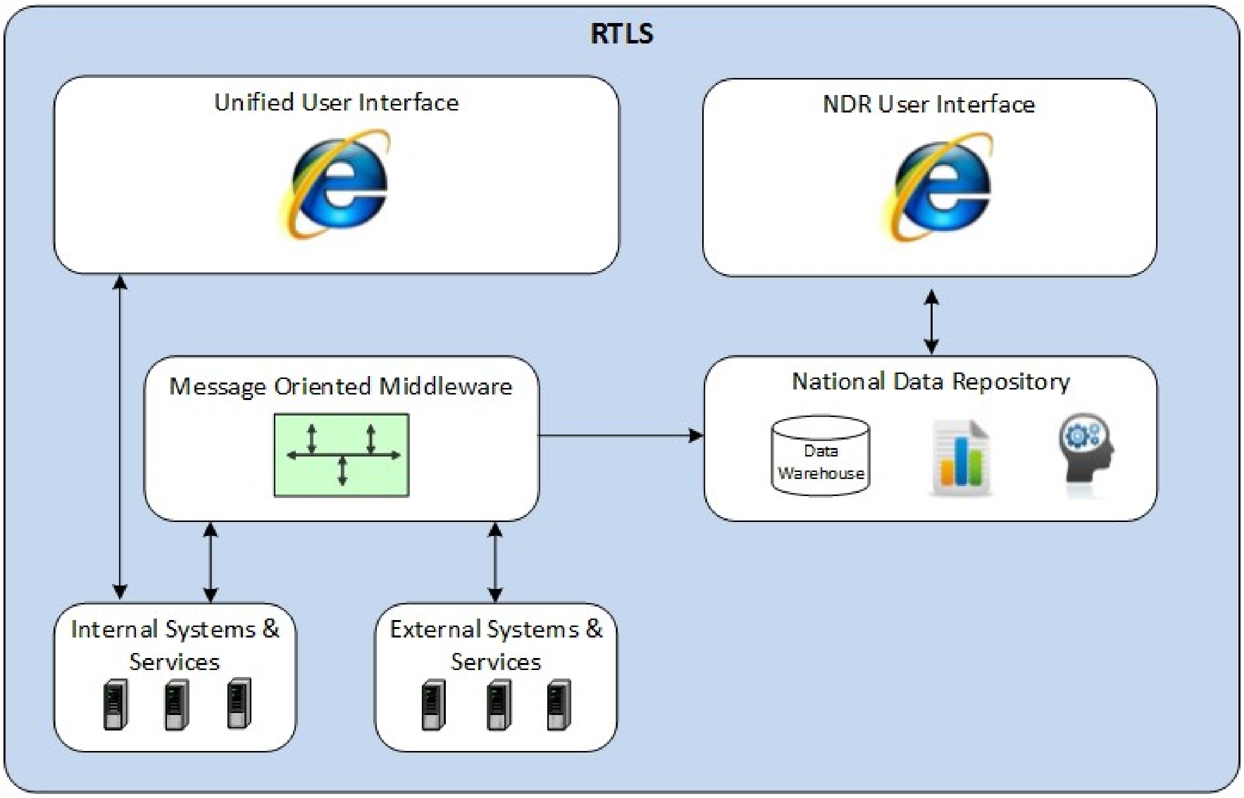
The software architecture takes advantage of several architecture and design patterns to ensure scalability, flexibility, and supportability. The RTLS system is a system of systems. As a system of systems, capabilities are implemented within the various systems that comprise RTLS. Therefore, the RTLS architecture describes the standards and services necessary to facilitate interaction among the capabilities in the systems under RTLS. The RTLS Architecture is being designed as a Service Oriented Architecture including the service inventories described in this and accompanying documents. For more detailed information, please see the Detailed Design Section.

The RTLS system is comprised of four main software modules:

- **User Interface:** A unified User Interface provides access to all of the RTLS underpinnings. The User Interface is a role based web based GUI that provides functionality into the RTLS system. An authenticated and authorized user will be able to view asset location, reports from local facilities, VISNs, and National levels.
- **Message Oriented Middleware:** The Message Oriented Middle layer serves an orchestration mechanism for the various middleware services within the RTLS system. The Message Oriented Middle layer contains a message bus which aids in communication between the various service components and systems. The Message Oriented Middle layer may interact with systems and services internal and external to the VA.
- **Internal Systems and Services:** These are the COTS software products that are used to handle Use Cases, Business Processes, and other functions to meet the designated requirements. These products communicate with data collectors such as active tag readers, each other, and external systems through the message oriented middleware.
- **National Data Repository (NDR)**: The National Data Repository is a data warehouse that is loaded from the various RTLS systems. The NDR provides reporting, analytics and business intelligence features.

Below is a high level view of the software architecture:

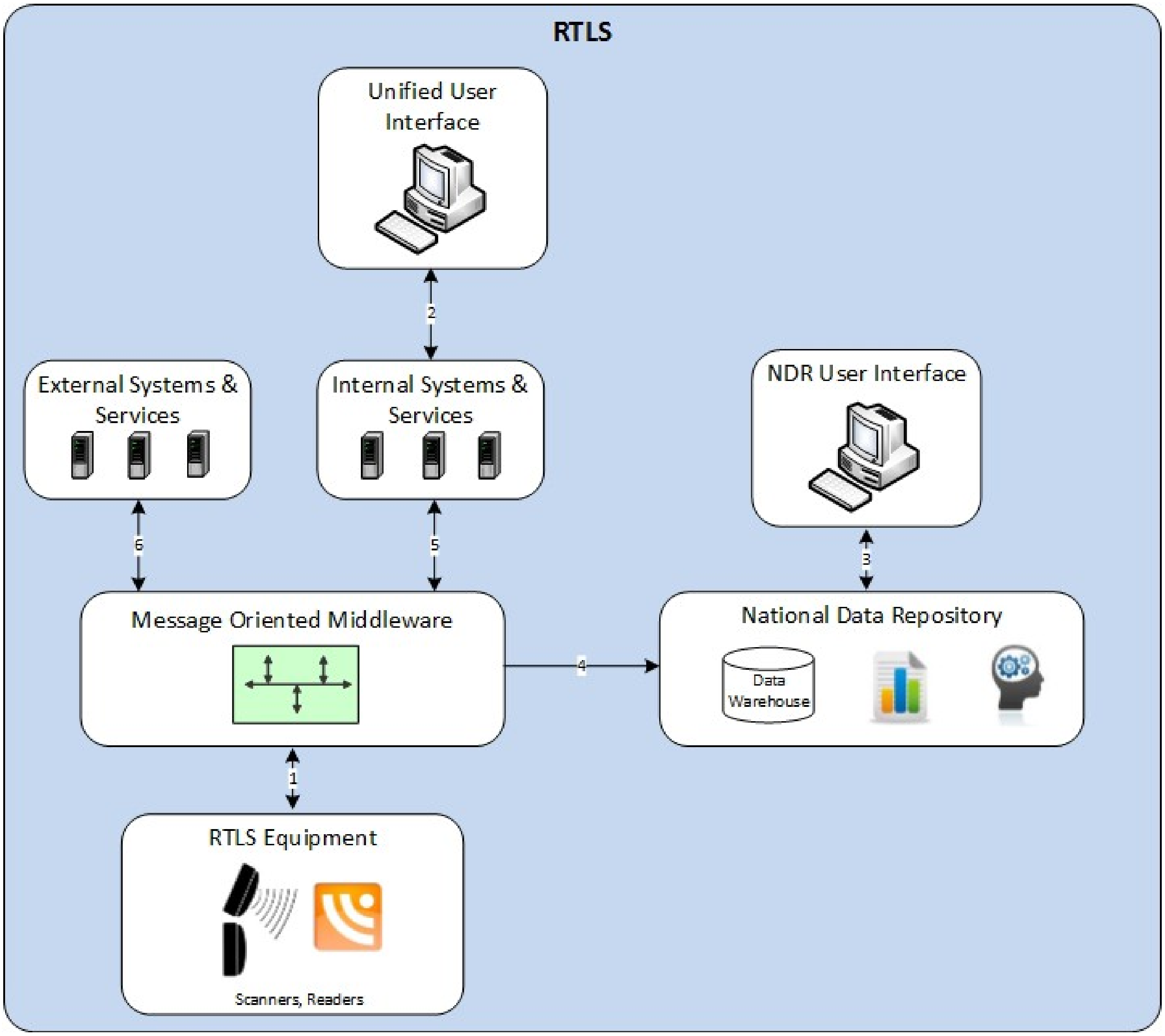
Figure 32: Enterprise High Level Software Architecture



4.3 Communications Architecture

The communications architecture will show what protocols the various components within RTLS system will communicate on.

Figure 33: Communications Architecture



The following table shows what protocols are used for communication between the various components in the above figure

Table 25: Communication Protocols

ID	Protocol	Component(s)/Module	Description
1	UDP-IP/SOAP/LLRP/NMSP	RTLS Equipment/Message Oriented Middleware	The communication to and from the RTLS Equipment (Readers, Scanners, etc.) to the Internal Systems &

ID	Protocol	Component(s)/Module	Description
			Services via the Message Oriented Middleware
2	HTTP(s)	Unified User Interface/ Internal Systems & Services	The communication to and from the Unified User Interface to the Internal System and Services
3	HTTP(s)	NDR User Interface/National Data Repository	The communication to and from the Unified User Interface to the National Data Repository
4	OLEDB/ODBC	Message Oriented Middleware/National Data Repository	The communication to and from the Message Oriented Middleware to the National Data Repository
5	(S)FTP/HTTP(s)/TCP-IP	Message Oriented Middleware/Internal Systems & Services	The communication to and from the Internal Systems & Services to the Message Oriented Middleware
6	(S)FTP/HTTP(s)	Message Oriented Middleware/External Systems & Services	The communication to and from the External Systems & Services to the Message Oriented Middleware

5 Data Design

This section includes the design of Database Management System (DBMS) and non- DBMS files associated with the RTLS system.

5.1 Database Management System Files

A large piece of the RTLS system is the data that it collects and stores. For more information on Entity Relationships, Data Mapping, Data Dictionaries, Database Model, and API, please see the RTLS Enterprise Data Architecture Document.

The following provides general information about the databases used in the RTLS Solution

Overall

- Data Retention is 5 years (1826 days)
- Archiving is expected to run periodically on a schedule defined by the VA requirements
- Recommend planning for an extra 100GB per year per VISN to manage any risk, incase additional use cases are needed or program requirements change.

Intelligent InSites Databases

- Estimated Initial Transactional Database Size: 50 GB per VISN
- Estimated Transactional Database Growth Per Year: 200 GB per VISN
- Estimated Initial Business Intelligence Database Size: 50 GB per VISN
- Estimate Business Intelligence Database Growth Per year: 450 GB per VISN

WaveMark Databases

- Estimated Initial Transactional Database Size: 1.5 GB per VISN
- Estimated Transactional Database Growth Per Year: 1 GB per VISN

CenTrak Databases

- Estimated Initial Transactional Database Size: 5 GB per VISN
- Estimated Transactional Database Growth Per Year: 750 GB per VISN *(includes archive storage)*

Censis Databases

- Estimated Initial Transactional Database Size: 1 GB per Facility
- Estimated Transactional Database Growth Per Year: 1 GB per Facility

OATSystem Databases

- Estimated Initial OATxpress Transactional Database Size: 2 GB per Facility
- Estimated OATxpress Transactional Database Growth Per Year: 10 GB per Facility
- Estimated Initial OAT Enterprise Administrator Database Size: 10 GB per VISN
- Estimated Enterprise Administrator Database Final Growth: 80 GB per VISN

The following table provides an initial sizing needed for the NDR with a data extraction from the base four use case COTS software products. The below equations are based on estimates of volume sizing on per VISN and Enterprise basis.

Table 26: Database Sizing Estimates

			Total Number of Data Store Installations by VISN						
VISN	Total Facilities	Planned Facilities	InSites (by VISN)	WaveMark (by VISN)	CenTrak (by VISN)	Censis (by facility)	OATxpress (by facility)	OAT Ent Admin (by VISN)	
1	51	11	1	1	1	51	51	1	
2	37	0	1	1	1	37	37	1	
3	37	2	1	1	1	37	37	1	
4	57	0	1	1	1	57	57	1	
5	24	5	1	1	1	24	24	1	
6	34	8	1	1	1	34	34	1	
7	46	0	1	1	1	46	46	1	
8	60	5	1	1	1	60	60	1	
9	51	0	1	1	1	51	51	1	
10	35	0	1	1	1	35	35	1	
11	40	7	1	1	1	40	40	1	
12	10	0	1	1	1	10	10	1	
15	63	0	1	1	1	63	63	1	
16	74	11	1	1	1	74	74	1	
17	25	12	1	1	1	25	25	1	
18	49	0	1	1	1	49	49	1	
19	44	6	1	1	1	44	44	1	
20	44	10	1	1	1	44	44	1	
21	30	9	1	1	1	30	30	1	
22	31	7	1	1	1	31	31	1	
23	71	8	1	1	1	71	71	1	
CMOP	0	3	1	1	1	1	1	1	
Installations (all facilities):			22	22	22	914	914	22	
Installations (planned):			14	14	16	104	97	13	
Initial Transactional DB Size (GB):			50	1.5	5	1	2	10	
Annual Transactional DB Growth (GB):			200	1	750	1	10	80	
Initial BI DB Size (GB):			50	0	0	0	0	0	
Annual BI DB Growth (GB):			450	0	0	0	0	0	
Initial Sizing Lower Limit (GB):			1,400	21	80	104	194	130	1.929 Terabytes
Initial Sizing Upper Limit (GB):			2,200	33	110	914	1,828	220	5.305 Terabytes
Annual Growth Lower Limit (GB):			15	15	17	3,150	2,940	14	6.151 Terabytes
Annual Growth Upper Limit (GB):			14,300	22	16,500	914	9,140	1,760	42.636 Terabytes

<u>Note:</u> The numbers in the above table may vary for any number of factors, these metrics attempts to roll up a bunch of complex situations into a simple form that helps deliver a basic order of magnitude sizing. What items that get tagged, how items are used, which use cases are implemented, data retention policies, new functionality/integrations added to the system over time all can have various effects on the amount of data that is required to be collected.

6 Detailed Design

This chapter will describe the design in detail of the RTLS system deployed in the VA's national data center. It will provide the necessary information for the development team to integrate the hardware components, write the software code, so that the hardware and software components will provide a functional product. The following architectures are found below.

- Integration Architecture (Figure 35) – this architecture shows the integration points between the various components of the RTLS System. The Integration Architecture shows the directionality of the interface among the various components of the RTLS System. The Integration Architecture does **<u>NOT</u>** depict the flow of data within the RTLS System. A .PDF version of the Integration Architecture, can be found here

  Integration Architecture.pdf

- Data Flow Architecture (Figure 36) – this architecture shows how data will flow between the various components of the RTLS System. The Data Flow Architecture shows the directionality of the flow of data made among the various components. The Data Flow Architecture does **<u>NOT</u>** depict the directionality of the interface between the RTLS Components. An additional data flow diagram can be found in the RTLS Enterprise Data Architecture. A pdf version of the Data Flow Architecture, can be found here

  Data Flow Architecture.pdf

Figure 34: Integration Architecture

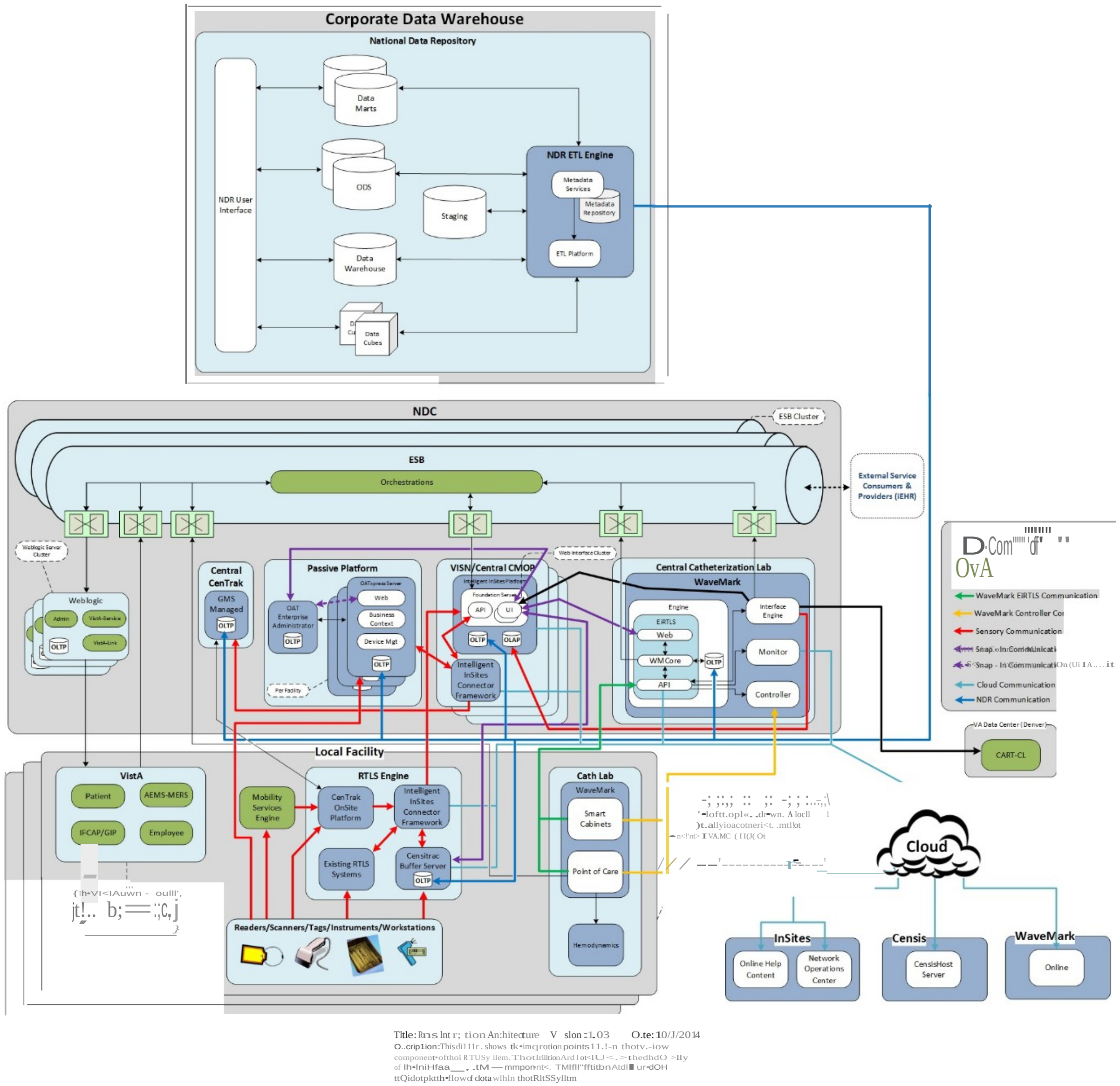
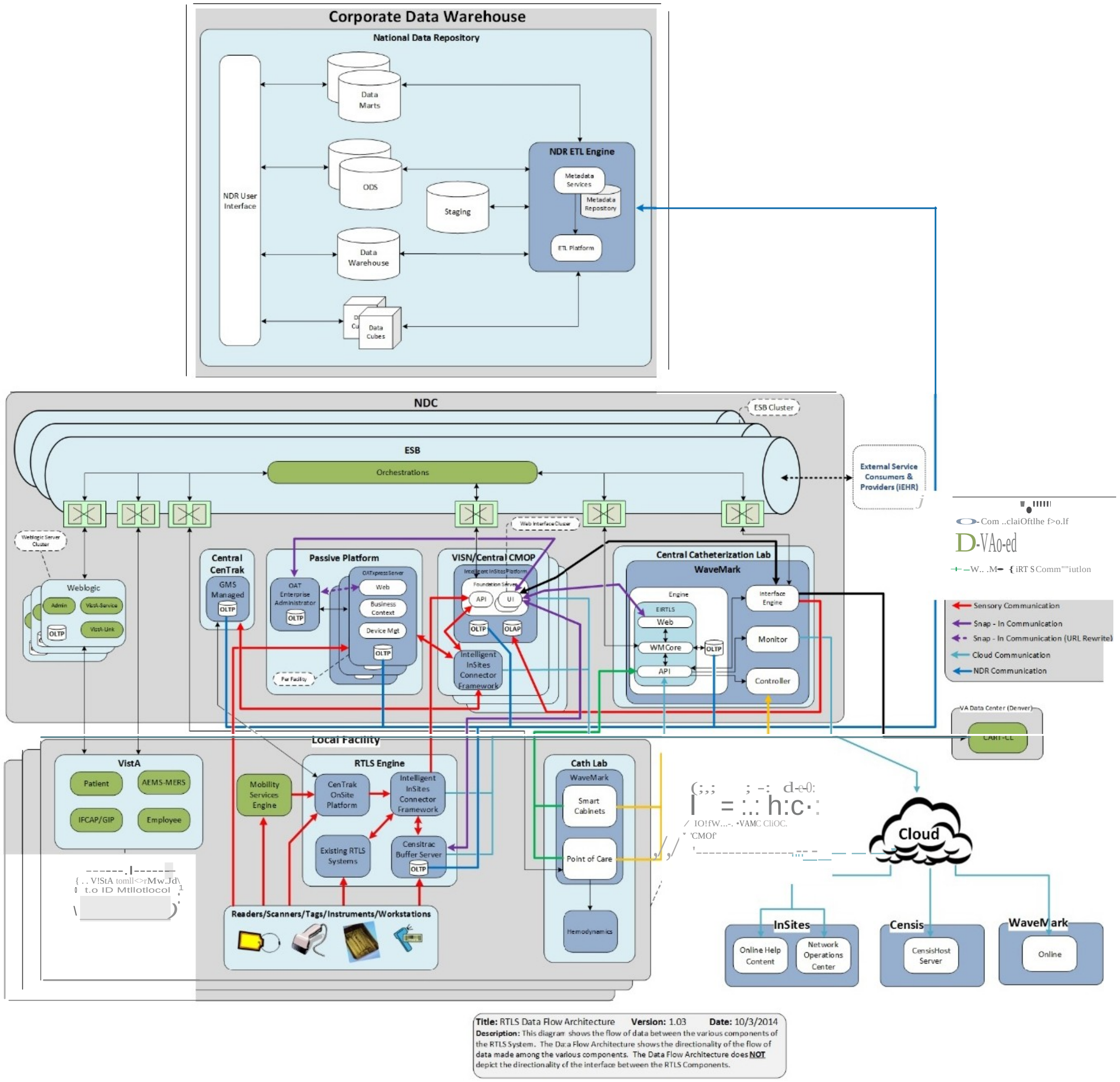


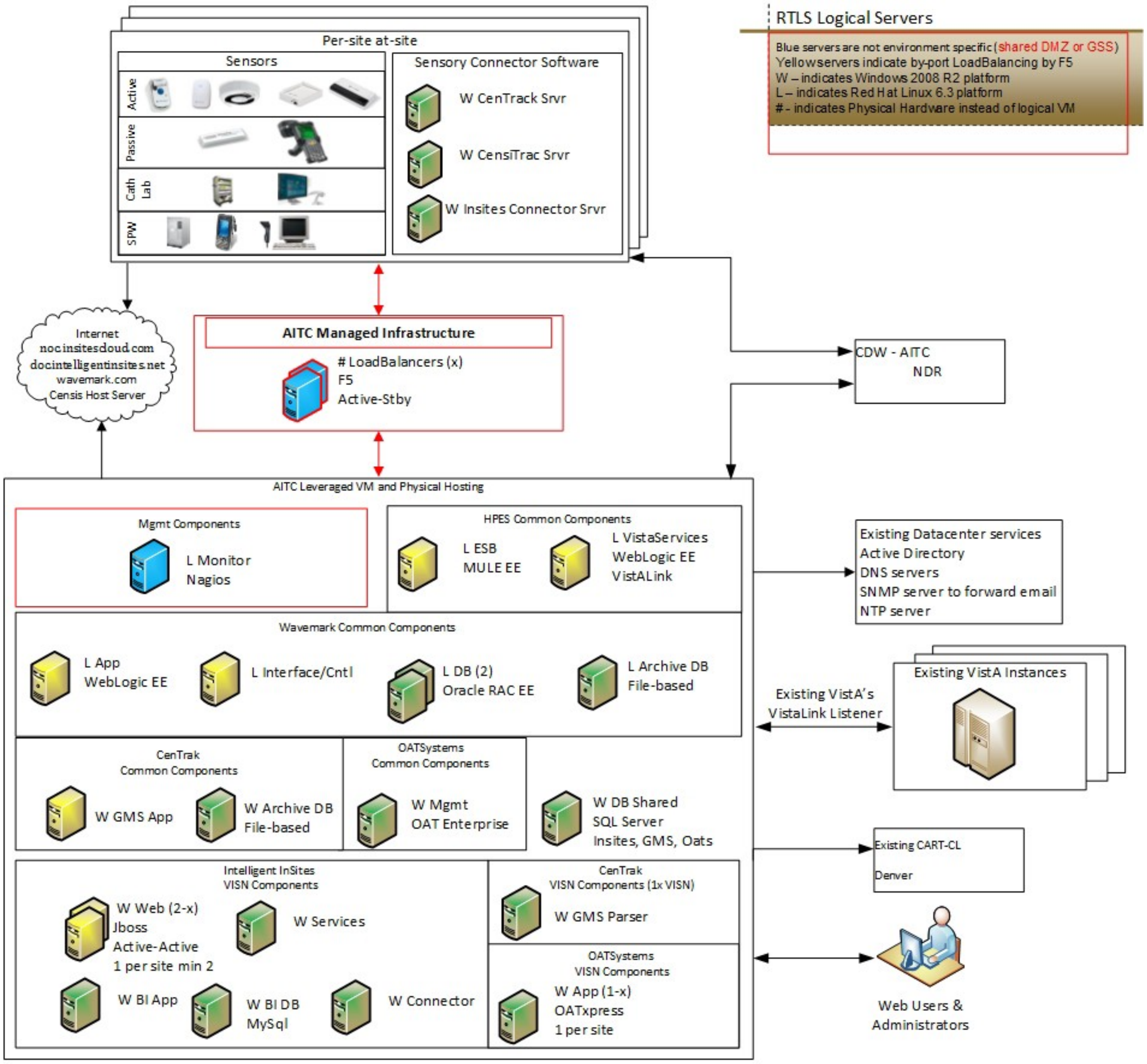
Figure 35: Data Flow Architecture



6.1 Hardware Detailed Design

In this section, there will be details on all pieces of the hardware belonging to the RTLS system. The figure below shows a typical National Deployment.

Figure 36: Logical Hardware Architecture



The RTLS components will be installed on existing VA owned hardware at the National Data Center. The table below represents the server requirements for a local facility deployment (production environment).

Table 27: Local Facility Server Requirements

Qty	Equipment Type	Rack Units	Rack Units Totals	Cooling Requirements (BTU/hr) per device	Cooling Totals (BTU/hr)	Electrical Consumption (Watts) per device	Electrical Totals (Watts)	Network Requirements (per device)	Comments
2	Small Rack Server	1	2	1235	2470	362	724	4 1GB connections	(2) C13 Power plugs per server
1	P2000 to support HA	4	4	2693	2693	789	789		(2) C13 Power plugs
	Totals		6		5163		1513		

Table 28: Detail Hardware Description

Component	Vendor/Model	Description	Specifications
Passive Tag	Emerson & Cuming Metal Tag Flex	Rugged and Flexible Metal-Mount UHF RFID Tag	*Data Sheet*
Passive Tag	Emerson & Cuming Metal Tag Echo	Rugged and Flexible Metal-Mount UHF RFID Tag	*Data Sheet*
Passive Tag	Emerson & Cuming Metal Tag Impact	Rugged and Flexible Metal-Mount UHF RFID Tag	*Data Sheet*
Passive Tag	Vizinex Sentry AST Slim	The Sentry AST Slim is a small footprint mount on metal tag that provides the read range and low profile desired for use on IT assets such as networking equipment and servers in data centers.	*Data Sheet*
Passive Tag	Vizinex Sentry-AST-Multi-Surface	Passive UHF Tag for Material Diverse Environments	*Data Sheet*
Passive Tag	Alien-Technology-Higgs-3-ALC-360	Higgs-3 is a highly integrated, 800-bit memory, single chip UHF RFID Tag IC. The chip conforms to the EPC global Class 1 Gen 2 specifications and provides state-of-the-art performance for a broad range of applications.	*Data Sheet*
Passive Tag Handheld Reader	Motorola MC3190Z	Handheld scanner used in conjunction with passive tags. Scanner will transmit tag location data to the network	*Data Sheet*
Passive Tag Fixed Reader	Impinj Speedway xPortal	The Speedway xPortal reader, an integrated UHF RFID portal reader, incorporates the industry-leading Speedway Revolution RFID reader and Impinj's Dual-Linear Phased Array (DLPA) antenna technology, yielding the industries smallest, most flexible and cost-effective RFID portal solution.	*Data Sheet*
Passive Tag Fixed	Motorola FX7400	Fixed RFID reader that is ideally suited for global enterprise RFID	*Data Sheet*

Component	Vendor/Model	Description	Specifications
Reader		deployment in space-constrained, customer-facing environments.	
Active Tag	CenTrak Multi-Mode Asset Tag (ITD-761E-G)	Active Tag that is attached to items that need to be tracked, located, and identified. Supports Wi-Fi, 900 MHz, LF, Gen2IR and Motion Sensors	
Active Tag	CenTrak Multi-Mode Patient Tag IT-723E-G	Active Tag that is attached to patients that need to be tracked, located, and identified. Supports Wi-Fi, 900 MHz, LF, Gen2IR and Motion Sensors	
Active Tag	CenTrak Multi-Mode Staff Badge (ITD-763E-G)	Active Tag that is attached to staff members that need to be tracked, located, and identified. Supports Wi-Fi, 900 MHz, LF, Gen2IR and Motion Sensors	
Active Tag	CenTrak Non-Wi-Fi Asset Tag (IT-713-G)	Active Tag that is attached to items that need to be tracked, located, and identified. Supports 900 MHz, LF, Gen2IR and Motion Sensors	
Active Tag	CenTrak Non-Wi-Fi Patient Tag (IT-723-G)	Active Tag that is attached to patients that need to be tracked, located, and identified. Supports 900 MHz, LF, Gen2IR and Motion Sensors	
Active Tag	CenTrak Non-Wi-Fi Staff Badge (IT-744E-G)	Active Tag that is attached to staff members that need to be tracked, located, and identified. Supports 900 MHz, LF, Gen2IR and Motion Sensors	
Active Tag	CenTrak Multi-Mode Autoclave Tags (ITD-718E-G)	Dual Mode tag that is water-tight and hermetically sealed. RTLS tag solution for trays and other items. The SPS process and workflow can be improved by enabling surgical tray and cart tracking with a CenTrak tag designed to track trays through the full SPS process.	
Active Tag	CenTrak Multi-Mode Autoclave Tag & Shell (ITDK-718E-G)		
Active Tag	CenTrak Asset Tag XL		

Component	Vendor/Model	Description	Specifications
	(IT-716-G)		
Active Tag	CenTrak Patient Tag XL (IT-724-G)		
Active Tag	CenTrak Temperature Tag with External Probe (IT-735)	CenTrak's Temperature Sensor Tags wirelessly track and report temperature levels of refrigerators and freezers in a healthcare setting, automating regulatory compliance documentation.	
Active Tag	CenTrak Temperature Tag with External Probe Kit (IT-735-G)		
Active Tag	CenTrak Temperature Tag with External Probe and GEN2IR and LF (IT-73E5-G)	CenTrak's Temperature Sensor Tags wirelessly track and report temperature levels of refrigerators and freezers in a healthcare setting, automating regulatory compliance documentation. This tag works with Gen2IR and LF.	
Active Tag	CenTrak Multi-Mode Temperature and Humidity Tag (ITD-739-G)	The ITD-739-x is a temperature and humidity sensing tag that has the ability to sense environmental changes reliably and accurately with customizable reporting rates down to a few seconds.	*Data Sheet*
Active Tag	CenTrak Multi-Mode Temperature Tag (ITD-738-G)		
Active Tag	CenTrak Temperature Tag Probe 20C to 50C		
Active Tag	CenTrak Temperature Tag Probe 100C to 20C		
Active Tag Reader	CenTrak LF Exciter	Installed in areas where chair-level location is desired or where 100%	*Data Sheet*

Component	Vendor/Model	Description	Specifications
		accurate egress detection is required. Battery operated for 5 years.	
Active Tag Reader	CenTrak 900MHZ Wi-Fi or Power –Over-Ethernet (POE) Star	Aggregates location data and used as a secondary source of location (estimated – RF). Relatively few required (POE and WIFI options)	*Data Sheet*
Active Tag Reader	CenTrak Gen2IR Monitor	Installed in areas where room level location is desired. Also used in hallways. Battery operated for 10 years	*Data Sheet*
Active Tag Reader	CenTrak Gen2IR Virtual Wall	Installed where bed-level location is desired (ED, PACU, semi-private rooms, etc.). Battery operated for 10 years.	*Data Sheet*
Decontamination – Medical Grade Workstation	Censis	Medical Grade PC, Instrument Scanner, Waterproof Keyboard, Wireless Bar Code Scanner	*Data Sheet*
Assembly (Prep & Pack) Workstation	Censis	PC, Touch Screen Monitor, Instrument Scanner, Zebra Printer	*Data Sheet*
Sterilization Workstation	Censis	PC, Touch Screen Monitor, Instrument Scanner, Wireless Bar Code Scanner, Document Scanner	*Data Sheet*
Sterile Storage Workstation	Censis	PC, Touch Screen Monitor, Wireless Bar Code Scanner	*Data Sheet*
Case Cart Assembly Workstation	Censis	PC, Touch Screen Monitor, Wireless Bar Code Scanner	*Data Sheet*
Loaner Tray Workstation	Censis	PC, Touch Screen Monitor, Wireless Bar Code Scanner, Zebra Printer	*Data Sheet*
OR Workstation	Censis	PC, Touch Screen Monitor, Hand Held Mobile PC	*Data Sheet*
Scope Reprocessing Workstation – Medical	Censis	Medical Grade PC, Instrument Scanner, Waterproof Keyboard, Zebra	*Data Sheet*

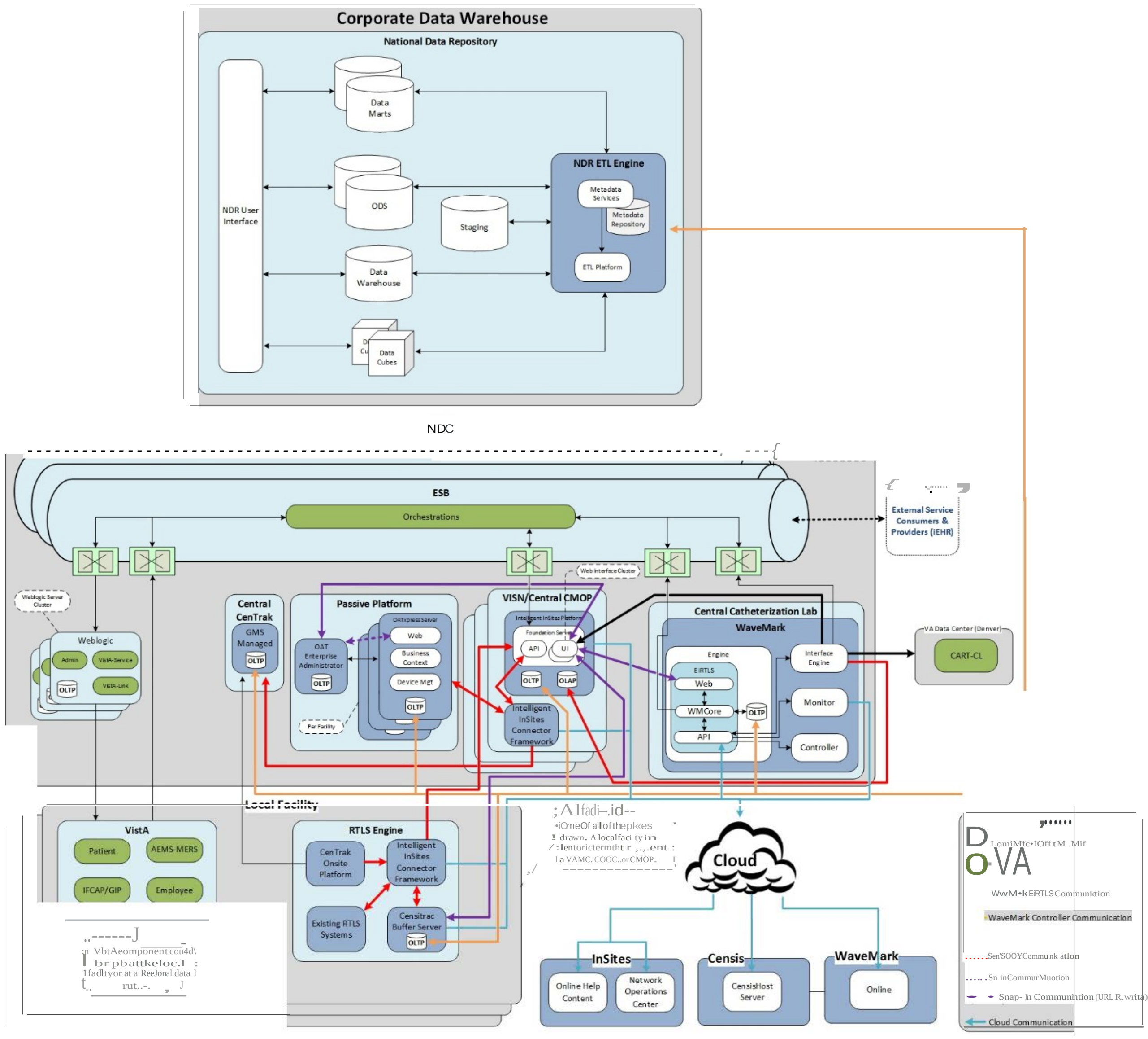
Component	Vendor/Model	Description	Specifications
Grade		Printer	
2D Electrochemical Marking Workstation	Censis	PC, Touch Screen Monitor, Instrument Marking Unit, Instrument Scanner	*Data Sheet*
Cardiac Catheterization Lab Passive Tags	Meyers Disposable Tag	Smart Inlay Label	*Data Sheet*
Cardiac Catheterization Lab Passive Tags	Avery Disposable Spine Tag	Spine RFID inlay tag	*Data Sheet*
Cardiac Catheterization Lab Passive Tags	WaveMark Hanging Tag	Streamlined hanging tag assembly	*Data Sheet*
Cardiac Catheterization Lab Smart Cabinet	WaveMark Smart Products Bin (HFS1500)	Smart product bin that holds up to 80 units of boxed guiding catheters. Configurable to all shapes of standing boxes	*Data Sheet*
Cardiac Catheterization Lab Smart Cabinet	WaveMark Smart Five Shelf (HF1500)	Smart Cabinet with 5 shelves that holds up to 225 units of standard square boxed product such as catheters, stents and balloons. This cabinet has a plastic dust cover door	*Data Sheet*
Cardiac Catheterization Lab Smart Cabinet	WaveMark Smart Door Cabinet (HFD1500)	Smart Cabinet with 5 shelves that holds up to 225 units of standard square boxed product such as catheters, stents and balloons. These cabinets have operating doors that open and close.	*Data Sheet*
Cardiac Catheterization Lab Smart Cabinet	WaveMark Smart Hanging (HFH1500)	Smart Cabinet that holds up to 160 units of guiding and angio catheters; slightly less for bulkier items	*Data Sheet*
Cardiac Catheterization Lab Smart Cabinet	WaveMark Smart Mobile (HFM1500)	Smart Mobile Cart/Cabinet with 4 shelves that holds up to 160 units of standard square boxed product such as catheters, stents and balloons.	*Data Sheet*
Cardiac Catheterization Lab Point of Care	WaveMark Point of Service (XPOS)	WaveMark's Point of Use Stations provides users with the ability to quickly and accurately capture product usage with the wave of the hand.	*Data Sheet*

Component	**Vendor/Model**	**Description**	**Specifications**
Blade Enclosure	HP BladeSystem c7000	The Blade Enclosure provides all the power, cooling, and I/O infrastructure needed to support modular server, interconnect, and storage components.	*Data Sheet*
Large Blade Server	HP BL460 Gen8	Server used at the Region Level, set up with VMware as high availability and clustered. (1/2" height, single wide Blade server with 2x E5-2667 2.9Ghz Six-core processors, 256GB memory, 2x 300GB disk drives, Ethernet & FC adapters, 3yr 24x7 4-hr Warranty coverage)	*Data Sheet*
Medium Blade Server	HP BL460 Gen8	Server used at the Region Level, set up with VMware as high availability and clustered. (1/2" height, single wide Blade server with 2x E5-2640 2.5Ghz Six-core processors, 128GB memory,2x 300GB disk drives, Ethernet & FC adapters, 3yr 24x7 4-hr Warranty coverage)	*Data Sheet*
Small Blade Server	HP BL460 Gen8	Server used at the Region Level, set up with VMware as high availability and clustered. (1/2" height, single wide Blade server with 2x E5-2643 3.3Ghz Quad-core processors, 32GB memory, 2x 300GB disk drives, Ethernet & FC adapters, 3yr 24x7 4-hr Warranty coverage)	*Data Sheet*
Small Rack Server	HP DL360p Gen8	Server used at the local facility Level, set up with VMware as high availability and clustered. (2U rack server with 2x E5-2643 3.3Ghz Quad-core processors, 32GB memory, 2x 300GB disk drives, redundant power and cooling, Insight Control Licenses, 3yr 24x7 4-hr Warranty coverage)	*Data Sheet*
Load Balancers	F5 LTM1600	Load Balancers used for Web Servers	*Data Sheet*
Storage Array	HP P2000 G3 MSA	Storage Array which contains multiple disk drives.	*Data Sheet*
NDR Server Cluster	*TBA*	NDR Level Business Intelligence Server cluster.	*TBA*

6.2 Software Detailed Design

A software module is the lowest level of design granularity in the system. In this section, there will be enough detailed information for the developers to write the source code for all modules in the system (and/or integrate COTS software programs). The figure below shows the RTLS system's detail software architecture.

Figure 37: RTLS Detailed Software Architecture



6.2.1 Sensory Data Collectors

This section will include details on sensory data collectors. The section will detail the products pertaining to the RTLS sensory infrastructure (RFID tags, scanners, readers, workstations, etc.) and software. The section will include the following:

- CenTrak – the RTLS active RFID solution
- OATSystems - the RTLS passive RFID solution
- Censis – the RTLS Reprocessing solution

6.2.1.1 CenTrak

As part of the RTLS System, an active RFID tracking solution is required. Asset tracking and environmental monitoring hardware and software solutions will be used from CenTrak. VA's Enterprise RTLS system will use active (multi-mode) tags and sensors. The CenTrak solution provides both Wi-Fi and non-Wi-Fi (also known as Clinical Grade) locating services. Wi-Fi uses multilateration of network Access Points to determine an estimated location of a tag within a 10 meter radius, with 90% confidence. This is the industry standard for Wi-Fi accuracy and provides facilities with the ability to determine if an asset is within a certain area. Connection to the Wi-Fi is through the network access points and uses the Cisco MSE.

The following CenTrak sensory equipment will used as part of the RTLS System:

- Multi-Mode Asset Tags – CenTrak's Multi-Mode Active Asset Tags attach to objects that need to be tracked, located, and identified such as mobile medical equipment. Location of tags can be determined using existing Wi-Fi network infrastructure and/or CenTrak's (900 MHz) Clinical Grade Location technology.
- Environmental Monitoring Tags – Environmental Monitoring Tags are similar to the Multi-Mode asset tags, however instead of being used to determine location, they determine and transmit environmental conditions, such as humidity and temperature.
- Low Frequency Exciters - The Low Frequency (LF) Exciter is a battery or AC powered device that emits a unique LF signal sphere which may be received by CenTrak Active Asset Tags to segment zones or designate egress points. LF Exciters create a detection "sphere." When a tag enters the LF Exciter sphere, the tag's LF sensor is triggered and the tag immediately reports this event to the CenTrak server via either Wi-Fi or 900 MHz.
- Monitors - The Monitor is a battery powered IR (infrared) signaling unit which enables room level certainty for CenTrak's suite of asset, staff, and patient tags. Each Monitor transmits a unique infrared signal that may be received by CenTrak's Active Asset Tags.
- Virtual Wall Monitors – Similar to a Monitor, a Virtual Wall uses IR as a signaling unit which enables sub-room level certainty for CenTrak's suite of asset, staff and patient tags. Each Virtual Wall transmits a unique infrared signal that may be received by CenTrak's Active Asset Tags. Virtual Walls applications include location resolution of bays typically found in Emergency Departments, Operating Rooms, or semi-private rooms. Virtual Walls may be utilized to define virtual spaces which are not separated by physical walls.
- Stars - Stars are POE powered, 900 MHz transmitting and receiving devices that communicate bi-directionally with Active Tags, LF Exciters, Monitors, and Virtual Walls. Stars are compatible with Ethernet and the TCP/IP protocol and use browser-based protocol for communication to the CenTrak OnSite Platform Server.

- Timing Stars - The Timing Star synchronizes CenTrak Stars and infrastructure devices within the RTLS network to be on the same system clock. A Timing Star is required for all CenTrak RTLS implementations.

CenTrak's family of multi-mode tags transmit in two modes and receive in three modes (see figure below).

Tag Transmission Types (a device that a tag sends data to)

- Wi-Fi – CCX (Cisco Compatible eXtension) beacons that may be received by Cisco Wi-Fi Access points. Most Wi-Fi only RTLS areas are in non-clinical areas such as cafeterias and office or research buildings.
- 900 MHz – 900 MHz allows Clinical Grade locating, which includes high-level resolution, rapid beacon rate sand extreme battery life. These capabilities are desirable and necessary for clinical workflow, hand hygiene, patient elopement and other advanced RTLS use cases. Tags communicate to a Star using 900 MHz. The star transmits the tag data to RTLS backend system using TCP-IP. There is a 10ms latency requirement between the Star and the OnSite Platform Server, which requires that the OnSite Platform Server to be on-site for a given facility.

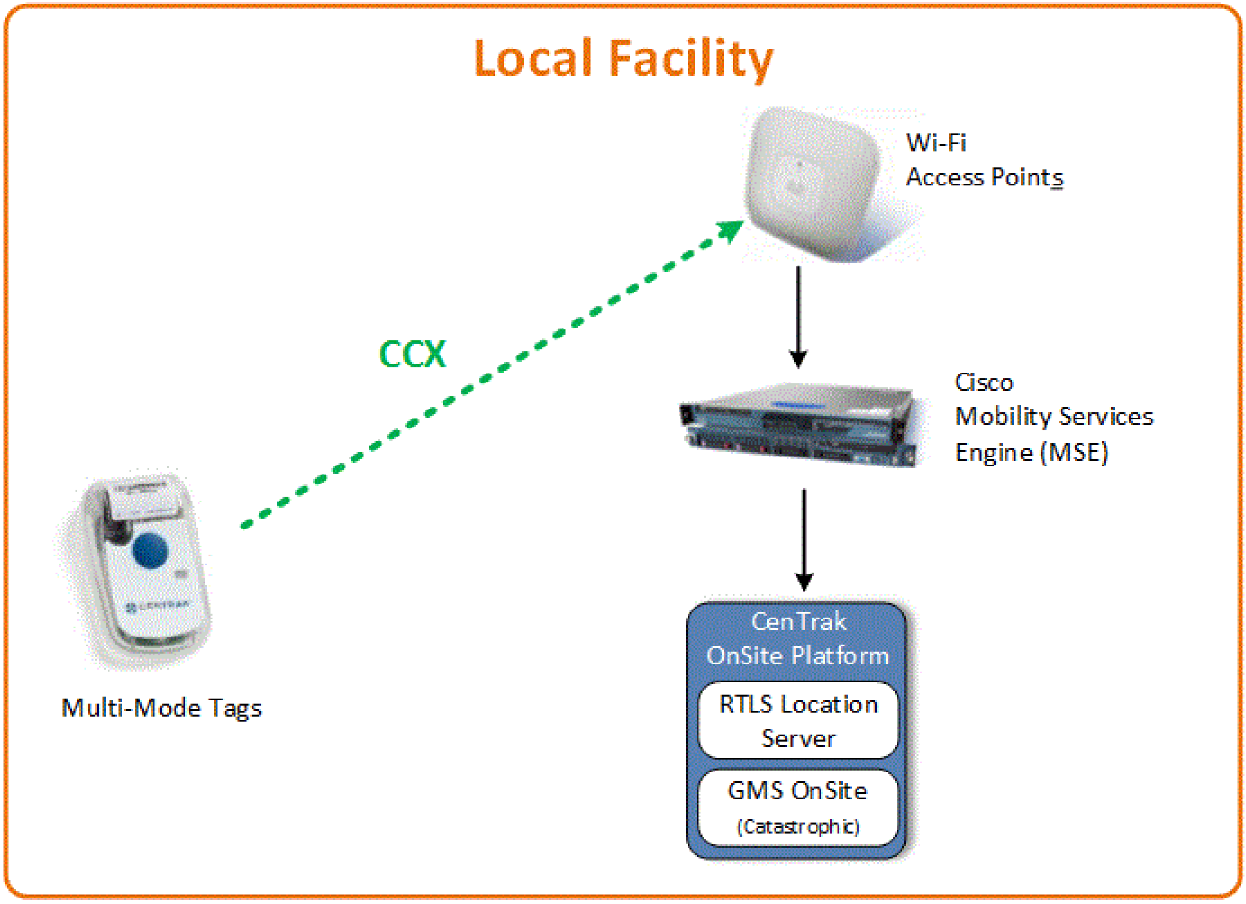
Tag Reception Types (a device that a tag receives data from)

- 900 MHz – a tag may receive data from a Star or Stars. This allows for confirmation of tag messages and for over the air programming and updating of Active Tags.
- Gen2IR (Infrared) - Gen2IR devices (Monitors and Virtual Walls) may be used to achieve room or sub-room level RTLS resolution and are frequently deployed in storage and patient rooms, hallways, and bays. Similar to light, the Gen2IR will not pass through walls. Gen2IR monitors can be profiled to flood a room or divide the room up (using Virtual Walls). The multi-mode tags can receive the infrared light from a monitor.
- Low Frequency – works similar to Gen2IR except these waves can pass through walls. Low Frequency is used in areas such as egress detection, chokepoints, and small bed/chair areas. Multi-mode tags can receive LF signals.

Figure 38: CenTrak Multi-Mode Tag – transmission and receiving capabilities

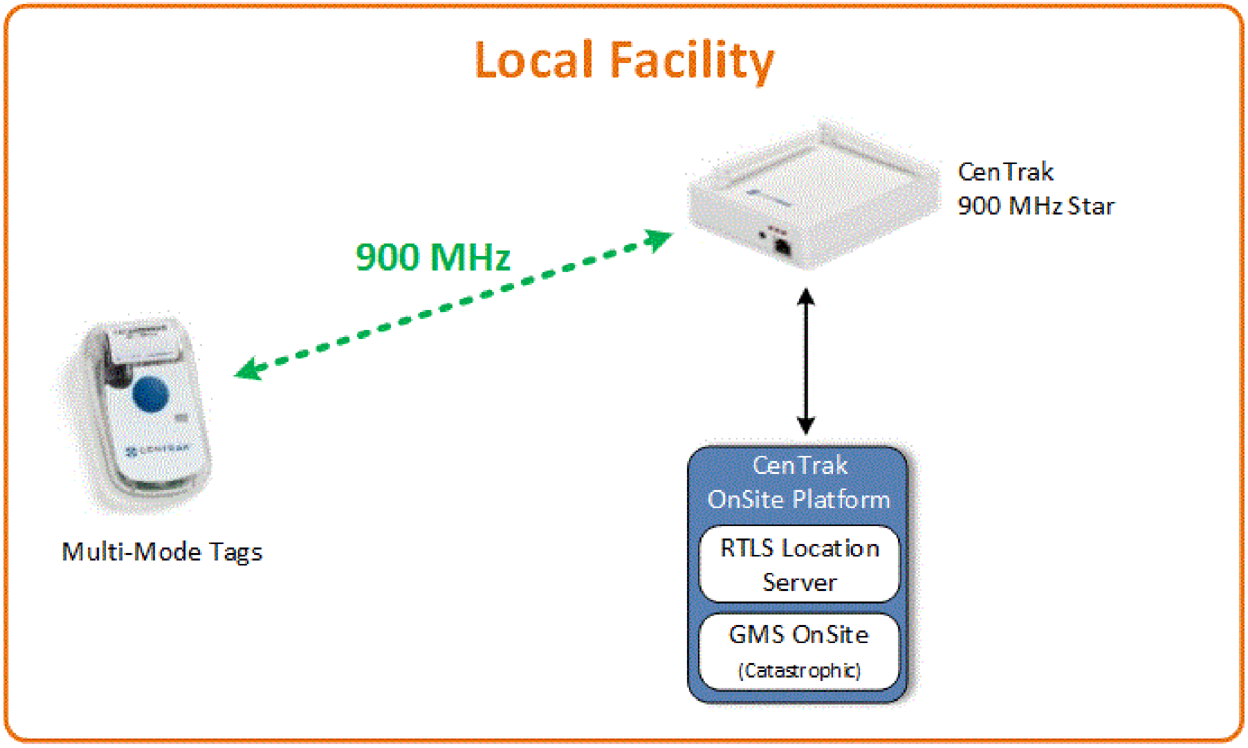
The figure below shows how the CenTrak Multi-mode tag operates in a Wi-Fi only mode. A tag will generally communicate to multiple (3 plus) Wi-Fi Access Points. The Access Points send that data to the Cisco MSE. The MSE then use multilateration to estimates tag location which is then passed to the CenTrak OnSite Platform.

Figure 39**: CenTrak Wi-Fi Only Mode**



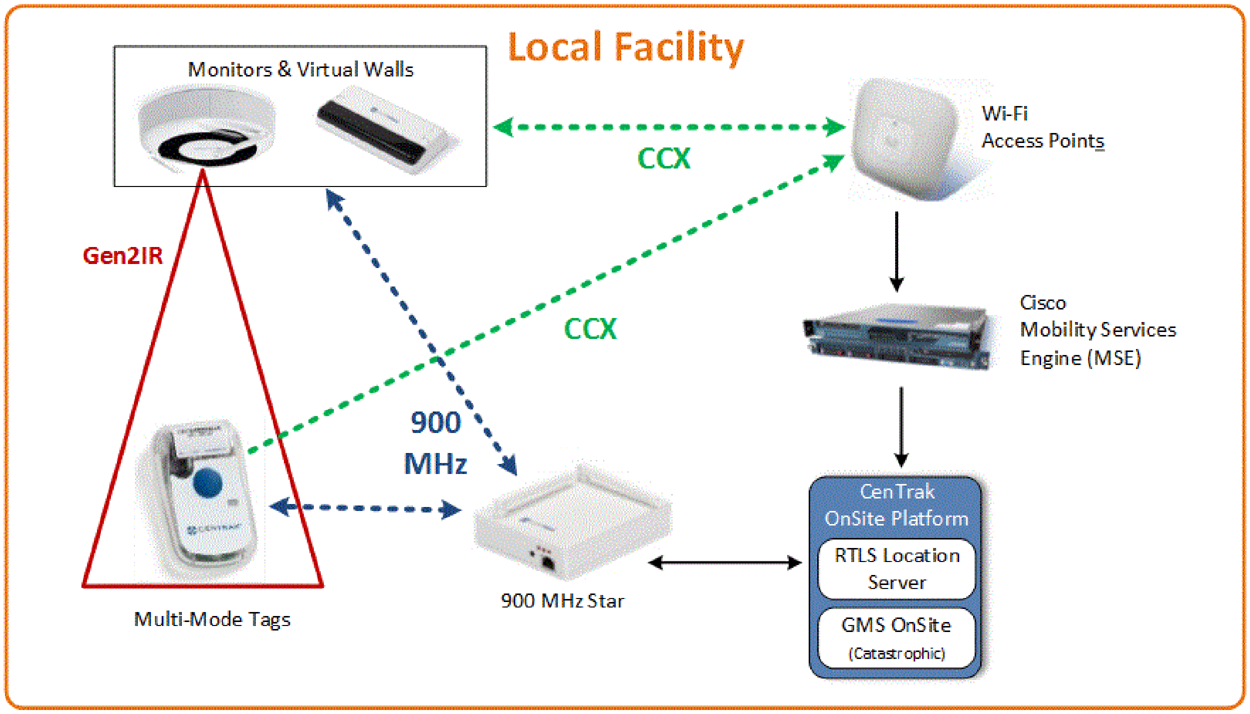
The figure below shows how communication flows using CenTrak's 900 MHz technology. The tag transmits a 900 MHz beacon which includes the tags unique identifier. The Star will report to the CenTrak OnSite Platform with the tag identifier, star identifier, and the signal strength. This information is streamed to Intelligent InSites where, based on signal strength, estimated tag location is determined, based on "closest Star" (strongest signal strength).

Figure 40: CenTrak 900 MHz Mode



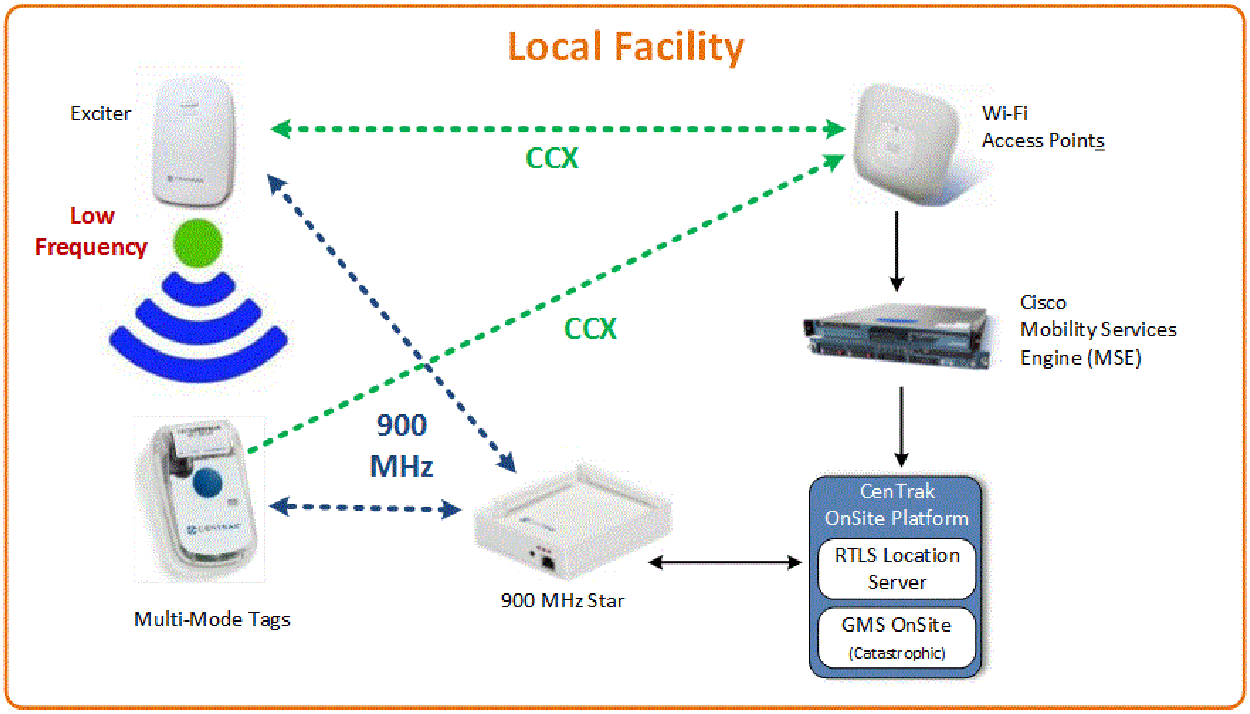
The figure below shows the steps in how a location is recorded using CenTrak's Gen2IR technology. A monitor will transmits it's identifier in IR. The multi-mode tag will pick up the IR and its unique identifier. The tag will transmit the monitor id and its tag identifier in both either 900 MHz (stars) and Wi-Fi network. In the case of a Star, an acknowledgement is sent back to the tag.

Figure 41: CenTrak Gen2IR Mode



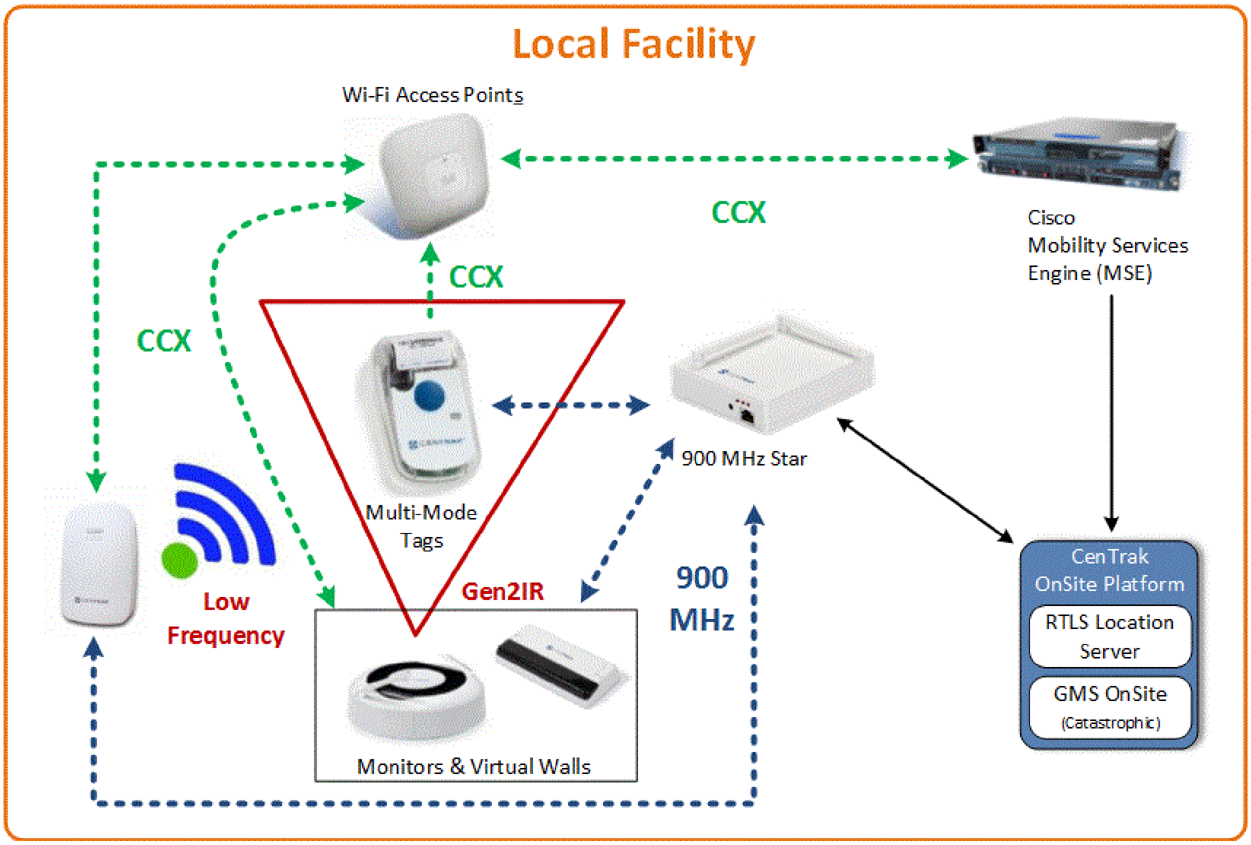
The figure below shows how a location is recorded using CenTrak's Low Frequency technology. A LF exciter will transmits it's identifier in LF. The multi-mode tag will pick up the LF and its underlying identifier. The tag will transmit the monitor id and its tag identifier in both 900 MHz (Stars) and Wi-Fi. In the case of a Star, the Star will send an acknowledgement back to the tag.

Figure 42: CenTrak Low Frequency Mode



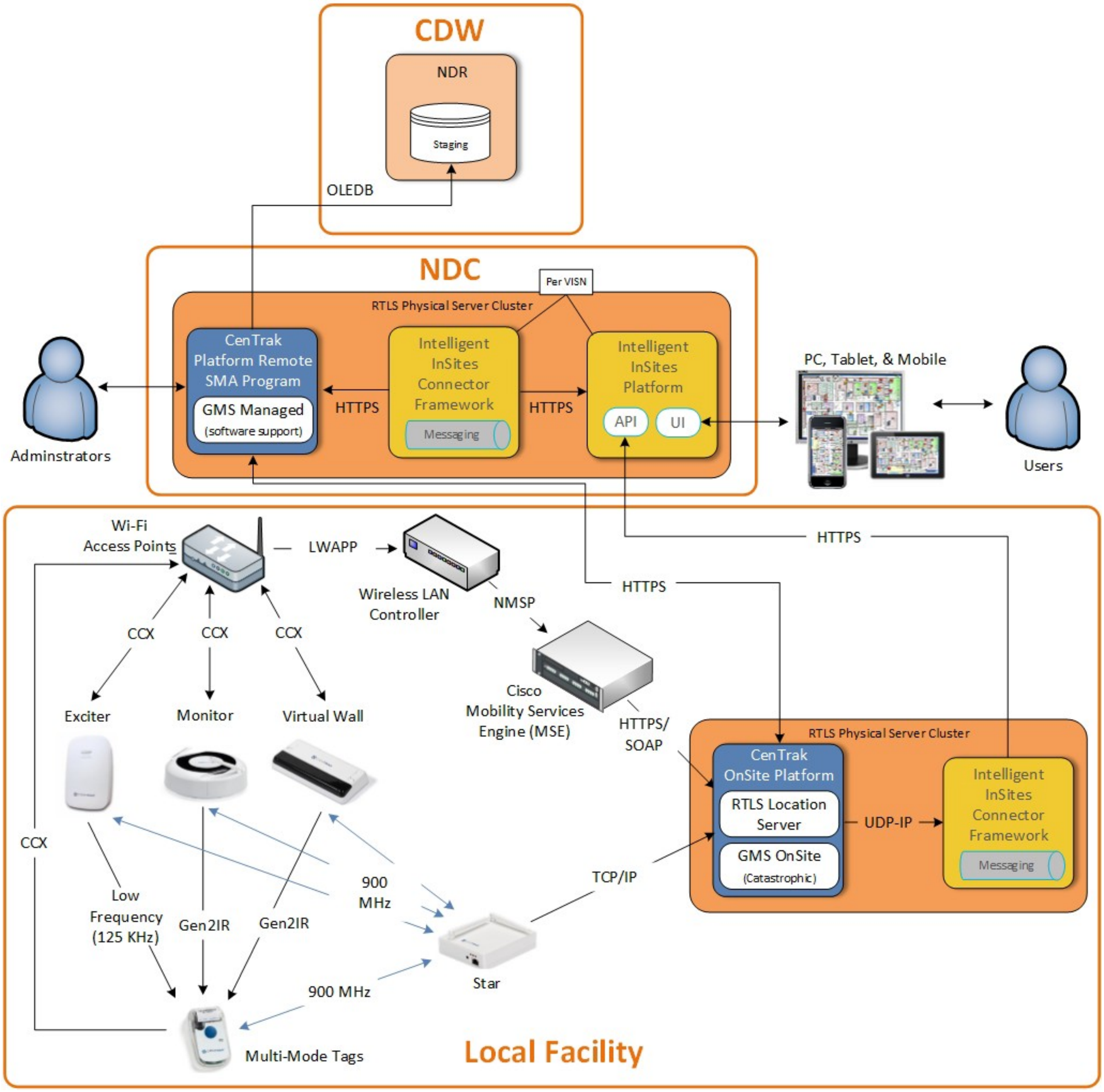
The figure below shows the how a tag would work when in full multi-mode. CenTrak's Multi-Mode technology combines Wi-Fi, 900 MHz, Low Frequency, and Gen2IR in a single platform.

Figure 43: CenTrak full Multi-Mode



The figure below shows the CenTrak Architecture and how it integrates into the Intelligent InSites Connector Frameworks. At that the local facility, the CenTrak OnSite Platform will stream data to the Intelligent InSites Connector Framework which will send the data to the Intelligent InSites Platform. The Intelligent InSites platform provides an RTLS user interface for RTLS. In addition, at the VISN level, a nightly scheduled job on the Intelligent InSites Connector Framework will contact the GMS Managed to receive data. The Intelligent InSites Connector Framework will then send that data to the Intelligent InSites platform for visibility of the data.

Figure 44: CenTrak Integration Architecture



The CenTrak solution has two software components, the OnSite Platform and Global Monitoring System (GMS).

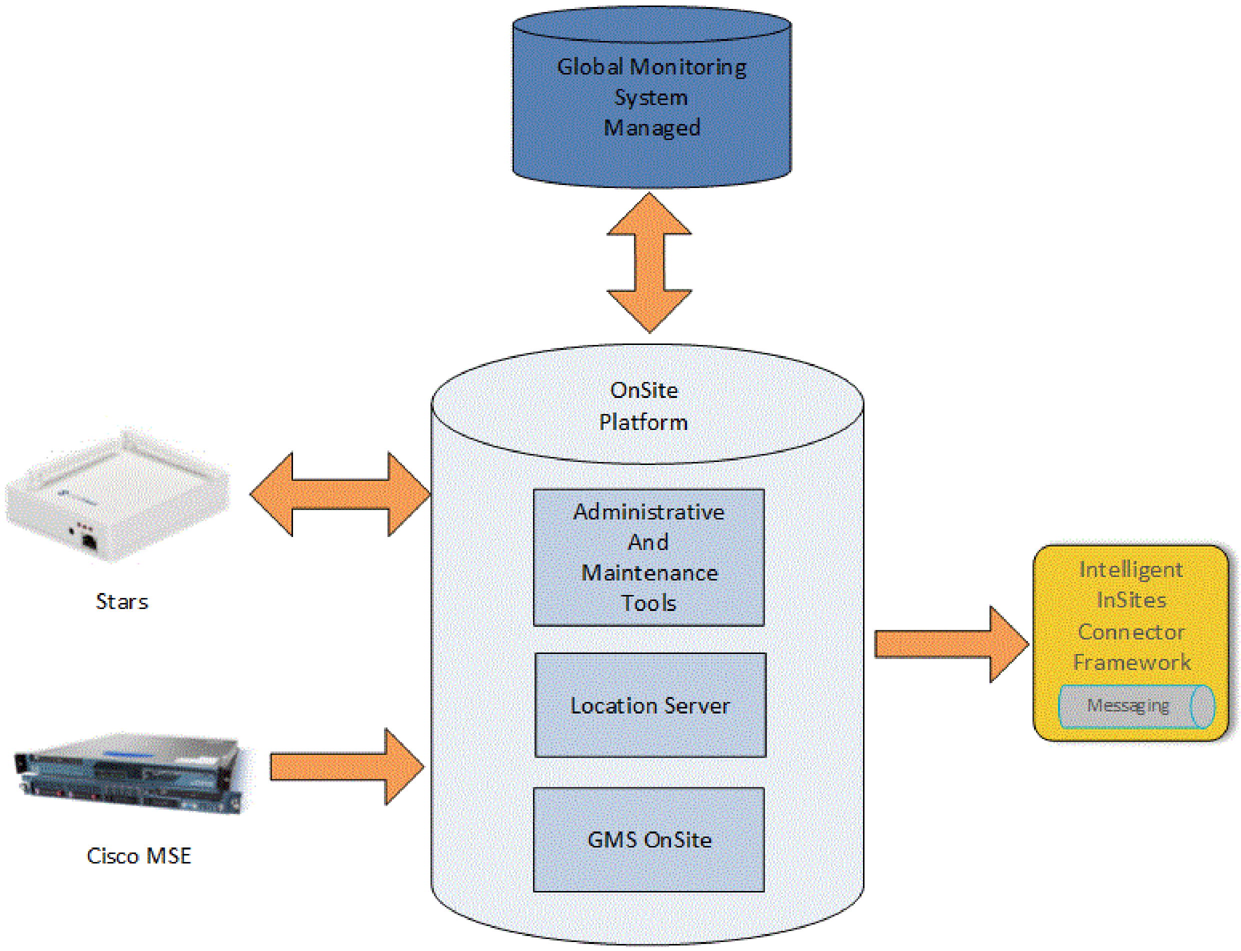
OnSite Platform

The OnSite Platform is software that will be deployed at local facilities through the VA. The OnSite Platform is used to consolidate tag data, provide catastrophic event processing, and CenTrak infrastructure maintenance/configuration and outbound data streaming. The OnSite Platform is composed of the following components:

- Administrative and Maintenance Tools – tools used to setup and maintain the CenTrak infrastructure and tags.

- Location Server – internal engine consolidates tag data and streams it out to partner applications, e.g. Intelligent InSites.
- GMS-OnSite - focuses on catastrophic events and buffers data when connection is lost to GMS-Managed (offsite).

Figure 45: CenTrak OnSite Platform Architecture



Global Monitoring System

GMS Managed monitors and checks the health of CenTrak RTLS infrastructure system components and tags, and maintains a reliable, high-performance RTLS infrastructure. GMS-Managed is part of the Software Management Agreement (SMA) program to efficiently monitor and maintain all implementations in one online location, and provides:

- Notification when battery life reaches a pre-defined threshold level
- Initiates alerts when a tag is removed from an asset (i.e. tamper signal)
- A means, where applicable, for wireless remote programming of tags and infrastructure devices
- Temperature tags, in addition to the list above, also: tag failure (stops reporting); and probe failure (temperature value ceases to be reported)
- Additional operational support features are available depending upon the type of service maintenance contract required and purchased by the VA

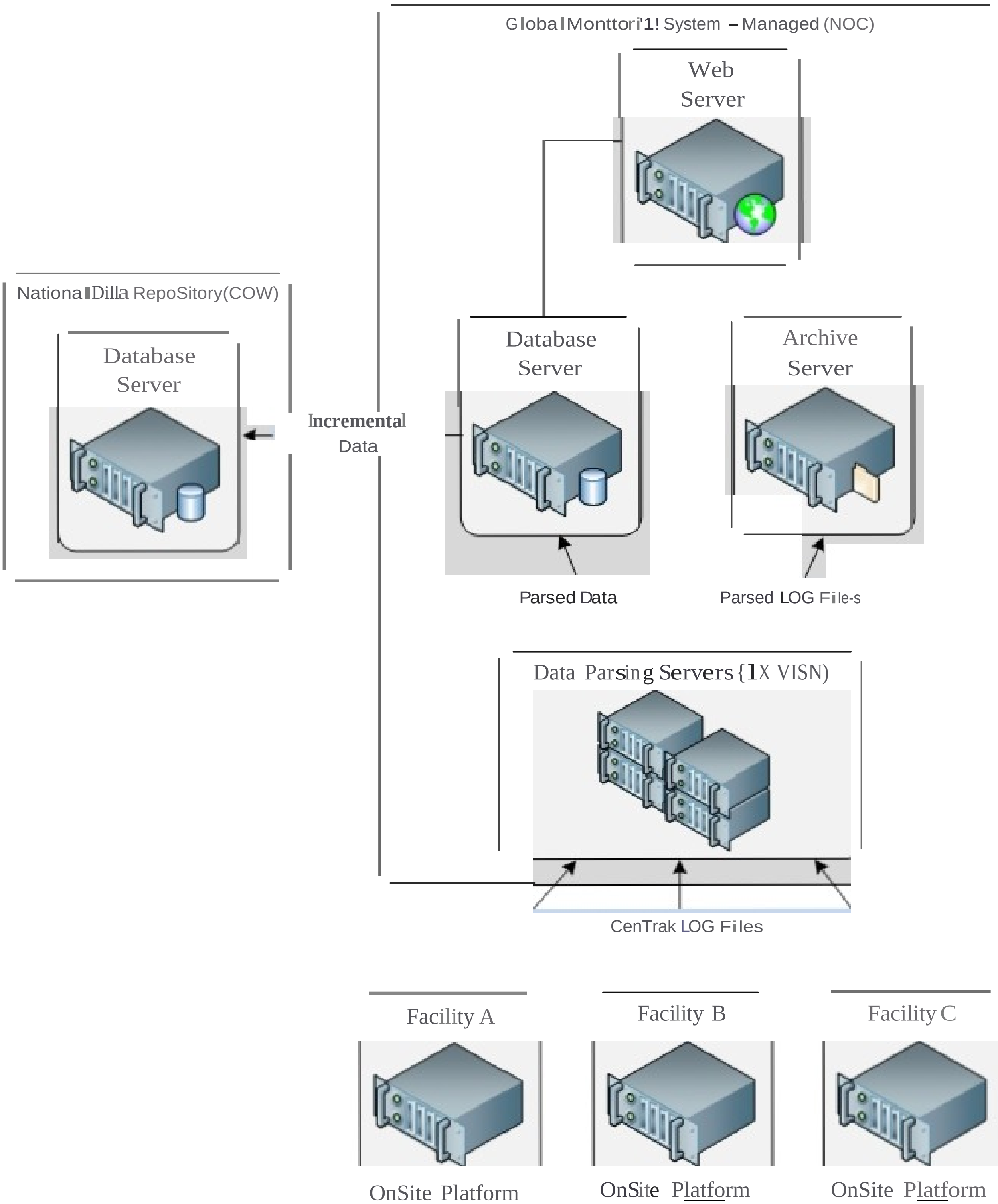
The GMS-Managed may be installed in the NDC to support the entire VISN or all the CMOPS. Access to the GMS-Managed should be limited only to authorized, trained personnel. Access in GMS-Managed can be segmented by facility and specific personnel that can view the related information to a particular site. CenTrak remotely monitors and supports the operation of GMS-Managed to ensure the RTLS networks in all facilities are operating in accordance to specification and optimized to achieve the desired performance.

The system is comprised of four distinct functional components:

1. The Web Application Server – This server provides the interface for users to retrieve data from the GMS. Data can be retrieved by direct login.
2. The Data Parsing Server – It receives hourly compressed raw data from each of CenTrak's OnSite Platform servers. Parsing Servers will be deployed on a per VISN Basis.
3. The Data Base Server – Its main functionality is to handle the storage and retrieval of "current and summary data".
4. Archive Server – Its function is the long term storage of all RTLS raw data.

CenTrak GMS architecture allows for smooth scale-up by adding Parsing Servers and database Servers as needs arise. The figure below shows the GMS Managed Architecture. Log files will be sent from the local facility OnSite Platform instances to the Central GMS. The data parsing components of the GMS will take the log files and parse them into a Microsoft SQL Server database and an archive server. A web based user interface can access the database to view metrics of the CenTrak infrastructure such as battery level of tags. Data from the GMS will be sent to the NDR for analytical purposes. The data will be extracted from Microsoft SQL Server database and loaded into the NDR Staging Area.

Figure 46: cenTrak GMS Archltecture



6.2.1.1.1 Data Flow

Data from Multi-Mode Tags will flow in following of ways:

- Using 900 MHz - The active tag data will flow from the tag to a Star using 900 MHz. From the star, the data will be sent to the CenTrak OnSite Platform over TCP-IP.
- Using Wi-Fi - The active tag data will flow from the tag to a Wi-Fi access point using CCX. From the Wi-Fi Access Point, data will flow to the Wireless LAN controller using LWAPP. From the Wireless LAN Controller data will flow to the MSE using NMSP. The data will flow from the MSE to the CenTrak OnSite Platform using SOAP over HTTPS.

Data from the CenTrak OnSite Platform Server will be processed and sent to the Intelligent InSites Connector Framework using UDP-IP. The Intelligent InSites Connector framework will queue the data and send to the Intelligent InSites Platform where it will persisted to the RTLS Data Model.

6.2.1.1.2 Interfaces

The CenTrak OnSite Platform Server will provide interfaces to the readers directly (Stars). The interface will accept SOAP and TCP-IP messages to retrieve estimated location data from the MSE or tag data from Stars. The CenTrak OnSite Platform Servers will stream data to the Intelligent InSites Connector Framework using UDP-IP. The GMS deployed at the VISN/Central CMOP level will provide an interface to the CenTrak Platform Server. This interface will transport data about performance metrics and system status from the individual CenTrak OnSite Platform Servers via HTTP. An interface from the GMS to the Intelligent InSites Connector Framework will exist using SOAP over HTTPS (for low battery indications, tamper events, etc.). The GMS will interface with the NDR Staging Database that is located in the CDW. The NDR ETL platform will extract the incremental data (data that has been inserted, updated, or deleted during a specific time period) from the GMS and load it into the NDR staging database.

6.2.1.1.3 Security

As the only data that will be transmitted is tag and monitor identifiers secure transmission is not required. There is no need for the transmission to be secure.

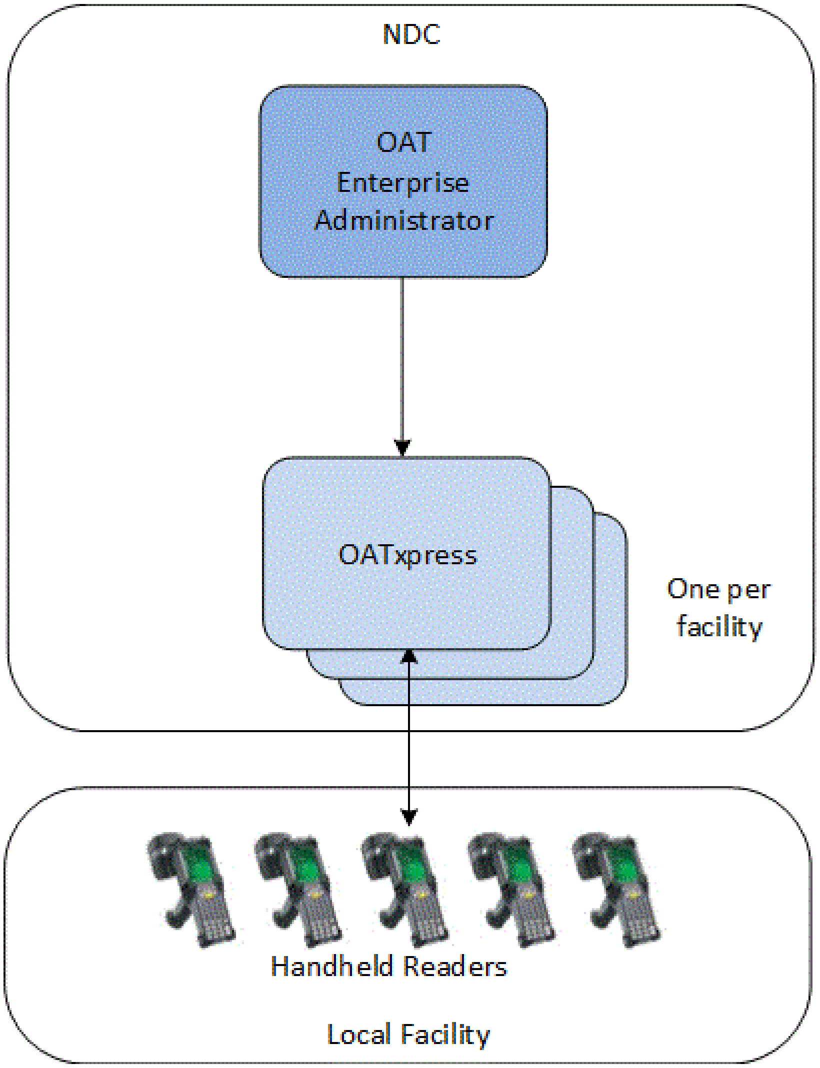
6.2.1.2 **OATSystems**

As part of the RTLS System, a passive RFID tracking solution is required. OATSystems will provide passive tags, scanners, and integration into the VA’s Enterprise RTLS System. On top of the tags and scanners, OATSystems provides two software components that are used for object tracking – OATxpress and OAT Enterprise Administrator. The OATxpress component is a RFID middleware for data capture and aggregation, device management and monitoring, EPC number and product management, and integration with business systems. Its core component is the scenario engine, an event-driven workflow engine, which executes RFID centric business processes (such as asset tracking) and allows business context data to be associated with RFID data. The OATxpress server can handle up to 200 readers per instance (one per facility [VAMC, CBOC, CMOP]).

The OAT Enterprise Administrator manages all OATxpress servers within the enterprise. It stores and distributes master data (such as locations, products and EPC number ranges) to the relevant OATxpress servers. It provides a single point to configure devices and scenarios at a server, and manages users and roles needed to access any server in the system. The OAT Enterprise Administrator also provides a dashboard for network wide monitoring of devices and process status. It allows for drill-downs into individual OATxpress Servers to identify problems. The OAT Enterprise Administrator also provides for event warnings to be raised to the enterprise level for immediate intervention. The OAT Enterprise

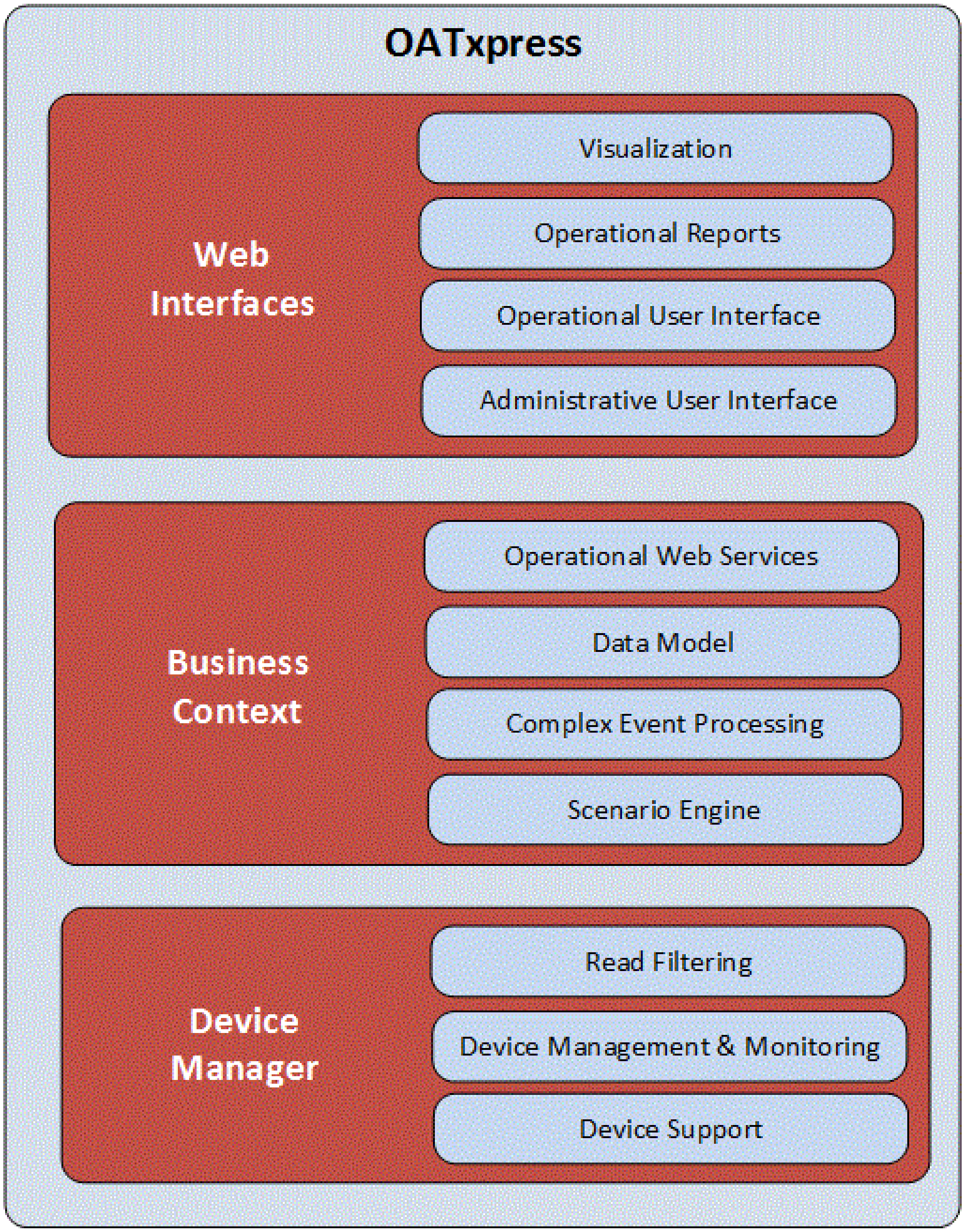
Administrator will have one central instance deployed at the National Data Center to administrator all OATxpress instances.

Figure 47: OATSystems Integration Architecture



The figure below shows the architecture of the OATxpress instances. An OATxpress instance will be installed in the NDC on a one per local facility basis.

Figure 48: OATxpress Architecture



The **OATxpress Web Interface** provides the administrative and operational interface to configure and run the OATxpress system. This Web Interface allows role based access to reports and administrative functions as well as business use cases.

The **Business Context** component links the use cases with the real time events generated by the RFID hardware. Those events may arrive from either fixed readers or mobile handheld devices and can contain information gathered by RFID readers, bar code scanners, or other sensors. The workflow engine processes those events according to the business rules and thereby translates them into an active business context. Data is persisted in the data model and exposed via a Web Service layer.

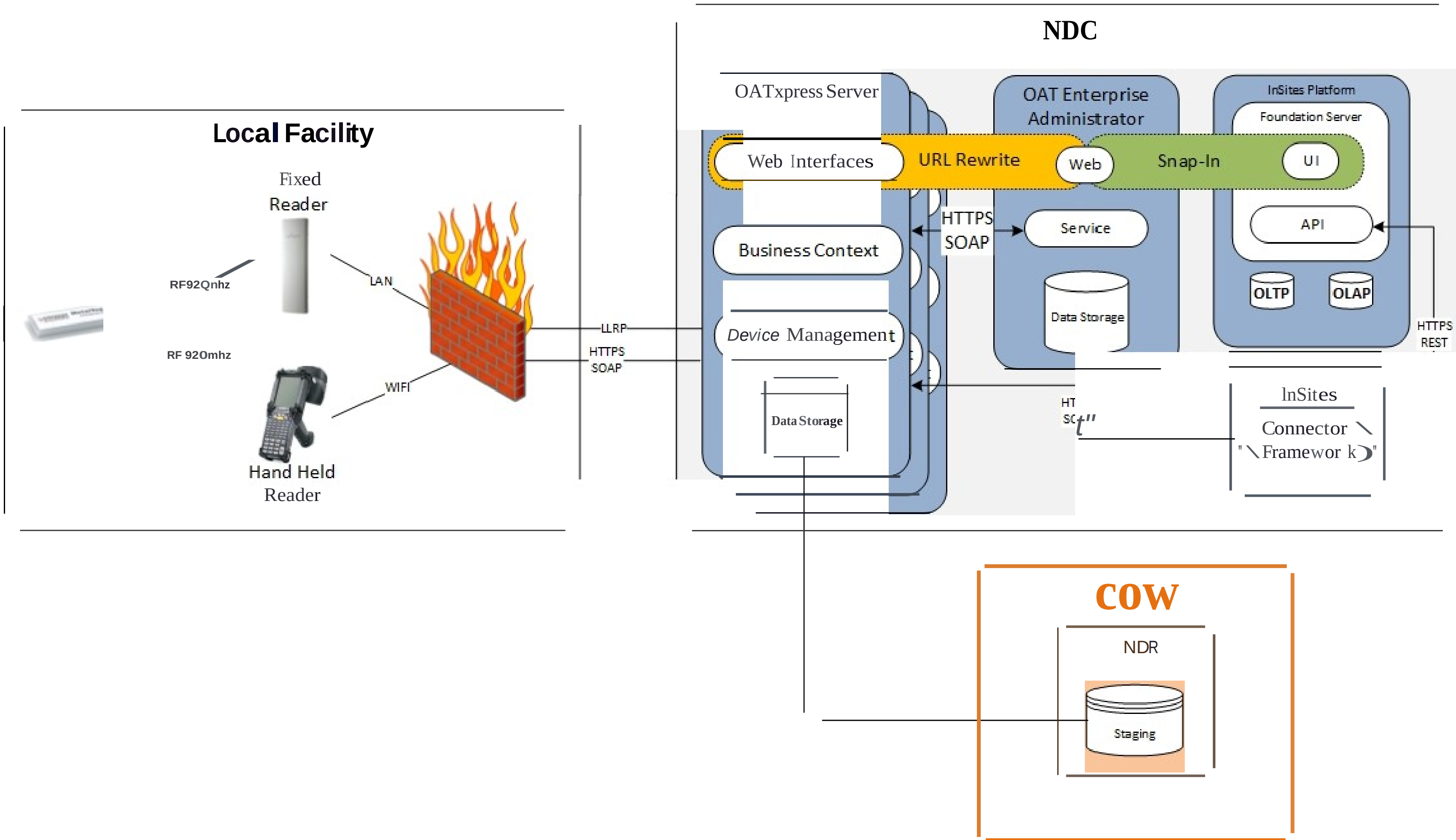
The **Device Manager** is the logical layer which interacts with the physical devices. It establishes the communication channels, monitors the status and health of the connected hardware, and it alerts the operator(s) when devices become unreachable. It also contextualizes events with the associated location information, which is defined in the OAT administrative interface and linked to an RFID device ("read point") on device configuration page.

The figure below shows the OAT System components integration with the Intelligent InSites components. The OATxpress instances will have a bi-directional interface with the Intelligent InSites Connector Framework. The OATxpress interface will use this interface to communicate the location of a passive tag in real time to the Intelligent InSites Connector Framework. OATxpress will pass the EE number that was scanned from the passive tag along with a tag identifier to the Intelligent InSites Connector Framework. The Intelligent InSites Platform will pass any object data (from AEMS-MERS interface) updates to the Intelligent InSites Connector Framework which will send the data on to OATxpress.

The OAT Enterprise Administrator will be part of the RTLS unified user interface. OAT Enterprise Administrator will make use of the Intelligent InSites snap-in framework for Single Sign On. Authenticated and authorized users will log into the Intelligent InSites Platform and click on the tab labelled OAT. Users will be able to view information in OAT Enterprise Administrator as well as the underlying OATxpress instances via a URL rewrite.

Each OATxpress instance will interface with the NDR Staging Database that is located in the CDW. The NDR ETL platform will extract the incremental data (data that has been inserted, updated, or deleted during a specific time period) from each OATxpress instance and load it into the NDR staging database.

Figure 49: OATSystems Integration with Intelligent InSites Platform



6.2.1.2.1 Data Flow

The start of a data flow begins when a passive tag is scanned by fixed or hand held scanner. The readers pick up the tags location over 920 MHz radio frequency. In the case of a fixed reader, the data flows over the LAN using the Low-Level Reader Protocol (LLRP) to the OATxpress server. When a hand held reader is used, the data flows through either the Wi-Fi network, where available or through a cradle that is connected to the LAN. The handheld readers will transmit SOAP (Simple Object Access Protocol) messages to the OATxpress server via a secure http (HTTPs) line. The data is persisted to a Microsoft SQL Server database from the OATxpress server. The data is then sent to the Intelligent InSites Connector Framework (VISN level) using a SOAP Message via HTTPS. The Intelligent InSites Connector Framework then sends a message to the Intelligent InSites Platform where it is persisted to the Intelligent InSites Transactional Data Model.

Intelligent InSites Platform will send tagged object data back to OATxpress via the Intelligent InSites Connector framework. Data will originate in the Intelligent InSites Platform and be sent a VISN/Central CMOP level Intelligent InSites Connector Framework. From the Connector Framework, the data will be sent to the facility level OATxpress instance (deployed in the NDC).

In the case of configuring or monitoring the OAT Enterprise Administrator will send SOAP messages to the all OATxpress Servers to retrieve monitoring and administrative data.

All incremental data within the OATxpress instances will be sent to the NDR Staging Database for use in analytical reporting.

6.2.1.2.2 Interfaces

The OATxpress Server will provide interfaces to the readers both fixed and hand held. These interfaces accept SOAP and LLRP messages to retrieve the location of the tagged assets. Likewise, the OATxpress Server provides an interface to the central OAT Enterprise Administrator. This interface uses SOAP messages to transport data back and forth about tag location as well as metrics about the OATxpress Server. The OATxpress Server will send SOAP based Web Service calls to an interface provided by the Intelligent InSites Connector Framework over HTTPS. Likewise, the OATxpress Server will expose a SOAP Web Service interface to accept updates from the Intelligent InSites Connector Framework.

Each OATxpress instance will interface with the NDR Staging Database that is located in the CDW. The NDR ETL platform will extract the incremental data using OLEDB.

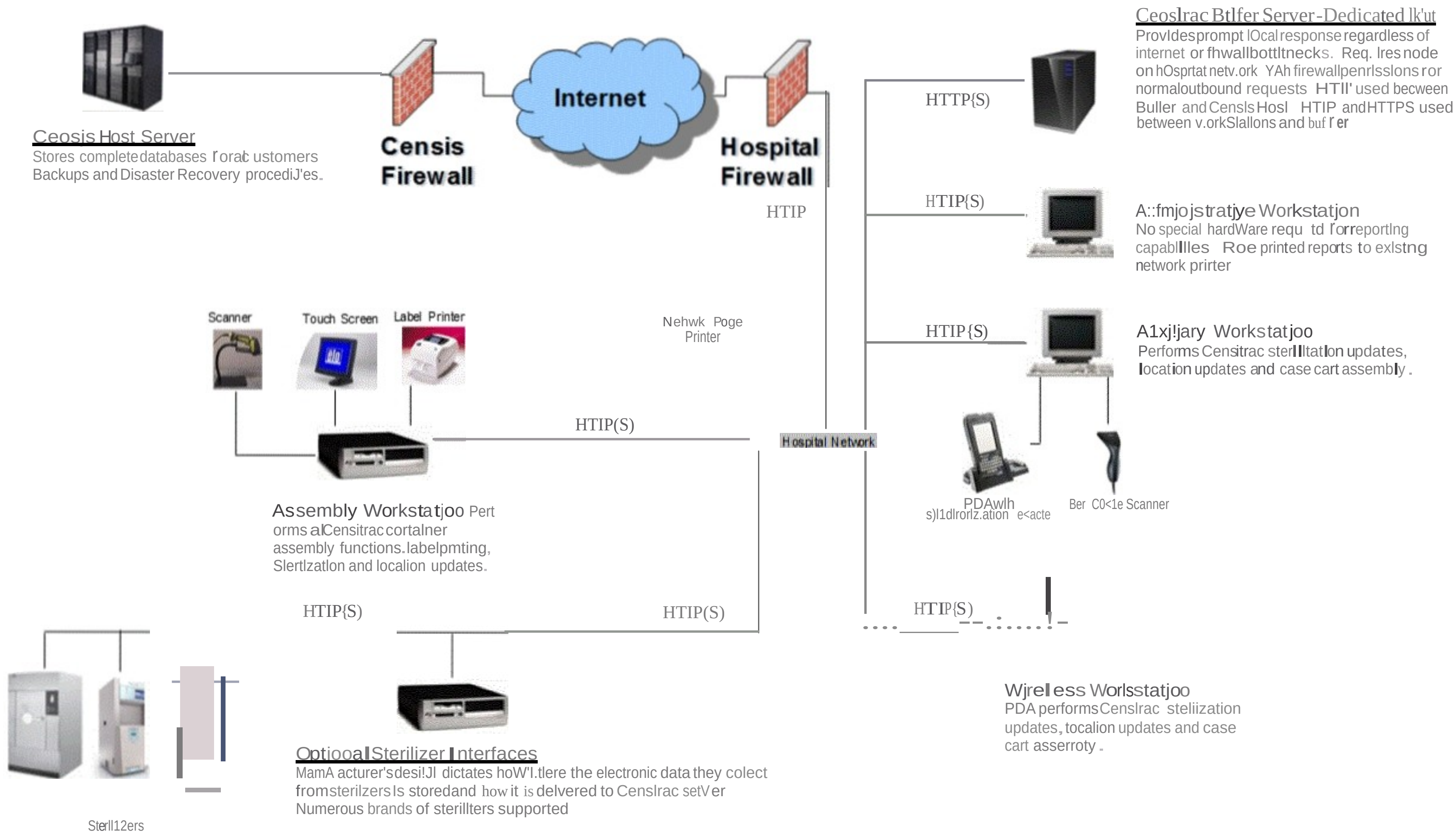
6.2.1.2.3 *Security*

In addition to securing messages using HTTPS, the interaction between the OATxpress server and the Enterprise Administrator is secured using a user name and password. The Enterprise Administrator makes use of the Intelligent InSites snap-in framework for securing the User Interface. The OATxpress web interface is secured using a URL redirect (HTTPS Token) from the Enterprise Administrator. The interaction between the OATxpress Server and the Intelligent InSites Connector is secured using x509 security. The RFID handheld readers are secured using HTTPS and Wi-Fi machine based certificates.

6.2.1.3 **Censis**

Medical/surgical instruments will be tracked as part of the VA Enterprise RTLS system. The VA Enterprise RTLS System will use Censis's InstrumentTrac solution to track the sterilization of medical and surgical instruments within the VA. Censis's InstrumenTrac electronic instrument tracking and management is a fully featured and robust instrument level tracking system. InstrumenTrac will also provide complete automation and recordkeeping for SPS terminal and Operating Room based flash sterilization. Because the RTLS system is tracking at the instrument level, InstrumenTrac facilitates target patient notification for instrument level recalls as well as immediate visibility to every instrument's reprocessing and use records. The figure below shows the Censis Architecture.

Figure 50: Censis Detailed Architecture



The figure below shows the flow of data within the Sterilization Processing Workflow.

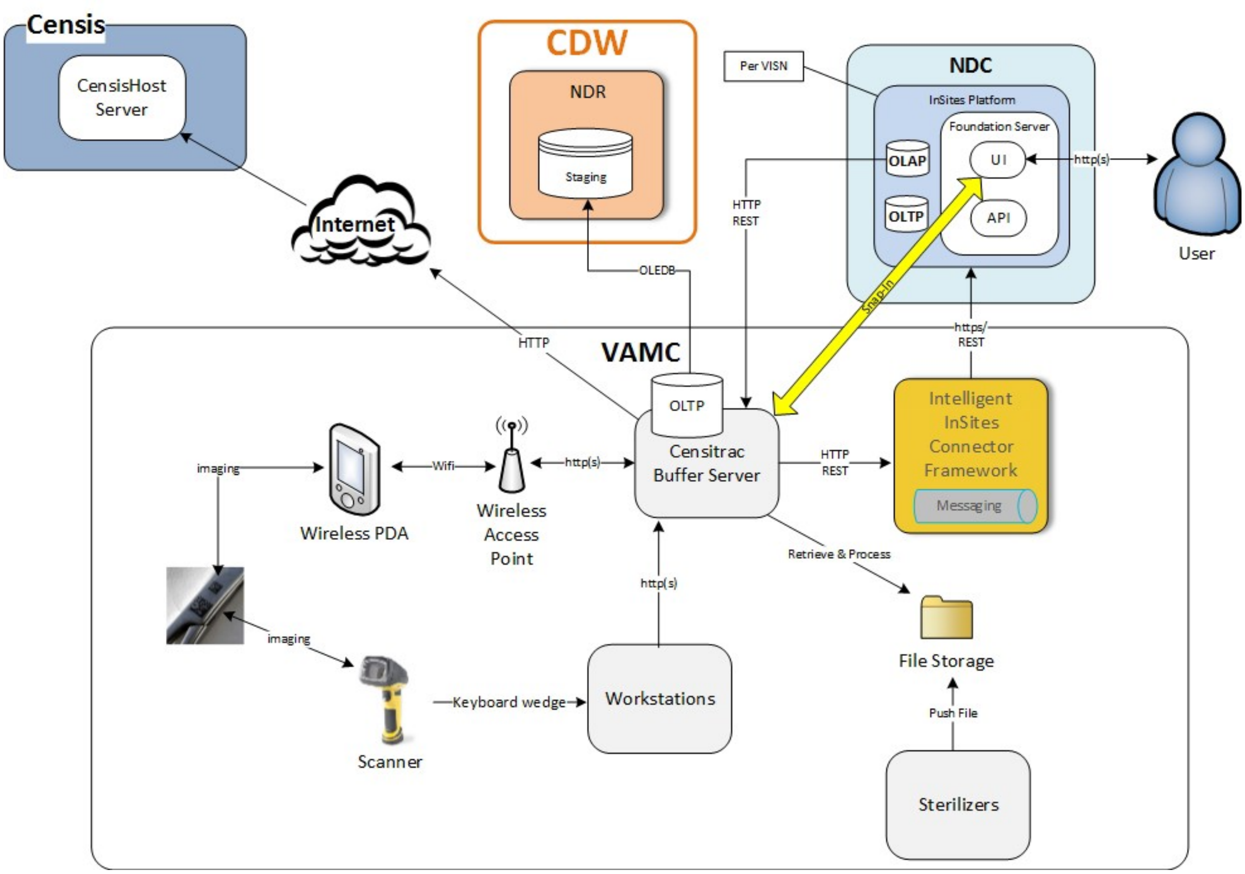
The Electrochemical/Electro-erosion markings on an instrument will be scanned by a wireless PDA or a scanner attached to a workstation via a keyboard wedge. In the case of the Wireless PDA, the data will be sent to the Censitrac Buffer Server via the VA's Wi-Fi network. If the marking is scanned by the workstation's scanner the data will be sent to the Censitrac Buffer Server via the VA's Ethernet using HTTPS. The data will be stored in the Censitrac Buffer Server's Online Transaction Processing database. The data will also be sent to the Intelligent InSites Connector Framework using a HTTPS secured REST Web Service. The Intelligent InSites Connector will send the data to the Intelligent InSites Platform via a HTTPS secured REST Web Service.

To full fill reporting requirements, the Intelligent InSites Online Analytical Processing database will pull additional report data on a nightly basis from the Censitrac Report API using a REST Web Service.

Censitrac will be part of the RTLS unified user interface. The Censitrac web application will make use of the Intelligent InSites snap-in feature. This will allow users to access Censitrac via the single sign on mechanism.

The Censitrac instance will interface with the NDR Staging Database that is located in the CDW. The NDR ETL platform will extract the incremental data (data that has been inserted, updated, or deleted during a specific time period) from Censitrac and load it into the NDR staging database

Figure 51: Censis Integration Architecture



6.2.1.3.1 Data Flow

When using Censis enabled equipment, there will be three inputs: Wireless Personal Digital Assistant (PDA), Scanners, and Third Party Sterilizers. The Wireless PDA running the Censitrac PDA client application will read the Electrochemical/Electro-erosion marking. The data will be sent by the Censitrac PDA client application in an HTTP message to the Censitrac Buffer Server by utilizing a Wireless Access Point using Wi-Fi.

A scanner attached to a workstation running the Censitrac client application will read the Electrochemical/Electro-erosion markings. The scanner will send the markings data to the Censitrac client application as a keyboard input. The data will be sent by the Censitrac client application to the Censitrac Buffer Server in an HTP message across the VA LAN.

Some third party sterilizers can collect data and place the data into a file in a designated location. The Censitrac Buffer server will receive this data in an HTTP message across the VA LAN.

From the Censitrac Buffer Server, data will be sent to the Intelligent InSites Connector Framework using a REST Web Service over HTTP. As various events occur in Censitrac, messages with specific data about the event will be sent to the Intelligent InSites system. The formats of the messages are JSON. The following events trigger a message push to Intelligent InSites:

- Location scan
- New tray assembly (to remove contents from tray)
- New cart assembly (to remove contents from cart)
- Instrument scanned to tray (message sent as each instrument scanned)
- Tray and Instrument scans to cart (message sent as each item scanned)
- Asset scans to decontamination (message sent as each item scanned)
- Update to sterilizer load results
- Recall for sterilizer load
- Inventory updates (send as changes occur)
- Remove instrument from tray
- Remove trays or instruments from carts

The Censis Technologies Report Service API facilitates similar real time access to Censitrac data by utilizing the Censitrac reporting system. Report data will be retrieved programmatically in an XML format via HTTP requests. To retrieve data produced by customized Censitrac reports, the client application will make HTTP or HTTPS requests to the Censitrac server. On a nightly basis, the Intelligent InSites Platform will make call to the Censis Report Service API to retrieve data to be used in the Intelligent InSites VISN level Business Intelligence system.

Censitrac may receive changes/updates from the Intelligent InSites system. An example would be location change updates from the Intelligent InSites system. For location changes, Intelligent InSites will FTP a file to Censitrac where it will be loaded into the system.

Data from the Censitrac Buffer Server will be sent to the Censis cloud over the Internet using HTTP for backup and disaster recovery purposes.

All incremental data within Censitrac will be sent to the NDR Staging Database for use in analytical reporting.

6.2.1.3.2 Interfaces

The Censitrac Buffer Server will provide interfaces to various workstations, wireless PDAs and indirectly to Sterilizers. In the case of the workstations and wireless PDAs the interfaces will use buffer readers using IP and Port over https. In the case of the Sterilizers, the Buffer Server will use a polling mechanism to poll for a file from the sterilizers at a desired increment.

For data that does not need to be sent in real time, data from Censitrac custom reports can be retrieved via http requests. These responses are sent back to Intelligent InSites Connector in a mock RESTful WebServices. This data is ultimately lands in the Intelligent InSites OLAP platform. Below is a sample of the report data that will be sent back to the client:

</row>
…
</table>

The Censis Buffer Server will interface with the NDR Staging Database that is located in the CDW. The NDR ETL platform will extract the incremental data using OLEDB.

6.2.1.3.3 Security

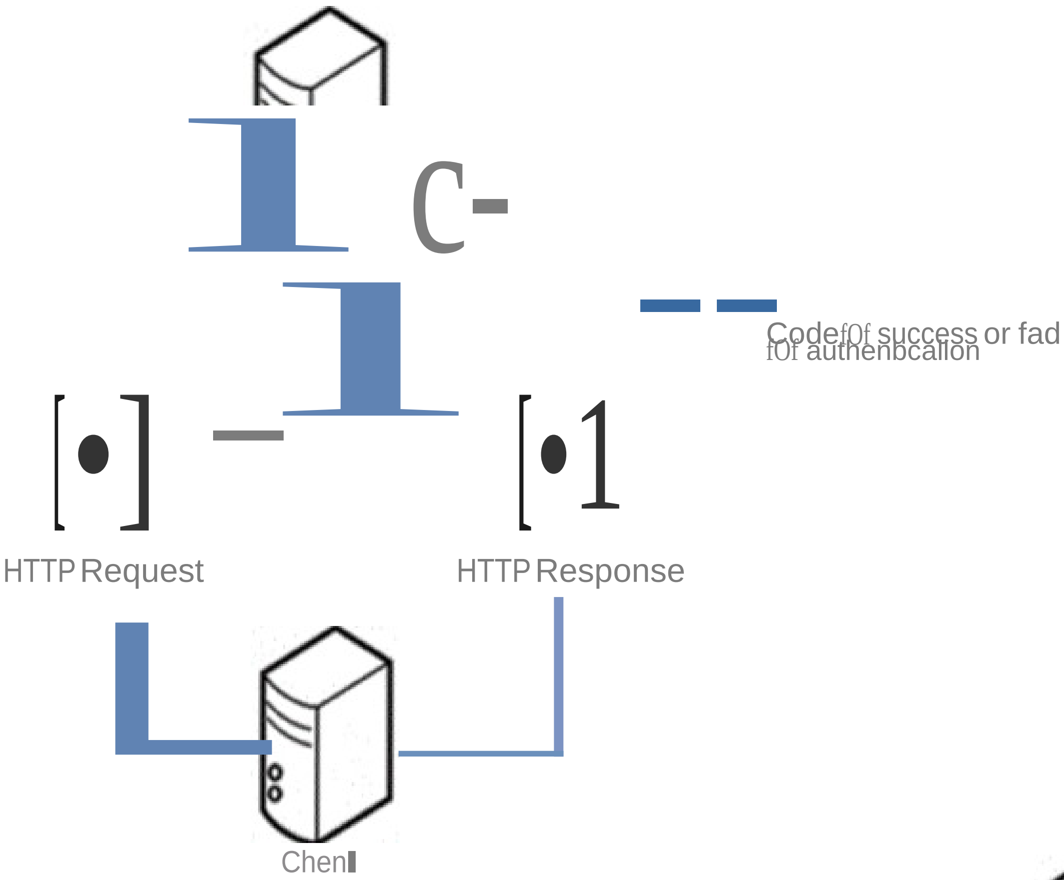
In addition to securing messages with HTTPS, Censitrac offers different methods for logging in.

1. Logon ID and password (available on both workstation and PDA)
2. Scanning badge generated from Censitrac (available on both workstation and PDA)
3. Scanning hospital generated badge (available on both workstation and PDA)
4. Active Directory authentication (available on workstation only, since PDA's do not require Windows logon)

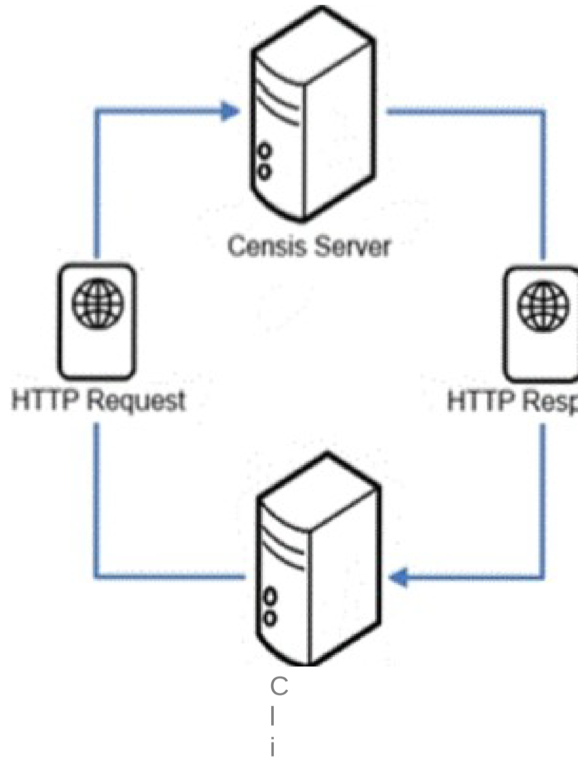
The interaction between Censitrac Buffer Server and the Intelligent InSites Connector Framework will be over standard http protocol.

Figure 52: Censls Security Mechanism

Step 1 – Request for Authentication



Step 2 – Request to send/retrieve data



ent

Repons Willreturn
XML f()(matted dala

Updates sent to Censrtrac
willreturn a success or farlcode

Below is an example of the authentication and report data request process

The first request must be an authentication request that sends valid Censitrac credentials as post data.

Table 29: Censis Authentication Request

Authentication Request	
URL	http(s)://[servername]:[SSL Port]/Login.asp

Table 30: Censis Data Post

Post Data		
Username	[Censitrac® User ID]	The Censitrac® User ID authorized to run the desired reports
password	[Password]	The Censitrac password for this user
hospital_id	[Hospital ID]	The customer's four digit identifier
silent	"y"	Required for API authentication

If authentication is successful, then the server will send the response string "ok", and an HTTP status code 200.

Subsequent requests should be for report data.

Table 31: Censis Report Request

Report Requests		
URL	http(s)://[servername]:[SSL Port]/rptAll_Body.asp?[parameters]	
Parameters		
report_id	[Report ID]	The ID for the desired report, as displayed on the Censitrac® reports submenu
renderType	"XML"	This parameter sets the output format to XML

6.2.2 Messaging Framework Engine

This section will discuss the software components used to securely transport messages within the VA's enterprise RTLS System.

6.2.2.1 Intelligent InSites Connector Framework

An instance of the Intelligent InSites Connector Framework will be installed on site at every local facility (VAMC, CBOC, or CMOP). The Intelligent InSites Connector Framework is a Microsoft Windows server with a collection of tools for providing connectivity to the Intelligent InSites Platform. The connector framework is a set of .NET libraries tools that allows for easy integration between 3rd party systems (CenTrak, Censis, etc.) and the Intelligent InSites Platform. All of the connectors are built as .NET class libraries and are run through a Microsoft Windows service. Some example libraries include:

- Object-oriented way of interacting with the REST APIs provided by the Intelligent InSites Platform
- Reliable message queuing and persistence of 3rd party data streams
- Connectors are "plug and play" so there is no need to restart the entire framework to deploy/update a single connector

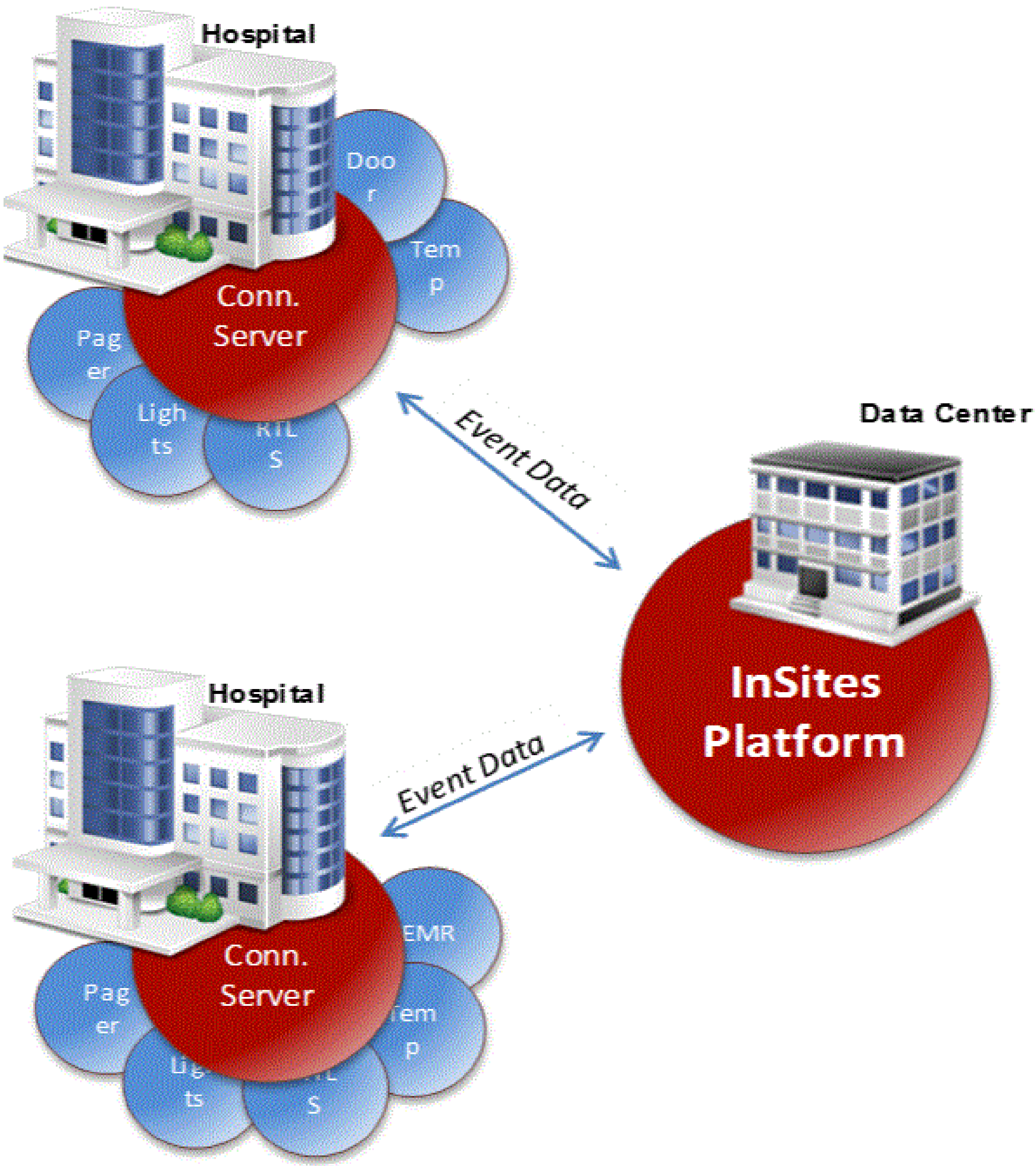
Here are some of the benefits/features of the Intelligent InSites Connector Framework

- Set of tools for managing connectivity and multiple systems/interfaces
- Translates standard formats of data into Intelligent InSites API calls
- Two-way communications channels between Intelligent InSites Platform
- Allows for the continual growth of additional integrations
- Contains event failure/retry and interpretation logic
- Designed specifically for RTLS; others might require framework changes
- Well-defined interfaces for plug-in support
- Reduces development time for connectors due to the use of existing libraries that handle common tasks
- Full control over the functionality of the connector from start to stop

The Connector framework will be used when low-level data, sensory networks, and real time system connectivity is required. Sensory data has specific volume and data characteristics, and low need for orchestration and transformation, which the InSites Connector Framework is designed to deal with. These integrations will be part of the COTS solution.

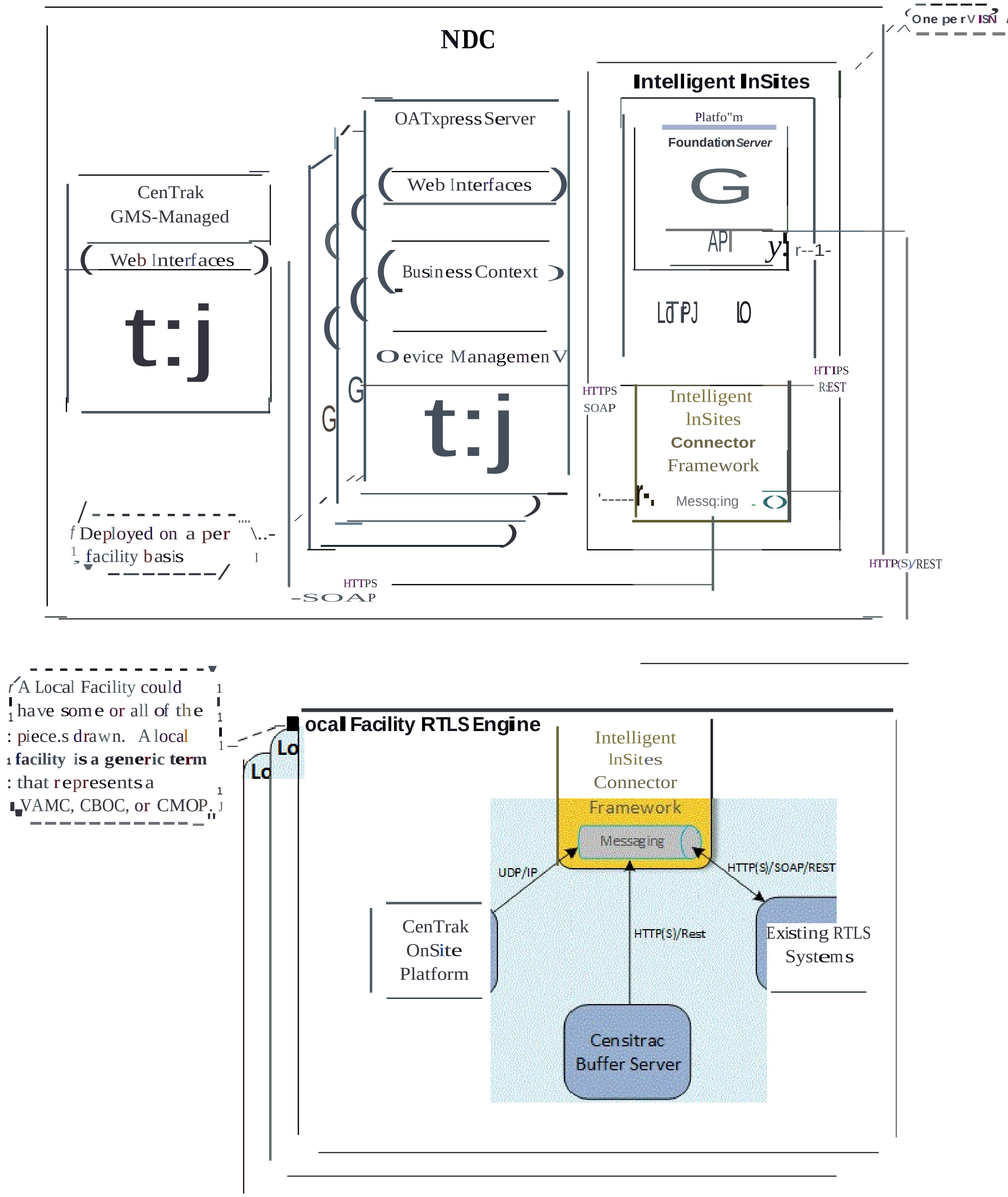
The figure below shows how multiple Connector Frameworks installed on site can feed one Intelligent InSites Platform either installed on site, off site of in a cloud environment.

Figure 53: Intelligent InSites Connector Framework Conceptual Architecture



The figure below shows the integration to and from the Intelligent InSites Connector Frameworks (per VISN and local facilities belonging to that VISN).

Figure 54: Intelligent InSites Connector Framework Integration Architecture



6.2.2.1.1 Data Flow

Data will flow in the form of messages from the sensory data producing software (CenTrak, Censis, and OAT Systems) and Existing RTLS Systems (Aeroscout, Ekahau, Sonitor, and Versus) to the Intelligent InSites Connector Framework via a secure channel such as HTTPS (UDP/IP will not be secured). The messages will be delivered using SOAP, REST and UDP/IP as the transport mechanism. From the connector framework to the Intelligent InSites Platform the data will travel over HTTPS using a REST Web Service.

Data will flow from the Intelligent InSites Connector Framework to the OATxpress instances when a tracked object's attribute has been changed or updated in the RTLS System. The data will flow to the appropriate OATxpress instance using SOAP over HTTPS.

Data will flow from the Intelligent InSites Connector Framework to the CenTrak GMS Managed instance on a nightly basis to retrieve report data. This data will be retrieved from the GMS using SOAP over HTTPS.

6.2.2.1.2 Interfaces

The Intelligent InSites Connector framework provides an interface to CenTrak, Censitrac, OAT Systems and any other existing RTLS system. The interface connection is created using a channel within the Connector Framework. The channels can utilize various protocols such as SOAP and REST Web Services. The Connector Framework will send the data to an interface exposed via the Intelligent InSites Platform. This interaction is over done over HTTP(S) using a REST Web Service.

6.2.2.1.3 Security

The Intelligent InSites Connector framework supports various security y mechanisms. For the interactions between CenTrak OnSite Platform, and Censis to the Connector Framework, there will be no encryption or passwords used. The data being transmitted is raw sensory information that contains no personal health information, there is no need to encrypt or secure this data. The interaction between the OATxpress server and the Connector Framework will be HTTPS with basic/digest authorization. Like the OATxpress server interaction, HTTPS with basic/digest authorization will be used to secure the communication between the Connector Framework and CenTrak GMS.

6.2.2.2 **ESB**

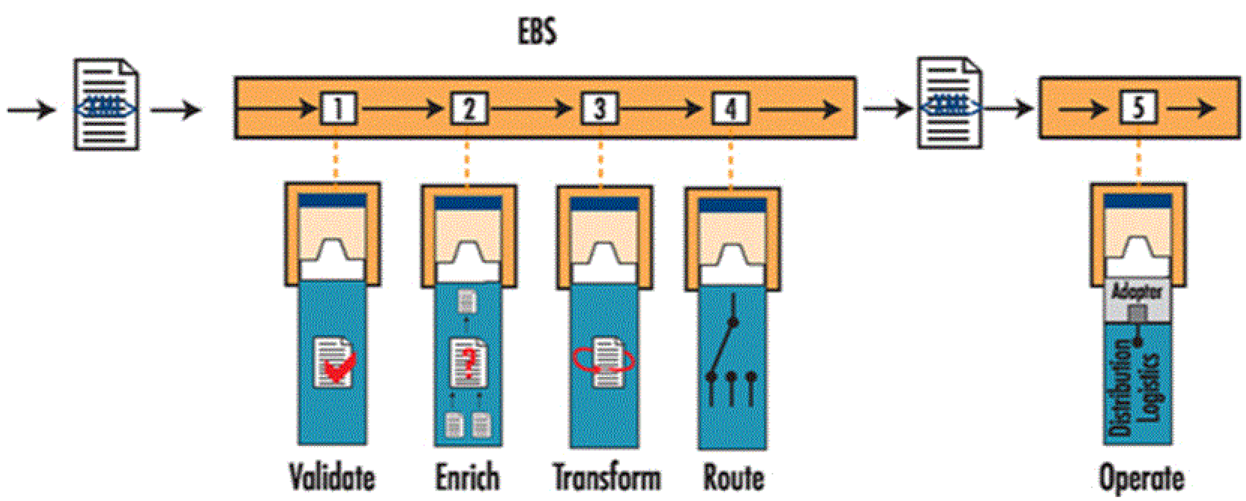
The VA RTLS system will utilize an Enterprise Service Bus. An ESB is software architecture for middleware that provides fundamental services for more complex architectures. For example, an ESB incorporates the features required to implement a service-oriented architecture. In a general sense, an ESB can be thought of as a mechanism that manages access to applications and services (especially legacy systems) to present a single, simple, and consistent interface. An ESB is a set of rules and principles for integrating numerous applications together over a bus-like infrastructure. The core concept of the ESB architecture is to integrate different applications by putting a communication bus between them and then enable each application to talk to the bus. This decouples systems from each other, allowing them to communicate without dependency on or knowledge of other systems on the bus. The concept of ESB was born out of the need to move away from point-to-point integration, which becomes brittle and hard to manage over time. Point-to-point integration results in custom integration code being spread among applications with no central way to monitor or troubleshoot. This is often referred to as "spaghetti code" and does not scale because it creates tight dependencies between applications.

In essence, ESB does for distributed heterogeneous back end services and applications and distributed heterogeneous front-end users and information consumers what middleware is really supposed to do: hide complexity, simplify access, allow developers to use generic, canonical forms of query, access and interaction, handling the complex details in the background. The key to ESB's appeal, and possibly also its future success, lies in its ability to support incremental service and application integration as driven by business requirements, not as governed by available technology.

An ESB promotes a way to meet the challenges of integrating applications and provide a single, unified architecture implementing a pattern called VETRO. VETRO stands for Validate, Enrich, Transform, Route and Operate:

- **Validate** – usually the first step. An example of validation is to simply verify that an incoming message contains a well-formed XML document and conforms to a particular XML schema or WSDL document that describes the message. This removes the burden of validation from all of the downstream service implementations and promotes reuse.
- The "**Enrich**" step involves adding additional data to a message to make it more meaningful and useful to a target service or application. The enrich service could be implemented to invoke another service to look up additional data, or it could access a database to get what it needs.
- The "**Transform**" step converts the message to a target format (converts the data format of a source data system into the data format of a destination data system). The target system may have its own built-in validation rules requiring that the transformation step modify the incoming data in order to prevent the target system from rejecting the message.
- **Route** is the routing of a message to one or more services. This step is also known as service orchestration.
- The "**Operate**" step is the invocation of the target service or an interaction with the target application. If the target operation is an enterprise application that requires its own data format, then the previous transformation step converts the message to the target format required by the application.

Figure 55: ESB VETRO Pattern



The VA RTLS System will use Mule ESB as its ESB solution. Mule ESB is a lightweight Java-based enterprise service bus and integration platform that allows developers to connect applications together quickly and easily, enabling them to exchange data. Mule ESB enables easy integration of existing systems, regardless of the different technologies that the applications use, including Java Message Service (JMS), Web Services, JDBC, HTTP, and more.

The key advantage of an ESB is that it allows different applications to communicate with each other by acting as a transit system for carrying data between applications within your enterprise or across the Internet. Mule ESB includes powerful capabilities that include:

- Service creation and hosting — expose and host reusable services, using Mule ESB as a lightweight service container
- Service mediation — shield services from message formats and protocols, separate business logic from messaging, and enable location-independent service calls
- Message routing — route, filter, aggregate, and re-sequence messages based on content and rules
- Data transformation — exchange data across varying formats and transport protocols

Figure 56: Mule Architecture

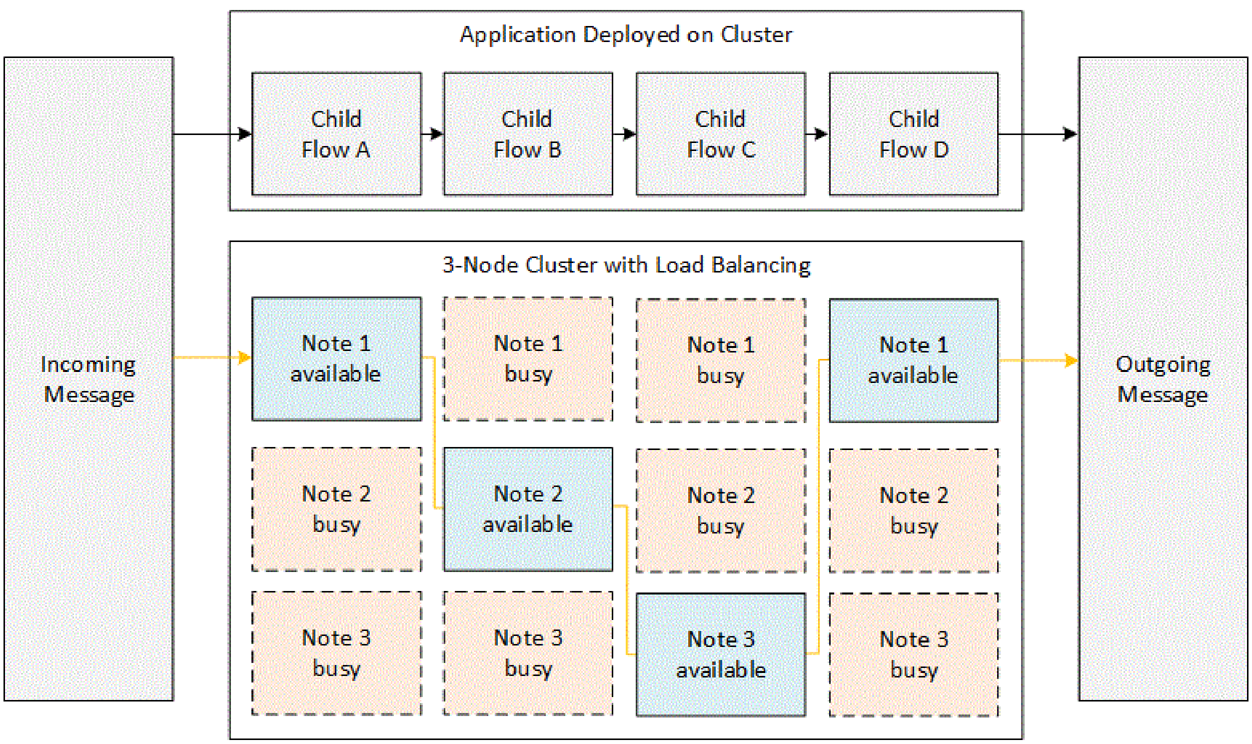
The Mule ESB will be used for integrations with 3rd party "system of records" which contain information that provides the RTLS system with a strong context for interpreting meaningful actions or events. These types of interfaces typical require higher levels of transformation and orchestration of the data such as field level mapping and two way synchronization processes that are ideal for an ESB topology. These integrations will be developed as part of the delivery of a National RTLS system and will be owned by the VA.

The VA RTLS System will use the Enterprise Edition of Mule ESB which allows for Mule ESB to be deployed in a clustered deployment model. A cluster is a set of ESB instances that act as a unit. In other words, a cluster is a virtual server composed of multiple nodes. The servers in a cluster communicate and share information through a distributed shared memory grid. This means that the data is replicated across memory in different physical machines. Here are some of the benefits of a clustered environment:

- High availability (high reliability – zero tolerance for message loss): Making the system continually available in the event that one or more servers fail. When the primary ESB instance becomes unavailable (e.g., because of a fatal JVM or hardware failure or it's taken offline for maintenance), a backup ESB instance immediately becomes the primary node and resumes processing where the failed instance left off. After a system administrator has recovered the failed ESB instance and brought it back online, it automatically becomes the backup node. Seamless failover is made possible by a distributed memory store that shares all transient state information among clustered ESB instances, such as:
    - Staged Event Driven Architecture service event queues
    - In-memory message queues
- Fault tolerance: The ability to recover from failure of an underlying component. Typically, the recovery is achieved through transaction rollback or compensating actions.
- Scaling: The ability to horizontally scale an application to meet increased demand (high throughput).

The following figure illustrates workload sharing in more detail. Three nodes process messages related to application containing a flow (four child flows). However, when one node is heavily loaded, it can move the processing for one or more steps (child flows) in the process to another node. Here, processing of the overall flow is moved among three nodes until it the flow is completed.

Figure 57: Clustered ESB



The ESB will handle interactions to the all VA-Owned services within the RTLS enterprise. Likewise, it will also provide a single view into the RTLS Service Portfolio for external communication such as iEHR. RTLS will deploy a clustered Mule ESB instances in the NDC. This clustered instance will be used to interface RTLS COTS products with VA owned systems, services and applications.

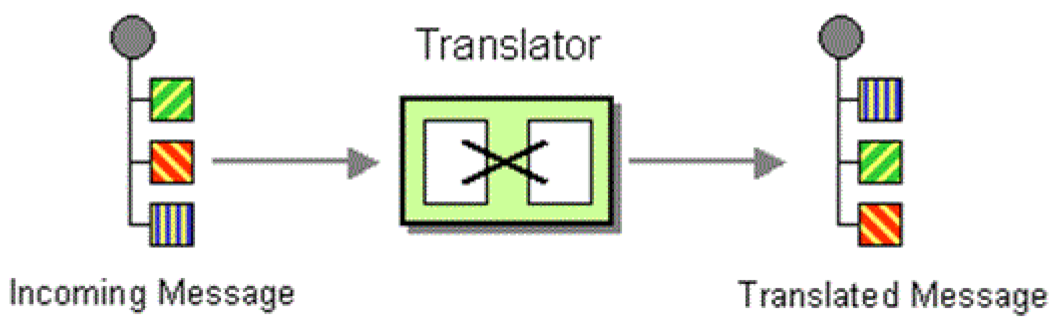
6.2.2.2.1 Data Transformation

VA and third-party information systems often have data fields and messages defined in many different ways. Enterprise integration models provide a foundation for a decoupled, consistent, reusable integration methodology which can be implemented using messaging supported by middleware products. A feature of ESB is the translators (also known as Data Transformation). Data transformation is the process of converting data from one format (e.g. a database file, XML document, or Excel sheet) to another. Because data often resides in different locations and formats across the enterprise, data transformation is necessary to ensure data from one application or database is intelligible to other applications and databases, a critical feature for applications integration.

The first step of data transformation is data mapping. Data mapping determines the relationship between the data elements of two applications and establishes instructions for how the data from the source application is converted before it is loaded into the target application. In other words, data mapping produces the critical metadata that is needed before the actual data conversion takes place.

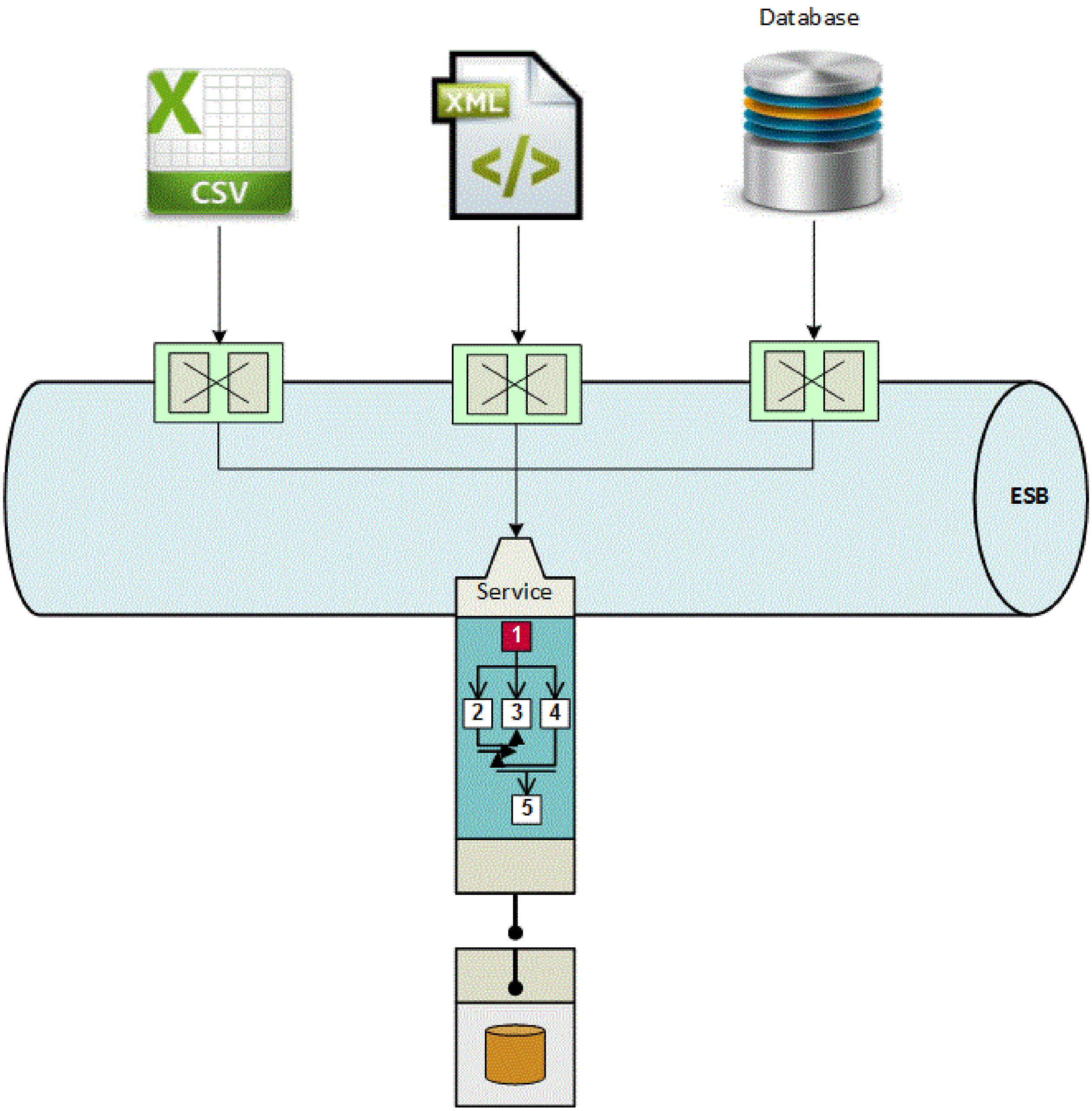
For instance, in field mapping, the information in one application might be rendered in lowercase letters while another application stores information in uppercase letters. This means the data from the source application needs to be converted to uppercase letters before being loaded into the corresponding fields in the target application. These features are functions of XSLT and xPATH. For more information on Translator see http://www.eaipatterns.com/MessageTranslator.html.

Figure 58: Translator



The figure below represents a conceptual view of how Data Transformation will take place among three different message formats. The inputs (csv file, XML file, and database) will be transformed to meet the format of the service endpoint prior to be persisted in the data store.

Figure 59: Conceptual Data Transformation



6.2.2.2.2 Security

Security on the ESB is very important. Mule ESB has a collection of security features that enforce secure access to the information that Mule connects to. The Mule ESB suite of security features provides various methods for applying security to Mule Service-Oriented Architecture (SOA) implementations and Web services. The following security features bridge gaps between trust boundaries in applications:

- **Mule Secure Token Service (STS) OAuth 2.0a Provider -** OAuth uses tokens to ensure that a resource owner never has to share credentials, such as a username or password, with a 3rd-party Web service.
- **Mule Credentials Vault -** encrypt properties in a .properties file. The .properties file in Mule stores data as key-value pairs. Mule flows may access this data — usernames, first and last names, credit card information — as the flow processes messages. In the context of Mule Enterprise Security, Mule refers to the .properties file in which it safely stores encrypted properties as the Mule Credentials Vault.
- **Mule Message Encryption Processor -** encrypt an entire payload or several fields of data within a message. Where sensitive information must move between users, yet remain hidden from them, a developer can encrypt message content to prevent unauthorized access. Typically, encrypt data such as a password, or social security number (SSN).
- **Mule Digital Signature Processor -** uses digital signatures to ensure that messages maintain integrity and authenticity. Mule can verify that an incoming Web service request originates from a valid source, and can sign an outgoing Web service response to ensure its contents. Digital signatures ensure that a sender is valid, that a message is not modified in transit between Web services, and that no unauthorized user has tampered with a message.
- **Mule Filter Processor -** can filter messages it receives to avoid processing invalid ones. With a filter processor in place, Mule discards any message it receives that does not match the filter's parameters — a message from outside a set range of IP addresses, for example.
- **Mule CRC32 Processor -** can apply a cyclic redundancy check (CRC) to messages to ensure message integrity. CRC uses an algorithm to apply a check value to a message when it enters a system, and verifies the value when the message leaves the system. If the entry and exit values do not match, CRC marks the message as changed. Generally, CRC32 (32 indicates the 33-bit polynomial length in the algorithm) detects unintentional changes to messages, such as the accumulation of "noise" between transmission points, but it can also detect unauthorized intentional changes – for instance, flagging a message that has been tampered with during transmission to change it into a Trojan horse.

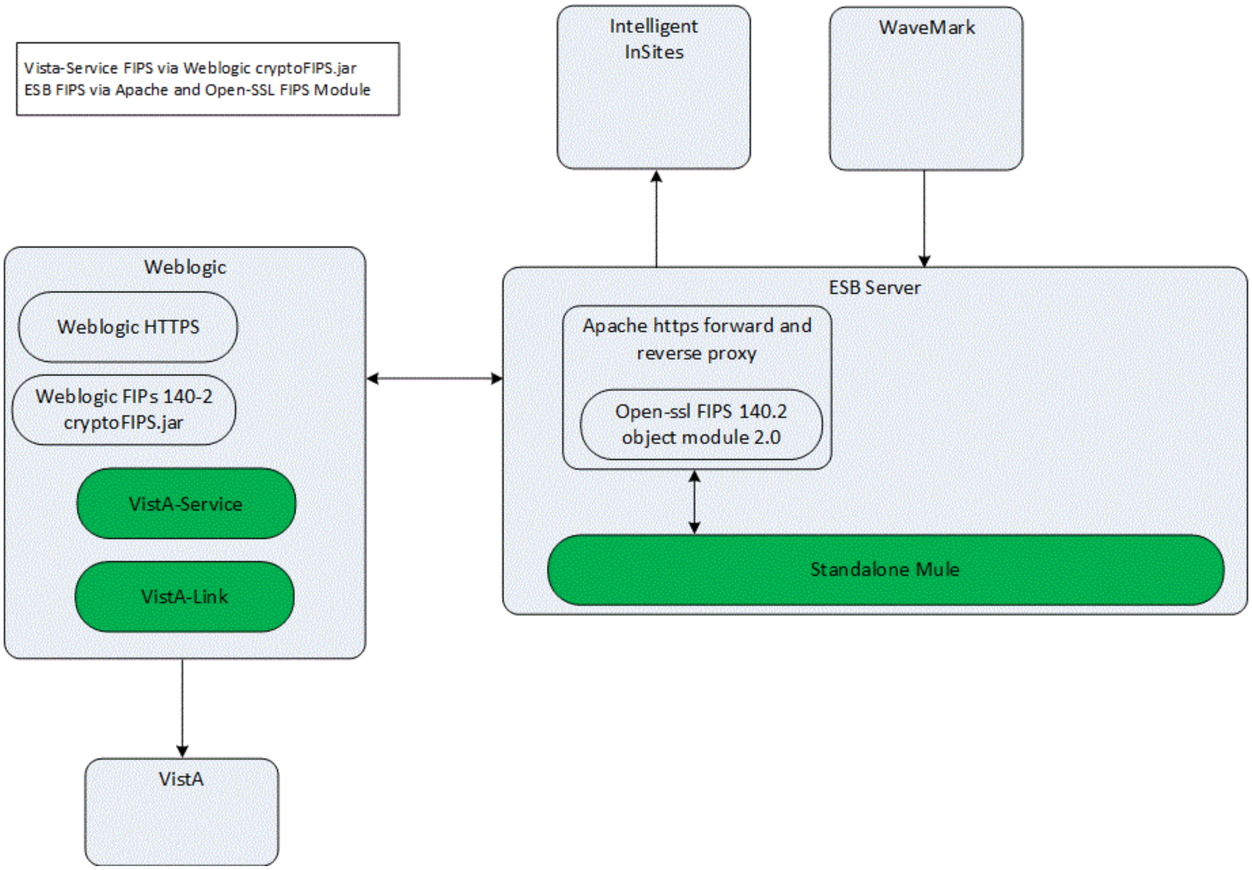
Mule ESB allows you to authenticate requests via endpoints using transport-specific or generic authentication methods. It also allows for control over method-level authorization on the components. The Security Manager is responsible for authenticating requests based on one or more security providers. All security is pluggable via the Mule security API, so it can easily plug into custom implementations. The main security that Mule ESB supports is WS-Security. WS-Security is a standard protocol for applying security to Web services. It contains specifications on how integrity and confidentiality in a SOAP message can be enforced via XML signatures and binary security tokens such as X.509 certificates and Kerberos tickets as well as encryption headers. It ensures end-to-end security by working in the application layer as opposed to the transport layer.

In addition, Mule ESB supports the following security protocols:

Spring Security	Aceji	PGP
SAML	JAAS	SSL/TLS
SAMl2	OAuth	

Currently at this time, Mule ESB is not FIPS-140.2 compliant. In order to make sure message transportation is FIPS-140.2, the RTLS system will use an Apache Web Server proxy in front of Mule ESB to confirm all traffic into the ESB is FIPS-140.2 compliant. The figure below shows the FIPS compliant communication between the integration points to and from the Mule ESB.

Figure 60: Mule ESB – Apache Proxy



6.2.2.3 VistA-Service

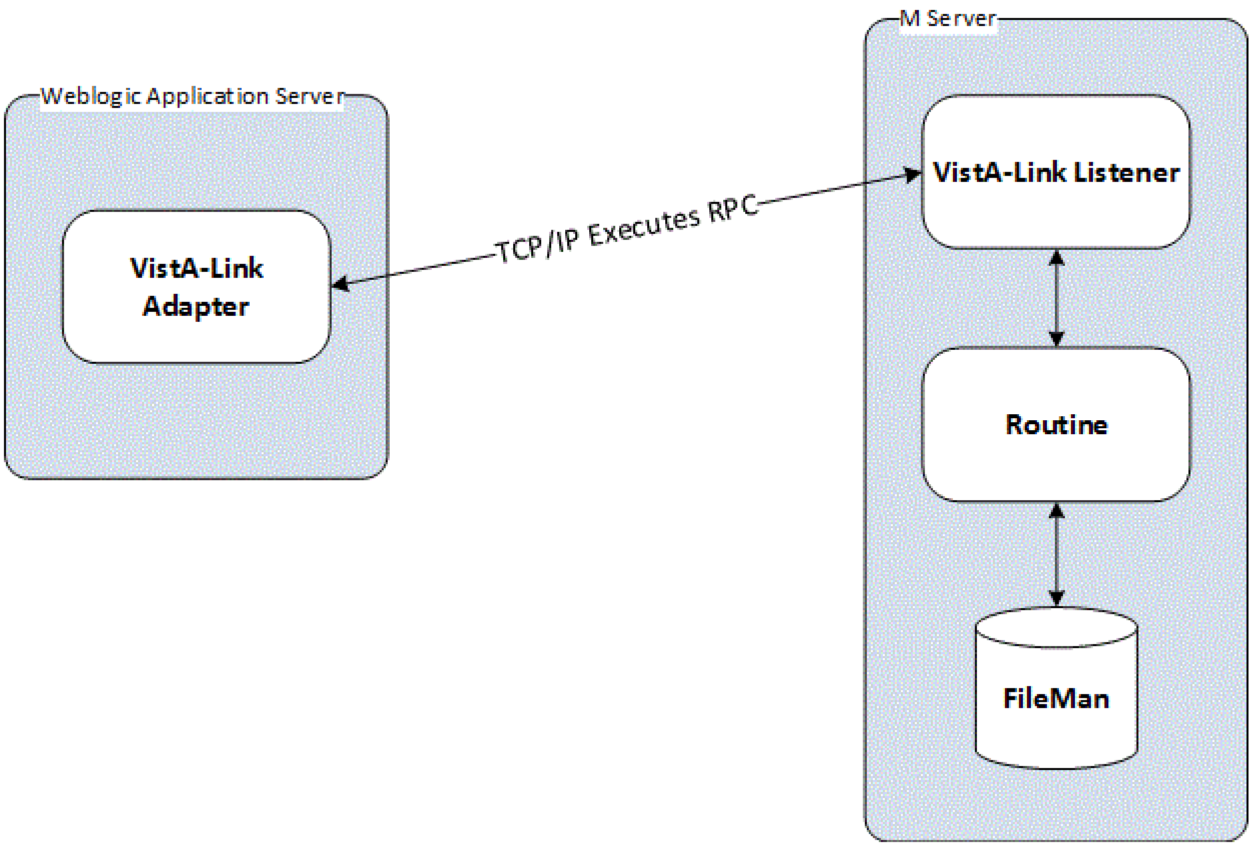
VistA is an enterprise-wide information system built around an Electronic Health Record, used throughout the United States Department of Veterans Affairs medical system. It consists of nearly 160 integrated software modules for clinical care, financial functions, and infrastructure. VistA was developed using the M or MUMPS language/database. The RTLS system will integrate with various applications within the VistA System.

Communication from the RTLS System to VistA will be managed with a series of Restful web service methods designed for the RTLS Enterprise solution called Vista-Service. Vista-Service is an interface to VistA creating a uniform calling method for underlying MUMPS Remote Procedure Calls (RPCs). The Restful web service methods provide a mechanism to encapsulate the VistA-Link calls into a standard format. This improves code maintainability, de-couples the service from the interface so multiple interfaces can use it, and provides for future scalability of the interface. Vista-Service has methods for creating, retrieving, and updating VistA data over HTTP using Restful semantics. Restful methods are called using a URL.

VistA RPCs are invoked by Vista-Service methods through the VistA-Link Adapter deployed as a separate component on the Weblogic server. The adapter is TCP/IP based and provides connection pooling for enhanced scalability. It is deployed using the VA standard as described in section 2 of the VistA-Link System Management Guide. Vista-Service methods invoke RPCs using the VistA-Link APIs described in the VistA-Link Developer Guide.

The VistA-Link resource adapter is a transport layer that provides communication between Java applications and VistA/M servers, in both client-server and n-tier environments. It allows RPCs to execute on the VistA/M system and return results to the Java enterprise system. VistA-Link consists of Java-side adapter libraries and an M-side listener. The adapter libraries use the J2EE Connector Architecture (J2CA 1.5) specification to integrate Java applications with legacy systems. The M listener process receives and processes requests from client applications. The adapter is TCP/IP based and provides connection pooling for enhanced scalability. It is deployed using the VA standard as described in section 2 of the VISTALINK SYSTEM MANAGEMENT GUIDE, Version 1.6 December 2010 named Deploying VistA-Link Adapters on J2EE.Interface Control Document 3 November 2012 Version 2.0 J2EE applications invoke RPCs using the VistA-Link APIs described in the VISTALINK DEVELOPER GUIDE Version 1.6 December 2010.

Figure 61: VistA-Link Components



The RTLS System will make use of the HealtheVet Web Services Client (HWSC). The HWCS allows VistA applications to invoke Web Service Methods on external servers and retrieve results.

HWSC supports two modes of synchronous web service access:

- SOAP (Service Oriented Architecture Protocol) – a formal XML-based protocol for accessing services
- REST (Representational State Transfer) – an architectural style of accessing services via programmatic access to web resources.

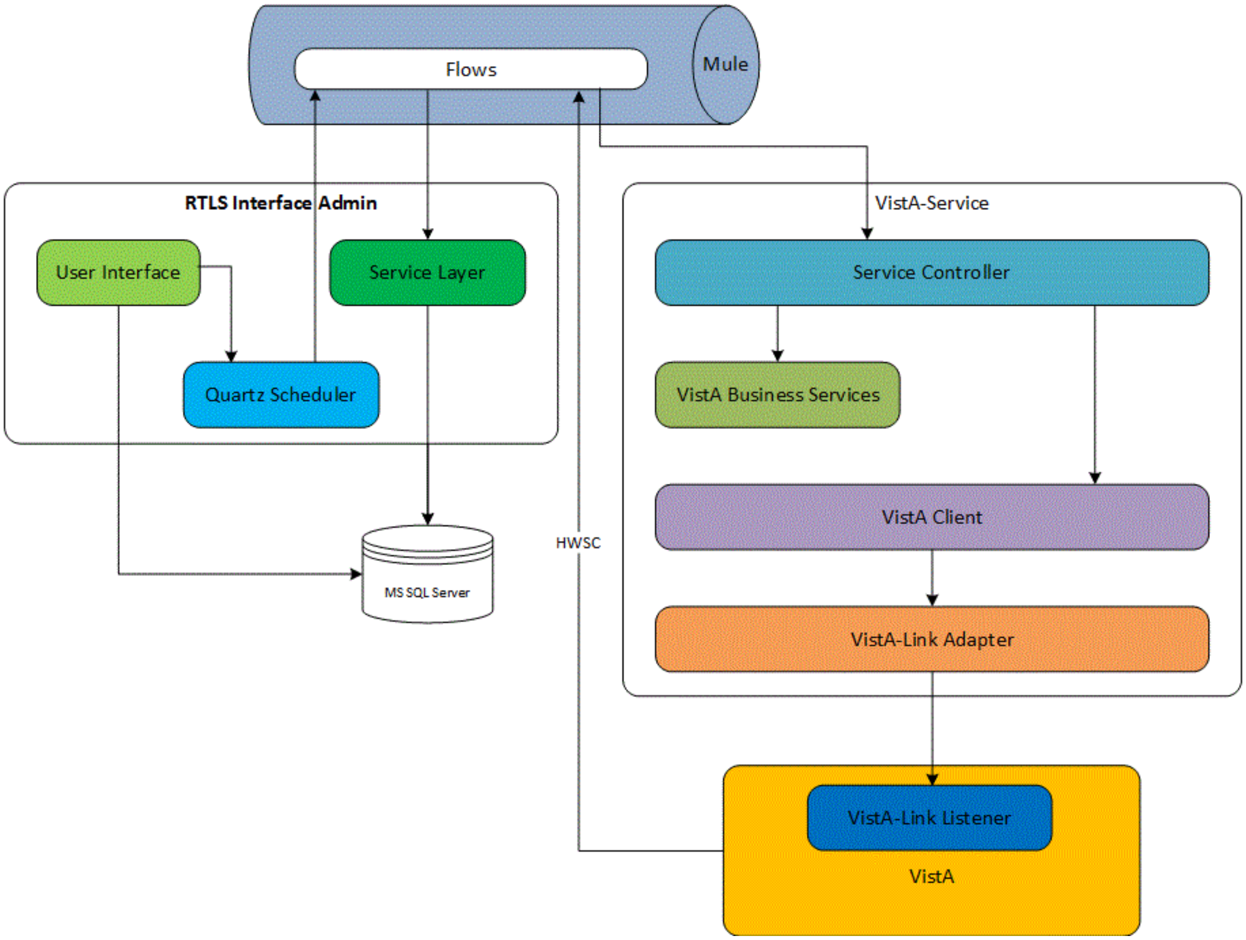
HWSC provides several management screens allowing RTLS to create and manage the web server and web service information needed by VistA applications to consume external web services. The management screens are:

- Web Server Manager
- Web Service Manager
- Lookup Key Manager

The following figure shows detail architectural components of the VistA-Service. Components with the VistA-Server are as follows:

- RTLS Interface Admin – provides an administration web site for authorized users to maintain and configure the VistA-Service:
    - User Interface – web-based graphical tool used for maintenance and configuration
    - Quartz Scheduler – job scheduling library used to execute Mule ESB flows on a configurable periodic basis
    - Service Layer – provides APIs to the configuration stored in the MS SQL Server database
    - MS SQL Server – stores any configuration needed to by the Mule ESB flows
- VistA Service – the adapter used to communicate RTLS COTS software components with existing VA systems:
    - Service Controller – Restful Web Service layer using CXF libraries. This layer provides input validation
    - VistA Business Services – this layer provides a centralized location to house and execute business logic.
    - VistA Client – this layer allows for a generic way to call VistA RPCs using VistA-Link
    - VistA-Link Adapter - provides communication between the JVM and the VistA/M servers
- VistA (not part of VistA-Service) – uses the HWSC to make Restful Web Service call to Mule ESB endpoints.

Figure 62: VistA-Service Architecture



RTLS will deploy a clustered VistA-Service instance in the NDC. This clustered instance will be used to interface RTLS COTS products with VA owned systems, services, and applications.

6.2.2.3.1.1 Data Flow

From Mule ESB

Messages will flow from the Mule ESB to the Service Controller in the VistA-Service over HTTPS. The Service Controller will call the VistA Business Services to execute any business rules on the inputted message. If the business rules are verified, the message will flow to the VistA Client which will call the VistA-Link Adapter. The messages will flow from the VistA-Link Adapter to the VistA-Link Listener over TCP/IP. The VistA-Link Listener will in turn execute the desired RPC, which will result in the procedure code in the routine being executed. The RPC will assembly the results and pass it back to the Adapter via the Listener.

The Mule ESB will make Restful Web Service calls over HTTPS to the Service Layer with in the RTLS Interface Admin component. The Service Layer will call the MS SQL Server database using JDBC.

To Mule ESB

The RTLS System will utilize HWSC to make Service (Endpoints) calls from VistA to the ESB. Additional information on HWSC can be found here.

The Quartz Scheduler in the RTLS Interface Admin Component will make Restful Web Service calls over HTTPS to execute a Mule flow.

User Interface

The User Interface with the RTLS Interface Admin Component will make a standard Java method call to the Quartz Scheduling component to provide on-demand job execution. In addition, the User Interface will call the MS SQL Server database using JDBC.

6.2.2.3.1.2 Security

Communications to and from the RTLS Interface Admin component and VistA-Service are secured using FIPS-140.2 compliant HTTPS transport.

Communication between VistA-Link Adapter and VistA-Link Listener is secured using the standard VistA-Link J2EE Security model. The RTLS solution will use an Application Proxy User.

HWSC http connections can be secured with SSL/TLS. Doing so makes those connections much more secure, by encrypting the authentication handshake as well as the message contents. SSL/TLS is not currently supported on OpenVMS systems due to a memory leak issue that has been diagnosed as an issue with a VMS-level library. In addition, HWSC supports two authentication mechanisms:

- HTTP Basic authentication
- Certificate-based authentication

6.2.3 Supply Management

Part of the VA's National RTLS is the tracking and managing of supplies within the facility Cardiac Catheterization labs, Electrophysiology Labs (EP), and any other locations where hospital supply management is needed. The VA RTLS system will use technology from WaveMark to accomplish this. WaveMark is a complete supply chain solution including both software and hardware. Using RFID, barcoding, and network technology, WaveMark will provide integration into legacy VA systems and enable hospitals to accurately manage supply levels, monitor expired products, and track products.

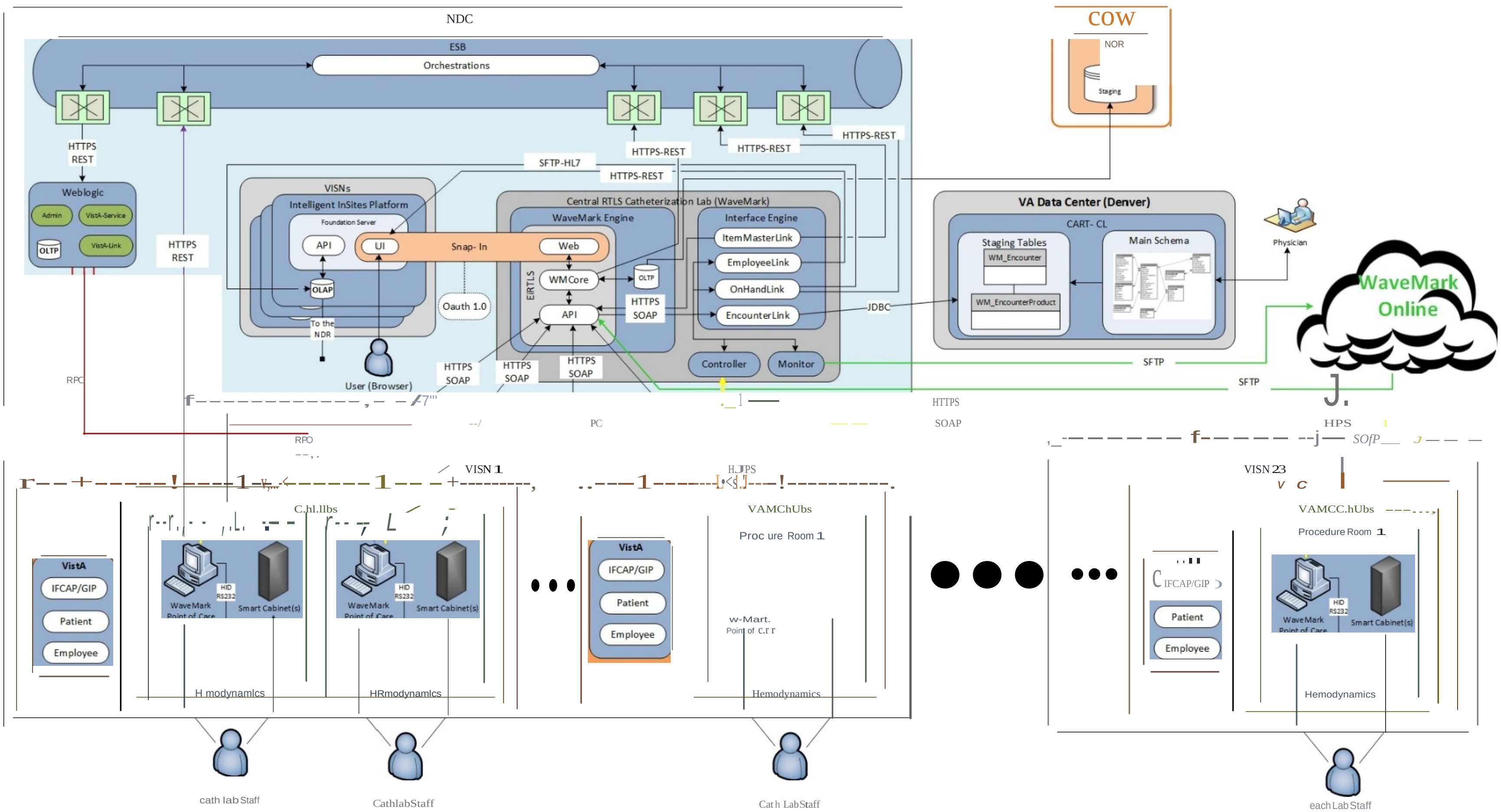
The central part of WaveMark's solution is the WaveMark's Supplies Management Software also referred to as Enterprise Inventory Real Time Location System (EiRTLS). EiRTLS is software for the management of hospital inventory and supplies using RFID. EiRTLS collects information from WaveMark's RFID Smart Cabinets, Point of Use Stations, and various other data collection devices, and aggregates them to an enterprise visibility layer that allows for the efficient management of supplies in hospitals and other healthcare providers.

WaveMark bridges the gap between medical device manufacturers and hospitals to provide true Enterprise Visibility to optimize workflow and the supply chain. WaveMark EiRTLS provides the following features:

- Track - the movement of all consumable assets.
- Alert - Staff of low supply levels, upcoming expiration dates and recalled products.
- Manage - all consumable assets throughout the hospital.
- Integrate - consumable asset information into clinical systems, like billing, Electronic Medical Record (EMR), Medicaid Management Information Systems (MMIS), Enterprise Resource Planning (ERP) and other hospital information systems.

The RTLS solution will use RFID-enabled smart cabinets, with fully integrated exciters and readers, in the designated rooms for storage of high-value products. The cabinets report their inventory of consumables or implantable devices through the hospital network every 20 minutes. When an item is taken from an RFID-enabled smart cabinet, it is automatically noted as removed from inventory with time stamp. When the tagged item is used, it is waved at the Point of Service Station (XPOS) in the room, and this completes the inventory transaction for this item, sending the item into the clinical documentation system in a hands-free manner. Any items that are removed from the cabinet but not waved are considered “Missing.” When they are placed back on the shelf, they are read back into inventory. Placing items back on the shelves reduces loss and shrinkage and improves patient documentation and charge capture. The figure below shows architecture of the WaveMark system within a Cardiac-Catheterization Lab setting and how it integrates into the existing VA systems such as VistA and CART-CL. The WaveMark system will also interface with the NDR. The WaveMark system will send raw supply data to the NDR, where it will be used for reporting and analytical purposes

Figure 63: RTLS Catheterization Lab Architecture



The WaveMark solution will be discussed in more detail in the following sections. The sections have been broken down into the following:

- Local Facility RTLS Supply Management
- National RTLS Supply Management

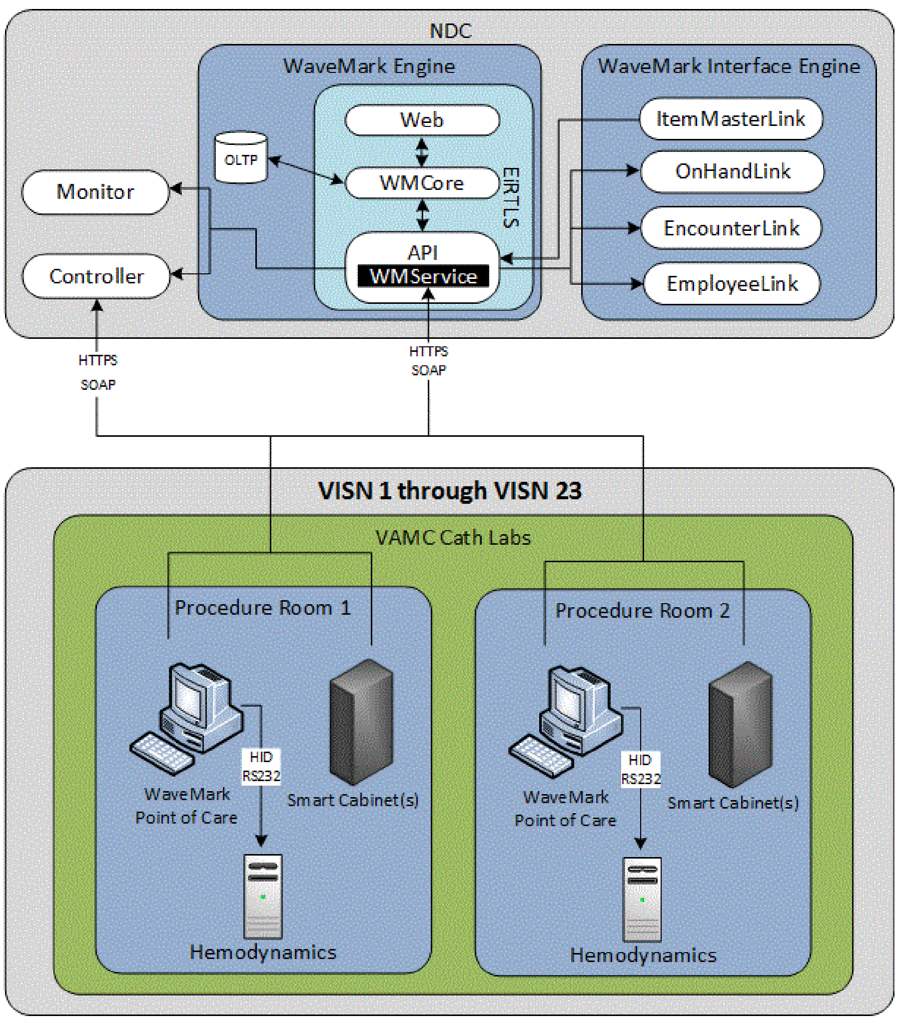
6.2.3.1 Local Facility RTLS Supply Management

RTLS will allow for supplies to be managed at the local facilities such as a VAMC. The local facility level RTLS Supply Management will consist of three parts:

- Smart Cabinets
- Point of Care
- Integration to Existing Hemodynamic Systems

The figure below shows the architecture on how supplies will be managed in a VAMC's Catheterization Lab using RTLS. All 23 VISNs local facilities (VAMCs Catheterization Lab Procedure Rooms) will report to one central WaveMark Engine.

Figure 64: Local to Central Catheterization Lab Architecture



6.2.3.1.1 Smart Cabinets

WaveMark's RFID Smart Cabinets will be installed the local facility VAMC level. The Smart Cabinets allow real time tracking of hospital inventory. Smart Cabinets allow for full visibility into their entire inventory without having to do physical counts. This enables alerts for expired, recalled, or missing products. Cabinets can be configured with a combination of regular boxed product storage shelves, hanging product storage, doors, drawers, and splitter shelves as needed to effectively store and track supplies. This level of storage flexibility supports a clinical workflow and addresses the challenge of space limitations in busy procedural areas. Using stationary and mobile smart cabinets with 13.56 MHz RFID-enabled technology and tagged medical supplies placed in the cabinets, high-cost physician preference items are counted every 20 minutes.

Cabinet features include:

- Automated continuous inventory reads
- A wide range of cabinet models and form factors to hold various product shapes and sizes
- Cabinet availability with and without access doors
- Plug-and-play installation
- Compliance with regulatory and safety standards:
    - FCC
    - Underwriters Laboratories (UL)
    - Conformité Européenne (CE)
    - Ion Chromatography (IC)
    - ISO 60601 and 60950
    - Office of Statewide Health Planning and Development (OSHPD)

6.2.3.1.1.1 Data Flow

The Smart Cabinets will report inventory every 20 minutes. When it is time for an inventory report, the data will flow from the Smart Cabinets to the WaveMark Engine via a SOAP Message. As part of the WaveMark product suite, a monitor system is built in to check the health of the cabinets. This is done using SOAP messages. Network bandwidth is very small; each cabinet sends out approximately 100kb per day.

6.2.3.1.1.2 Interfaces

The Smart cabinets provide an interface to the WaveMark Engine system and monitor system. This interface passes data using SOAP Web Services. The interface between the cabinet and the Engine is called WMService and the interface between the cabinet and the Monitor is called ControllerService

6.2.3.1.1.3 Security

The interface between the Smart cabinet and E-RTLS system uses HTTPS. In addition to the HTTPS, each cabinet is required to send an ID and a unique identifier that is assigned to that device. If the cabinet identifier pair don't match then it is unauthenticated and doesn't transmit any data. All data sent from cabinets is encrypted using secure sockets layer (SSL), and all passwords are hashed in the WaveMark Database using SHA-2 (Secure Hash Algorithm). The HIPAA-related data is encrypted.

6.2.3.1.2 Point of Care

WaveMark's Point of Use Stations provides users with the ability to quickly and accurately capture product usage with the wave of the hand. The Point of Use Stations will be deployed onsite at the local VAMC facilities. The Point of Use Stations manages patient encounters within the Cardiac-Catheterization and EP labs. An encounter is considered to be clinical procedure where supplies are managed by WaveMark. WaveMark's Point of Use Stations feature set includes:

- Alerts for expired and recalled products
- Direct plug-and-play interface to clinical documentation systems
- Easy to use touch screen
- Ergonomic and attractive design

6.2.3.1.2.1 Data Flow

As the patient encounter is in process, supplies (data) will be scanned by the RFID reader and stored in the Point of Care system. When the encounter (procedure) has ended, the data will be sent to the WaveMark EiRTLS via a SOAP Message. When Volcano IVUS Ultrasound 7778 is present the xPOS will send a message to the cabinets to "pause" the RFID reads. A message is sent from the XPOS to the cabinets, and then an acknowledgement is sent back to the xPOS.

6.2.3.1.2.2 Interfaces

The Point of Care Stations provides an interface to the WaveMark EiRTLS system. This interface passes data using SOAP Web Services. The interface between the Point of Care and the EiRTLS is called WMService.

6.2.3.1.2.3 Security

The interface between the Point of Care and EiRTLS system uses HTTPS. In addition to the HTTPS, each Point of Care is required to send an ID and a unique identifier that is assigned to that device. If the Point of Care identifier pair don't match then it is unauthenticated and transmit any data. All data sent from the Point of Care systems, and to/from a browser is encrypted using secure sockets layer (SSL), and all passwords are encrypted in the WaveMark Database using SHA-2. The HIPAA-related data is encrypted.

6.2.3.1.2.4 Interface to Patient

To ensure patient safety, the WaveMark Point of Care Station will associate the patient and procedure information with the supplies used for patient care. A uni-directional interface between the WaveMark Point of Care Station and the VistA Patient file will exist. This allows for VA staff members to provide a level of accuracy to ensure the patient is positively identified during a procedure.   The WaveMark Point of Care Stations will use the Patient file to do a lookup of patient name by providing the patient's unique identifier which is scanned from the patient wristband. The figure below shows how the local facility Point of Care Stations will contact an endpoint on the Mule ESB to retrieve Patient information from the VistA Patient file. More detailed information pertaining to the Patient Interface can be found under the Interface Section in section 6.2.6

Figure 65: WaveMark to Patient Interface

Integration to Existing Hemodynamics Systems

Hemodynamic monitoring systems (HD) are used extensively throughout VA within Cardiac Catheterization Labs for workflow monitoring, recording physiological data and notes during procedures, storing data and generating reports. With the introduction of RTLS, supplies used on a patient during a Cardiac Catheterization Lab procedure will now be automatically tracked. An interface between the RTLS system (WaveMark Point of Care) and the existing hemodynamic monitoring systems VA owns, to enable the automated download of data from the RTLS to these hemodynamic systems.

Once products are used at the XPOS, the information about the used products will also be populated in the hemodynamic system via an interface between the XPOS and the hemodynamic system. The interface is called BarcodeConnect. With one wave of the product, both the WaveMark system and hemodynamic system are populated with the product information.

WaveMark BarcodeConnect is a physical USB or RS232 connection that allows the WaveMark XPOS to transmit product barcodes and other data to the connected hemodynamic (HD) system. The WaveMark XPOS emulates the HD system's standard barcode reader's output. The barcode emulation allows WaveMark BarcodeConnect to automate certain, previously manual keystrokes, improving staff workflow and scanning accuracy.

WaveMark BarcodeConnect works in parallel with the barcode scanners provided by the Hemodynamics system vendor. The diagrams below show the cable/connection configuration for both RS232 and USB (HID).

Figure 66: Point of Care RS232 Connection

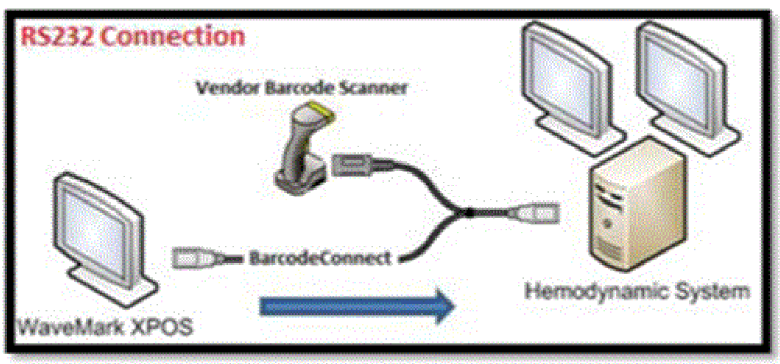
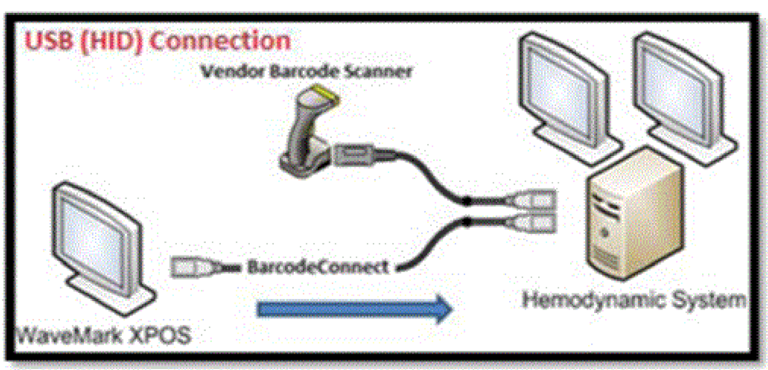


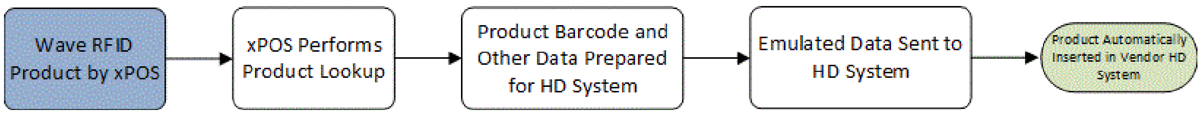
Figure 67: Point of Care HID Connection



In addition to the barcode emulation, WaveMark BarcodeConnect can also be configured to send additional product data, including lot numbers, serial numbers and expiration date, as well as certain keystrokes.

The flowchart below outlines the data flow of the solution. The end user simply waves the WaveMark tracked RFID tag by the XPOS reader and the data is prepared and sent to the vendor HD system.

Figure 68: Hemodynamics Flowchart



The xPOS will work with the following Hemodynamic Systems

Table 32: Hemodynamics Vendors

Hemodynamics System	Compatible Version(s)	Connection Type
GE Mac-Lab/CardioLab	6.8 or newer	USB (HID)
McKesson Horizon Cardiology	12.x or newer	RS232
Merge – Camtronics PhysioLab	Most versions	RS232
Merge – Heartsuite Hemo	7.x or newer	RS232
Philips WITT CALYSTO	Most versions	USB (HID)
Philips XPER	Most versions	USB (HID)
Siemens Axiom Sensis XP	VC03F or newer	RS232

6.2.3.2 **National RTLS Supply Management**

The National RTLS Supply Management component will be part of the NDC deployment model. The National level Supply Management Component is the parent to all the local facility level RTLS supply management components. The National RTLS Supply Management component will consist of the WaveMark Engine and its integrations to CART-CL, to the Intelligent InSites Platform, and to the VistA System (IFCAP/GIP and Employee Modules)

6.2.3.2.1 WaveMark Components

Software installed at the VISN Computer Room by WaveMark will consist of four components:

- WaveMark Engine
- Interface Engine
- Controller
- Monitor

WaveMark Engine Server

WaveMark Engine is the core WaveMark platform software that provides the backbone infrastructure required for running WaveMark Enterprise Inventory Real Time Location System (EiRTLS). The WaveMark Engine is a J2EE application built on top of WebLogic 11g and Oracle 11g database software. The engine consists of an Oracle Database and a software component called EiRTLS. WaveMark EiRTLS is a consumable supply inventory management and analytics application. This software application interfaces with WaveMark SmartCabinets and Point of Care stations (XPOS) to collect on hand inventory and product usage information. EiRTLS also provides a web application reporting framework that presents the user with alerts, inventory management reports and tools, graphical analytics, and utilities allowing end users to register and manage RFID tagged products. EiRTLS's additional features include:

- An advanced alert-driven mechanism for the management of supplies
- Support for a variety of mobile devices including iPad and iPhone
- Easy to use and intuitive user interface

The EiRTLS component consists of three main components

- Web - provides a graphical web based user interface for authorized and authenticated users to manage inventory levels.
- WMCore – the main piece of the software that is responsible for running business rules and managing the service calls to the Oracle database.
- API – exposes Web based APIs to WaveMark components such as Smart Cabinets and Point of Care Stations.

WaveMark Interface Server

WaveMark Interface Engine is a sophisticated interface software platform that provides the capability for scheduling and running data interfaces, called Links, between WaveMark EiRTLS software and non-WaveMark systems. The Interface Engine provides the capability to schedule and manage interface jobs, configure interface parameters, and view errors and the current status of scheduled interface jobs.

WaveMark Controller Server

WaveMark Controller is software that provides the capability to monitor and manage the WaveMark data collection devices (e.g. SmartCabinets and XPOS). This software provides the ability to monitor the hardware and software, perform remote commands and firmware upgrades, and report on device status and errors of the data collection devices.

WaveMark Monitor Server

WaveMark Monitor is software that provides the capability for monitoring the health of the EiRTLS software. The Monitor aggregates data from multiple sources to provide operational and trend reports that provide insight into system performance, system errors, and usage.

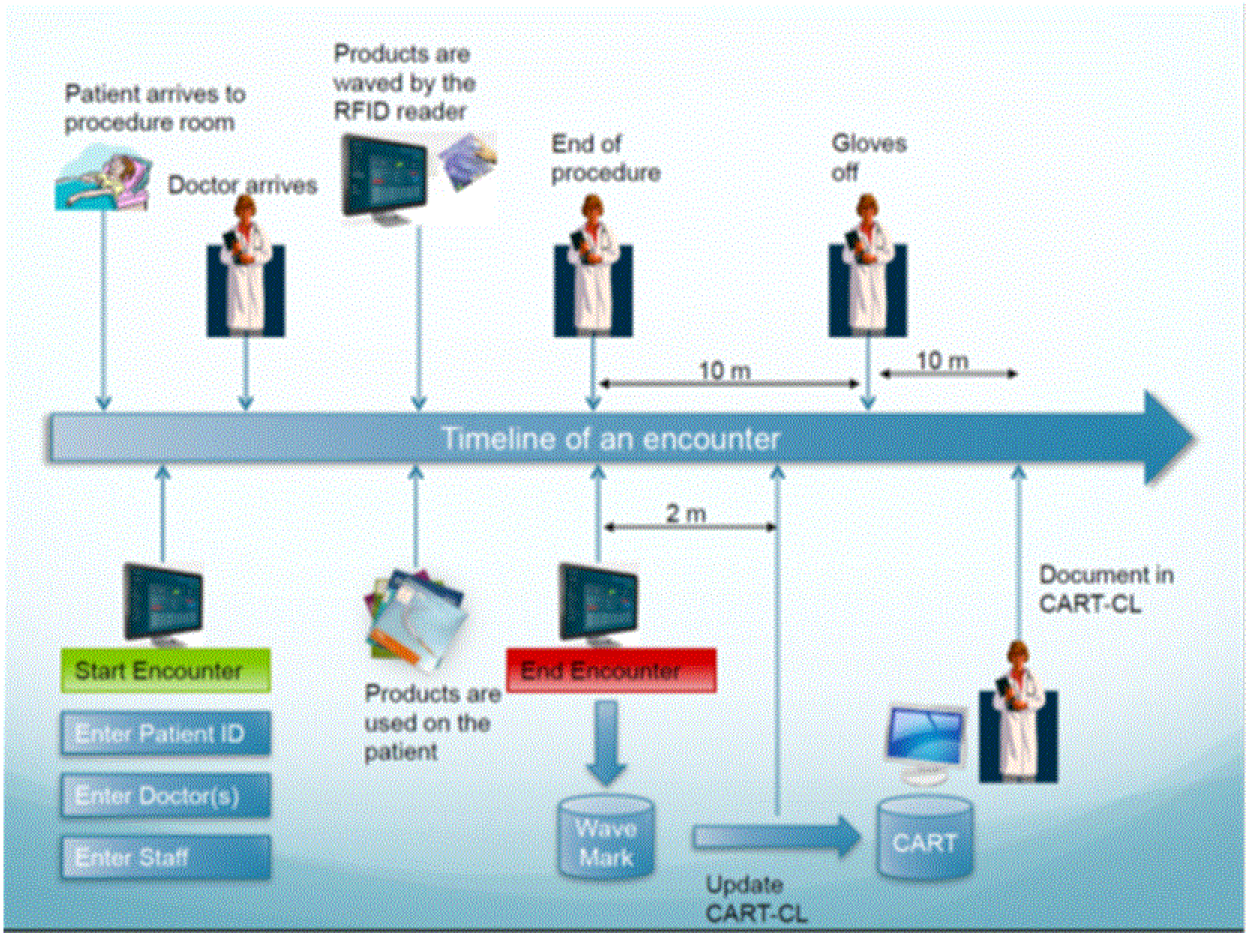
6.2.3.2.2 Interfaces and Integrations

6.2.3.2.2.1 Interface to CART-CL

The Cardiovascular Assessment Reporting and Tracking system for Catheterization Labs (CART-CL) is a VHA developed software application for standardized data capture and report generation, national SQL data repository, and national quality improvement program for VA Catheterization labs. The application is integrated with VA's Computerized Patient Record System and Electronic Health Record system enabling providers to document care as part of routine clinical work. The CART-CL application provides discrete data entry (based on American College of Cardiology standards) with narrative text for customization. All CART-CL data is stored in a single national repository. Predefined data entry fields will be sent from the RTLS enabled smart cabinets to prepopulate a patient procedure report. The information required is identifiable from the Catheterization lab item consumables and devices used during the case and patient information.

The following figure shows the Timeline for an encounter in the Catheterization Lab.

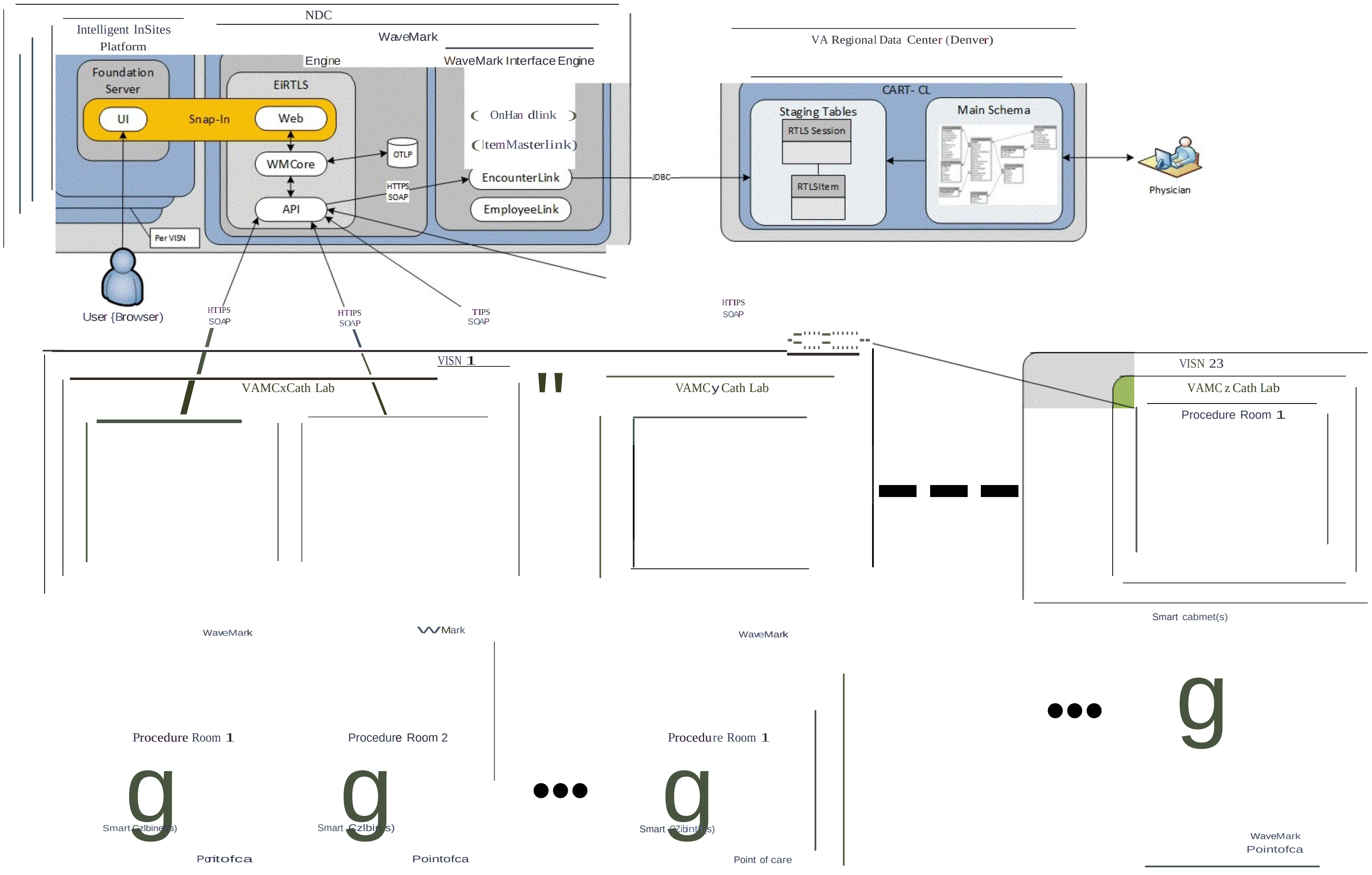
Figure 69: Catheterization Lab Timeline Encounter



As an encounter has ended the data from the Point of Care system is sent to the WaveMark Engine. The Data will be stored in the WaveMark database and sent to CART-CL via a Java Database Connectivity (JDBC) mechanism located in the WaveMark Interface Engine.

The following figure shows the interface between WaveMark and CART-CL.

Figure 70: WaveMark to CART-CL Interface



6.2.3.2.2.2 Interface to IFCAP/GIP

The use of inventory in the Medical Centers will need to be updated in the VA's existing legacy systems (IFCAP/GIP). The figure below shows the integration points for Items on Hand and Master Item inventory interfaces.

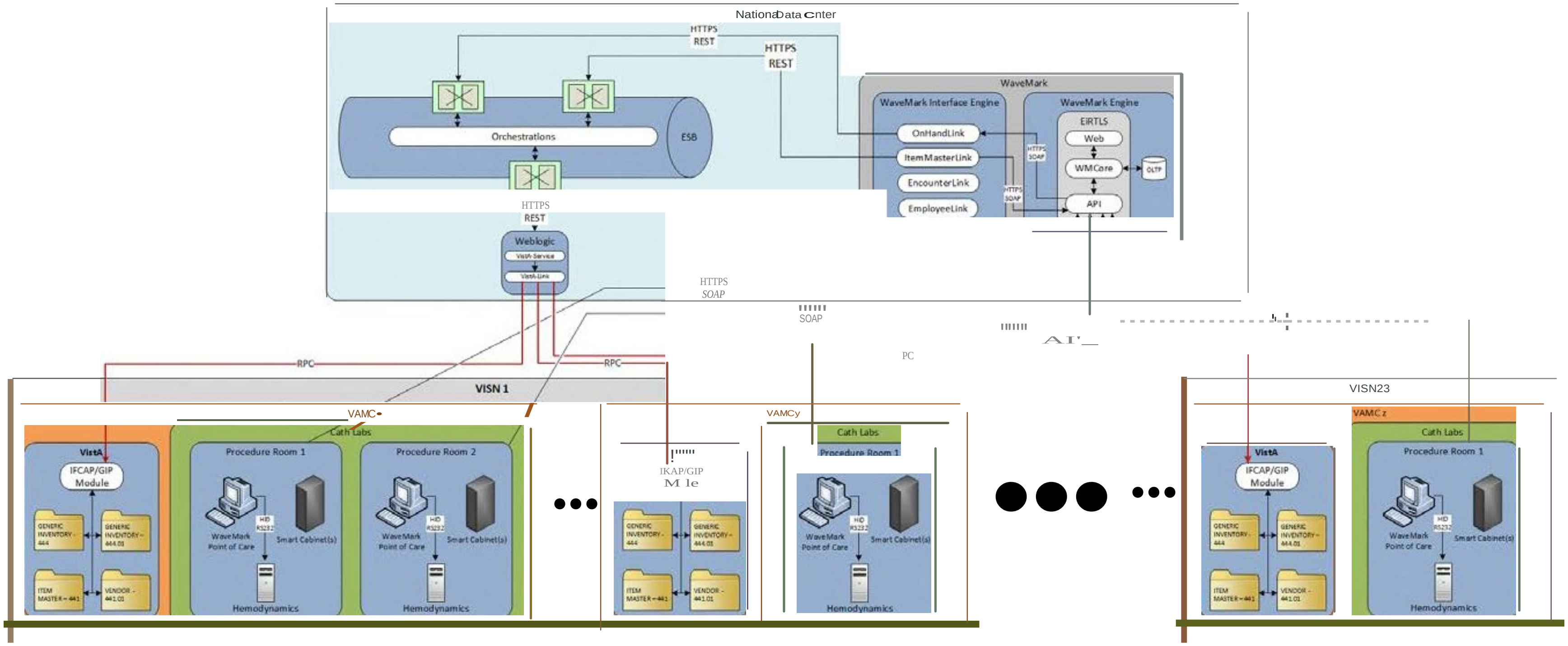
Item on Hand

As supplies are used or added in the Medical Centers, the inventory count will be sent to the central instance of the WaveMark Engine. The WaveMark Engine on a scheduled basis will create a HTTPS request that contains a XML message to be sent to the Mule ESB via a RESTful Web Service. The ESB will transform the XML Message to a desired message and send the message to the VistA-Service (housed in WebLogic) interface which in turns sends the request to the VistA IFCAP/GIP routine via VistA-Link through a RPC innovation.

Master Item

If a new item has been added to IFCAP/GIP or if an item's meta-data has changed (I.E: the category of an inputted item has changed) within IFCAP/GIP, this data needs to be reflected in the WaveMark Engine/Database. A scheduled process within WaveMark will make a RESTful web service call over HTTPS to the Mule ESB to obtain this data. Once the Mule ESB receives this request, the Mule ESB will make a call to the VistA-Service interface (housed in a WebLogic instance) to pull data from VistA's IFCAP/GIP via an RPC innovation (VistA-Link). The data is then formatted into XML and sent back in a response to the WaveMark engine. The WaveMark Engine will process the XML response into the WaveMark Engine/Database.

Figure 71: WaveMark to IFCAP-GIP Interface

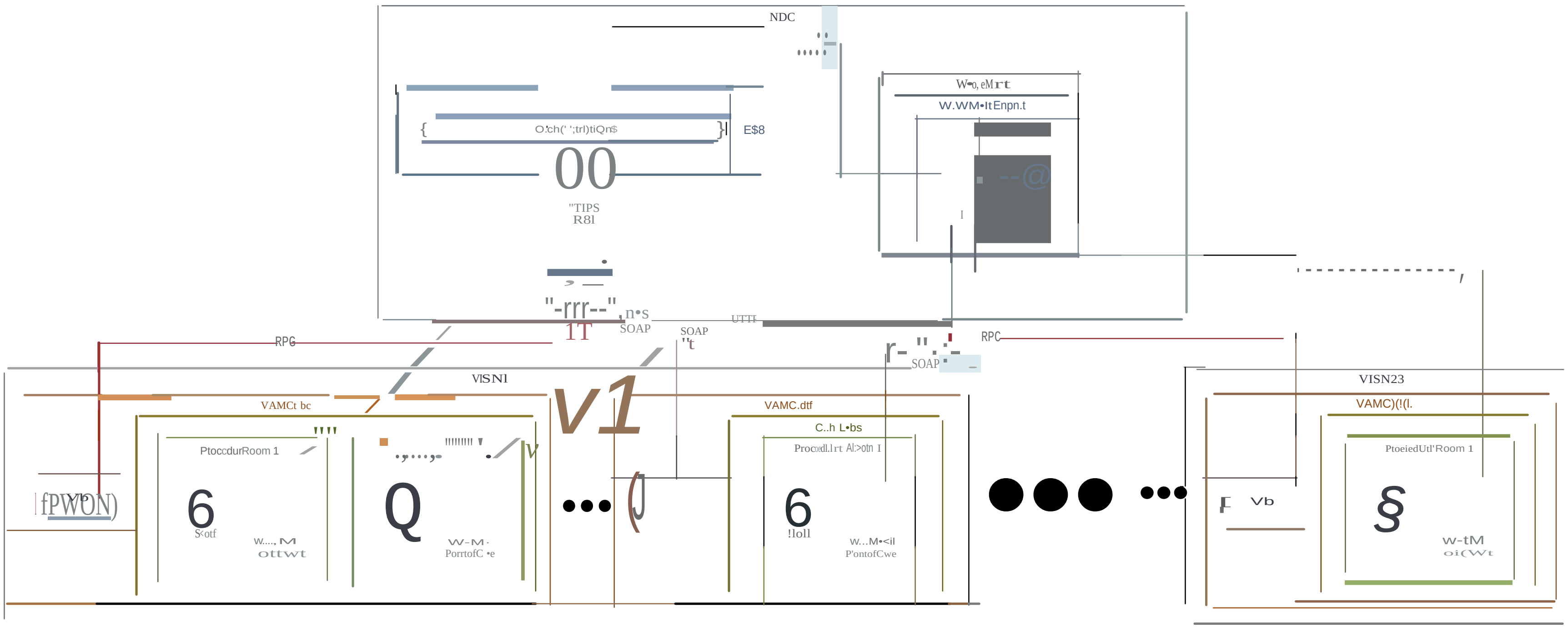


6.2.3.2.2.3 Interface to Employee

As part of the goal of improving employee identity verification for VA healthcare, the joint commission recommends positively identifying the employee. The accurate identification of employee is improved by using a unique identifier IEN (Internal Entry Number). The real time lookup of the employee information that is relevant to the process is retrieved and displayed for the clinician to confirm through WaveMark Point of Care Station (XPOS). Employee registrations are captured in the NEW PERSON file which is part of the VistA Registration package. The NEW PERSON file is the VistA system of record for providing employee information for identification purposes.

The staff members are present in the Medical Centers' Catheterization Labs during procedures. The staff members including physicians will be recorded in the Point of Care Solution. The Point of Care station downloads a list of staff members from the Central RTLS Catheterization Lab System (WaveMark Engine). Sometimes, a staff member is not in the Point of Care station (I.E: new hire or visiting doctor). In this case (Cath Lab Staff Event), an administrator will log into the WaveMark Web Application. The WaveMark Web Application will contact the VistA Person file via the ESB and VistA-Service components. The figure below shows the integration points for Employee Search:

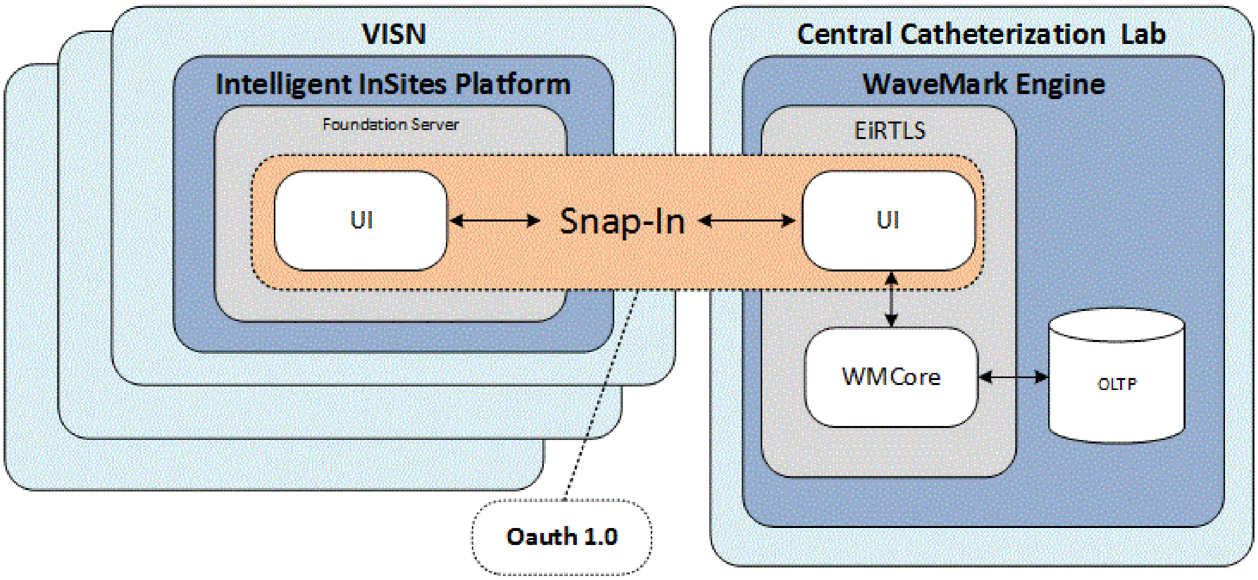
Figure 72: WaveMark to Employee Interface



6.2.3.2.2.4 Integration to Intelligent InSites

The WaveMark User Interface will be accessed through Intelligent InSites with single sign-on support for user authentication. The EiRTLS web component will be a Snap-In to the Unified User Interface (Intelligent InSites Platform). The Snap-In framework provides a standard way to extend the functionality of the User Interface within the Intelligent InSites Platform. The figure below shows how the WaveMark EiRTLS snaps into the Intelligent InSites Platform.

Figure 73: RTLS Supply Management User Interface Architecture

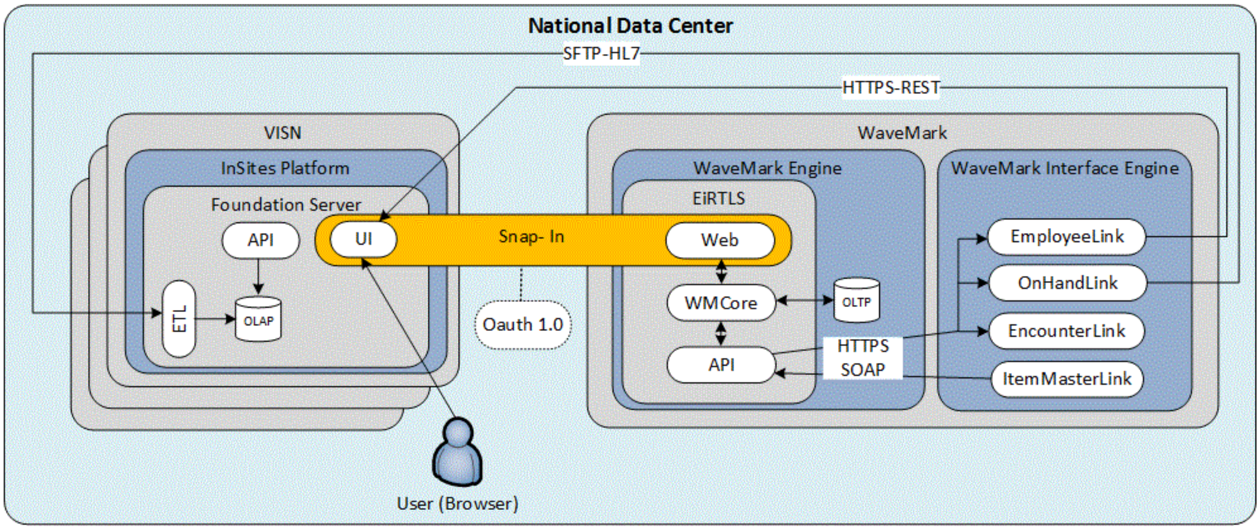


In addition to the snap-in, the WaveMark solution will integrate with the Intelligent InSites solution through a variety of interfaces. The table and figure below shows the integration points.

Table 33: WaveMark and Intelligent InSites Integration

Interface Name	Data Direction	Protocol/Message	Description
EmployeeLink	Intelligent InSites to WaveMark	HTTPS- Restful Web Service (JSON)	WaveMark calls web service to get a listing of active users (userid, first and last name, email, list of departments). This listing is used to create the user in the WaveMark system and allow access to the WaveMark portal via the Intelligent InSites snap-in.
WaveMark SSO	Intelligent InSites to WaveMark	OAuth 1.0	Single sign on for the UI snap-in.
OnHandLink	WaveMark to Intelligent InSites	SFTP/HL7 message	Provides supply level inventory data to Intelligent InSites.

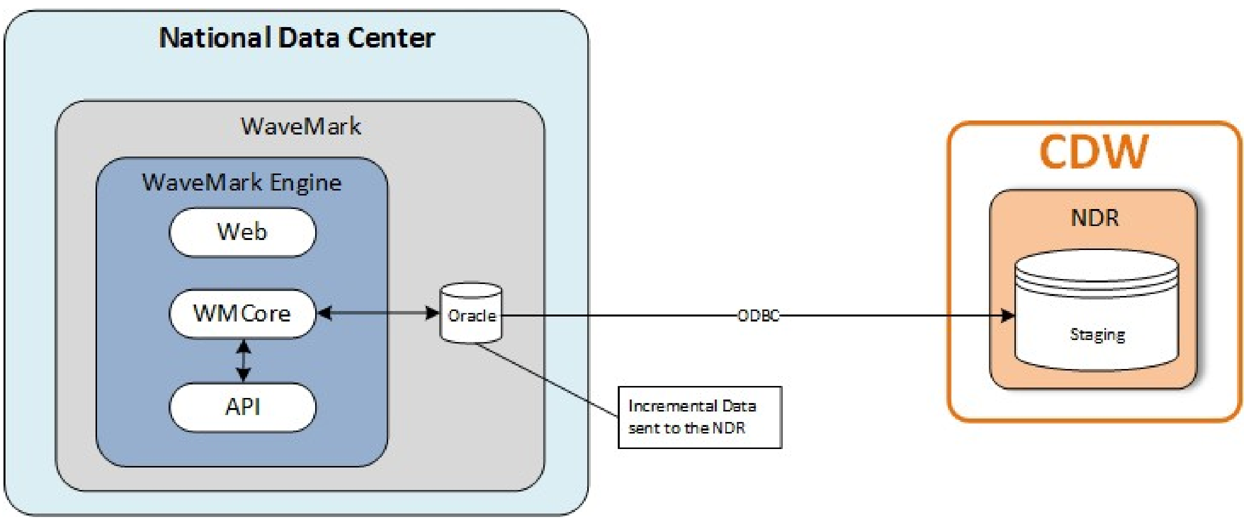
Figure 74: WaveMark - Intelligent InSites Integrations



6.2.3.2.2.5 Interface to NDR

The WaveMark EiRTLS will interface with the NDR Staging Database that is located in the CDW. The NDR ETL platform will extract the incremental data (data that has been inserted, updated, or deleted during a specific time period) from WaveMark and load it into the NDR staging database. The NDR ETL platform will extract the incremental data using ODBC.

Figure 75: WaveMark to NDR Interface



6.2.4 Information Platforms

This section will discuss the platforms used to get information to users and consumers. In addition, this section will discuss the underlying RTLS Data Model (RDM).

6.2.4.1 Intelligent InSites Foundation

The Intelligent InSites Foundation server is part of the overall Intelligent InSites Platform. The Intelligent InSites Platform also contains the Intelligent InSites Business Intelligence component (see section 6.2 – Analytical Platforms for more information). The Intelligent InSites Platform will be deployed on one per VISN/Central CMOP basis.

The Intelligent InSites Foundation server provides real-time visibility and services to asset and workflow management, environmental monitoring, and staff and patient safety. The Foundation Server consists of the following Components:

- Distributed Services – services that are exposed data consumers external to the platform. The Distributed Service components consists of:
    - User Interface – is a web-based User Interface that allows for users to view locations and monitors among other administrative tasks.
    - API Services – is a REST based API that provides interfaces that handles the creation, retrieval, and updating of RTLS data.
- Centralized Services – these services are encapsulated from the public APIs and only consumable by the distributed services. The Centralized Service components consists of:
    - CEP (Complex Event Processing)/Rules Engine - handles the business rules and complex events that need processing.
    - Queuing Services – queuing mechanism to ensure persistence to the database.
    - Scheduling Services - a configurable periodic scheduling mechanism.

The following figure shows the Intelligent InSites Foundation Architecture and how it integrates with web browsers and the Intelligent InSites Connector Framework.

Figure 76: Intelligent InSites Foundation Architecture

6.2.4.1.1 Snap-In Framework

The Snap-in Framework is an application framework which allows for the development of snap-in applications. It provides a set of APIs upon which custom web services can be built, and the execution environment required to run them. The Framework defines what can be bundled into a snap-in, and provides a mechanism to extend the Intelligent InSites Web UI and data model. A snap-in is a deployable bundle of code, static web resources, and configuration instructions which can be deployed onto the platform to facilitate data flow between the platform and external systems, augment the Intelligent InSites Web UI, and extend the Intelligent InSites data model. Snap-ins can be developed on any computer with some basic tools, and deployed onto the platform using the snap-in compiler.

The Snap-In provides the following features:

- Create tabs and sub-tabs within the Intelligent InSites User Interface
- Tunnel web applications into the Intelligent InSites User Interface through an iFrame
- Write server-side code in the form of Ruby scripts exposed as web services
- Add custom attributes to existing web resources
- Validate, compile, and quickly deploy snap-ins on the fly

6.2.4.1.2 Unified RTLS User Interface

A large part of the RTLS system is the Unified User Interface. The Unified User Interface is a single sign on portal to all the products and applications that make up the enterprise RTLS System. The Unified User Interface provides VAMCs, CBOCs, and CMOPs users the ability to more effectively manage their processes at a local and VISN aspect through a single unified view of data from multiple databases. The data is accessible through a user interface for real-time status and reporting through data analysis tools. A snapshot of the user interface with map view is shown the figure below.

Figure 77: Unified View of Data

The RTLS System includes the user interface capabilities and reporting capabilities, and is compliant with the user access requirements detailed in the following table.

Table 34: User Interface Capabilities

User Interface Capabilities	
Graphical and Tabular Views	The application has a robust map view mode, which can display all items (whether of type equipment, supply, patient, or staff) in their appropriate locations on the map at the same time, automatically updated each time a location movement happens. Users can limit the display on the map to only certain classes of items or items based upon a search term (such as pump or id). The RTLS System software allows for configuration tabular views showing information about a device – such as equipment name, type, status, locations, asset make and model, EE number, usage, and preventative maintenance status. Users see only those applications and data that they are entitled to view from their security roles. Each view is automatically refreshed and can be filtered (data seen) and configured (columns displayed and sorted) to meet the user's specific need at that time.
Real Time Location	The RTLS System suite collects data on tagged items including people, assets, supplies, specimens, and implants and reports in real time via a web-based interface with minimal latency, well below VA threshold of less than 15 seconds after beacon pulse in streaming mode. The RTLS system also has a batch mode which has periodic synchronization schedule. The batch mode will show real time location 15 seconds after the batch mode processing has completed.
Queries	Users can filter their searches for items by location in the hierarchy (VISN level down to sub-room level) or type, status, or key word. Results can be displayed on a list or map view. Search returns can be sorted across multiple fields, including time in location, service status, model number, and utilization. Filters and sorting is built into the application, without the need to write separate queries. A wide range of reports, including location history, average utilization, status history, alert history, and proximity history are available. This solution supports VA requirements for one/two click access to identify availability assets.
Service Alerting	All types of tags (Assets, Supplies, and Sensory) tracked by RTLS System will have configurable statuses appropriate to that type. The status will be changed automatically by the rules engine whenever a configured event occurs. Changes in status can generate alerts or other notifications and can be searchable based on a particular status such as recall or due for service.
Staff Panic	Each button on a tag can be programmed to have different meaning by the Intelligent InSites rules engine. Based on the

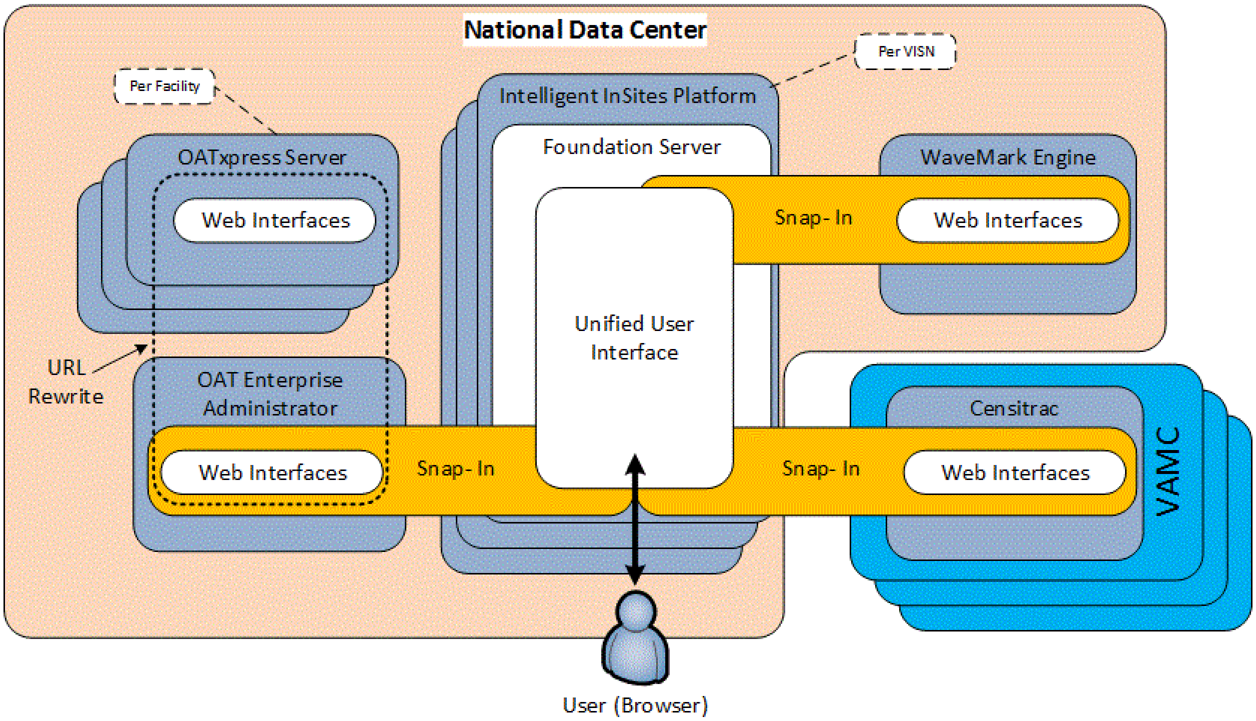
Button Alerting	button pressed, different events can fire from the rules engine, such as alerts or status changes. For example, alerts sent as a result of a panic button press will include the time, the name of the associated staff member, the location of the alert, and the location of the staff member.
Static Position Reporting	The architecture of the platform enables managing RTLS data at multiple levels, in a federated model, through a nine-level location hierarchy. Data is assigned at the lowest level (sub-room) and aggregated up the hierarchy. A user can view on a map or in list view the time a tagged item has been in a location without moving and can generate reports with this data.
Par Level Configuration	The Intelligent InSites Platform allows for staff to configure par levels for rooms and establish rules for alert generation as thresholds are surpassed or about to be met. Staff can obtain alerts, messages, and notifications through the integration of communication devices (in other words, email, pagers, Smartphones, wireless PDAs, and IP phones or a unified facility communication system).
Alert on Non-Reporting Tags	The Intelligent InSites system has a complex event processing engine (rules engine) that listens for configured events (such as location, button presses, and so forth) and generates resulting actions, such as alerts, tasks, messages, status changes, and context modifications. If a tagged item passes through an egress point or has not been detected for a certain amount of time, the RTLS system will recognize that and send an alert, task, or message based on the configuration. Notifications are not limited and can be modified by admin users at any time. The rules can be established on a type or per tag basis allowing staff to configure different alerts for different types of assets.
Asset Detection Across Facilities	Because the Intelligent InSites platform is based on a nine-level location hierarchy with data assigned at the lowest level (room or sub-room) and aggregated for action, viewing, or analysis up the hierarchy from sub-room to room, zone, department, floor, building, campus, or VISN, assets can be detected and viewed across facilities.
Reporting Capabilities	
Reporting	The Intelligent InSites solution provides reporting at VISN and local level views and also allows access to data through the API to use other available reporting systems. Multiple filters within the web-based application allow simple and quick creation of ad hoc report views that can then be easily exported to PDF, Excel, or .csv. Similarly, the Intelligent InSites reporting and Analytics tools allows access to the data, which can also be quickly exported. Users will be trained in ad hoc creation of custom reports and templates. Reports can be generated and modified based on user access level and can be prescheduled and automatically delivered or created on demand. Data intensive reports will have indicators that report generation is in progress. Report layouts can be graphical or list-based and templates can be shared among facilities. Administrative reports include, but are not limited to, Users Logged On, System Health, and Reader Status. The Intelligent InSites solution also provides dozens of additional built-in reports for a variety of use cases.
Workflow Management	The Intelligent InSites Platform contains a location hierarchy that allows rules, workflows, and reports to be run at any level within the hierarchy. The software can be deployed at each facility with nationally defined workflows/alerts, with the ability for each VISN to configure a set of workflows/alerts across the VISN and the ability to customize at the facility level. Access to the capabilities to configure within the administrative area is managed by security roles and can be specific to type of workflow, type of item tracked, and location. Workflows are configured to track an item through a series of pre-defined milestones, some of which can be optional, and to trigger status changes, alerts and notifications, and reports based on those milestones. Milestones can be determined by location of an item, its co-location with other items or people (even if the tag types are different), button presses, or notifications from other systems. Status changes can also be driven from these types of events. Tag assignment is simple and can also be made from other systems – such as the medical record or asset management systems.
Scheduled Maintenance Reporting	All types of tags (Assets, People, Supplies, and Sensory) tracked by the Intelligent InSites platform will have configurable statuses appropriate to that type. The status will be changed automatically by the rules engine whenever a configured event occurs – such as an item becoming due for preventative maintenance. Changes in status can generate alerts or other notifications and can be searchable based on a particular status such as recall or due for service.
User Access Requirements	
Role-based Access	Users access the system through a web interface. Security roles are created for users, providing assigned authorizations to access applications and features of the Intelligent InSites Platform. Users can be restricted to specific application views, as well as restricted to their own facility's data, or they can be provided access to data across the facilities in the VISN. The Intelligent InSites Platform uses a series of enterprise queues and topics to make every user's web session aware of his or her specifically interested location, alerts, messages, and task updates occurring across the distributed system that enables access simultaneously for an unlimited number of users.
Directory Services	VA users can access the web-based Intelligent InSites system with authentication through VA's Active Directory infrastructure, and can be adjusted if needed based on VA directory service needs. The system implements a multi-level role-based authorization scheme. Intelligent InSites Security Roles are used to manage permissions and Intelligent InSites Functional Roles are tied to a user's active directory login in data to manage a user's ability to interact with specific types of data. Security roles are created and assigned certain authorizations and features of the Intelligent InSites Platform. Users can be associated to one or more security roles and granted access to all features that are allowed by the cumulative set of security roles owned.
Role-based Controls	Users can be restricted to specific application views or their own facility's data, or they can be provided access to data across the facilities in the VISN or all of VA. Access levels can be configured from view-only to administrative access based on role-based group privileges only providing access to the information allowed for the group to which they belong.

The Unified User Interface uses the Snap-In feature. The Snap-In framework provides a standard way to extend the functionality of the User Interface within the Intelligent InSites Platform. The user interface is composed of tabs and pages. Pages are areas to display content, while tabs organize related pages into groups. Additional tabs and pages can be added using snap-ins. The tab and page hierarchy, as well as the page content, is defined in snap-in.xml.

Figure 78: User Interface Snap-In

The figure below shows the integration of the Snap-ins on a per VISN/Central CMOP instances. The Intelligent InSites VISN/Central CMOP UI will provide snap-ins to the VISN/Central CMOP OAT Enterprise Administrator, the VISN/Central CMOP WaveMark instance, and the multiple facility (belonging to that VISN) Censis Censitrac

Figure 79: RTLS Snap-In User Interface Architecture



6.2.4.1.3 API

The main communication channel in and out of the Intelligent InSites platform is through the REST API. The API is composed of many web services, each designed to perform operations on resources. The REST API is based on resources. A resource in Intelligent InSites is a collection of data fields. Each resource in Intelligent InSites has a type, some of which represent more concrete objects such as equipment, location, or sensor, while others are more abstract such as functional-role, or location-status-change.

To interact with the REST API, the following parameters can be used:

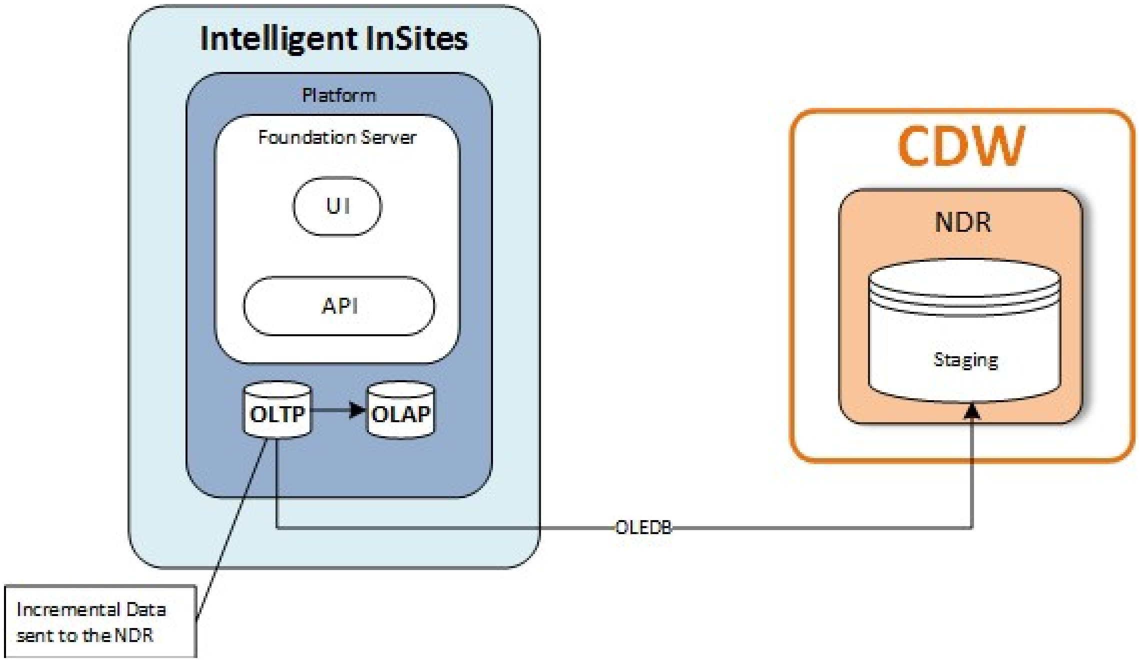
- expand – expand nested elements in a resource response
- select – returns only the designated fields
- sort – sorts the result list returned
- filter – returns results matching the given filter expression
- limit – limits the number of results returned in the list
- first-result – puts the designated result number first in the list of returned values

For a more information on the Intelligent InSites API, please see https://doc.insitescloud.com/4.3/DevDoc/

6.2.4.1.4 Interface to NDR

The Intelligent InSites Platform will interface with the NDR Staging Database that is located in the CDW. The NDR ETL platform will extract the incremental data (data that has been inserted, updated, or deleted during a specific time period) from the Intelligent InSites OLTP and load it into the NDR staging database. The NDR ETL platform will extract the incremental data using OLEDB.

Figure 80: Intelligent InSites to NDR Interface



6.2.4.1.5 Security

The Intelligent InSites Foundation requires HTTPS (in Production environments) and a UID/PWD for any calls to the APIs (these can be supplied via HTTP Basic Authorization), so any communication between Connector Framework and the Platform is handled this way (as well as any communication between any other system such as Mule ESB and the Platform).

6.2.4.2 **RTLS Database Model**

The Common Data Model defined in the VA RTLS ESE PWS will be referred to as the RTLS Data Model (RDM) and it includes all data stores purchased as part of the RTLS System. This RDM provides a data storage container for users to access the data real time through a series of user interfaces and services. The following data stores are part of the RTLS Data Model:

- Intelligent InSites Foundation
- CenTrak GMS
- WaveMark EiRTLS
- Censis Censitrac HL
- OATSystems OATxpress[1]
- OATSystems Enterprise Administrator[2]
- Intelligent InSites Business Intelligence
- Intelligent InSites Censitrac Analytical[3]

---

[1] OATSystem's OATxpress and Enterprise Administrator are exactly the same database schema, just configured and used for different business purposes.

[2] OATSystem's OATxpress and Enterprise Administrator are exactly the same database schema, just configured and used for different business purposes.

- Intelligent InSites WaveMark Analytical[4]

The union of all data store models addresses the RTLS Phase One Applications:

- Asset Tracking
- Cardiac Catheterization Laboratory supply tracking
- Sterile Processing Service (SPS) workflow and medical/surgical instrument tracking
- Temperature Monitoring

The RDM will have a reliable uptime which will be based on VA standards for COOP set by OIT. In addition, OTA will set a plan for maintenance of the servers including the following regularly scheduled tasks: Backups, Re-Indexing, Archiving Processes, and Purge Processes.

For additional information about the RDM, please see the RTLS Enterprise Data Architecture document.

6.2.5 Analytical Platforms

A large part of the RTLS system is the information it provides. The RTLS system will provide the VA with accurate and timely information for local, VISN and national-level reporting, sharing, and decision support. The RTLS System will have two analytical platforms used for Business Intelligence.

6.2.5.1 VISN/CMOP Business Intelligence

The RTLS VISN Level Business Intelligence (BI) solution, which is powered by Pentaho, gives users access to vast amounts of contextual data stored in a VISN-level BI Data Warehouse, allowing users to analyze trends, identify improvement opportunities within the VA, and report on key performance indicators (KPI's). The RTLS VISN Level Business Intelligence (BI) solution is part of the Intelligent InSites Platform. This enables users to gain enterprise-wide visibility into their processes and make a transformational impact on the VA’s performance. With RTLS VISN Level Business Intelligence Component, VA leaders will have access to information that will help them make timely, informed decisions. As a result, VA leaders can deploy resources more efficiently and improve both patient care and financial health.

Here are a couple key features of the RTLS VISN Level Business Intelligence Solution:

- Gain Enterprise-Wide Visibility into the Operations to Improve Performance - With access to data from all of the operational units, users can easily compare KPI's between different departments, across the hospital, or across multiple hospitals throughout the entire organization. Gain insight on what works and what doesn’t so users can apply best practices across the enterprise. Plus, use the flexible and easy-to-use ad hoc reporting capabilities to create custom views containing the specific information you are seeking.
- Monitor Process Changes to Confidently Assess Their Impact - With BI reports, users have data at their fingertips to build business cases for implementing changes in the organization. And, users are able to track changes to quickly learn what worked and what needs further improvement.

---

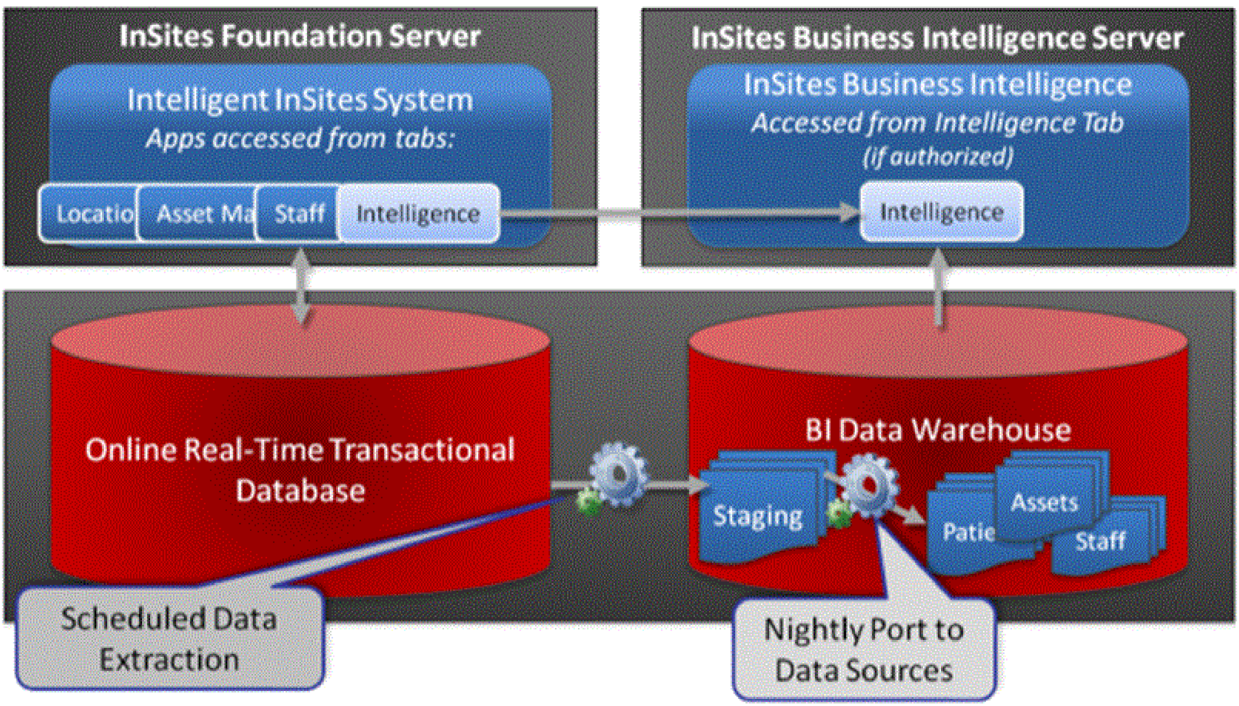
[3] The Intelligent InSites Censitrac Analytical Database sits inside of an Intelligent InSites database called Intelligent InSites Third Party Analytics.

[4] The Intelligent InSites WaveMark Analytical Database sits inside of an Intelligent InSites database called Intelligent InSites Third Party Analytics.

- Get the Information Users Want, When Users Need it, to Make Sound and Timely Decisions - With Business Intelligence, users can view and modify example reports provided by the RTLS system that can help them track and analyze the VA's key performance indicators. Each individual BI user may save frequently used reports as Favorites for easy access. In addition, reports can be scheduled for daily, weekly, monthly, or yearly distribution to selected recipients.

The figure below shows the RTLS VISN Level Business Intelligence Architecture. Throughout the day, data is gathered by the Intelligent InSites Foundation from all the sensory inputs and any integrated third-party application. Data is taken from the Intelligent InSites Online Transactional database on a scheduled time frame (configured to nightly) and placed in a staging area. From the staging area, the data undergoes porting into data sources, sometimes referred to as "cubes." Data sources contain sorted and organized data that speeds the access and processing routines required for advanced reporting and analytics the BI Data Warehouse. Reports are executed against the BI Data Warehouse and accessed through the Intelligent InSites User Interface.

Figure 81: VISN/CMOP Business Intelligence Architecture Overview



The Business Intelligence solution is located on a separate server to ensure data security and optimal performance of both the Business Intelligence and Intelligent InSites solutions. The Intelligence tab appears to those Staff members who are given access when they login to the Unified User Interface.

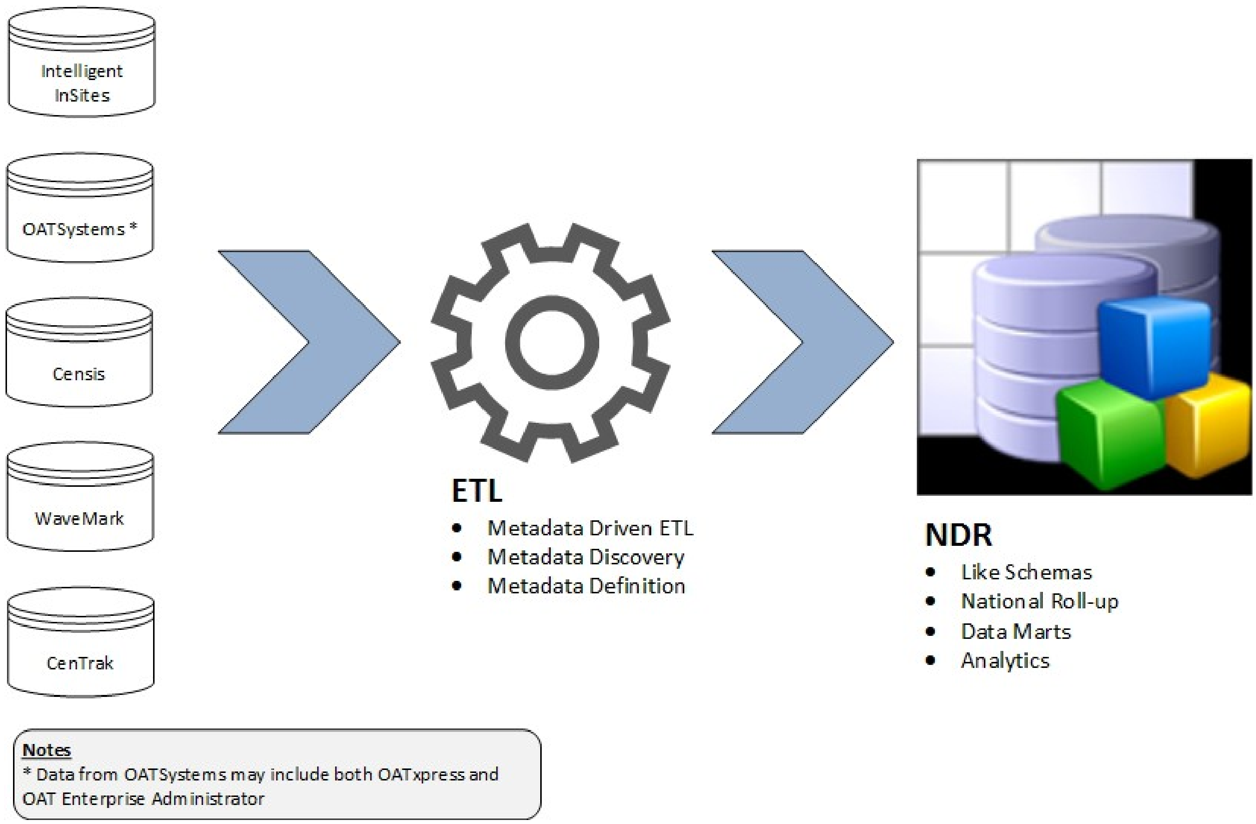
6.2.5.2 National Data Repository (NDR)

The RTLS System includes the implementation of a National Data Repository (NDR) for housing all RTLS data from all RTLS facilities and VISN systems (located at the NDC). The NDR will be built using a flexible and highly scalable architecture. The NDR will have analytic and reporting capabilities for process improvement, business intelligence, and workflow and research analyses. The NDR will provide accurate and timely information for local and national-level reporting, information sharing, and decision support. The NDR will include an aggregation of data from the multiple RTLS source systems that may reside in different physical locations. The end results and goal will be to create analytical data stores and produce KPIs used to enable visibility for the purpose of planning and making strategic business decisions.

The RTLS NDR will reside in VA's existing CDW environment. The NDR will leverage the business intelligence and analytical tools that are available in the CDW. Tool sets from Microsoft and SAS will be used to collect, maintain, and organize data.

Data will be ETL'd from the facility and VISN level source systems (located at the NDC) to the NDR. The following diagram depicts how data will flow from the RTLS source systems to the NDR using a Metadata driven ETL platform.

Figure 82: NDR Data Flow



6.2.5.2.1 Data Modeling Approaches

Building the NDR will employ different data modeling approaches. Unlike transactional systems that are built for a large user base to help manage dynamic data in real-time, the NDR is built to manage extreme data volume, complex and resource intensive queries, and a smaller user base. In data modeling, analytic is the antonym of transactional.

The following data modeling approaches are provided to build a common understanding of the NDR and the framework and methods used in design and development.

- ***Operational Data Store (ODS)—***An ODS removes reporting from the transactional system and has a schema similar to the source system but is tuned and indexed for reporting. An ODS only keeps a short period of history anywhere from 7 to 120 days.

This type of reporting is more for operational management and is limited by its source system.

- ***Data Warehouse (DW)—***A DW is a system used for reporting and data analysis. A DW is often a materialized version of a logical model that represents the whole enterprise. For example, the concept of an Asset within the DW might be sourced and built from multiple sources (e.g., instruments from Censitrac and equipment from Intelligent InSites). It is also a normalized model that carries the relationship of objects from its disparate source systems. The amount of history is normally three years and greater. Where needed for performance and ease of use, objects can be de-normalized.
- ***Data Mart (DM)—***A DM is designed using Dimensional Modeling for the purpose of solving a subject area or a departmental need. The topology of data marts are built with fact tables and dimensions called a star schema. Fact Tables are de-normalized tables joining attributes and measures from multiple tables. Dimensions are lookups for the attributes within the fact and often contain information about a relational hierarchy. For example, a calendar dimension will have a date as the key and store Year, Quarter, Month, Week, and Day as the relational hierarchy.

The NDR will be built using is a hybrid of the data modeling approaches described above.

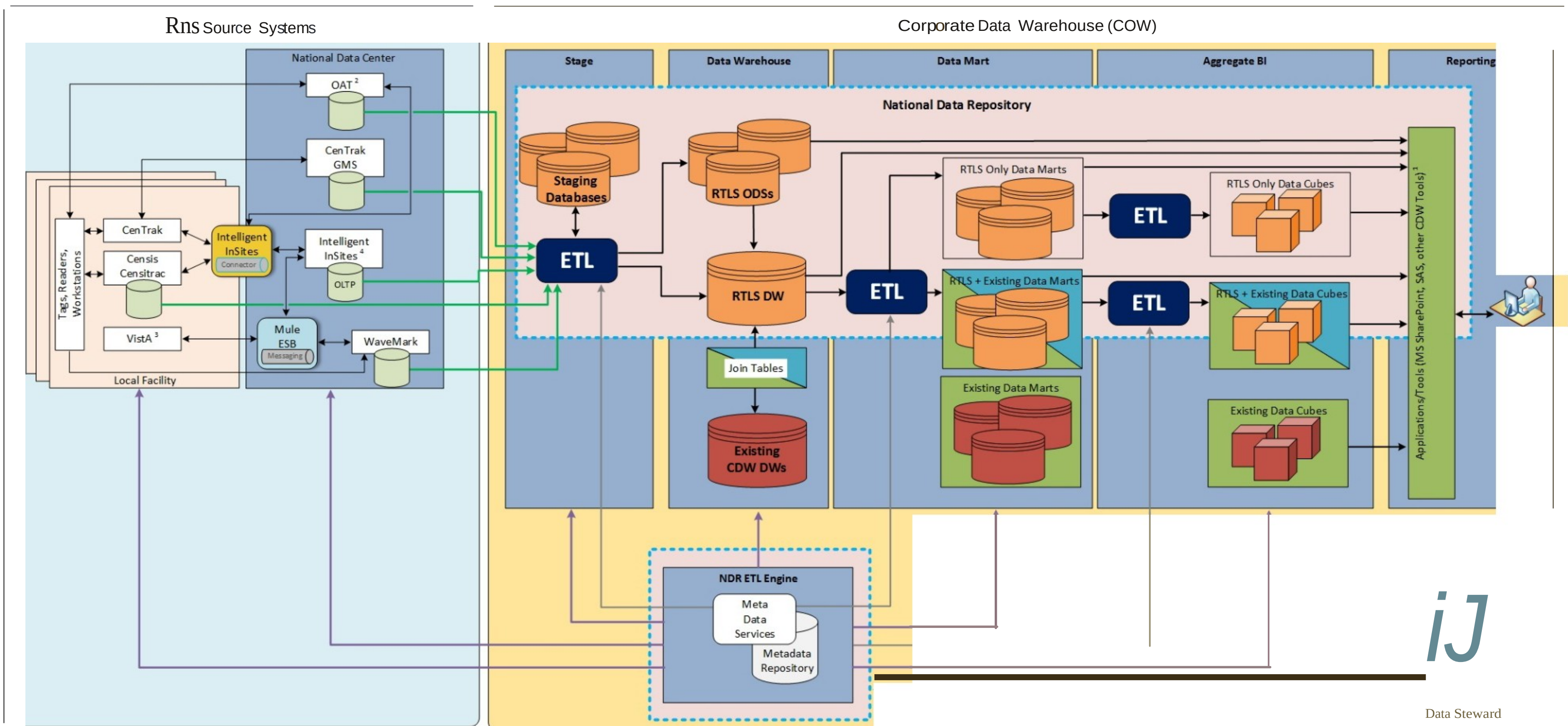
6.2.5.2.2 NDR Architecture

The NDR Architecture will be built using layers. The layers help in managing and containing the business logic, data transformations, and aggregations. By using a layered approach, the NDR can be developed one layer at a time which greatly reduces project risk. In addition, the layered approach allows for easier system maintenance and for addressing any data quality issues. The NDR Architecture is broken down into the following layers:

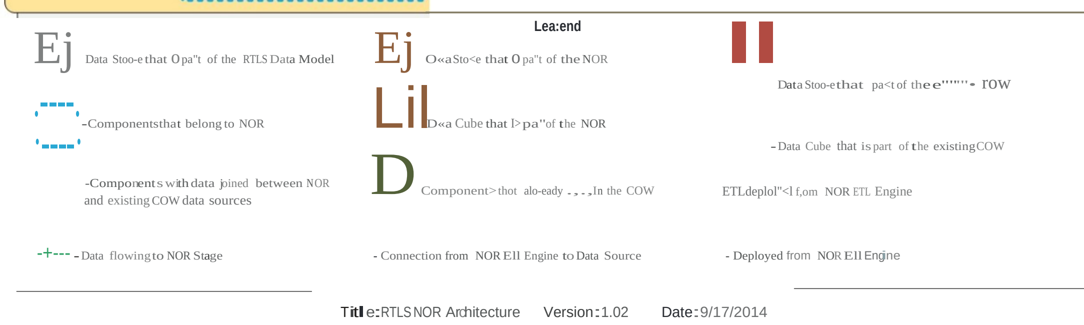
- Source Systems
- Stage
- Data Warehouse
- Data Mart
- Aggregation BI
- Reporting

This section contains details about each of the architectural layers listed above. The figure below shows the NDR Architecture and its layers. The layers are labeled along the top of the figure. Data flows from left to right in the figure. Starting on the left, data is ETL'd from the Source Systems to the Stage Layer using the NDR ETL Engine. Once the data is aggregated in the Stage Layer, the NDR ETL Engine ETLs the data from the Stage Layer into the Data Warehouse Layer (including ODS). Data Marts will be constructed using ETL from the NDR ETL Engine. The Data Marts are populated with data taken from the Data Warehouse. The Aggregate BI Layer will contain Data Cubes which will be constructed by using the NDR ETL Engine. The NDR ETL engine will ETL data from the Data Marts to the Data Cubes. The Reporting Layer provides user visibility to the Data Warehouse (including ODS), Data Marts, and Data Cubes. In addition, the NDR can join with existing CDW data sets such as clinical data. The NDR can join with existing CDW data sets at the Data Warehouse, Data Marts, and Aggregation BI (Data Cubes) Layers.

Figure 83: NOR Architecture



Notes
1. The NOR wl create reports using the existing ГOW reporting tool set
2. The data stores from OAT wl l contain the OATxpress instances (depk>yed oo a facility ba5is) and the OAT Enterprisf! Administrator
3. The VistA Is deployed logkallyon a faclIty basis, but physically deployed In regional data centers
4. The Intelli ent InSites will contain multiDie instances de loved on a oer VISN basis.



6.2.5.2.2.1 Source Systems

Complex organizations are made up of multiple data systems that operate their daily business. The RTLS System is no different. The RTLS System is a system of systems and is made up of several source systems. Source systems are the data feeding pipes to the Staging Layer. The data within a Source System is raw and unchanged (not aggregated). Below is a list of the source systems for the NDR:

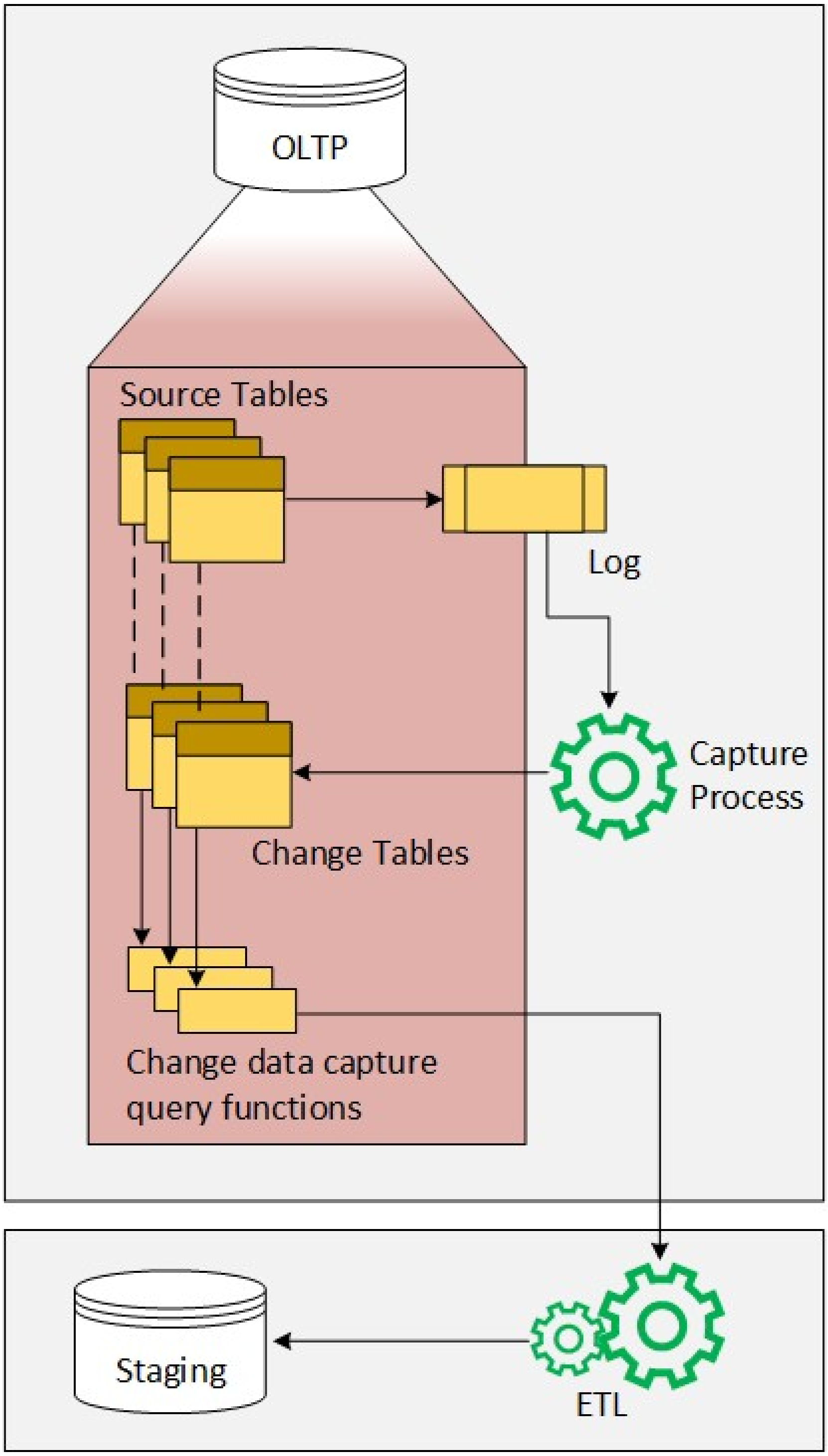
- Intelligent InSites OLTP
- CenTrak GMS
- WaveMark EiRTLS
- Censis Censitrac
- OATSystems OATxpress
- OATSystems Enterprise Administrator

On startup of the NDR, an initial load of data will be ETL'd from the source systems to the NDR staging layer. On a configurable basis (defaulted to daily), incremental data will be ETL'd from the source systems to the NDR. The incremental data loads are reserved for transactional data. A transactional data table is a database table that has 10 or more SQL transactions of either create, update, or delete performed on a daily basis. Tables that are not transactional data tables are considered static reference data tables and will be loaded directly into the staging layer using complete copies or snapshots similar to the initial load process. Executing a copy of reference table is quicker than creating and executing an ETL method.

Incremental data will be taken from the transactional data tables within the source systems using a technique called Change Data Capture (CDC). CDC is designed to capture insert, update, and delete activity applied to designated tables, and to make the details of the changes available in an easily consumed relational format. The change tables used by change data capture contain columns that mirror the column structure of a tracked source table, along with the metadata needed to understand the changes that have occurred. CDC provides information about Data Manipulation Language changes on a table and a database. By using CDC, the NDR will eliminate expensive techniques such as triggers, timestamp columns, and join queries.

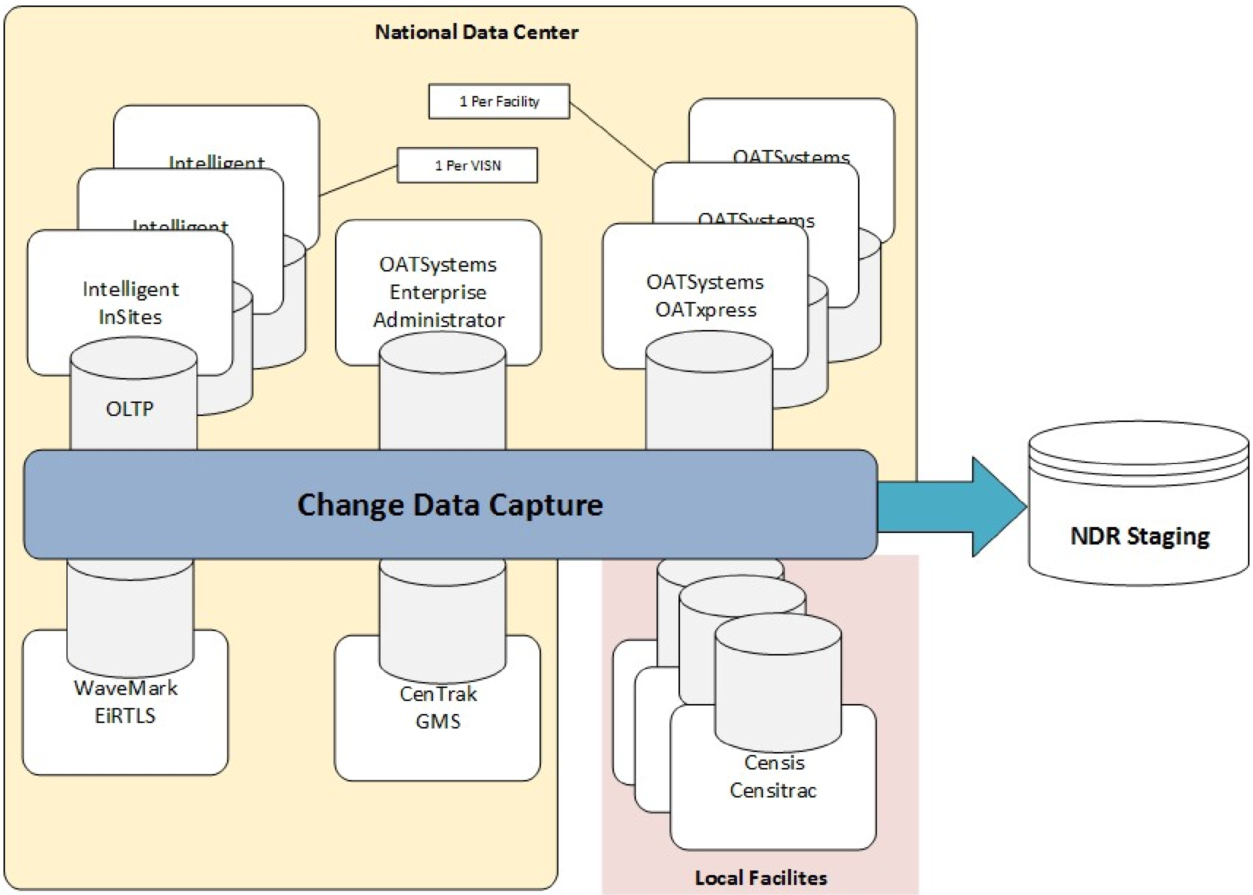
The figure below shows the flow of data when implementing CDC. The source of change data for change data capture is the database transaction log. As inserts, updates, and deletes are applied to tracked source tables, entries that describe those changes are added to the log. The log serves as input to the change data capture process. The data capture process reads the log and adds information about changes to the tracked table's associated change table. Functions are provided to enumerate the changes that appear in the change tables over a specified range, returning the information in the form of a filtered result set. The filtered result set is used by an application process to update a representation of the source in some external environment. In the case of the NDR, the external environment is the NDR Staging Layer.

Figure 84: CDC Data Flow



CDC will be implemented for all RTLS Source Systems. The following figure shows the RTLS Source Systems that will use CDC and how the data will flow into the NDR Staging Layer.

Figure 85: RTLS NDR Data Sources



6.2.5.2.2.2 Stage Layer

The first area of aggregation where all the RTLS data is collected into one area is called the Staging Layer. The staging layer is a temporary location used by the data warehouse loading programs and can take the form of relational database tables and operating system files. This layer sits between the source and target systems for the data and is designed to assist in efficiently moving the data from source to target. The staging layer allows for the de-coupling of the processes with the goal of freeing the source system resources as soon as possible. As data is read incrementally over time, this staging provides a temporary storage of the delta data so that it can be further processed into the data warehouse. The staging layer data is temporary and is kept for a short period of time to allow for the restart of ETL processes and possible debugging scenarios.

Initial and incremental (data from CDC) data loads will be executed (see Section 6.2.5.2.3.5 – Job Control) within a window of time that will not interfere with the source systems. For more information on each data load from the source system to the NDR, please see the appropriate ICD.

6.2.5.2.2.3 Data Warehouse Layer

A data warehouse is a logical model of the enterprise materialized into a physical database and is normalized with relationships. The data warehouse layer consolidates and bridges data from multiple sources. The data warehouse will receive data from the staging layer and store it until its retention period is expired. The Data Warehouse layer also includes an Operational Data Store (ODS) which is optional and not needed to promote data to the data warehouse. An ODS is a less normalized version of its source and only holds a short history of transaction data for operational reporting, typically 7 to 120 days or more. The data warehouse will provide data for reporting (including ad-hoc) and analytics. The ODS will provide data for operational reporting by having its structure and data performance tuned using database features such as indexes and keys. Data from the data warehouse will be ETL'd into the Data Mart layer.

6.2.5.2.2.4 Data Mart Layer

A Data Mart serves as a single departmental or subject area solution. It will serve as the base data for many metrics within VA. The Data Marts topology will be star and snowflake schemas. Star schemas consist of a single fact table surrounded by lookup tables called dimension tables. In a Snowflake schema, the dimensions have relationships with each other; a single dimension within a hierarchy can be leafed out into many tables, or the attributes within a large dimension can be built out into a separate table. Many fact tables and star schemas can be generated to produce multiple Data Marts from a single data warehouse. With conforming dimensions (e.g., time and location), reporting can be consistent and comparable across different data marts.

A large component of the Data Mart Layer is formed by the Conforming Dimensions. This is a collection of dimensions that will be used in several analytic domains; the collection is controlled and administered by a committee of people called Data Stewards. Data from the data marts will be ETL'd to the Aggregate BI Layer to build data cubes.

6.2.5.2.2.5 Aggregate BI Layer

Pre-aggregated data is useful if the data is frequently aggregated at common levels or the size and processing time makes the data unavailable for quick queries. The aggregates will be generated from the Data Marts and will be cascaded for dimension drill downs and roll ups. These aggregates often make up most of the KPIs needed to make business decisions. Another common aggregate is cube technologies, used for On-Line Analytical Processing (OLAP) and Data Mining. Cube building technology allows for quick drag and drop of dimensional data to cross hatch/pivot measurements. Aggregation is a shared effort between the ETL tools and the BI tools. An aggregate can be stored in either a database table or a cube. A cube can be a proprietary vendor format, like Microsoft SQL Server Analysis Services (SSAS), that exists within a database or file. Within the Data Mart Layer fact tables will be aggregated to higher levels based on one or more dimension tables. The aggregated facts are supported by a snowflake data mart topology.

6.2.5.2.2.6 Reporting

Reporting is a generic term for a large area of output that can come from the DW and BI tools. The NDR will make use of the existing CDW reporting tool set which includes Microsoft SQL Server Reporting Services (SSRS), SAS, and Microsoft Excel. A SharePoint portal will be used to provide controlled user access and several options for data presentation. The portal will include dashboards, an Excel interface, formatted pre-defined reports, and ad hoc query access to cube technology. A portal will also host output generated from complex report writers that perform statistical processing on a scheduled basis.

The reporting component will provide historical, current and predictive views of the RTLS Business operations.

The NDR reporting consists of two components:

- Queries, Reports, and Dashboards
- Data Mining

Queries, Reports, and Dashboards

Microsoft Business Intelligence Suite (BIS) and the SAS Enterprise Guide will be used to develop and maintain queries, reports, and workflows. This tool set will provide the capabilities to perform searches using multiple filters, display results in various forms-based and graphical formats, create and share ad-hoc reports, export results to other MS Office applications, and provide appropriate access controls and indications to users on the status of their query or report generation.

SSAS is used to build queries and provide multi-dimensional analysis capabilities. SSAS is used to pre-aggregate large amounts of data from the data marts into an Online Analytical Processing (OLAP) cube format. The NDR cubes will leverage the structures, calculations, facts, and dimensions in the OLAP cubes. Additional structures, calculations, facts, and dimensions can be added to the NDR cubes to meet the enterprise-level analytic requirements.

SSRS will be used to create, manage, and deliver reports. For the NDR, SSRS will be used to provide reports based on both the raw data and the SSAS OLAP cubes. Types of reports include static reports, parameterized reports, dynamic reports, and subscription-based report delivery. Users will be able to create interactive, tabular, and graphical reports, including map-based displays.

The SharePoint Portal and the Microsoft Office suite will be used to access data, dashboards, and reporting capabilities. Microsoft Excel is used to provide a robust ad hoc capability with direct access to the data warehouse and/or analytical cubes with a user-friendly interface. Data connections using Microsoft Excel connect directly to analytical cubes and to the data warehouse so users can utilize pivot tables and charts to query and analyze data. The pivot tables and charts will be shared online in the SharePoint Portal using Excel Services. Excel Services also allows users to interact with and analyze data through web portal pages in a user-friendly interface. Microsoft PerformancePoint services will be used for dashboards, scorecards, and KPIs with drill-down and drill-across capability.

SAS users within the NDR will be able to leverage existing SAS Enterprise Guide (EG) client software for querying and reporting. Enterprise Guide is an easy-to-use windows client application that provides access to SAS with an intuitive, visual, customizable interface. SAS EG will allow users to develop queries and reports for all data available within the NDR and will provide the ability to perform drill-down analysis using multiple filters and dynamic prompts. Users who do not have SAS programming experience, but need to access to the NDR data, can take advantage of menu-driven tasks in SAS EG. The point-and-click interface in EG can create queries and present results in reports and graphs.

The SharePoint Portal will be used to create actual workflows with its graphical user interface. The SharePoint interface allows end users to publish new or updated workflows for use by other users and execute workflow analysis and reporting at recurring times or on demand. SharePoint provides individual and aggregate workflow reports that allow users to assess the efficiency of their workflows and related business processes. Reports can be used to identify problems with processes or to determine whether a group or individual is meeting performance targets for a particular business process. SharePoint includes two Excel reports:

- Activity Duration Report - provides data on how long each workflow activity takes to complete
- Cancellation and Error Report - shows workflows that were cancelled or which encountered errors before completion

Data Mining

Data mining is the discovery mode of data analysis. Data mining provides a means to unearth unsuspected or unknown relationships, patterns, and associations within a set of data. Data mining is most often associated with predictive analysis, which is a process of analyzing large amounts of data to identify patterns, trends, activities, and relationships of data. The NDR Data Mines will be built using existing CDW tools from Microsoft and SAS. This tool set includes features for predictive analytics, forecasting, and optimization.

One of the Data Mining components within the CDW will be SAS Enterprise Miner. SAS Enterprise Miner is software that provides a wide range of capabilities for exploring and analyzing data to help reveal patterns, opportunities, and information that can drive proactive, evidence-based, and strategic decision making.

Simple daily tasks such as finding a staff member, patient, or piece of equipment consume staff time and increase patient wait times. Bottlenecks created by inefficient patient flows in emergency department and operating rooms, in-patient beds, out-patient exam rooms, and procedure areas create a ripple effect through the entire facility. The data mining component will facilitate modeling and studying of correlations in causes for bottlenecks using various data mining techniques such as regression, decision trees, and neural networks to prevent such incidences. SAS ACCESS will be used to retrieve data from the MS SQL Server database. SAS ACCESS allows for reading of entire blocks of data from the database instead of reading data just one record at a time. This block read capability reduces I/O bottlenecks and allows procedures to read data as fast as they are able to process it.

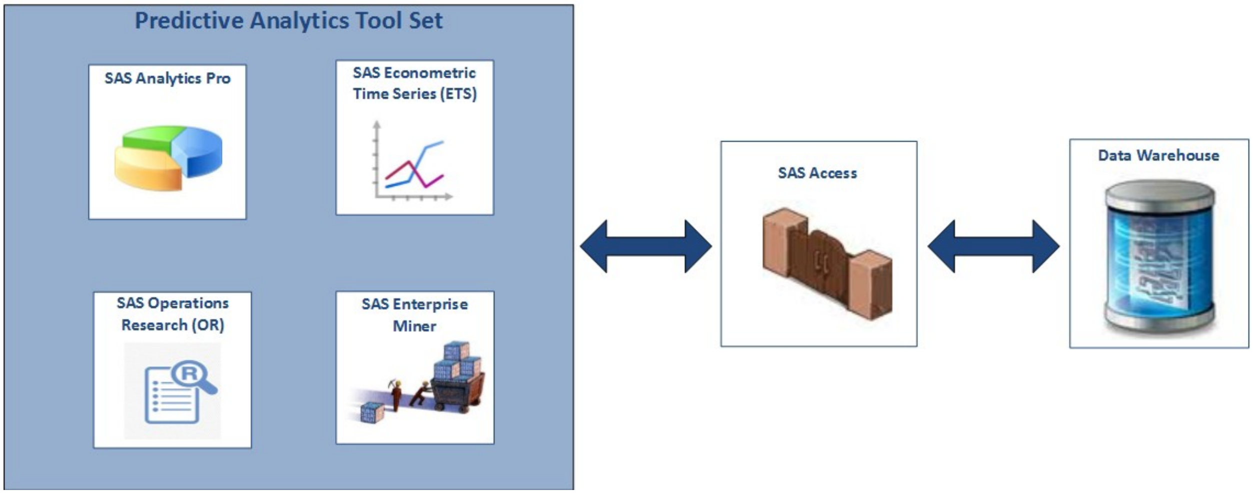
Forecasting

SAS Econometric Time Series (ETS) forecasting integrates time series and econometric techniques for modeling, forecasting, and simulating business processes. SAS Forecast Server generates large quantities of high-quality forecasts quickly and automatically, allowing VA to plan more effectively in the future. With the enterprise-wide RTLS data available through NDR, VA will be able to generate a variety of supply-demand forecast models for in-patient and out-patient visits and expensive surgical and non-surgical assets. The software automatically chooses the most appropriate forecasting model, optimizes the model parameters and produces the forecasts. Time series data management capabilities are also included. The ability to preprocess transactional data can save significant time and resources, and the unsurpassed scalability of SAS Forecast Server, enables VA to operate more efficiently.

Optimization

The SAS Operations Research (OR) product provides a powerful array of optimization and simulation techniques to enable VA to consider alternative actions and scenarios and to determine the best allocation of resources and the best plans for accomplishing goals. Using OR, analysts will be able to build models interactively, modifying constraints or variables and experimenting easily with the effects of changes to underlying data. In mathematical optimization, a specialized modeling language enables the analysts to work transparently and directly with symbolic problem formulations, and an appropriate solution method for the current problem can be chosen automatically. This allows problems to be formulated and solved intuitively and efficiently, whether they are linear, nonlinear, or quadratic. SAS OR also provides network flow optimizations such as shortest path, maximum flow, and minimum cost flow to understand and optimize the utilization of various assets.

Figure 86: Predictive Analytics/Data Mining



6.2.5.2.3 NDR ETL Engine

A large portion of the NDR development effort involves moving data from the source systems to the NDR. The NDR ETL engine will use a metadata driven approach. Metadata is identified as a critical factor in data warehouse projects. Metadata is the data about data; it describes other data and provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. Using a metadata approach, the NDR ETL engine will capture information necessary to extract, transform, and load data from source systems into the data warehouse, and later interpret the data warehouse contents.

6.2.5.2.3.1 Metadata Strategy

The NDR will use a metadata strategy to drive its ETL Engine and manage RTLS master data.

The following figure shows the inputs and outputs to the NDR Metadata Strategy. The Metadata Repository is a database (MS SQL Server) used to store metadata; it physically stores and catalogues metadata. Data in the metadata repository will be generic, integrated, current, and historical. The NDR metadata strategy will use a meta-model. A meta-model or surrogate model is a model of a model. A meta-model defines the components of a conceptual model, process, or system. The meta-model serves for an explanation and definition of relationships among the various components of the applied model. The Meta-model will store the metadata by generic terms instead of storing it in an applications-specific defined way, so that if the data base standard changes from one product to another the physical meta-model of the metadata repository will not need to change. Integration of the metadata repository includes all business area metadata in an integrated fashion, covering all domains and subject areas of the organization. The metadata repository should have accessible current and historical metadata.

The Inputs to the NDR Metadata Strategy are the following:

Rules Engine — A specific collection of design-time and runtime software that enables an enterprise to explicitly define, analyze, execute, audit, and maintain a wide variety of business logic, collectively referred to as “rules.”

EDA — A document describing the enterprise data architecture to support the implementation of RTLS. It can be thought of as a “user’s guide” to the underlying data for the RTLS ecosystem. This document has defined the data captured, stored, and used within all data stores that comprise RTLS. The Source System database tables defined in the EDA will be used as an input to the NDR Metadata Strategy.

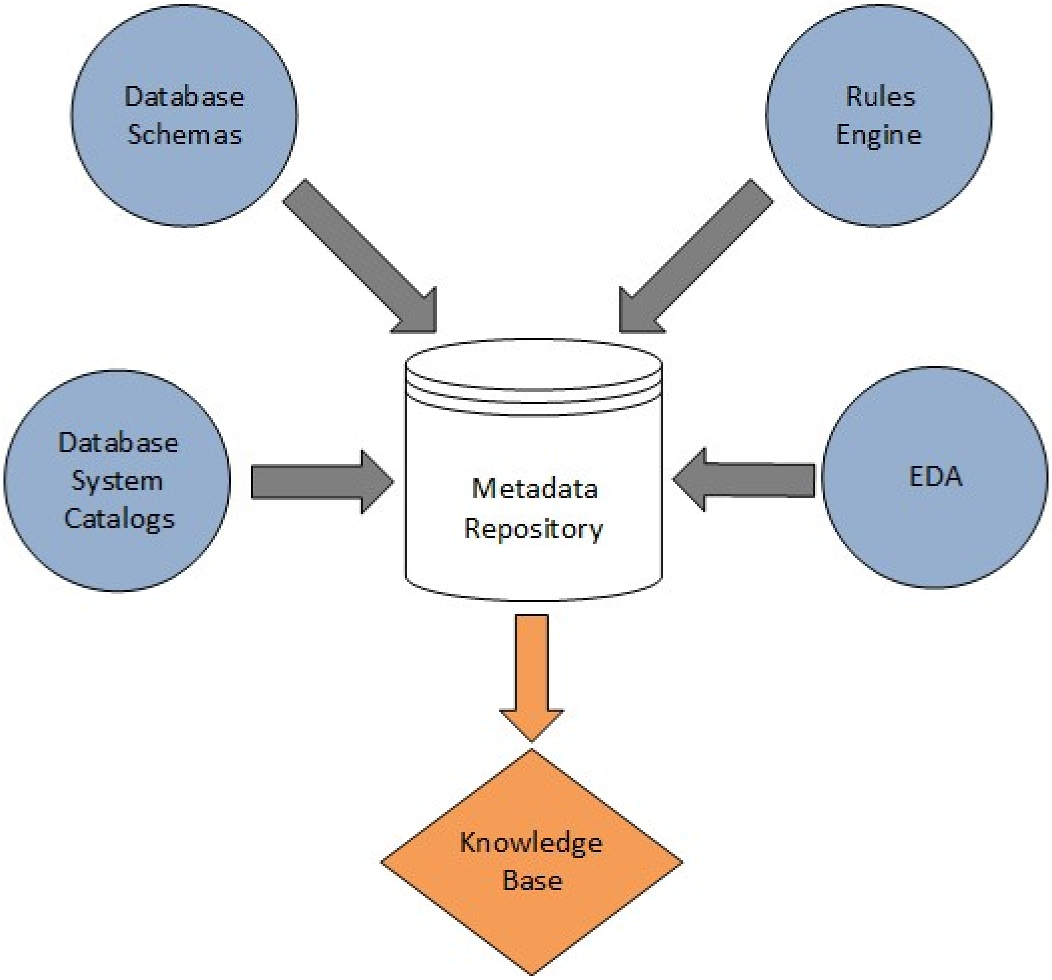
Database System Catalogs — A set of information describing the contents, format, and structure of a database and the relationships between its elements, used to control access to and manipulation of the database. The Metadata Strategy will use database system catalogs from source sources as well as from the NDR.

Database Schemas — Database Schemas are ways to logically group database objects such as tables, views, stored procedures, etc. The Metadata Strategy will use the database tables and columns from the RTLS database schemas. The Metadata strategy will cross reference the tables from the database schemas with the database tables defined in the EDA to validate the correct tables and their underlying columns will be used in the Metadata Strategy.

Outputs

By using the inputs, a Knowledge Base is generated using the Metadata Repository. The Knowledge Base is a store of information with an underlying set of facts, assumptions, and rules that allows resources (whether a computer system or person) the ability to solve a problem. The knowledge base helps unlock the secrets of RTLS data as the NDR is designed and developed. The knowledge base will assist with the understanding, planning, designing, implementing, and maintaining of the NDR. The knowledge base will aid in such tasks as Data Modeling, ETL design and development, and Data Mining. In addition, the knowledge base provides insights into Data Discovery and Quality for future reports and issues in current reports.

Figure 87: NDR Metadata Strategy



6.2.5.2.3.2 Master Data Services (MDs) and Data Quality Services (DQS)

Microsoft SQL Server 2012 Enterprise Edition provides Master Data Services (MDS) and Data Quality Services (DQS). The NDR solution will utilize both of these components. Master data as defined for the NDR task order falls into two categories:

1) Metadata extracted from the multiple data stores used for RTLS

The NDR solution includes an ETL generation process that depends on discovering metadata.

- The metadata includes specific information, such as table names and column names, that is available from the RTLS vendors' data schemas and system catalogs. This information is retrieved and managed as master data using SQL Server Master Data Services. MDS provides for the versioning of the metadata discovered from the vendors' schemas. ETL code can be deployed at multiple locations using different metadata to allow for variances in a vendor's schema by software version. Detecting metadata modifications will allow for processing changes to be introduced into the ETL process; for example, a new table could be introduced into the data warehouse by modifying the metadata and following the procedures for changes to the ETL process.

- The data also includes the system names, connection parameters, partitioning schemes, environment definitions, ETL design pattern process definitions, and other items of data that will enable the consistent design pattern and deployment of the metadata driven processing ETL solution across the enterprise.

2) RTLS data standards maintained by VA

It is possible to check and correct data during the ETL process using the MDS data and DQS business rules. This can be accomplished by loading VA Data Standards into MDS and creating business rules in DQS used during the ETL process to correct data errors or flag rows not meeting VA standards. The NDR solution does not implement DQS business rules at this time.

Microsoft provides a free MDS Excel add-in download that enables manual connectivity and the ability to create, modify, and manipulate data located in the master data repository. This approach allows for ease of the creation and versioning of the data needed for the ETL solution.

6.2.5.2.3.3 Metadata Driven ETL

Metadata driven ETL will be used to move data across the enterprise, reducing time to develop and increasing the quality and consistency of ETL design patterns.

The NDR will have roughly 325 source systems, including the following:

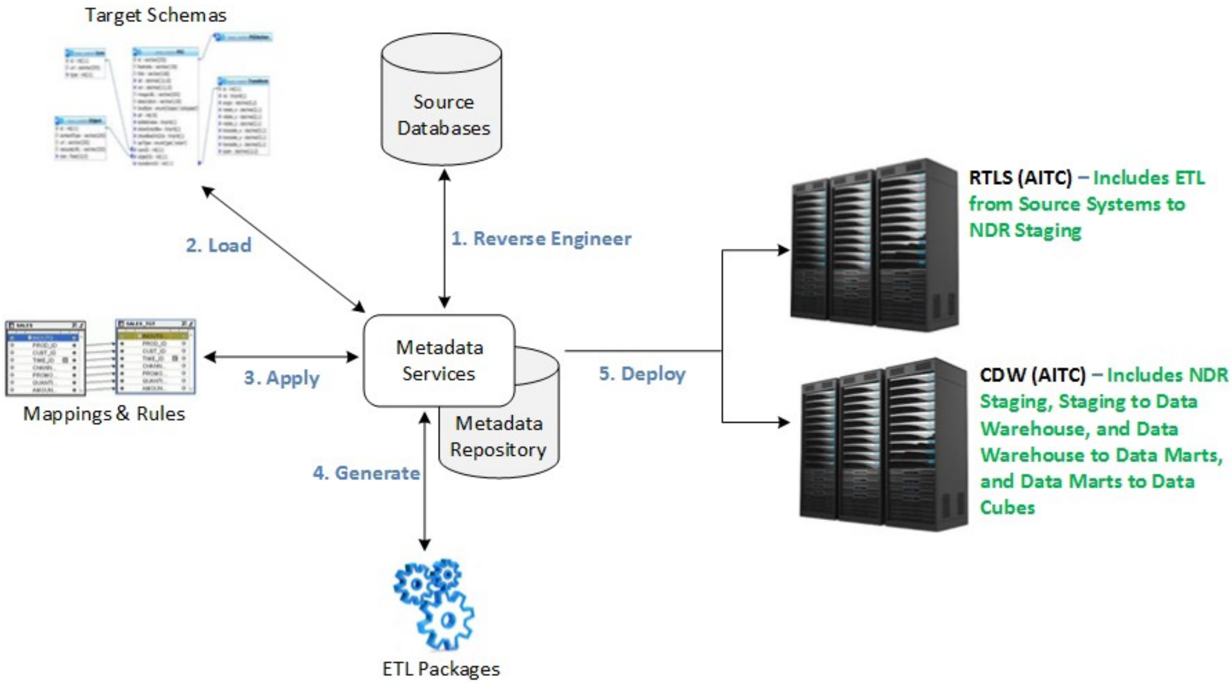
- 22 Intelligent InSites Platforms
- 1 WaveMark EiRTLS
- 1 CenTrak GMS
- ~150 Censis Censitrac
- ~150 OATSystems OATxpress

As additional use cases are added to the RTLS enterprise, new sources systems will be added.

Currently, all of the source systems have several tables. This will require the NDR to have a large number of ETLs to build and maintain. Given the source systems, we expect to have over 2000 ETLs to manage.

The following figure shows how a Metadata driven approach will be used for ETL within the NDR.

Figure 88: Metadata Drive ETL



The Metadata driven ETL will be built using the Microsoft SQL Server platform, using the following steps shown in the figure above:

1. A data modeling tool, such as ER/Studio from Embarcadero software, will be used to Reverse Engineer the source systems into a single metadata repository. The metadata will fully describe all the source system table and column attributes. Other auxiliary attributes will be added to support the technical approach such as source system name and versions.
2. The target systems will be designed to meet requirements of the NDR, and these schemas will be included in the metadata repository like the source systems in Step 1.
3. Data Transformation mappings from source to target schemas will be applied. In addition, any business rules can be applied at this time. These rules are used to satisfy any business requirements. The mappings and rules will be maintained either within the data modeling tool or with Microsoft Master Data services.
4. Using the .Net framework, C# and the SSIS libraries, the ETL packages will be generated and maintained using the metadata repository.
5. The ETL packages will be deployed to the appropriate servers using the technology stack available within the CDW environment.

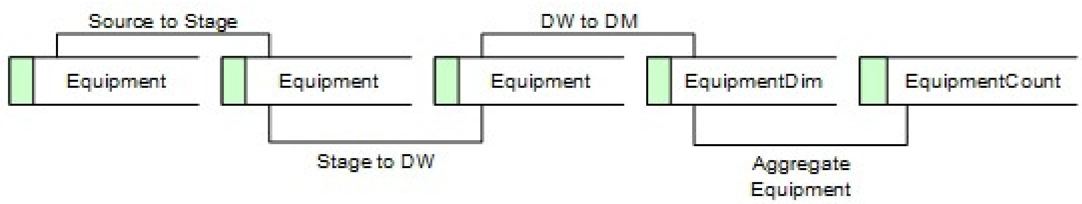
The above technical approach will also have SSIS package templates and configuration files that will allow ETL packages to be reused across the DW/BI Framework. This will greatly reduce the number of ETLs and maintenance to ensure process quality. The ETLs will be managed using an ETL Framework using a master and child packages method. The ETL framework will be replicated for each ETL layer described above and will be the container of the ETL logic and transformation needed to maintain that layer. The framework will also capture runtime data and will be logged for process monitoring, health checks, and audit reports.

6.2.5.2.3.4 ETL (Extract, Transform, and Load)

Data movement from source to target should encapsulate only the logic needed to move through that layer. This helps in managing the roles and expertise needed at each layer for sustainability, extensibility, and operations. New requirements can focus on each layer that is impacted by changes in the enterprise.

Data Mappings per object (Tables and Columns) shows the full path that data will take within a DW/BI Framework. Source → Stage →Data Warehouse →Data Mart →Aggregate

Figure 89: ETL (Extract, Transform, and Load)



The diagram above shows four tables used as targets to move (ETL) equipment data to the Aggregate BI layer. It can take four or more interfaces to transport the (ETL) data depending on the requirements for the system in general and the level of aggregation needed.

Metadata management and discovery will draw the focus of the implementation to designing and producing an effective analytics environment by automating the creation and execution of ETL design patterns based on the metadata.

6.2.5.2.3.5 Job Control: an ETL Framework

Job control is needed for managing the overall batch of ETL processes to complete an application. Each application will have many ETLs, ranging in the hundreds to thousands. To manage all processing and to allow for detection of failures and re-starts without manual effort, a job control ETL framework will be implemented. Following are the concepts and requirements for the ETL framework.

Units Of Work (UOW)

A Unit of Work is the number of subordinate tasks that need to be completed to establish a commit point within a larger Unit of Work. Therefore, a unit of work can have a recursive relationship. For example, the highest level of UOW for the NDR purpose is “Load Data Warehouse (NDR).” To accomplish this UOW, “Load InSites,” “Load WaveMark,” and “Load Censitrac” would be subordinate UOWs because the subordinates need to be completed before the NDR is completely loaded. This logic can be followed to the Nth degree, but for the purposes of ETL management, a single Data Flow (i.e., an SSIS package) will be the lowest unit of work. For readability and understanding a UOW is also called a job.

Each job has dependencies and cannot be started without successful completion of the previous job(s). All jobs are not dependent on each other within larger jobs, which allows for multiple jobs to run in parallel. Therefore, the superior or highest level job can be optimized by leveling and grouping subordinate jobs.

To manage the throughput of superior jobs, subordinate jobs can be grouped or blocked into manageable units of work to complete the larger jobs without over taxing the given resources. For manageability a job will be small and easy to maintain, allowing changes on only the objects that need to be updated or corrected as the data requirements change.

6.2.5.2.4 Partitioning

When working with large amounts of data, both logical and physical partitioning is needed to make the data more manageable and accessible. These partitions allow the database processes to read and write data in parallel to improve throughput. The processing is called “multi-threaded processing.”

Logical partitions will be applied to add extensibility and to limit the size of any area within the DW/BI Architecture. Logical Partitioning is the act of partitioning database objects such as a table by using a partitioning key. Each row in a logically partitioned table is unambiguously assigned to a single partition. The partitioning key consists of one or more columns that determine the partition where each row is stored. Physical partitioning is the act of dividing a disk storage drive into multiple logical storage units. Physical partitioning treats one physical disk drive as if there were multiple disks.

The NDR will use logical partitioning based on a schema naming convention to isolate each VISN’s data. For example, a VISN will have 5 sub schemas and will also be rolled up into Regional and National schemas:

- **VISN Partitions** – this partition is created at the VISN level (xy denotes the VISN number below) and its underlying facilities are rolled up. A column called FacilityIDDW is populated to identify its particular facility.
    - VISNxy_Insites
    - VISNxy_Censitrac
    - VISNxy_CenTrak
    - VISNxy_OAT
    - VISNxy_Wavemark
- **Regional Partitions** – this partition is created at the Regional level (X denotes the Region number below) and its underlying VISNs are rolled up. A column called VISNIDDW is populated to identify its VISN.
    - RegionX_Insites
    - RegionX_Censitrac
    - RegionX_CenTrak
    - RegionX_OAT
    - RegionX_Wavemark
- **National Partitions** – this partition is created at the National level and its underlying Regions are rolled up. A column called RegionIDDW is populated to identify its region.
    - NDR_Insites
    - NDR_Censitrac
    - NDR_CenTrak
    - NDR_OAT
    - NDR_Wavemark

Within each of the vendor’s schemas large transaction tables will be physically partitioned by date. The periodicity used to partition will depend on the volume of data coming from the RTLS. For example, we will use the period of a month to partition and manage data. If the volume causes constants within the NDR resources or a portion of the database to require tuning, partitioning can be adjusted. These physical partitions are managed within the Data Definition Language (DDL) of the database management system (DBMS).

As data is rolled up into Regional and National, more partitioning will be added. Within the Regional and National partitions, NDR could add a partition by date.

With physical partitioning the data can be physically separated for better management and performance. As the NDR develops, new data issues can bring the need to implement different partitioning scheme in place to solve loading or reporting requirements.

6.2.5.2.5 Security

Many levels of security will be implemented within and outside of the NDR. The CDW provides the group of generalized security clearances (i.e., NDS authorization categories) that NDR will make use of. This section describes security at a layer below the CDW authorizations and only addresses the software and applications and what will be built-in by design. The SharePoint portal will be used to control user access and the level of access with VA's Active Directory and groups. Role-based security limits a user's access to only the areas allowed with the configurations of the portal. Role-Based security will also be implemented within the NDR Architectural layers that will limit the data a user can view using Microsoft SQL Server management user groups. Row-based security and column-based security will be implemented into the Data Marts and reporting system.

The NDR will not be storing or ETL'ing any PHI data. The NDR will store PII data and transport PII data. The PII data is taken from the WaveMark EiRTLS database and loaded into the various NDR components (Staging, DW, Data Marts, and Cubes). The PII data will travel across established VA WANs from the VISN Data Centers to the NDR using FIPS-140.2 compliant encrypted protocols.

6.2.6 Interface to the VA Systems

This section will detail any applications, systems or services that are interfaced with the Enterprise RTLS System.

6.2.6.1 AEMS-MERS

VA Medical Centers are responsible for tracking all assets. VA currently employs asset tracking tools to assign codes to individual assets as they are deployed at VAMCs and CMOPs. Data about these assets, including equipment maintenance records, are managed by an automated system called AEMS-MERS. AEMS-MERS, also known as the Engineering Package within VistA, is the official asset management product in use today at all VHA facilities and some other VA entities. AEMS-MERS is currently used for asset tracking and allows for identification of the assets and associated data maintenance, locating the assets in the facility.

An interface between AEMS-MERS and Intelligent InSites Platform via the Mule ESB exists. This interface is used to populate Intelligent InSites with data about newly entered assets and to update AEMS-MERS with asset location. A uni-directional interface exists between Mule ESB and the Intelligent InSites Platform. A bi-directional interface exists between Mule ESB and VistA's AEMS-MERS.

The figure below shows the overall AEMS-MERS interface architecture. One interface sits in the Intelligent InSites Platform (receives data from Mule ESB and responds to requests for data by Mule ESB). The Intelligent InSites Platform does not directly contact the ESB, only accepting data and passing data back when requested by Mule ESB. A second interface sits on the Mule ESB that receives requests from the HealtheVet Web Service client that is used to send data from VistA. Mule ESB exposes its services via RESTful Web Services over standard HTTP/HTTPS protocols. A third interface sits within the Weblogic server that receives requests from Mule ESB. This interface also retrieves data from VistA. The VistA (AEMS-MERS) interface is exposed via RPCs on VistA using a VistA-Link listener. The figure below shows the integration architecture of the AEMS-MERS to/from RTLS interface.

Figure 90: AEMS-MERS Interface Architecture

Data will flow in the following manners

- **Mule ESB between Intelligent InSites Platform (bi-directional data flow)** – Mule ESB only connects to Intelligent InSites Platform. Intelligent InSites Platform accepts data that is pushed from Mule ESB as well as responds to requests for data from Mule ESB. The interface sits within the Intelligent InSites Platform
- **Mule ESB to VistA-Service ([Deployed on Weblogic] bi-directional data flow)** – Mule ESB connects to VistA-Service. VistA-Service accepts data being pushed from Mule ESB. VistA-Service will also pass data back to Mule ESB when a request for data is made from Mule ESB.
- **VistA-Service to VistA (AEMS-MERS bi-directional data flow)** – VistA-Service makes a connection to VistA using RPC. VistA-Service pushes data to VistA to be stored in the AEMS-MERS files. VistA also accepts requests for data retrieval being made by VistA-Service.
- **VistA (AEMS-MERS) to Mule ESB (uni-directional data flow)** – Upon a triggered event in VistA; VistA will make a HTTP request to the Mule ESB.

The AEMS-MERS RTLS System Interface will use two mechanisms for data movement:

- Scheduling Component - The VistA system is queried by the VistA-Service application via an ESB flow (Mule ESB) at scheduled intervals (defaulted to daily) and push data to the Intelligent InSites Platform
- VistA Trigger Mechanism - A trigger is fired when the VistA's AEMS-MERS application recognizes a data change. Data is sent to the Intelligent InSites Platform via the Mule ESB.

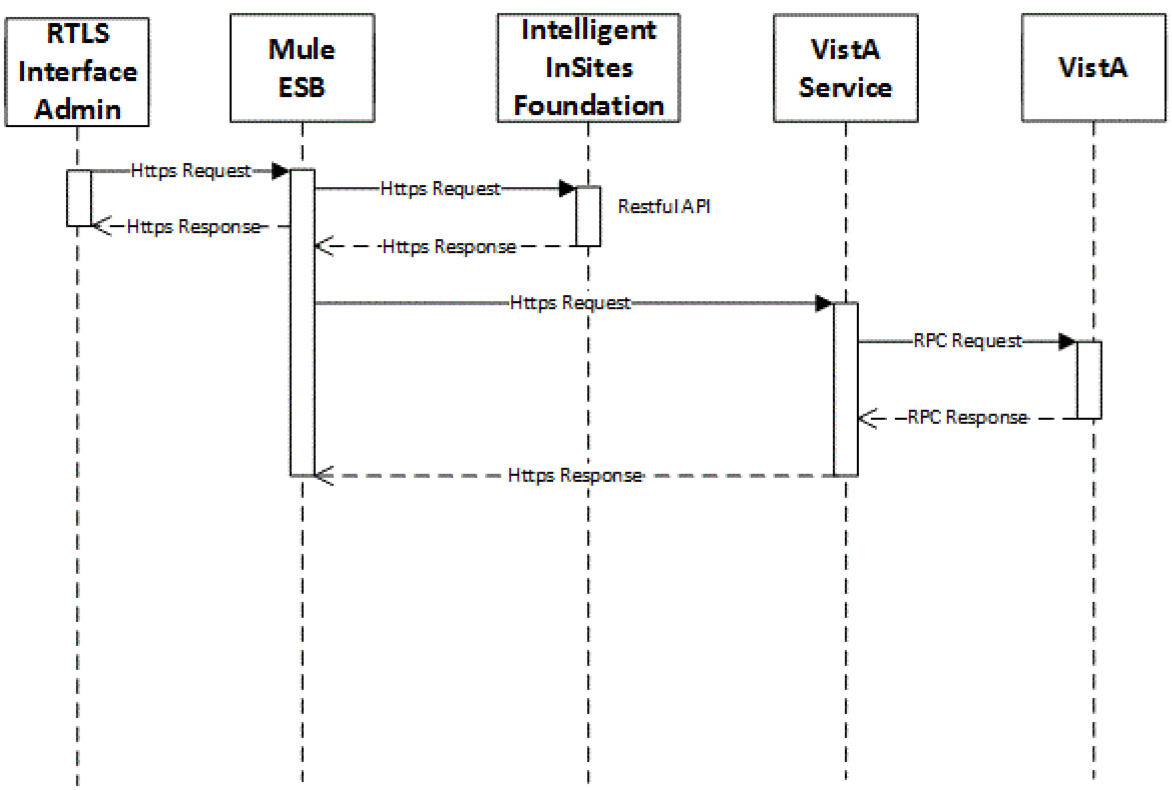
The following interactions will be featured within the AEMS-MERS Interface to the RTLS System (Intelligent InSites Platform):

- Equipment Movement (Bulk Update utilizing Scheduling Component) - Changes to equipment location are gathered by tag readers and stored in RTLS and then populated to AEMS-MERS to improve inventory processes. The uni-directional interface moves the location data from the Intelligent InSites Platform to AEMS-MERS.
- Equipment Details/New Equipment (Individual Update utilizing VistA Trigger Mechanism) - Details about equipment stored in AEMS-MERS including, but not limited to, EE number, serial number, equipment category, and Category Stock Number is sent from AEMS-MERS to the Intelligent InSites Platform. This provides the data necessary for RTLS users to create business rules to establish alarms or alerts when certain conditions apply.

6.2.6.1.1 Scheduling Component

The scheduling component is one of the two mechanisms for the interface between AEMS-MERS and the VISN/CMOP RTLS Engine (Intelligent InSites Platform). The figure below shows the sequence of events in the Scheduling Component.

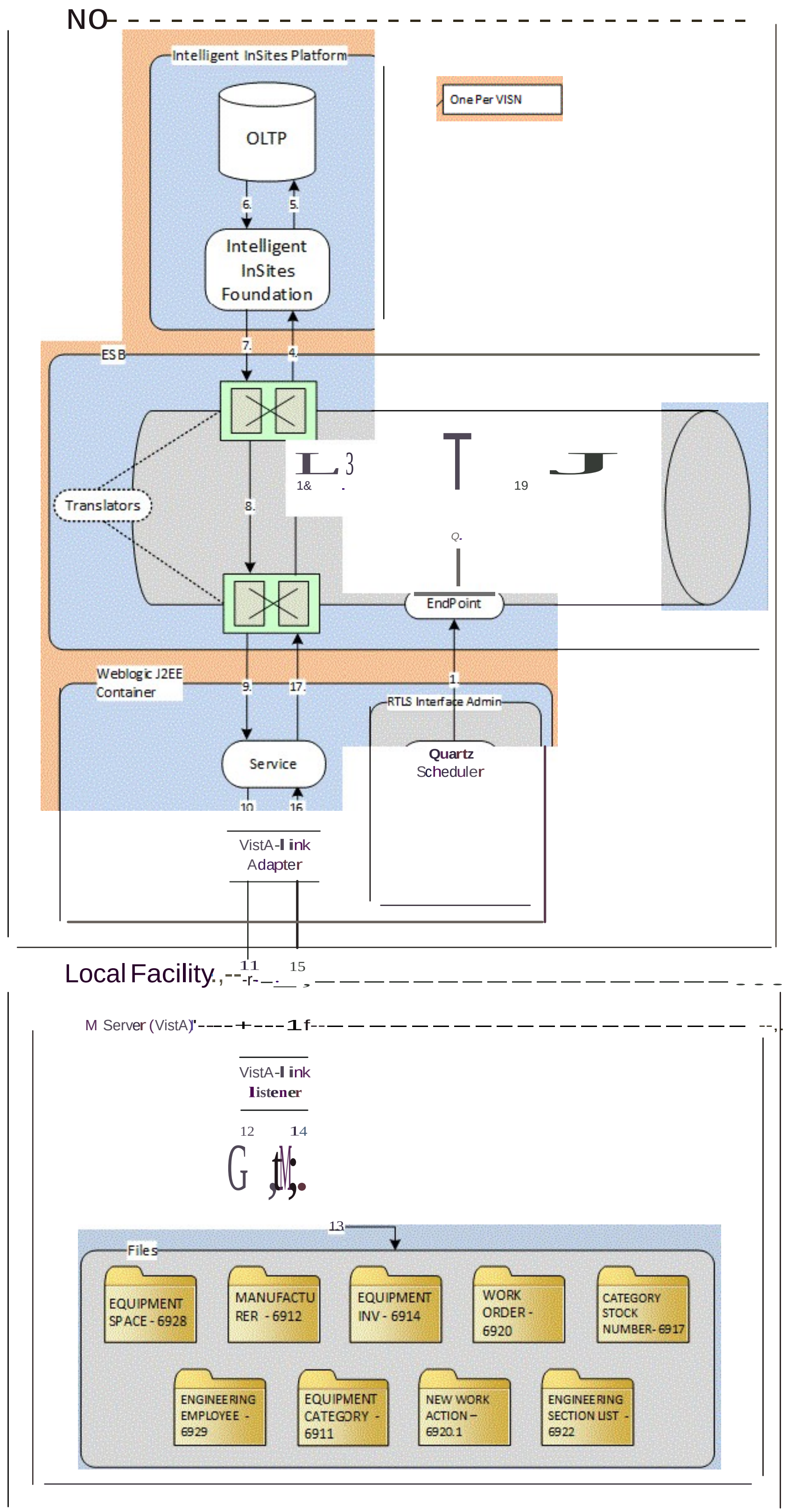
Figure 91: AEMS-MERS Scheduling Component Sequence



The figure below represents the scheduling component interactions between the VistA AEMS-MERS's application and the RTLS System. Data will flow in the following sequence based on the below figure:

1. A Java Quartz Scheduler from the RTLS Interface Admin Container will trigger a job to be processed. The Quartz Scheduler calls an endpoint exposed on the Mule ESB.
2. The Endpoint will push the message to the flow (Service Orchestration).
3. The flow will transform/build the message to send to the Intelligent InSites Platform.
4. The flow will make one or more RESTful calls over HTTP/s to the Intelligent InSites Platform with the necessary parameters.
5. The Intelligent InSites Platform will process the request and call its local database to gather any necessary data.
6. The data from the database is passed back to the Intelligent InSites Platform.
7. The Intelligent InSites Platform passes the data back to the flow.
8. The flow transforms the message to the VistA-Service message format.
9. The message is sent to the VistA-Service service layer over HTTPs using a RESTful interface.
10. The service inside of VistA-Service receives the request and makes a procedure call to the VistA-Link layer.
11. The Service acquires a connection to the VistA-Link listener and makes RPC call to the AEMS-MERS module.
12. The AEMS-MERS modules receive the RPC call and pre-process it (formatting & scrubbing).
13. A call is made to the various files in AEMS-MERS.
14. The AEMS-MERS module assembles any data that is returned by the file system.
15. The reply message is sent back over TCP-IP to the VistA-Link Adapter.
16. The Service receives the message and processes it for return to the ESB (build message).
17. The reply message is sent back to the ESB.
18. The message is returned to the flow.
19. A result (processed or failure) is logged.

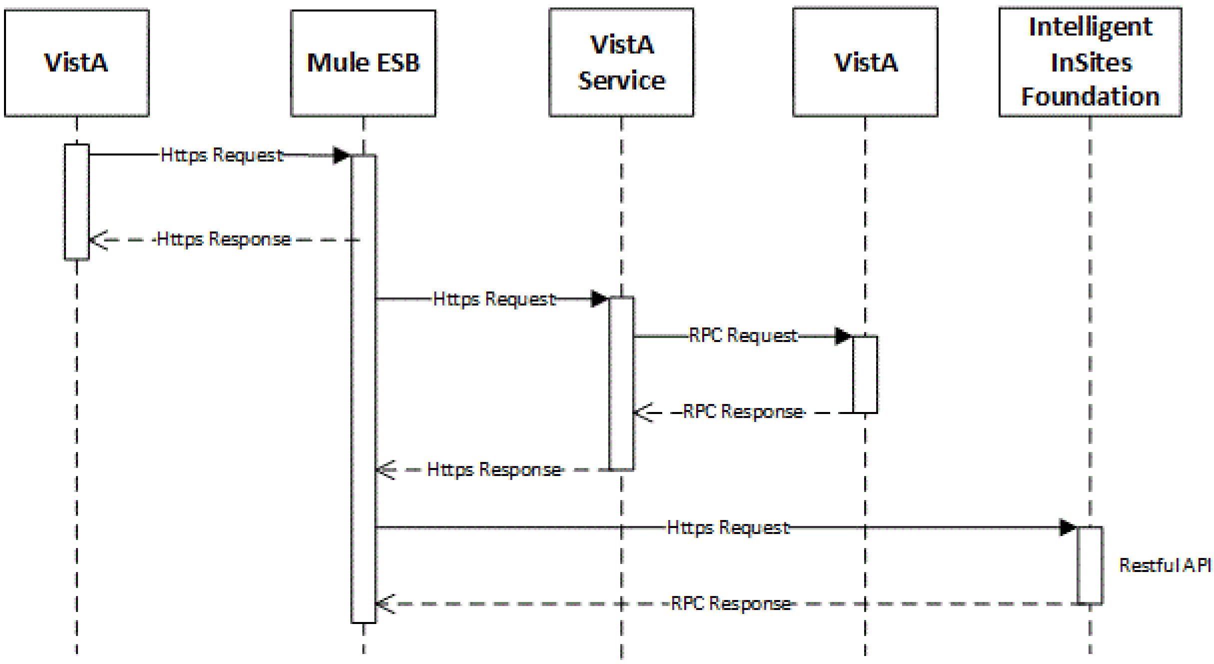
Figure 92: **Scheduling Component Data Flow**



6.2.6.1.2 AEMS-MERS Trigger Mechanism

The AEMS-MERS Trigger Mechanism is the second of the two mechanisms for the interface between AEMS-MERS and the VISN/CMOP RTLS Engine (Intelligent InSites Platform). The figure below shows the sequence of events in the AEMS-MERS Trigger Mechanism.

Figure 93: AEMS-MERS Triggered Mechanism Sequence

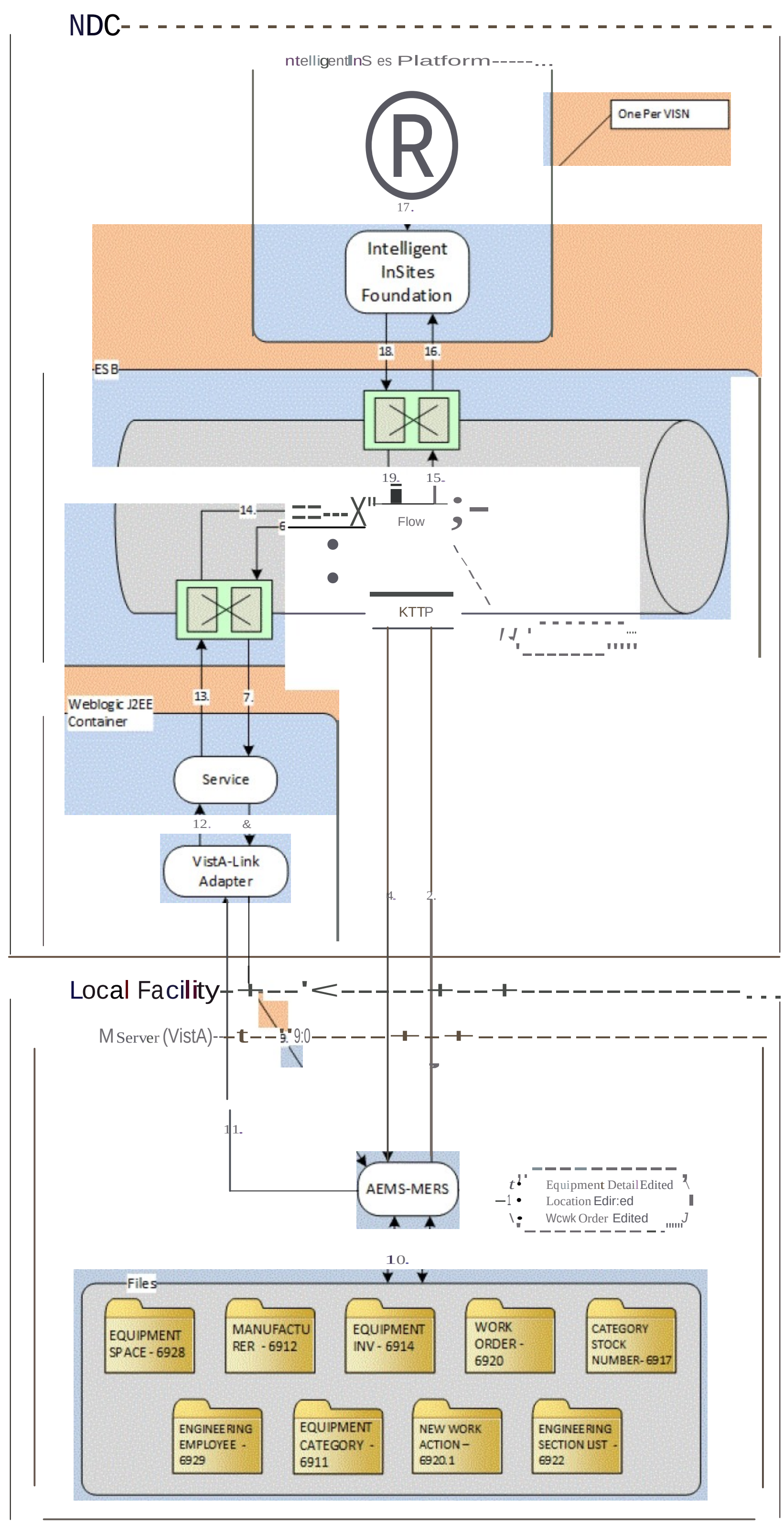


The figure below represents the AEMS-MERS Trigger Mechanism component interactions between the VistA AEMS-MERS's application and the RTLS System. Data will flow in the following sequence based on the below figure:

1. A field in AEMS-MERS is edited.
2. AEMS-MERS calls an HTTP/S Endpoint.
3. The message is placed in a Persisted Queue.
4. A message is sent back to AEMS-MERS (success or failure – failure the message is queued in VistA and retried).
5. A Polling mechanism (flow) pulls the message out of the queue (Note: Any failure from this point on the message is re-queue and the flow begins at step #4).
6. Polling mechanism (flow) sends a request to the VistA-Service (build/transform message via other flow).
7. VistA-Service receives the request.

8. The service acquires a connection to the VistA-Link listener and makes RPC call to the AEMS-MERS module.
9. The AEMS-MERS modules receive the RPC call and pre-process it (formatting & scrubbing).
10. A call is made to the various files in AEMS-MERS.
11. The AEMS-MERS module assembles any data that is returned by the file system.
12. The reply message is sent back over TCP-IP to the VistA-Link Adapter.
13. The Service receives the message and processes it for return to the ESB (build message).
14. The reply message is sent back to the ESB.
15. The flow (polling mechanism) will transform/build the message to send to the Intelligent InSites Platform.
16. The flow will make one or more RESTful calls over HTTPs to the Intelligent InSites Platform with the necessary parameters to obtain all of the relevant data elements.
17. The Intelligent InSites Platform will process the request and call its local Database to gather any necessary data. The data from the database is passed back to the Intelligent InSites Platform.
18. The Intelligent InSites Platform passes the data back to the flow.
19. The flow transforms the message.
20. A result (processed or failure) is logged.

Figure 94: AEMS-MERS Triggered Mechanism



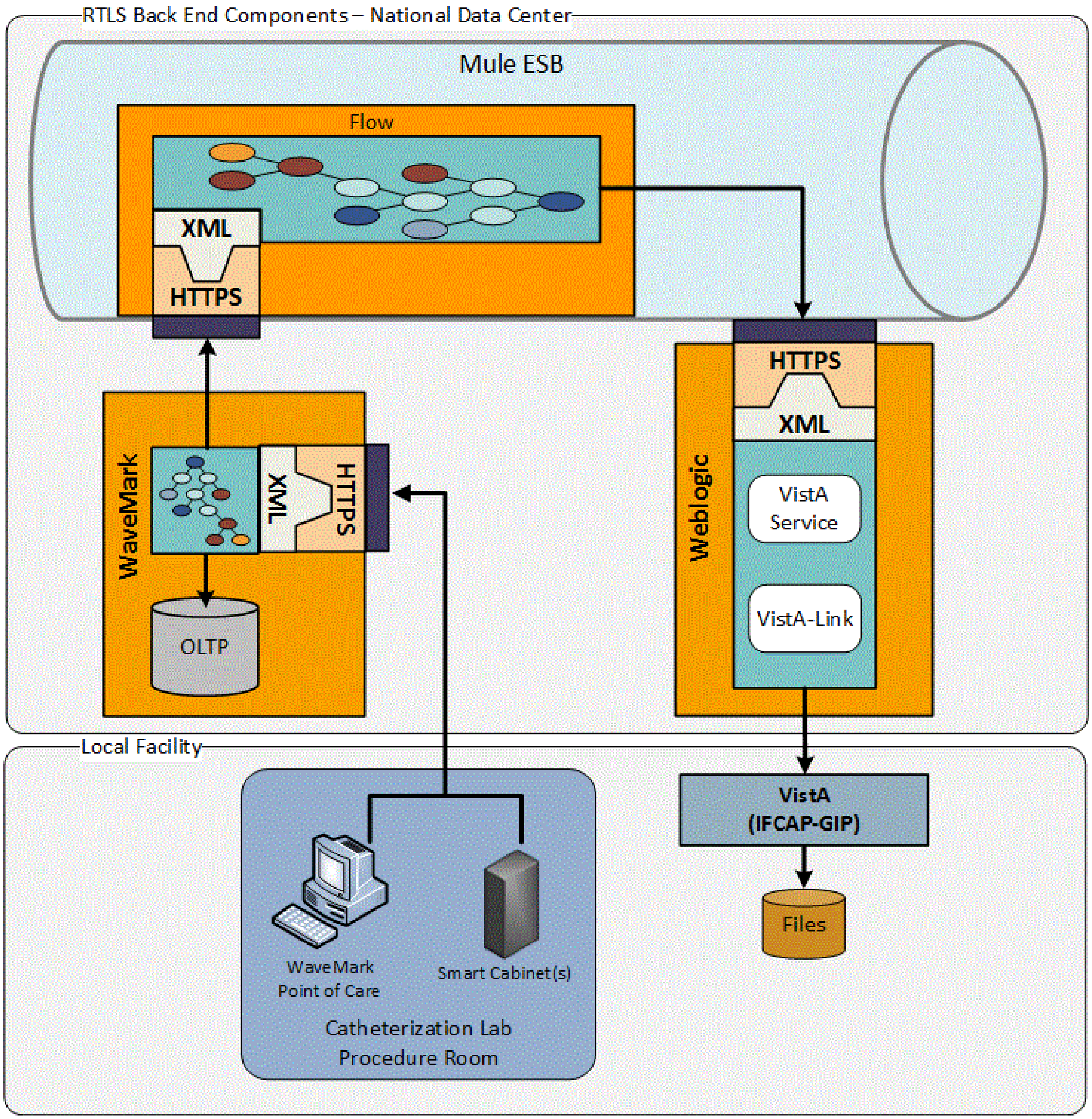
6.2.6.2 IFCAP/GIP

The Generic Inventory Package is a module of VistA Integrated Funds Control, Accounting and Procurement System that resides locally and manages the receipt, distribution, and maintenance of stock items received for the supply warehouse from outside vendors and distributed to primary inventory points. The GIP maintains the inventory record for expendable/consumable supplies, such as those typically stored in cabinets and storage rooms and used for patient care. When some of these items are tagged with RFID passive tags, the system will automatically update GIP with current inventory levels and tagged item location information.

An interface between IFCAP-GIP and the WaveMark Engine via the Mule ESB exists. This interface is used to populate item data in the two systems. The interface is used to sync supply details such as quantities and item master numbers. A uni-directional interface exists between Mule ESB and the WaveMark Platform. A uni-directional interface exists between Mule ESB and VistA's IFCAP-GIP.

The figure below shows the overall IFCAP-GIP interface architecture. One interface sits on the Mule ESB that receives requests from the WaveMark Engine. Mule ESB exposes its services via RESTful Web Services over standard HTTPS protocol. The Mule ESB does not directly contact the WaveMark Engine, only accepting data and passing data back when requested by the WaveMark Engine. A second interface sits within the Weblogic server that receives requests from Mule ESB. This interface also retrieves data from VistA. The VistA (IFCAP-GIP) interface is exposed via RPCs on VistA using a VistA-Link listener.

Figure 95: IFCAP-GIP Interface Architecture



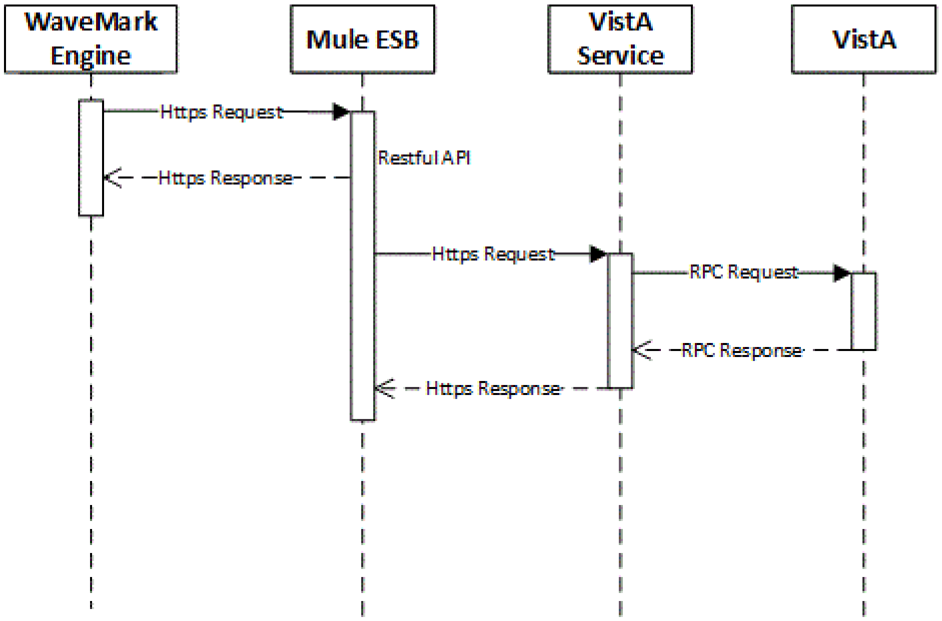
The IFCAP/GIP RTLS System Interface will use two interactions for data movement:

- On Hand Link (uni-directional data flow) – WaveMark will send an XML request detailing what items are in the departmental servers (cabinets) and the quantity of those items by inventory point.
- Master Item Update (bi-directional data flow) – WaveMark will make a request to receive IFCAP-GIP data using XML which details expendable/consumable supplies' master item number (manufacturer and model number).

6.2.6.2.1 On Hand Link

The On Hand Link component is the first of the two mechanisms for the interface between IFCAP-GIP and the WaveMark Engine. The figure below shows the sequence of events in the One Hand Link Mechanism.

Figure 96: IFCAP-GIP On Hand Link Sequence

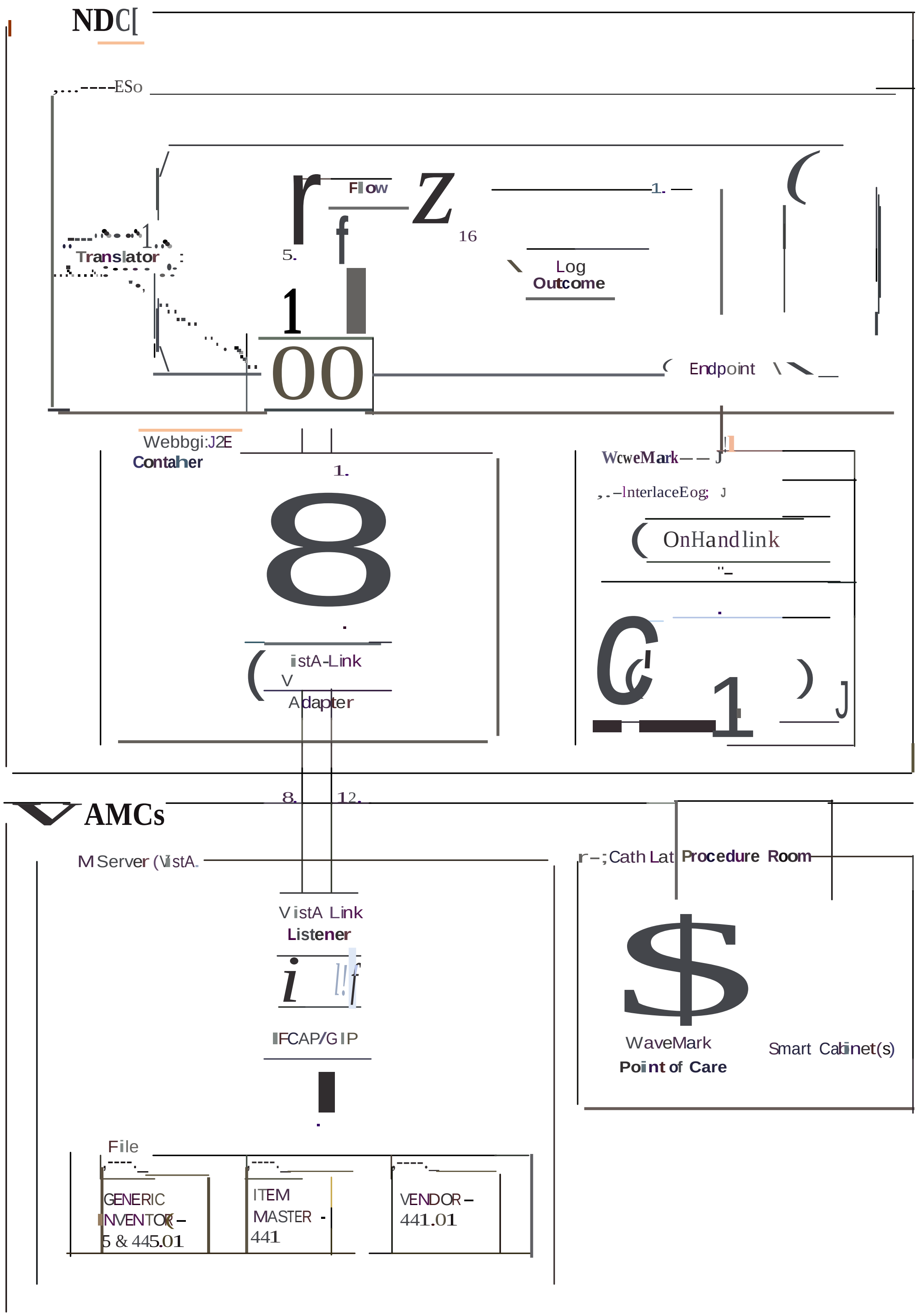


The figure below represents the RTLS IFCAP/GIP Interface data flow for the inventory on hand process. Data will flow in the following sequence in the below figure:

1. The WaveMark equipment (Smart Cabinet(s) and Point of Care) will make a call to the Engine's API service with updated quantity information.
2. The WaveMark engine pushes the quantity information to the OnHandLink interface within the WaveMark Interface Engine.
3. The OnHandLink interface formats the message and makes a call to the endpoint on the ESB.
4. The endpoint pushes the message to the flow (Service Orchestration).
5. The flow acquires a connection to the VistA-Service layer
6. The message is sent to the VistA-Service.
7. The service inside of VistA-Service receives the request and makes a remote procedure call to the VistA-Link layer.
8. The Service acquires a connection to the VistA-Link listener and makes RPC call to the IFCAP/GIP module.
9. The VistA-Link listener receives the RPC and funnels it to the IFCAP/GIP Module.

10. The IFCAP/GIP modules receive the message and a call is made to the various files in IFCAP/GIP (GENERIC_INVENTORY_445 and INVENTORY_TRASACTION_445_2).
11. The IFCAP/GIP module assembles a reply message and sends it back through the VistA-Link Listener.
12. The reply message is sent back over TCP-IP to the VistA-Link Adapter.
13. The Service receives the response.
14. The Service builds a message and returns to the ESB.
15. The reply message is received by the flow.
16. A result (processed or failure) is logged.

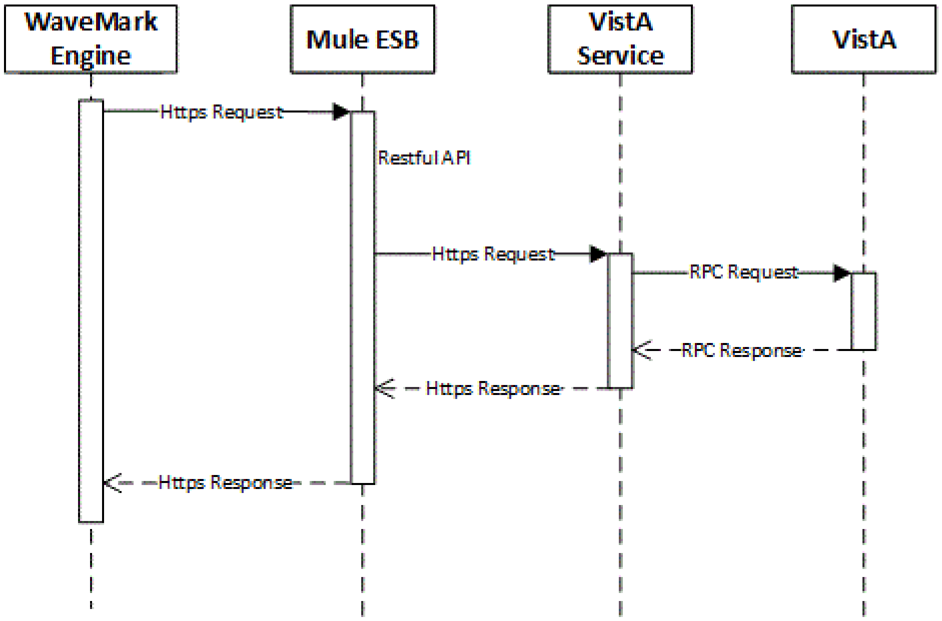
Figure 97: IFCAP/GIP On Hand Link Data Flow



6.2.6.2.2 *Master Item Update*

The Master Item Update component is the second of the two mechanisms for the interface between IFCAP-GIP and the WaveMark Engine. The figure below shows the sequence of events in the Master Item Update Mechanism.

Figure 98: IFCAP-GIP Master Item Update Sequence

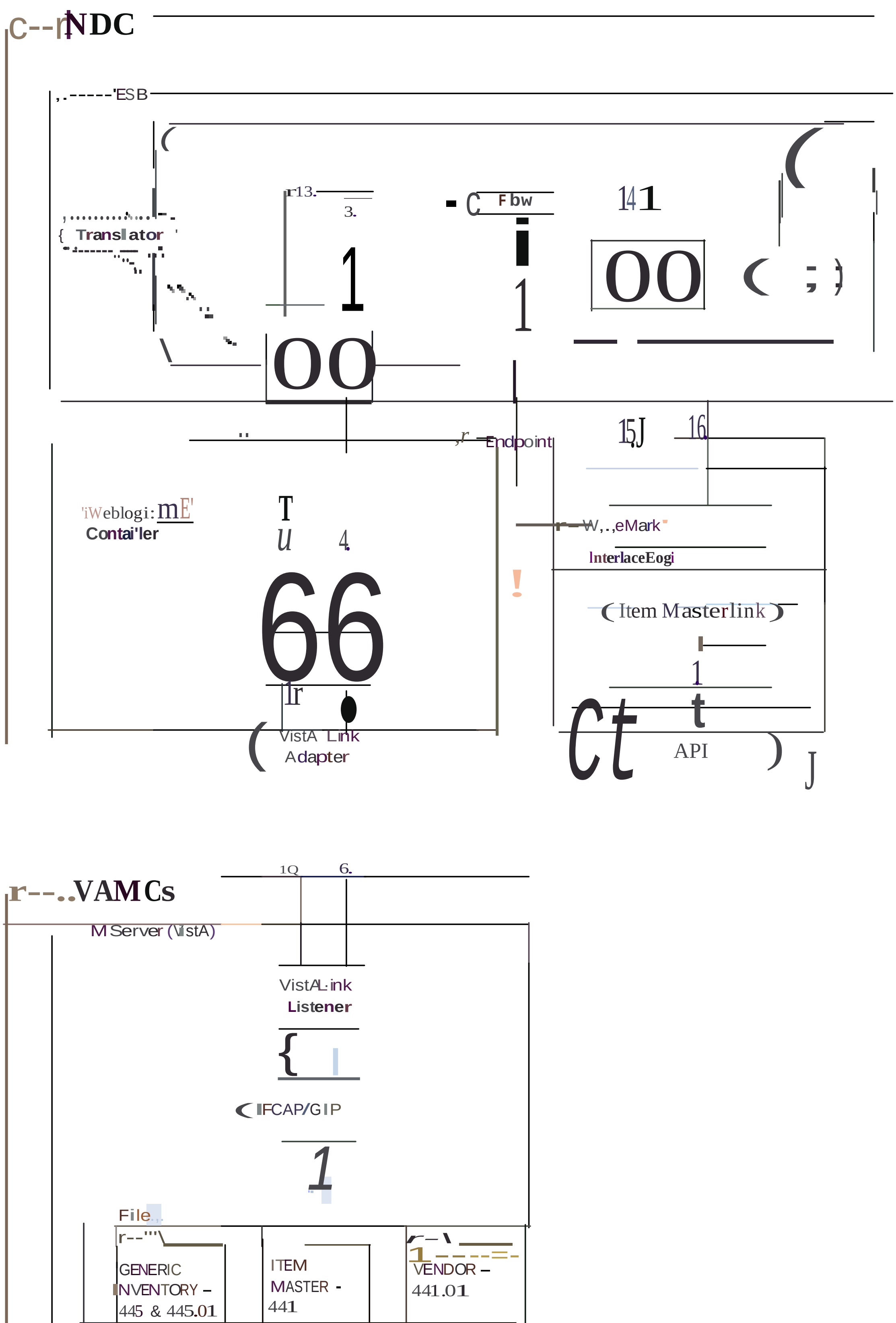


The figure below represents the RTLS IFCAP/GIP Interface data flow for the item master update process. Data will flow in the following sequence in the below figure:

1. A Scheduled job will be triggered with the WaveMark Interface Engine. The ItemMasterLink calls the endpoint on the ESB.
2. The endpoint pushes the message to the flow (Service Orchestration).
3. The XML message will be transformed to the VistA-Service message format.
4. The message is sent to the VistA-Service service layer over HTTPs using a RESTful interface.
5. The service inside of VistA-Service receives the request and makes a procedure call to the VistA-Link layer.
6. The service acquires a connection to the VistA-Link listener and makes a RPC call to the IFCAP/GIP module.
7. The IFCAP/GIP modules receive the RPC call and do some pre-processing on it.
8. A call is made to the various files in IFCAP/GIP.
9. The IFCAP/GIP module assembles response data.
10. The reply message is sent back over TCP-IP to the VistA-Link Adapter.
11. The Service receives the message and processes it for return to the ESB (build message).
12. The reply message is sent back to the ESB.

13. The flow calls the transformer.
14. The XML within the file will be transformed to the WaveMark desired message format.
15. The formatted message is pushed back through the connection (response).
16. The WaveMark engine receives the response.
17. The message is sent to the WaveMark API where the Item Master Numbers are synced with IFCAP-GIP.

Figure 99: IFCAP/GIP Item Master Data Flow

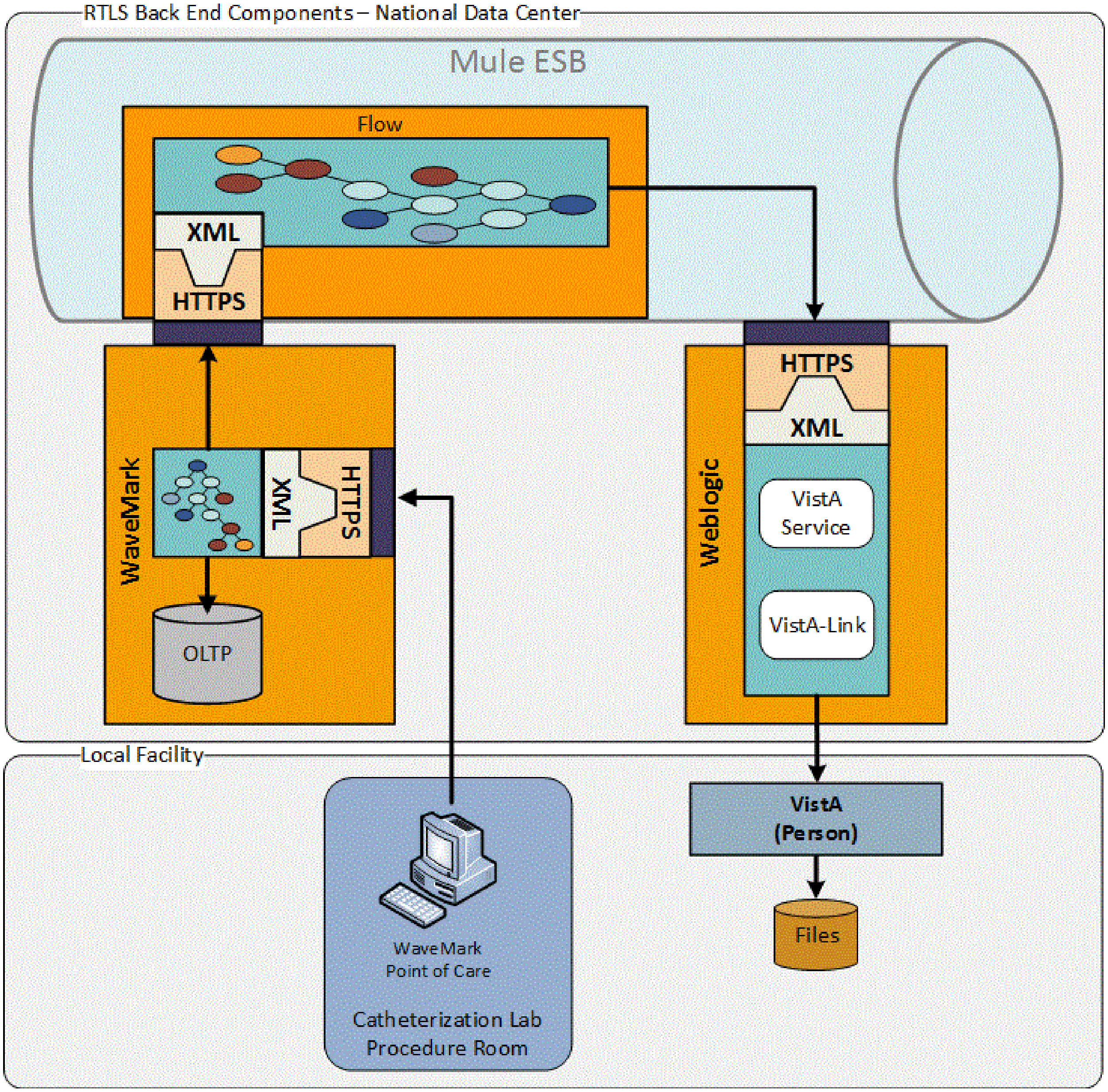


6.2.6.3 Employee

An interface between Employee (VistA) and WaveMark Engine via the Mule ESB exists. This interface is used to populate WaveMark Engine with data about employees. A uni-directional interface exists between Mule ESB and the WaveMark Engine. A uni-directional interface exists between Mule ESB and VistA's Employee.

The figure below shows the overall Employee interface architecture. One interface sits on the Mule ESB that receives requests from the WaveMark Engine. Mule ESB exposes its services via RESTful Web Services over standard HTTPS protocol. A second interface sits within the Weblogic server that receives requests from Mule ESB. This interface also retrieves data from VistA. The VistA (Employee) interface is exposed via RPCs on VistA using a VistA-Link listener.

Figure 100: Employee Search Interface Architecture



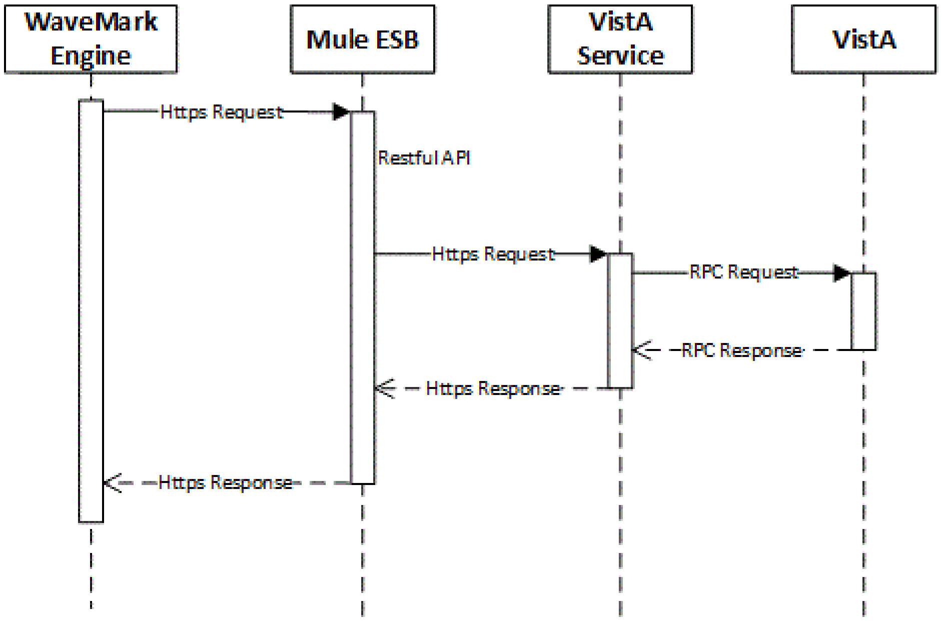
The Employee RTLS System Interface will use the following interaction for data movement:

- Employee Search (bi-directional data flow) – search for an employee to be added to the WaveMark System for download to the Point of Care Station.

Employee Search

The Employee Search component is the mechanism for the interface between Employee and the WaveMark Engine. The figure below shows the sequence of events in the Employee Search Mechanism.

Figure 101: Employee Search Interface Sequence



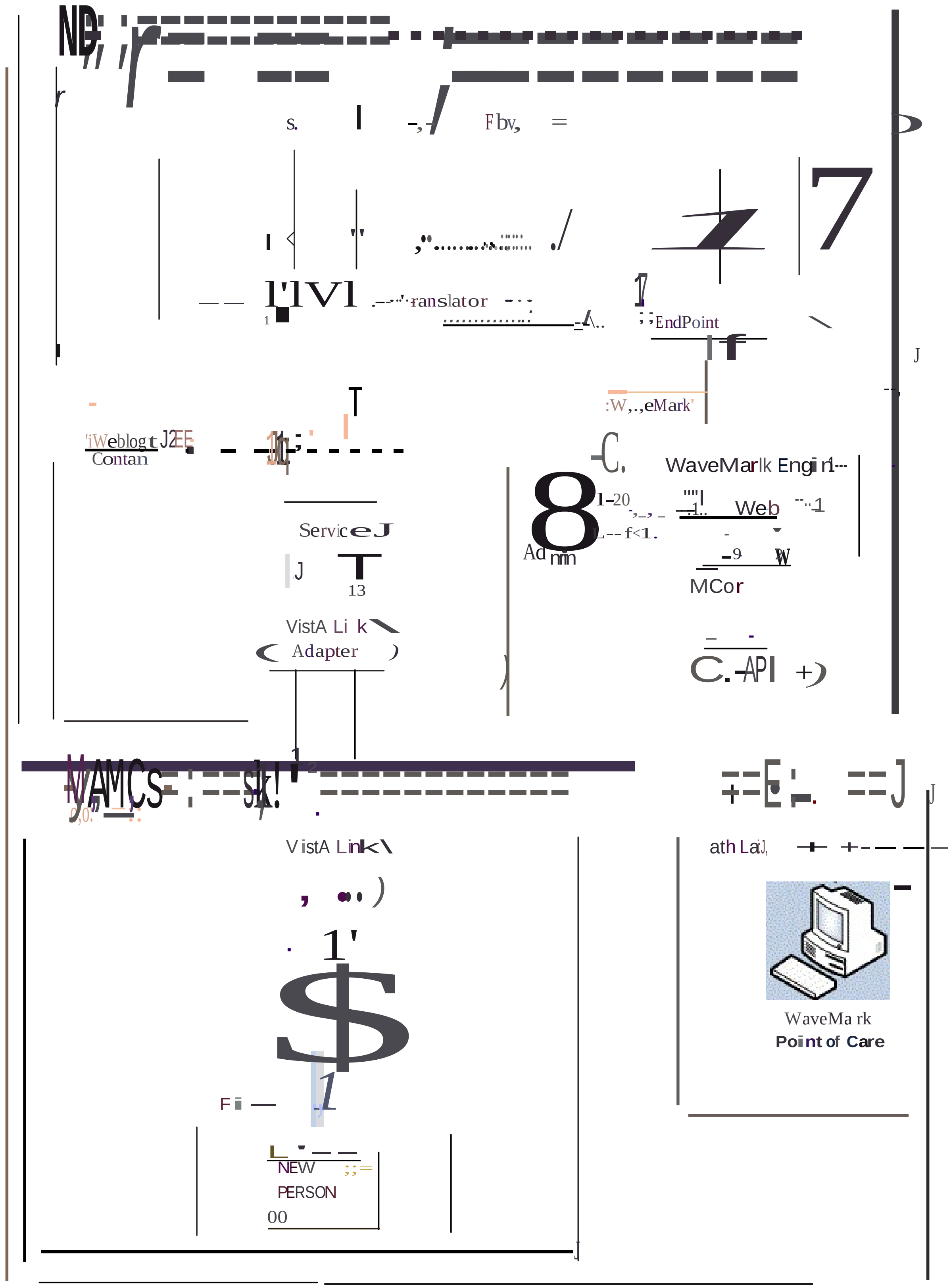
The figure below represents the RTLS Employee Interface data flow for the Employee Search process. Data will flow in the following sequence in the below figure:

1. An Administrator enters search criteria in a web browser.
2. The WaveMark Web Component receives the message and forwards it to the WMCore.
3. The WaveMark WM Core sends a message (REST message over HTTPS) to an endpoint on the ESB.
4. The endpoint passes the message to the flow (Service Orchestration) on the ESB.
5. A message is transformed to the VistA-Service desired message input.
6. VistA-Service receives the request.
7. The Service acquires a connection to the VistA-Link listener.
8. The VistA-Link Listener makes a RPC call to the Employee module.
9. The Employee modules receive the RPC call and pre-process it (formatting & scrubbing).
10. A call is made to the various files in Employee (NEW PERSON #200).
11. The Employee module assembles any data that is returned by the file system.
12. The reply message is sent back over TCP-IP to the VistA-Link Adapter.
13. The VistA-Service receives the message and processes it for reply to the ESB (build message).
14. The reply message is sent back to the ESB.

15. The flow receives the message.
16. The flow calls the transformer to format the message to the WaveMark format.
17. The endpoint receives the message.
18. A response is sent back to the WaveMark Core.
19. The WaveMark WMCore receives the reply and sends a message to the Web Component.
20. The Web Component displays the Search Results to the Administrator.
21. The Administrator selects the appropriate employee member to be added to the System.
22. The WaveMark Point of Care Station periodically requests for an updated Employee File.
23. The WaveMark API forwards the request to the WMCore and the update Employee File is sent back to the API.
24. The API forwards the file back to the Point of Care Station.

Notes: Steps 20 through 21 can be overridden by the Administrator. The Administrator can force an immediate update to the Point of Care Station by pressing "Refresh" in the Web Component.

Figure 102 Employee Search DataFlow

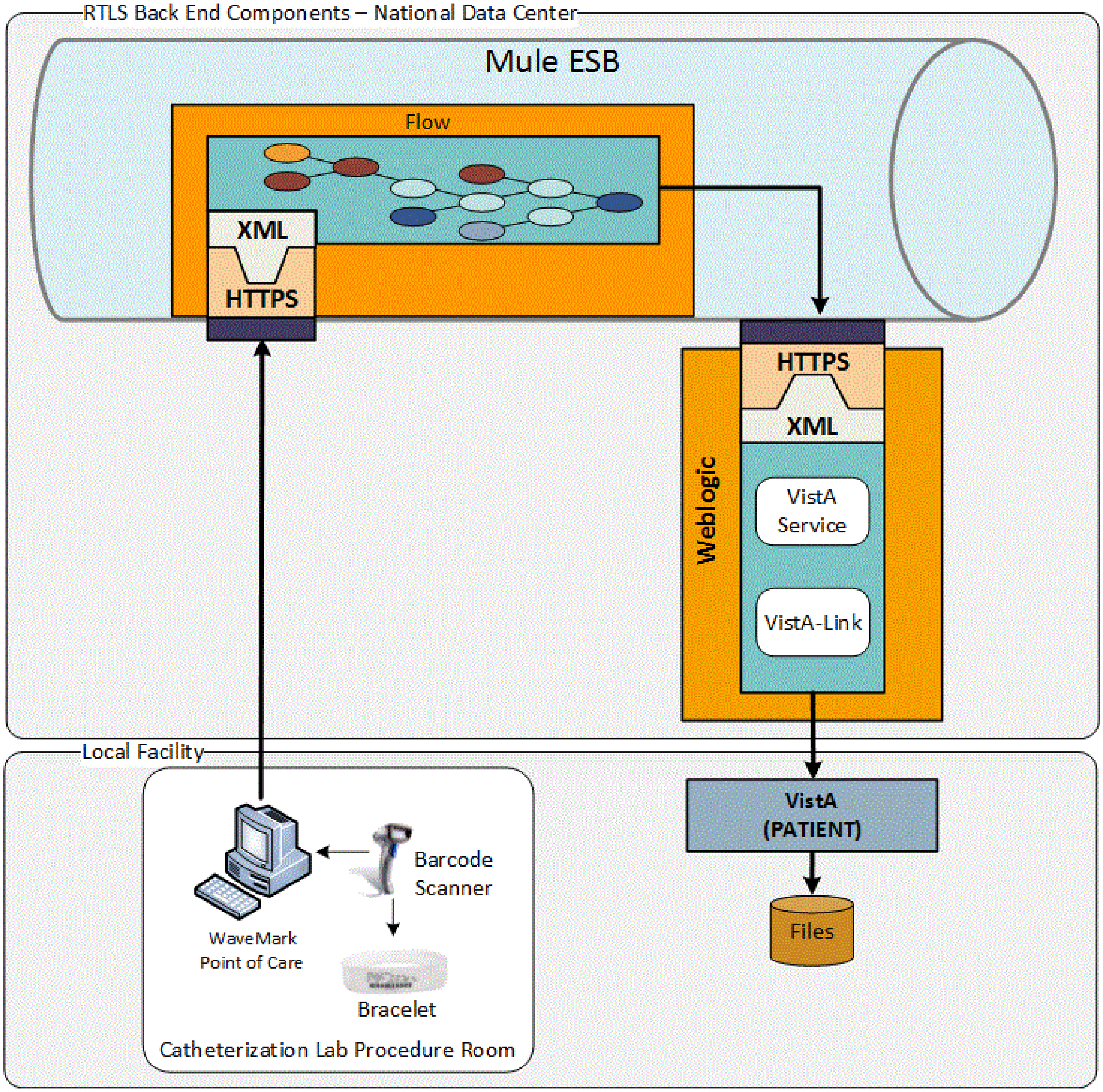


6.2.6.4 **Patient**

To ensure patient safety, the WaveMark associates the patient and procedure information with the supplies used to capture usage and document supplies used for patient care. A uni-directional interface between the VistA Patient file and WaveMark provides a level of accuracy to ensure the patient is positively identified during a procedure. WaveMark uses the Patient file to do a lookup of patent name by providing the patient's unique identifier which is scanned from the patient wristband.

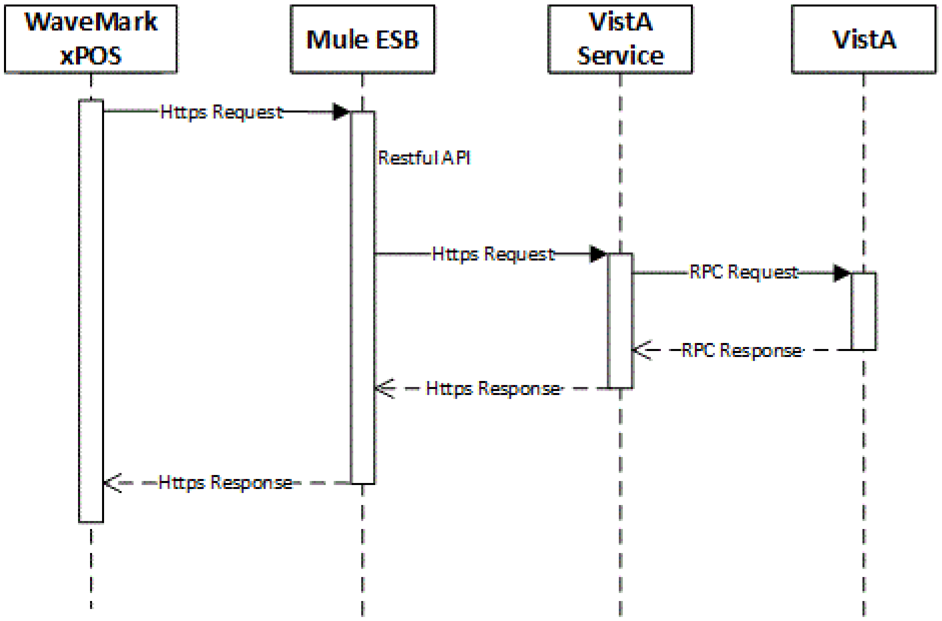
The figure below shows the overall Patient interface architecture. One interface sits on the Mule ESB that receives requests from the WaveMark xPOS. Mule ESB exposes its services via RESTful Web Services over standard HTTPS protocol. This is a real time process initiated by a barcode scanner connected to the WaveMark xPOS system that scans the patient wristband to collect the patient's unique identifier. A second interface sits within the Weblogic server that receives requests from Mule ESB. This interface also retrieves data from VistA. The VistA (Patient) interface is exposed via RPCs on VistA using a VistA-Link listener. The unique identifier from Mule ESB is passed as a parameter via a RESTful API call to the Patient file. The patient data is retrieved by executing the RPC.

Figure 103: Patient Interface Architecture



The Patient component is the mechanism for integration between Patient and the WaveMark xPOS. The figure below shows the sequence of events in the Patient Interface.

Figure 104: Patient Interface Sequence

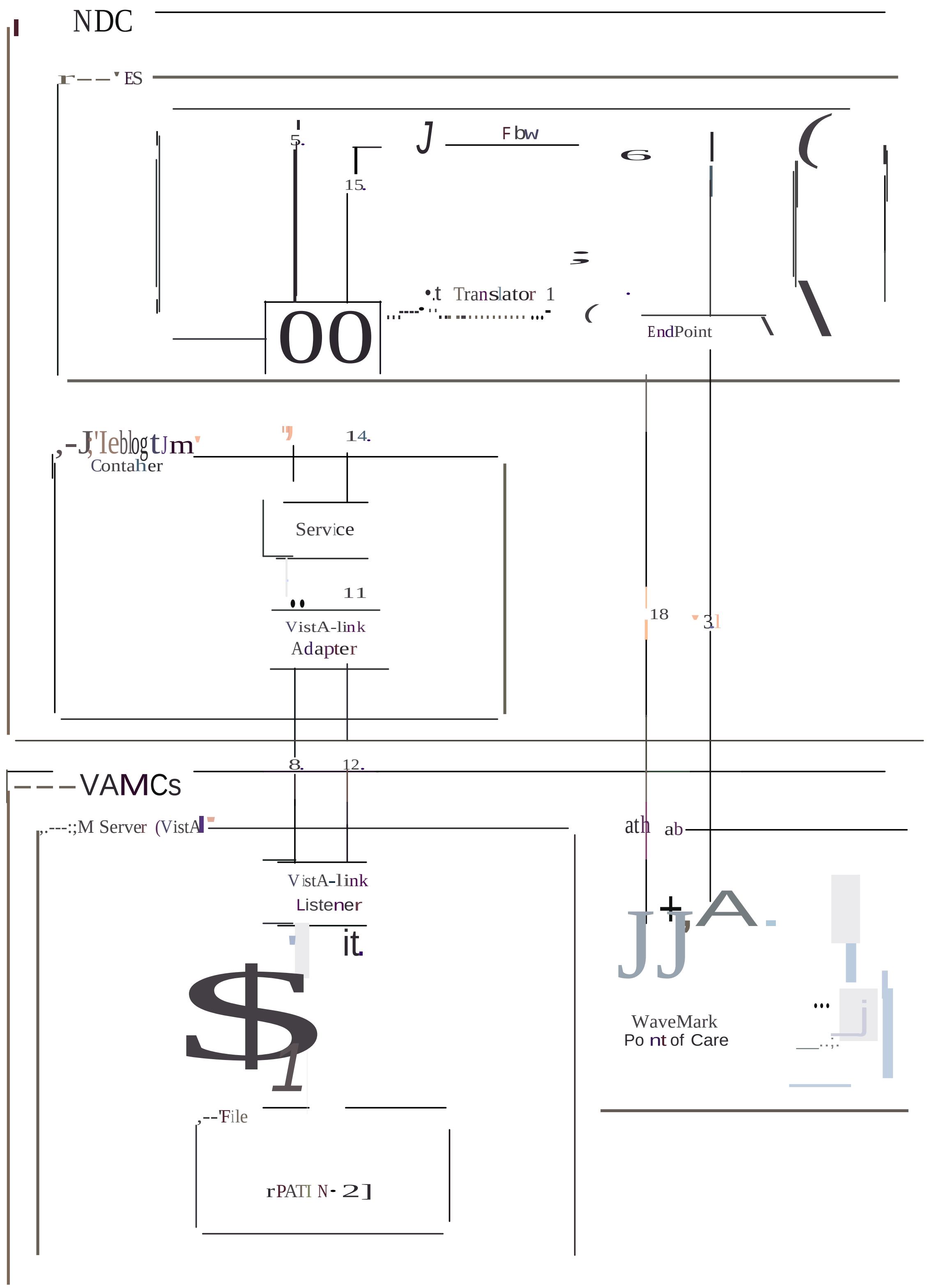


The figure below represents the Patient Search interactions between the RTLS Catheterization Lab System and the VistA Patient application. Data will flow in the following sequence based on the below figure:

1. An employee scans a patient's bracelet.
2. The scanner transmits the data to the Point of Care System.
3. The Point of Care System sends a message (REST message over HTTPS) to an Endpoint on the ESB.
4. The Endpoint pushes the message to the flow (Service Orchestration) on the ESB.
5. A message is transformed to the VistA Service desired message input.
6. VistA-Service receives the request.
7. The Service acquires a connection to the VistA-Link listener.
8. The VistA-Link Listener makes a RPC call to the PATIENT module.
9. The PATIENT modules receive the RPC call and pre-process it (formatting & scrubbing).
10. A call is made to the various files in PATIENT.
11. The PATIENT module assembles any data that is returned by the file system.
12. The reply message is sent back over TCP-IP to the VistA-Link Adapter.
13. The VistA-Service receives the message and processes it for reply to the ESB (build message).
14. The reply message is sent back to the ESB.
15. The flow receives the message.

16. The flow calls the transformer to format the message to the WaveMark format.
17. The Endpoint sends the response back to the Point of Care System.
18. The Point of Care System receives the reply.

Figure 105: Patient Search Data Flow



6.2.6.5 **CART-CL**

The Cardiovascular Assessment Reporting and Tracking system for Catheterization Labs (CART-CL) is a VHA developed software application for standardized data capture and report generation, national SQL data repository, and national quality improvement program for VA Catheterization labs. The application is integrated with VA's Computerized Patient Record System and Electronic Health Record system enabling providers to document care as part of routine clinical work. The CART-CL application provides discrete data entry (based on American College of Cardiology standards) with narrative text for customization. All CART-CL data is stored in a single national repository. Predefined data entry fields will be sent from the RTLS enabled smart cabinets to prepopulate a patient procedure report. The information required is identifiable from the Catheterization lab item consumables and devices used during the case and patient information.

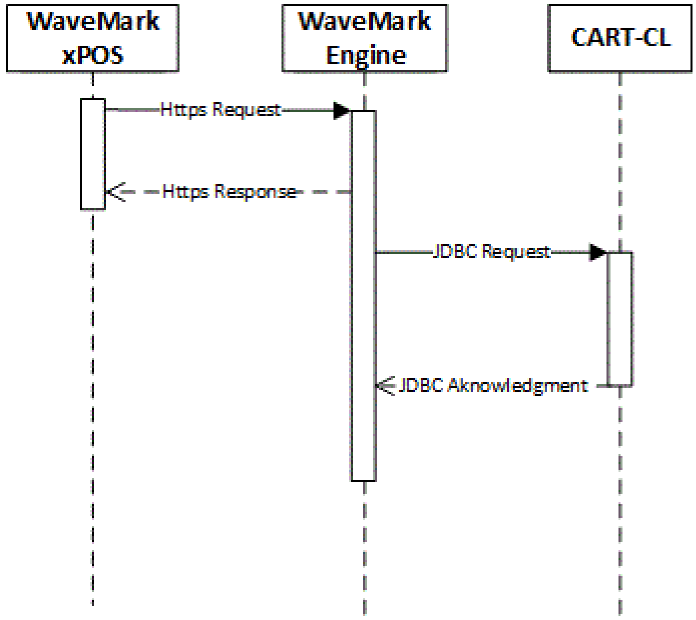
An interface between the WaveMark Engine and the CART-CL database will exists. This interface is used to populate CART-CL with data about consumable supplies used during patients' encounters in the Cardiac-Catheterization Lab. A uni-directional interface exists between the WaveMark Engine and CART-CL.

The figure below shows the overall CART-CL interface architecture. The interface sits in the CART-CL and receives data from the WaveMark Engine.

Figure 106: CART-CL Interface Architecture

The WaveMark Engine is the mechanism for the interface between the WaveMark xPOS and CART-CL. The figure below shows the sequence of events in the CARTL-CL Interface.

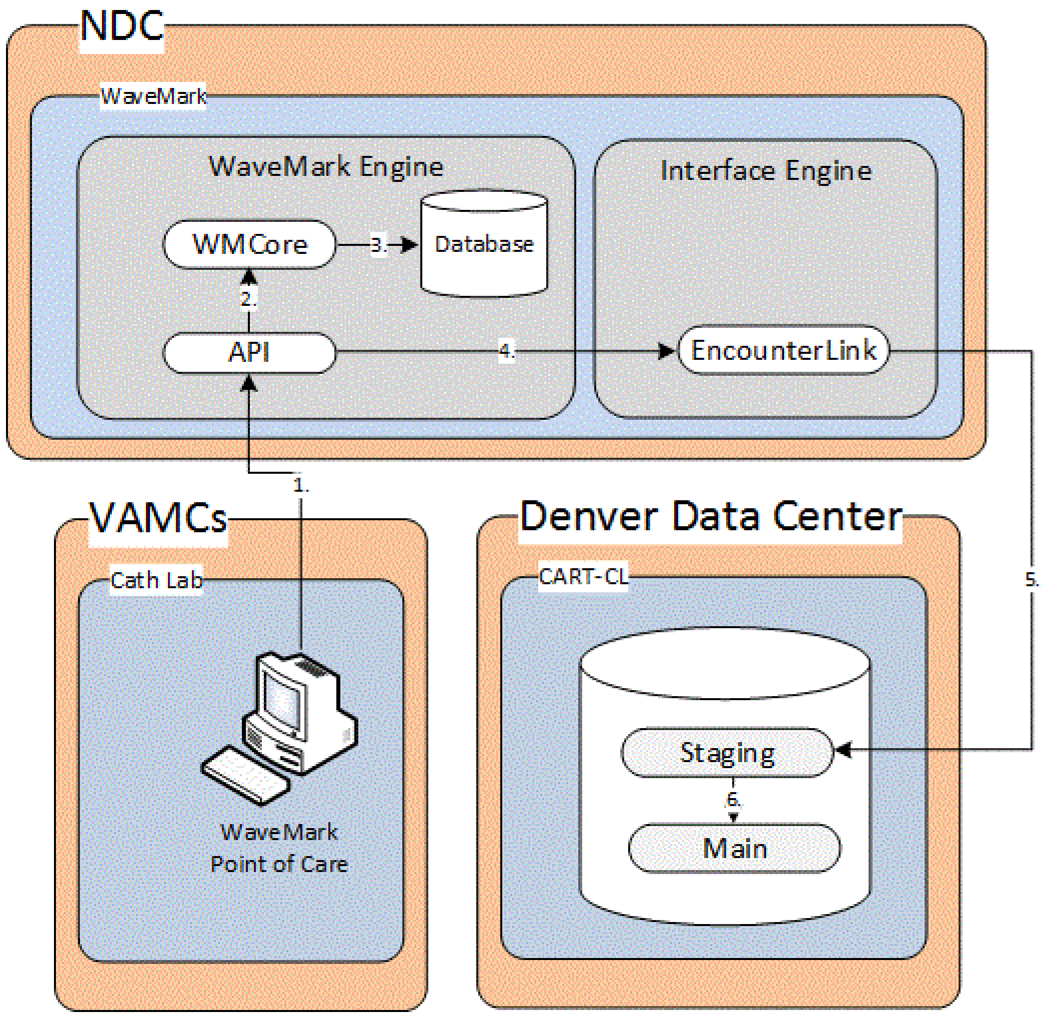
Figure 107: CART-CL Interface Sequence



The figure below represents the WaveMark to CART-CL Interface Data Flow. Data will flow in the following sequence in the below figure:

1. A Patient Encounter is closed and the encounter data is sent to the WaveMark Engine from the WaveMark Point of Care
2. The data is sent to the WMCore where any business rules are applied
3. The processed data is sent to the WaveMark database for persistence
4. The data is sent to the WaveMark Interface Engine (EncounterLink)
5. The data is sent to the staging schema within CART-CL
6. The data is massaged and placed the Main CART-CL database

Figure 108: CART-CL Data Flow



6.3 Communications Detailed Design

The RTLS system will use a variety of protocols to communicate between the various systems and components. This section will provide details about the protocols that are used and blueprints on how the communications happen at a software and hardware level.

6.3.1 Protocols Used

6.3.1.1 Low Level Reader Protocol

Low Level Reader Protocol (LLRP) is an EPCglobal standard that specifies an interface between RFID Readers and clients. It is designed as a standard in order for developers to have a common programmatic interface to RFID readers from different manufacturers. The design of this interface recognizes that in some RFID systems, there is a requirement for explicit knowledge of RFID air protocols and the ability to control Readers that implement RFID air protocol communications.

LLRP provides means to command an RFID Reader to inventory RFID tags (read the EPC codes carried on tags), read tags (read other data on the tags apart from the EPC code), write tags, and execute other protocol-dependent access commands (such as 'kill' and 'lock' from EPCglobal Class 1 Generation 2).

LLRP is specifically concerned with providing the formats and procedures of communications between a Client and a Reader.

6.3.1.2 Network Mobility Services Protocol

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility services engine and the controller. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller is managed by this protocol. NMSP runs between the switches and MSE to provide the location information to the MSE. Location information may include the physical address (also known as the civic address) as well as other information about endpoints such as the Internet Protocol (IP) address, Media Access Control (MAC) address, port, Virtual Local Area Network (VLAN), and username.

6.3.1.3 User Datagram Protocol

User Datagram Protocol (UDP-IP) is one of the core members of the Internet protocol suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol network without prior communications to set up special transmission channels or data paths.

UDP uses a simple transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes any unreliability of the underlying network protocol to the user's program. As this is normally IP over unreliable media, there is no guarantee of delivery, ordering or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.

UDP is suitable for purposes where error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real time system.

6.3.1.4 Transmission Control Protocol

Transmission Control Protocol (TCP-IP) is a set of rules (protocol) used along with the Internet Protocol to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent to a browser from a Web server, the Transmission Control Protocol program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end (browser on the computer), TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

6.3.1.5 HyperText Transfer Protocol

HyperText Transfer Protocol (HTTP) is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when a user enters a Uniform Resource Locator (URL) in their browser, this sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it.

HTTP functions as a request-response protocol in the client-server computing model. A web browser, for example, may be the client and an application running on a computer hosting a web site may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body.

6.3.1.6 Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol Secure (HTTPS) is the combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer (SSL) / Transport Layer Security (TLS) protocol to provide encrypted communication and secure identification of a network web server. HTTP operates at the highest layer of the Open Systems Interconnection (OSI) Model, the Application layer; but the security protocol operates at a lower sub layer, encrypting an HTTP message prior to transmission and decrypting a message upon arrival. Strictly speaking, HTTPS is not a separate protocol, but refers to use of ordinary HTTP over an encrypted SSL or TLS connection.

6.3.1.7 File Transfer Protocol

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. TP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

6.3.1.8 Secure File Transfer Protocol

Secure File Transfer Protocol (SFTP) is a network protocol that provides file access, file transfer, and file management functionalities over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capability, but is also intended to be usable with other protocols. The IETF Internet Draft states that even though this protocol is described in the context of the SSH-2 protocol. This protocol assumes that it is run over a secure channel, such as SSH, that the server has already authenticated the client, and that the identity of the client user is available to the protocol.

6.3.1.9 Java Database Connectivity

Java Database Connectivity (JDBC) is a software component enabling a Java application to interact with a database. To connect with individual databases, JDBC requires drivers for each database. The JDBC driver gives out the connection to the database and implements the protocol for transferring the query and result between client and database.

6.3.1.10 Open Database Connectivity

Open Database Connectivity (ODBC) is Microsoft's strategic interface for accessing data in a heterogeneous environment of relational and non- relational database management systems. Based on the Call Level Interface specification of the SQL Access Group, ODBC provides an open, vendor- neutral way of accessing data stored in a variety of proprietary personal computer, minicomputer, and mainframe databases.

6.3.1.11 Object Linking Embedded Database

Object Linking Embedded Database (OLEDB) is an API designed by Microsoft, allows accessing data from a variety of sources in a uniform manner. The API provides a set of interfaces implemented using the Component Object Model (COM). OLE DB interfaces provide applications with uniform access to data stored in diverse information sources, or data stores. These interfaces support the amount of DBMS functionality appropriate to the data store, enabling the data store to share its data.

6.3.1.12 Human Interface Device

Human Interface Device (HID) is a type of computer device that interacts directly with, and most often takes input from, humans and may deliver output to humans. In the HID protocol, there are two entities: the "host" and the "device". The device is the entity that directly interacts with a human, such as a keyboard or mouse. The host communicates with the device and receives input data from the device on actions performed by the human. Output data flows from the host to the device and then to the human.

6.3.1.13 Java Message Service

Java Message Service (JMS) is a Java Message Oriented Middleware (MOM) API for sending messages between two or more clients. JMS is a part of the Java Platform, Enterprise Edition, and is defined by a specification developed under the Java Community Process as JSR 914. It is a messaging standard that allows application components based on the Java Enterprise Edition (JEE) to create, send, receive, and read messages.

6.3.1.14 Lightweight Access Point Protocol

Lightweight Access Point Protocol (LWAPP) is the name of a protocol that can control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring or troubleshooting a large network. The system will also allow network administrators to closely analyze the network. The LWAPP runs on a Wireless Local Area Network (WLAN) controller and on lightweight access points (LWAPs) to route packets in and out of the WLAN on optimal routes. In other words, the WLAN controller is the gateway of the WLAN to the LAN.

6.3.1.15 Cisco Compatible Extensions

The Cisco Compatible Extensions (CCX) Specification describes a list of functional extensions to the IEEE 802.11 Wireless LAN standard to support fast roaming (CCKM) with upgraded security, reliability, and diagnostic performance. This specification is Cisco proprietary and a device manufacturer requires a Cisco license agreement in order to develop mobile devices with this technology.

6.3.1.16 Gen2IR

Gen IR devices can be positioned wherever accurate location data is needed including rooms, hallways, and bays. Similar to light, Gen2IR will not pass through walls, and it does not suffer from traditional infrared and ultrasound line of sight limitations.

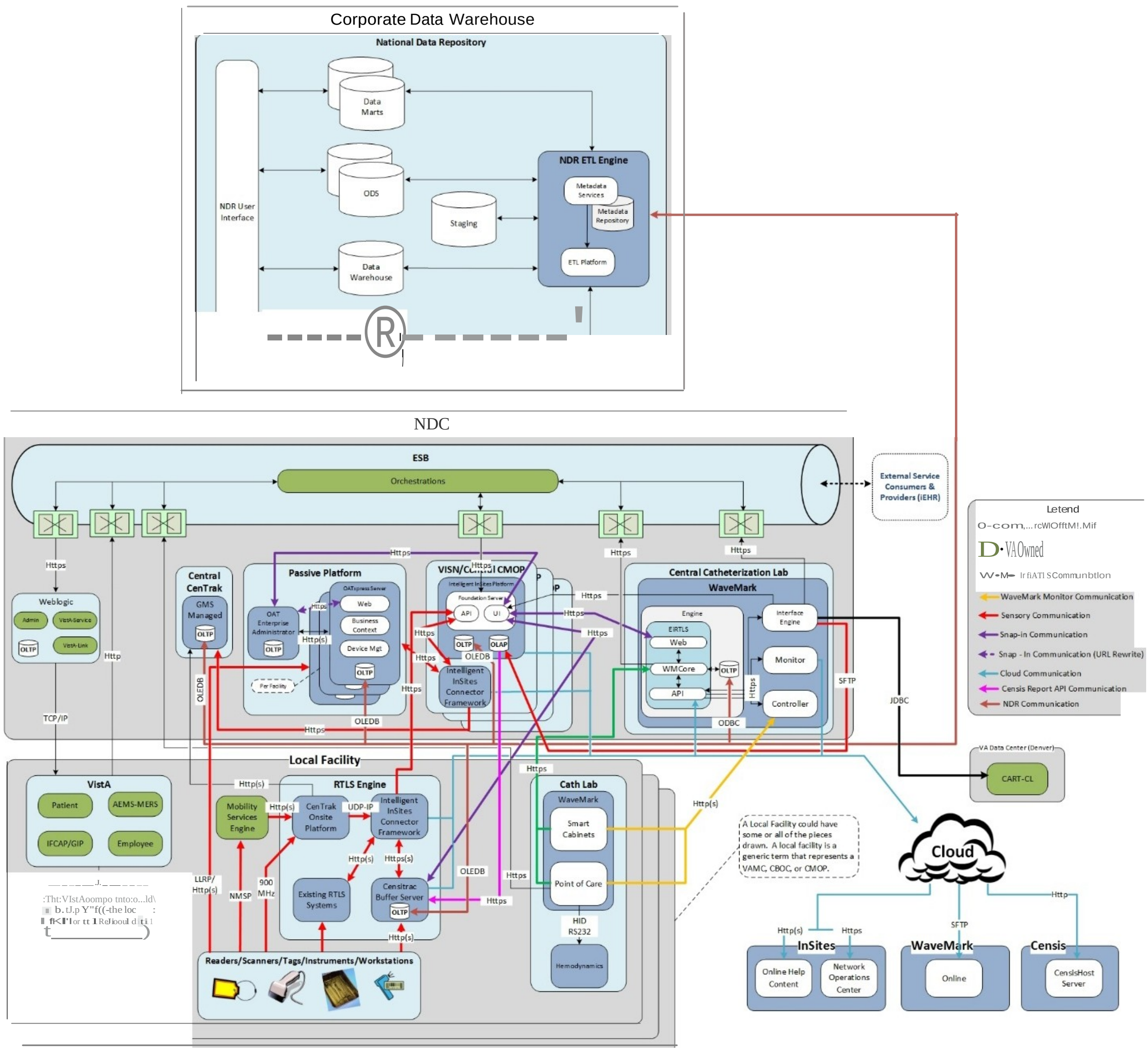
6.3.1.17 RS232

In telecommunications, RS-232 is the traditional name for a series of standards for serial binary single-ended data and control signals connecting between DTE (data terminal equipment) and DCE (data circuit-terminating equipment). The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pin out of connectors. In RS-232, user data is sent as a time-series of bits. Both synchronous and asynchronous transmissions are supported by the standard. In addition to the data circuits, the standard defines a number of control circuits used to manage the connection between the DTE and DCE. Each data or control circuit only operates in one direction that is, signaling from a DTE to the attached DCE or the reverse. Since transmit data and receive data are separate circuits, the interface can operate in a full duplex manner, supporting concurrent data flow in both directions.

6.3.2 Software Communications

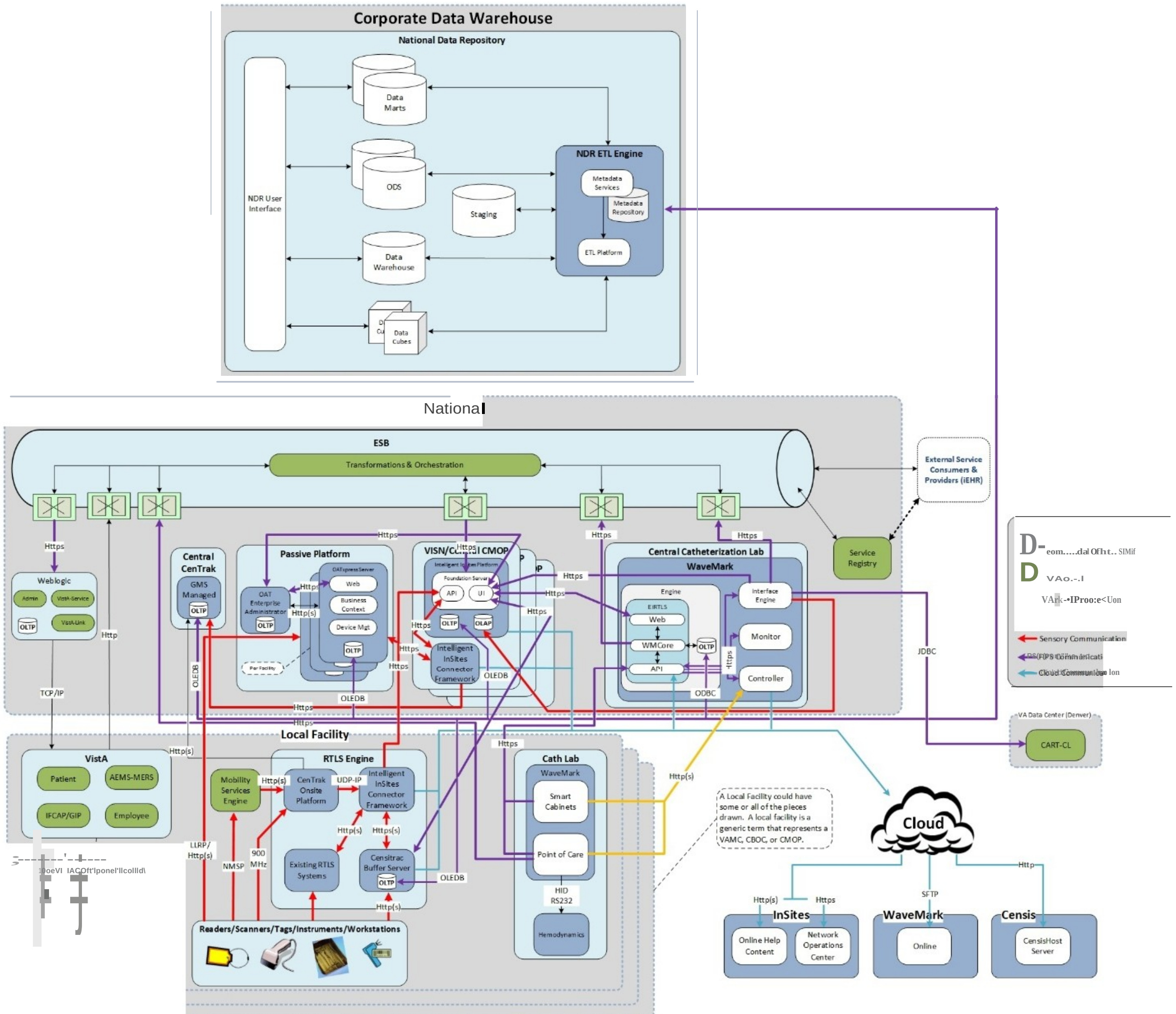
The figure below shows the communications of the integration architecture and the used protocols.

Figure 109: Software Communication Architecture



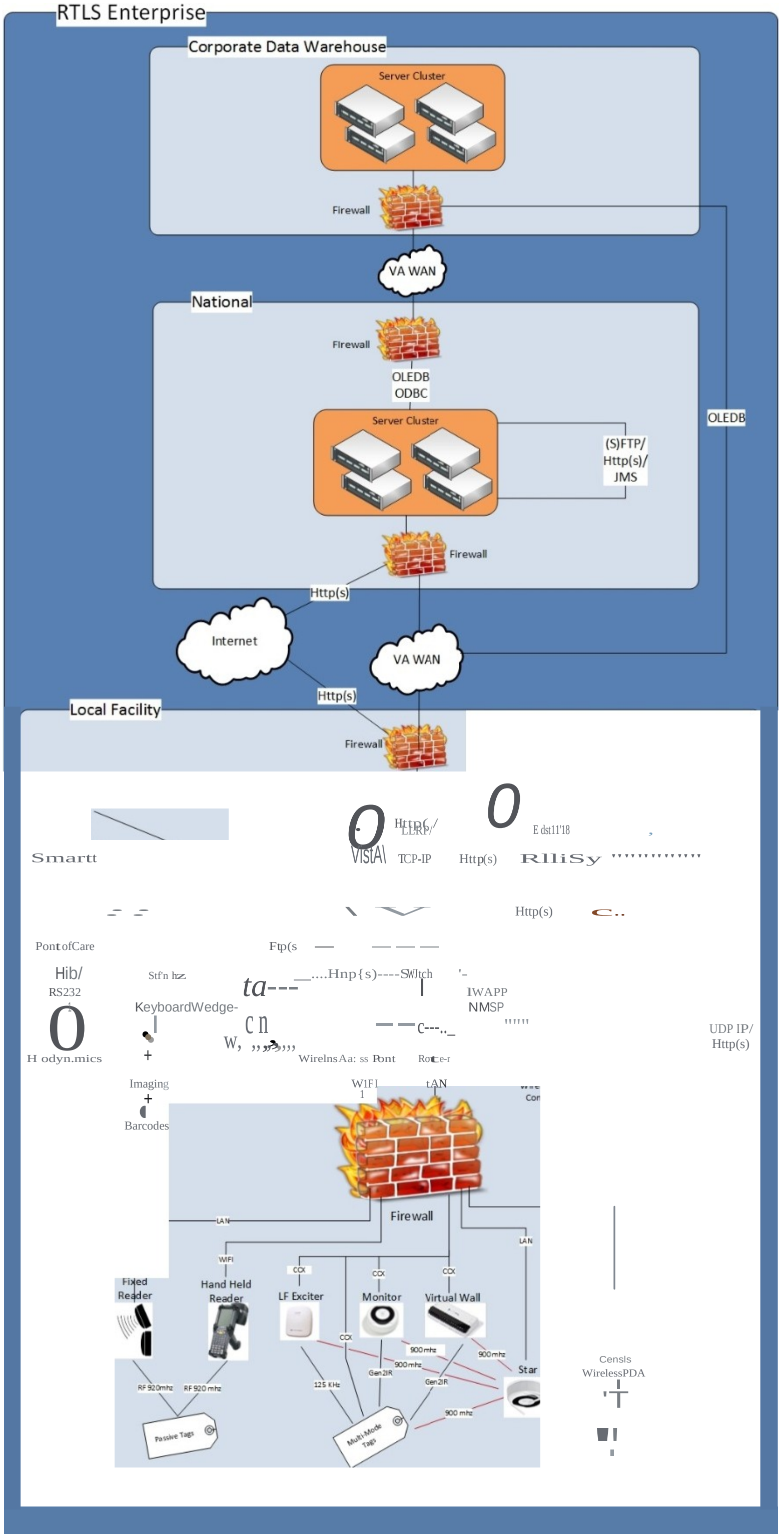
The figure below shows the FIPS communications of the integration architecture and the used protocols.

Figure 110: FIPS Communication Architecture



6.3.3 Hardware Communications

Figure 111: Hardware Communication Architecture



7 External Interface Design

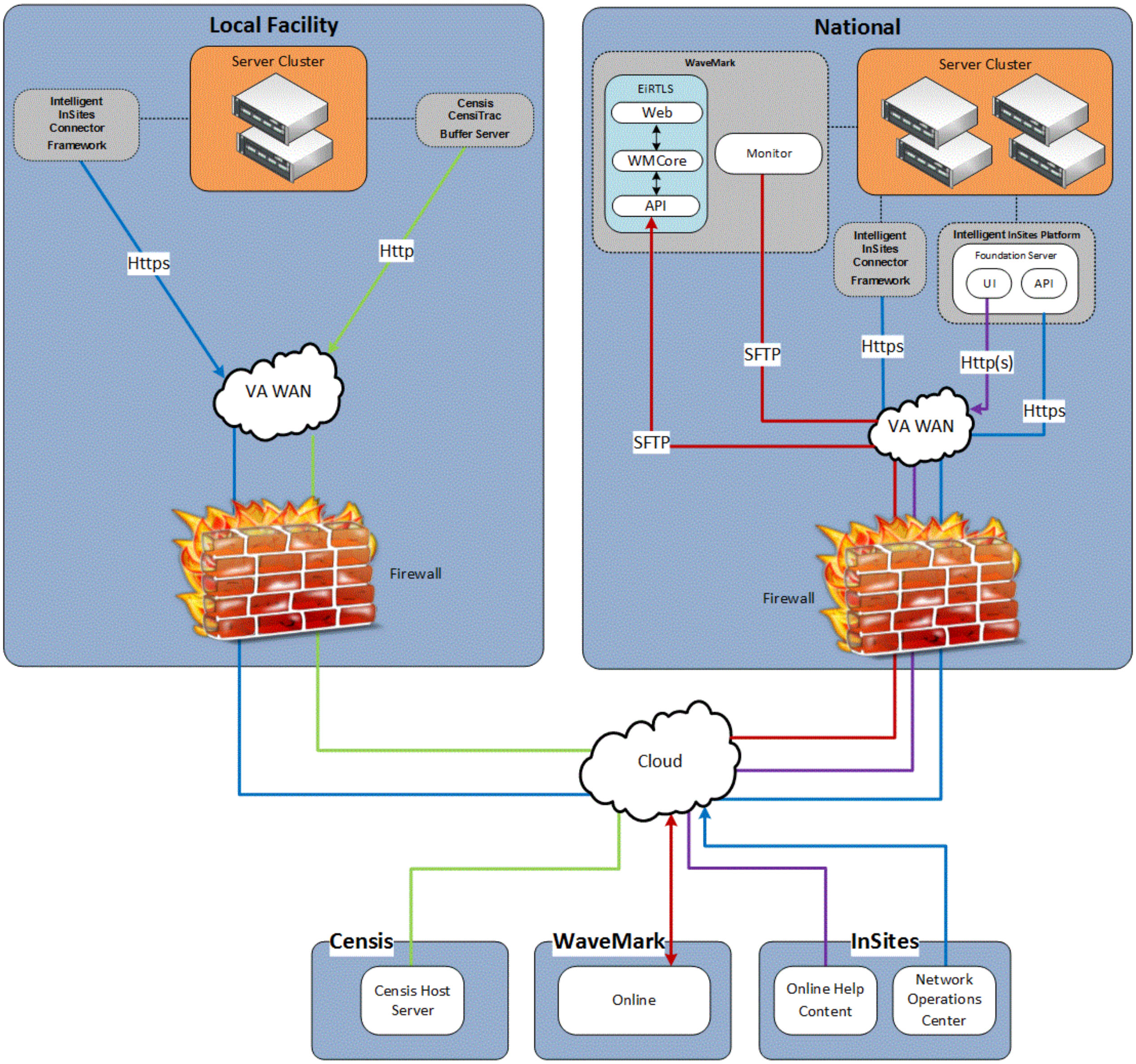
The RTLS system is a system of systems (pattern within Service Orient Architecture) which primarily utilizes secured web services for the invocation of and transfer of data between systems. Other protocols and payloads are utilized only when the service communicating with the RTLS System does not support a web service interface (such as the Censis Host Server). This section of the SDD describes the interfaces exposed by the RTLS System to external systems.

7.1 Interface Architecture

The diagram below illustrates the RTLS External Interface Architectures including all network pathways and protocols used by all systems participating. The arrows included in the diagram indicate which systems are originating requests. For instance, communication between the Intelligent InSites Connector Framework and the Intelligent InSites Network Operations Center (NOC) originate from the Intelligent InSites NOC.

All web content exposed by the RTLS System to the outside world (whether it be VA Wide Area Network (WAN) or via the Internet) is secured (payload is encrypted). Any communications between systems hosted within the overall system are also secure and communications between these systems are encrypted.

Figure 112: External Interface Architecture



7.2 Interface Detailed Design

7.2.1 Intelligent InSites External Interfaces

The Intelligent InSites COTS has a built-in feature which provides monitoring of the deployed software pieces at both the local facility and national levels. This feature is referred to as Network Operations Center (NOC). The NOC handles server monitoring as well as configuration of the Intelligent InSites Services.

Local Facility Level Interfaces

The Intelligent InSites Connector Framework at each local facility will "check-in" with the NOC once every 60 seconds. The call will take place using HTTPs using a RESTful Web Service message.

National Level Interfaces

The National Level external Interfaces have two pieces. One, for every VISN and one CMOP level Intelligent InSites Platform and Connector Framework will call the NOC in a similar fashion to the local facility level Connector Framework (once every 60 seconds over HTTPs using a RESTful Web Service message). The second piece is the Intelligent InSites Online help content. The Unified User Interface housed in the Intelligent InSites Platform will access the Intelligent InSites Online Help through the Internet (HTTP/s).

7.2.2 Censis External Interfaces

The Censis CensiTrac Buffer System (local facility) will connect to an external interface located on the Censis cloud. The CensiTrac Buffer System will connect to the Censis Host Server using HTTP and send bytes over the IP and port connection. The data that will be sent to the Host Server is needed for database backups and discovery procedures.

7.2.3 WaveMark External Interfaces

The WaveMark Online component will provides interfaces to support inbound and outbound SFTP data exchanges.

Inbound Data: This unidirectional software interface will import RFID product registration data from WaveMark's server. This interface captures the data created by medical devices suppliers who are using WaveMark to RFID tag and register products for the VA. When these pre-tagged RFID products arrive they will not need to be tagged and registered by VA personnel as they will already be defined in the VA RTLS system. This interface downloads the data using a secure FTP (SFTP) connection.

Outbound Log Data: This unidirectional software interface will export WaveMark performance and log data from the VA environment to a centralized WaveMark monitoring server. The data is uploaded using a secure FTP (SFTP) connection. (*Note: This is an optional interface. WaveMark does not require this interface to manage the system. If this interface doesn't exist then management will be done from behind the VA firewall using the software on the monitoring server.)*

8 Human-Machine Interface[5]

The RTLS Human-Machine Interface will accessed in two ways:

- **Web Based User Interface** – Users will access the web browser-based user interface via the Intelligent InSites Platform. Users will be able to access data from Intelligent InSites, OAT Systems (both the Enterprise Administrator and facility level OATxpress), WaveMark, and Censis. The Intelligent InSites Platform provides a single sign on mechanism via the VA Active Directory.
- **Thick Client** – RTLS Users within the supply management workflow (Cardiac-Catheterization Labs and EP Labs) will access a thick client installed on a WaveMark provided hardware called

[5] This section will be updated for the NDR User Interface when the requirements have been created

the Point of Care. RTLS users within the reprocessing/sterilization workflows will access a thick client installed on VA Workstations called Censitrac

8.1 Interface Design Rules

The user interface shall comply with VA standards and guidelines including Section 508 compliance and all applicable VA standards. The RTLS User Interfaces shall be compatible with Internet Explorer 7 or greater. The RTLS browser and desktop configuration shall be in accordance with Federal Desktop Core Configuration (FDCC). The RTLS browser configuration shall not require custom browser configuration.

8.2 Inputs

The RTLS user interfaces will use standard workstation input methods. The RTLS web-based user interfaces will avoid dependence on session variables to ensure that the interface can run in more than one server to support High Availability/Fault tolerance requirements for production applications.

The following User Interfaces are accessed through the Intelligent InSites Platform:

- **Intelligent InSites –** provides real time data views (list and map views) of tagged items including people, and assets. The User Interface also provides a wide range of reports, including location history, average utilization; status history, alert history, and proximity history are available. In addition the user interface provides alerting, messaging and notifying among the users of Intelligent InSites. Online help documentation is available to users.
- **WaveMark EiRTLS** - provides a view of critical usage information such inventory levels that were collected from the point of care stations and smart cabinets. The user interface includes views into product and patient encounter information as well as providing alerts for expired and recalled products. In addition, an online help document is available for users.
- **Censis Censitrac** - provides complete automation and recordkeeping for SPD terminals and OR-based flash sterilization. The user interface provides notifications for instrument level recalls as well as immediate visibility to every instrument's reprocessing and use records. The user interface allows users to perform/view container and case cart assembly functions, label printing, sterilization and location updates. In addition, an online help document is available for users.
- **OAT Enterprise Administrator** - manages all OATxpress servers in the enterprise. It stores and distributes master data (such as locations, products and EPC number ranges) to the relevant OATxpress servers. It provides a single point to configure devices and scenarios at a server, and manages users and roles needed to access any server in the system. It also provides a dashboard to monitor events. In addition, it provides a way to seamless access each OATxpress server within the VISN. By accessing the OATxpress server, a user can configure the scenario engine, which is an event-driven workflow engine that helps execute business processes. In addition, an online help document is available for users.

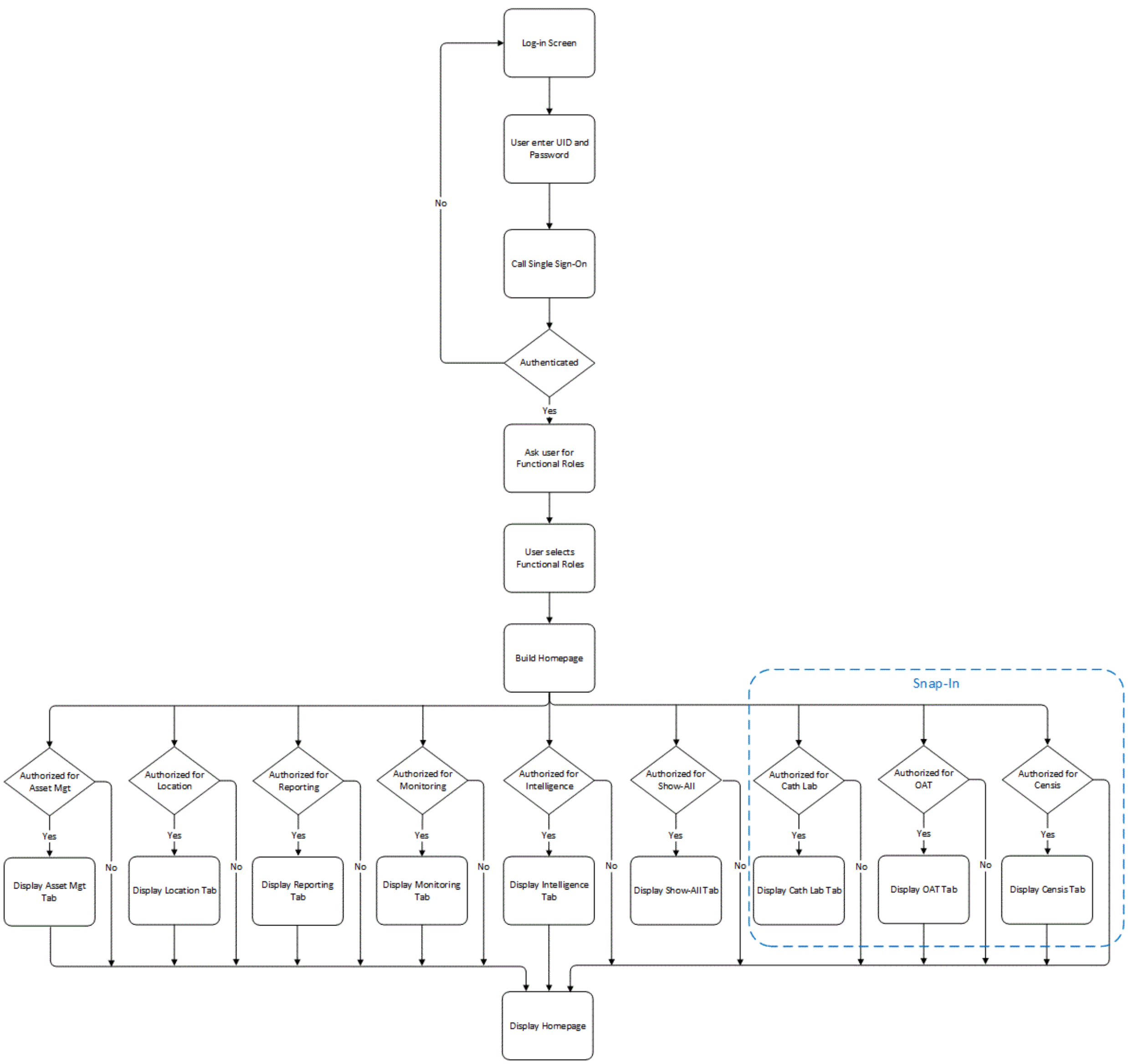
8.3 Outputs

The RTLS output is displayed within a web browser also in keeping with commonly used web development practices. The application has been tested to support Internet Explorer 7 or greater.

8.4 Navigation Hierarchy

The below diagram depicts RTLS System process flow from login to the homepage. It shows how a user moves through the user interface. Additional or customized tabs may be preset based on user and user's authorizations. These addition and customized tabs are functionality built into the Snap-In framework that was discussed earlier in the document.

Figure 113: Navigation Hierarchy



8.4.1 Login Screen

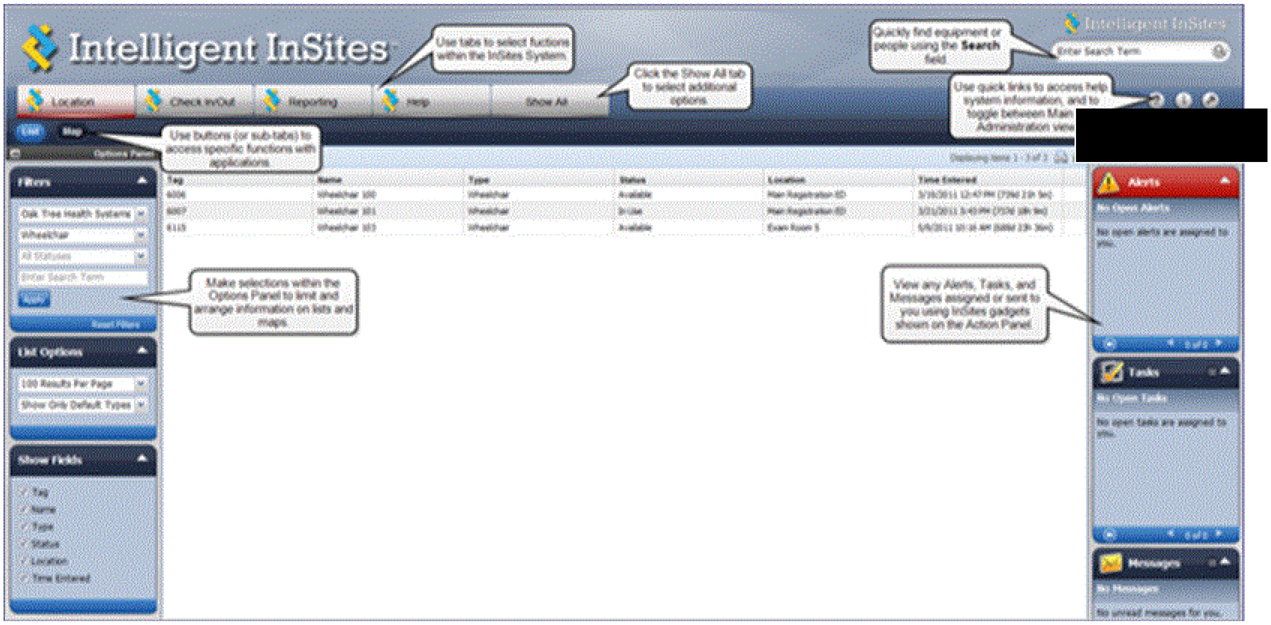
This is the initial screen to the application. It enforces authentication using VA credentials.

Figure 114: Login Screen

8.4.2 Homepage Screen

This is the system homepage which displays the tabs show in the Navigation Hierarchy, along with the various other tools shown in the figure below.

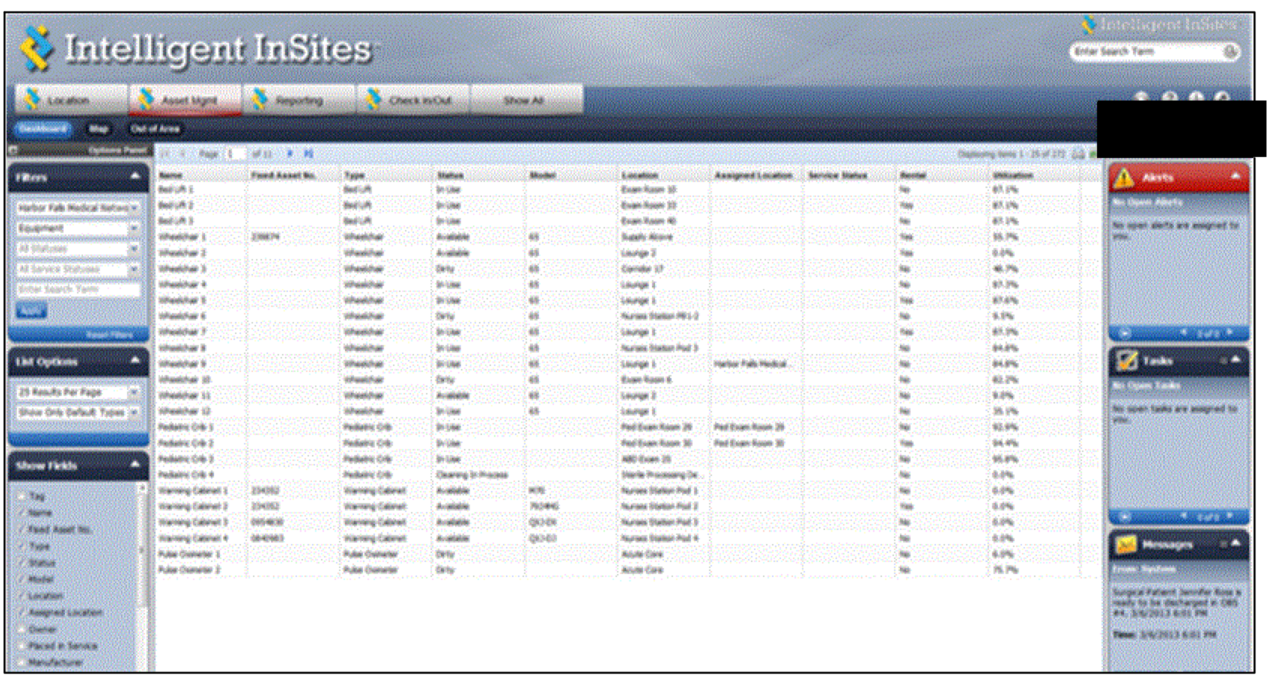
Figure 115: Homepage Screen



8.4.3 Asset Management Screen

This screen enables users to easily find, track, and oversee items that can be associated to a tag or sensor.

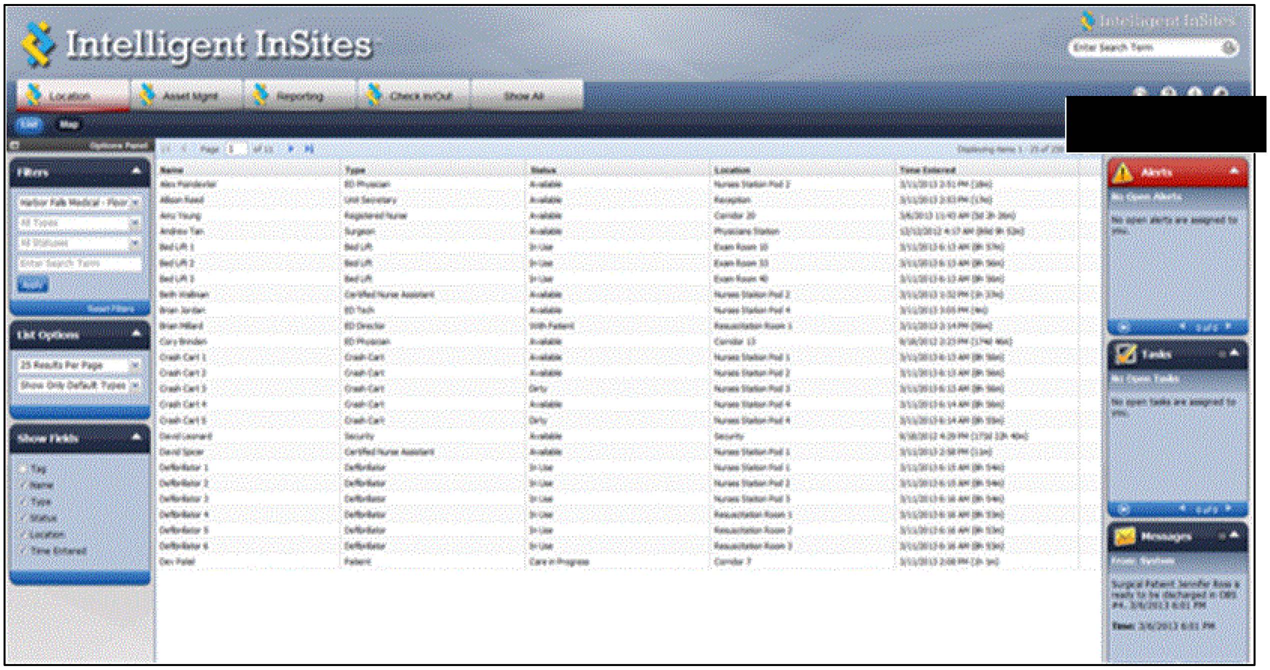
Figure 116: Asset Management Home Page



8.4.4 Location Screen

This screen provides location information for patients, residents, staff, and other tagged equipment in a List or Map view

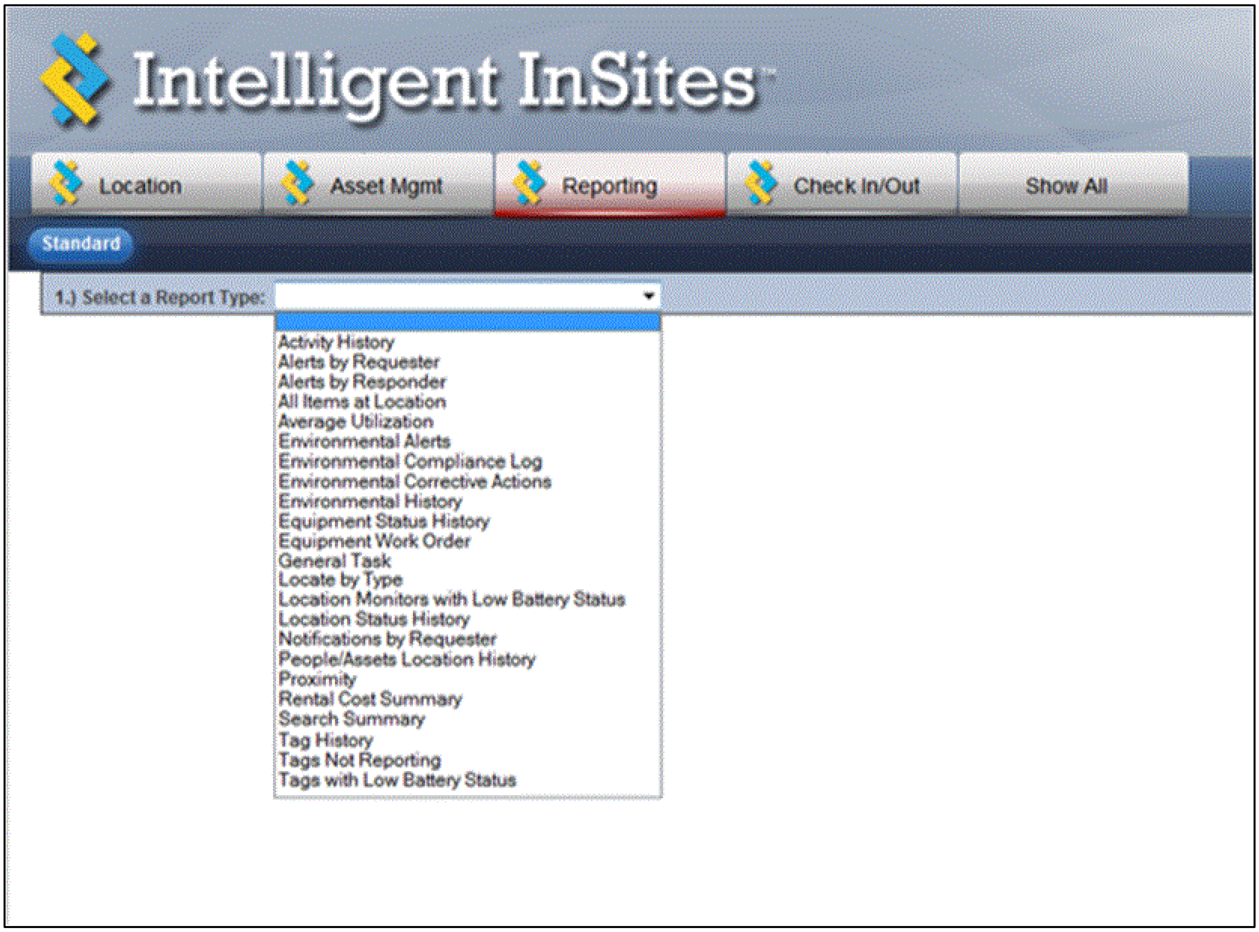
Figure 117: Location Homepage



8.4.5 Report Screen

This screen allows users to select a pre-defined report to execute.

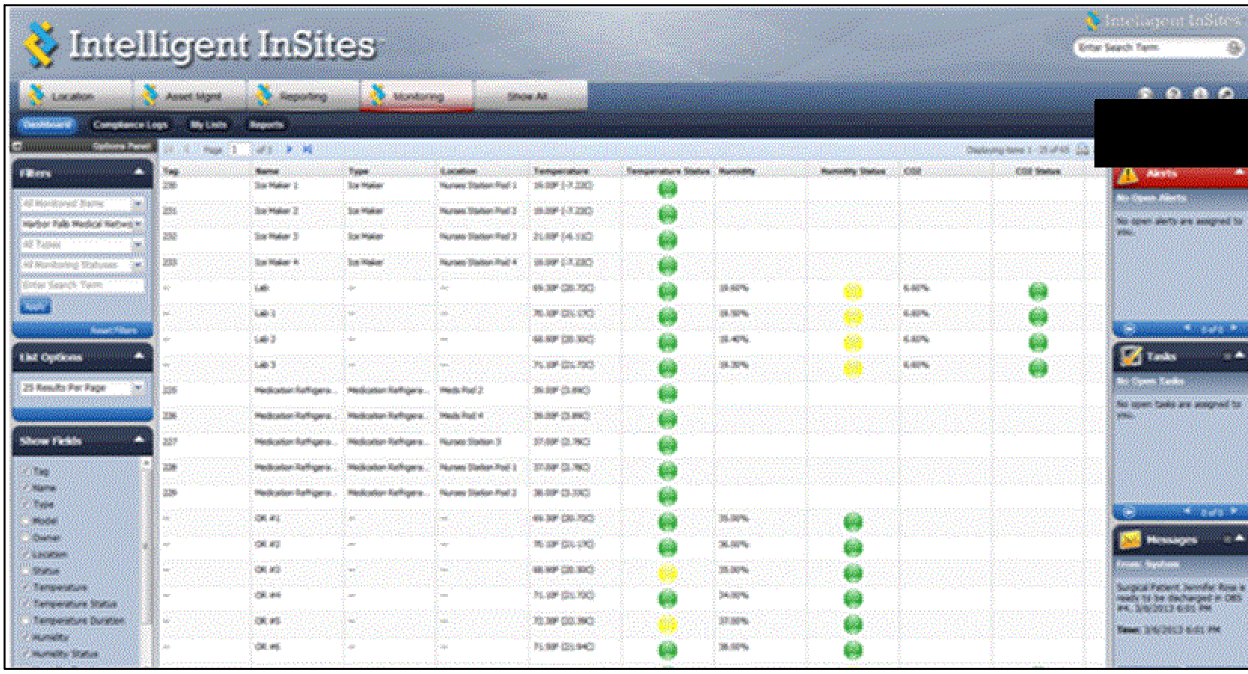
Figure 118: Report Homepage



8.4.6 Monitoring Screen

The Monitoring screen allows users to monitor temperature, humidity and CO_2 levels.

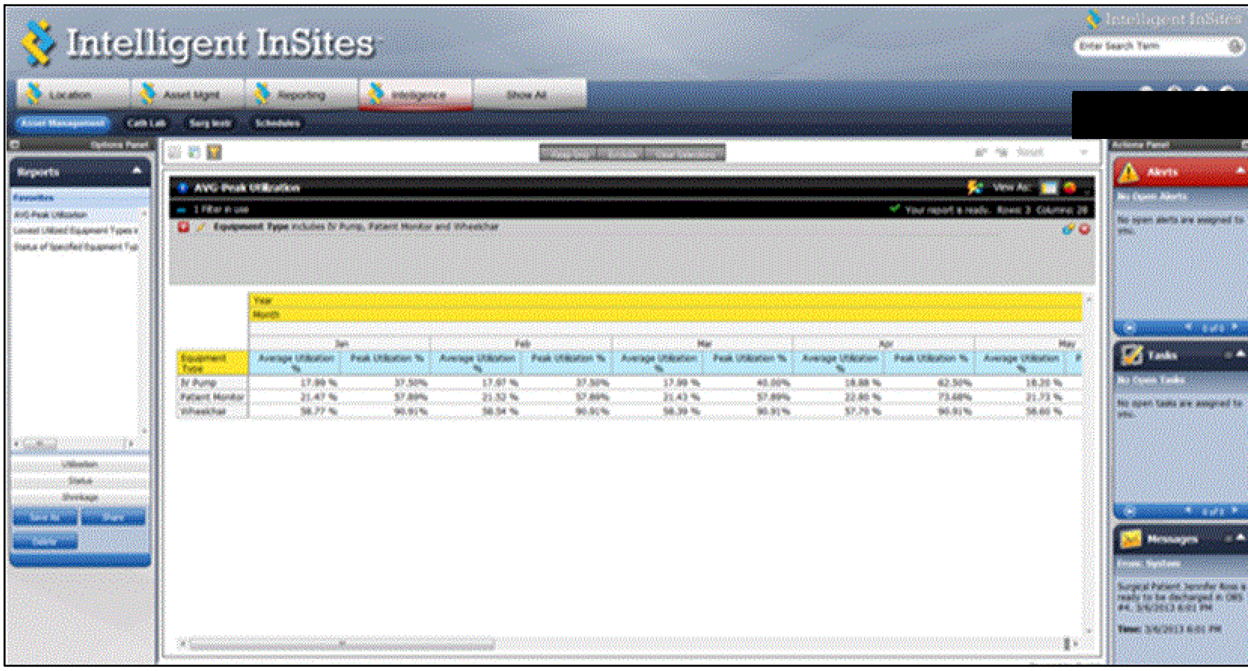
Figure 119: Monitoring Homepage



8.4.7 Intelligence Screen

This screen allows users to access to vast amounts of contextual data stored in the Intelligent InSites BI Data Warehouse. It allows users to analyze trends, identify improvement opportunities, and report on key performance indicators.

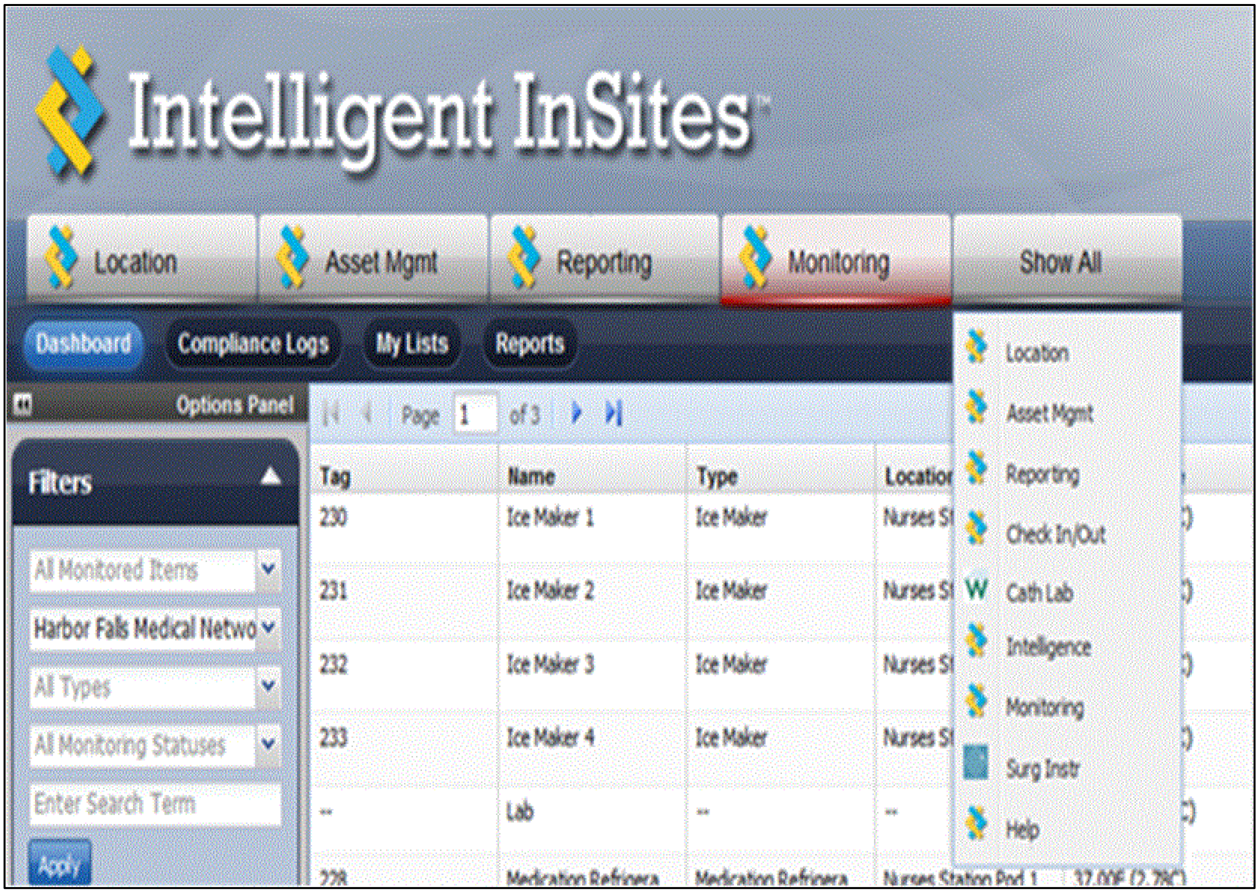
Figure 120: Intelligence Homepage



8.4.8 Show-All Screen

This screen gives the user the option of selecting any application (tab) within the RTLS system that the user is authorized for.

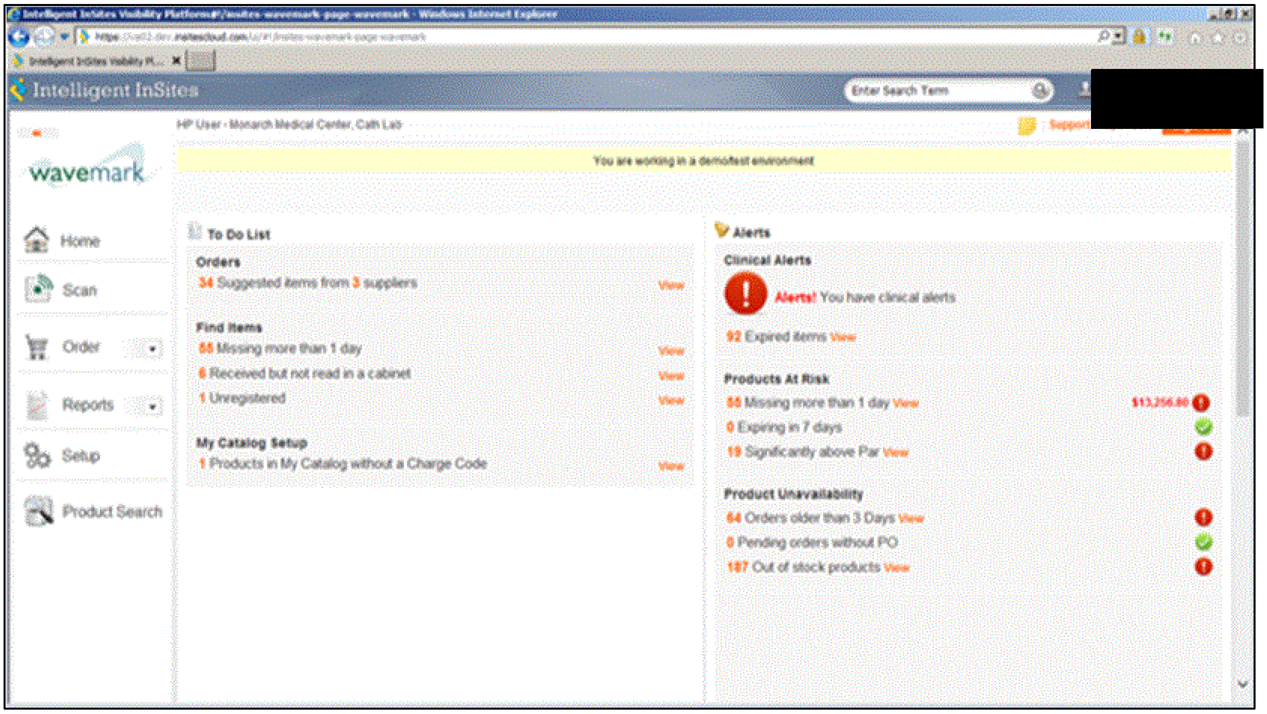
Figure 121: Show-All Menu



8.4.9 WaveMark Homepage

This screen allows the users to perform various duties and tasks within the management of supplies within the WaveMark system.

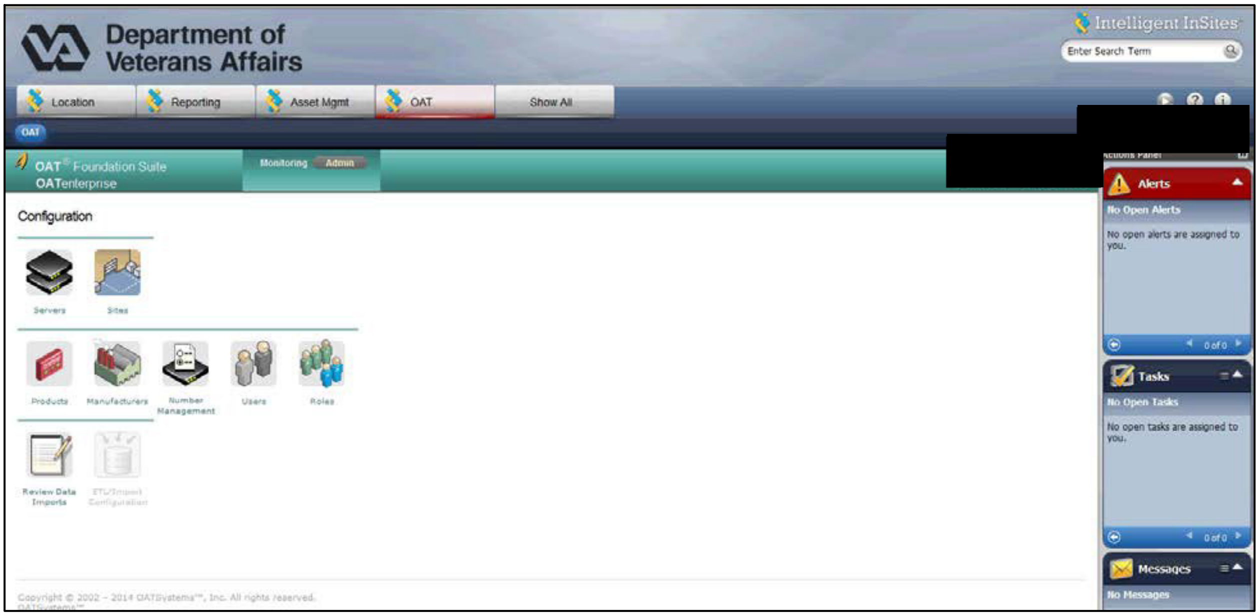
Figure 122: WaveMark Homepage



8.4.10 OAT Homepage

This screen allows users to perform various duties and tasks within the passive tracking of objects within the OAT system.

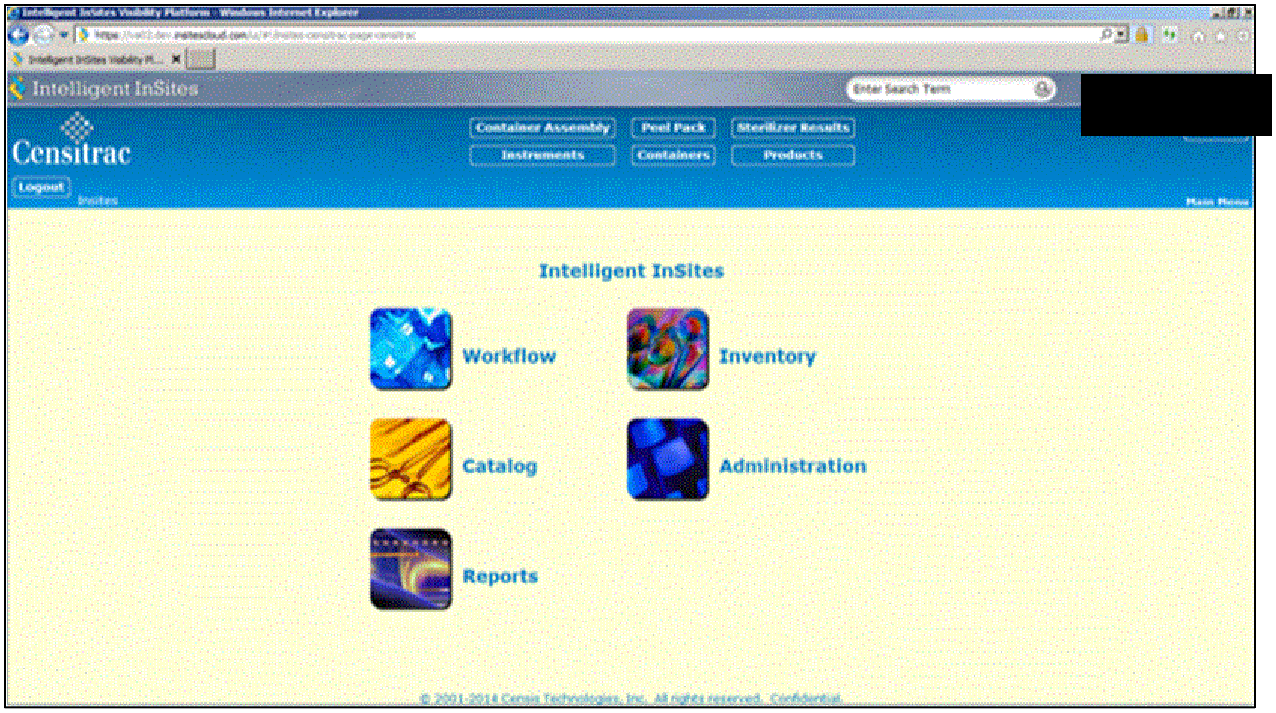
Figure 123: OAT Homepage



8.4.11 Censitrac Homepage

This screen allows the users to perform various duties and tasks within the Reprocessing of medical/surgical instruments within the Censis Censitrac system.

Figure 124: Censitrac Homepage



9 System Integrity Controls

The following sections detail the RTLS System Integrity Controls.

9.1 User Permissions

RTLS system users are primarily tasked with completing Hospital clinical tasks. Users include those in the following roles, Biomedical Technicians, Biomedical Specialists, Biomedical Engineers, Biomedical Engineering Managers, Administrative Support Staff, and Logisticians, The RTLS administrator may assign preconfigured user roles within the RTLS system, or may assign privileges on a custom basis for specific users. RTLS practices the principle of “least privilege”. That is, each user is granted only those privileges needed to perform authorized tasks supporting separation of duties.

The following user roles are associated with RTLS:

Table 35: User Rights

User	Permissions/User Rights (Access)	Position Risk Level
RTLS System Administrators	• Force shutdown from a remote system. • Manage auditor roles.	Moderate/MBI

User	Permissions/User Rights (Access)	Position Risk Level
	• Manage user accounts (create and delete). • Modify application roles. • Shut down and restart the server(s).	
RTLS Operating System and Database Auditors	• Manage auditing and security logs. • Review audit logs.	Moderate/MBI
RTLS Support Staff	• Access server(s) from network. • Access the database. • Archive security logs on another media. • Log on remotely. • Scan and patch the server(s).	Moderate/MBI
RTLS Users	• Access the Real Time Applications. • Access the NDR	Moderate/MBI
Intelligent InSites Administrators	• Access server(s) from network. • Access the database. • Administer the database. • Log on remotely.	Moderate/MBI
WaveMark Administrators	• Access server(s) from network. • Access the database. • Administer the database. • Log on remotely.	Moderate/MBI
CenTrak Administrators	• Access server(s) from network. • Access the database. • Administer the database. • Log on remotely.	Moderate/MBI
OATSystems Administrators	• Access server(s) from network. • Access the database. • Administer the database. • Log on remotely.	Moderate/MBI

User	Permissions/User Rights (Access)	Position Risk Level
Censis Administrators	• Access server(s) from network. • Access the database. • Administer the database. • Log on remotely.	Moderate/MBI

All RTLS users are cleared in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," with appropriate Minimum Background Investigation (MBI).

NIST Special Publication 800-53 Revision 3 control AC-1 require all RTLS developers, users, and contractors to be identified as a Minimum Background Investigation (MBI). A MBI is conducted by OPM and covers a 5-year period. All RTLS users (end-users, developers, and contractors) are required to be screened for access in accordance with VA 0710 personnel security policies prior to being given access to RTLS. End-users with access to RTLS data are assumed to have been cleared by their sponsoring organization. RTLS developers, engineers, testers, trainers, operational and management personnel are cleared in accordance with VA directives. Workstations are administered and operated by the local Office of Information Technology (OIT) using qualified local area network (LAN) and/or technical support personnel.

9.2 RTLS National Auditing Practices

Systems auditing mechanisms are implemented and monitored by RTLS systems administrators using Windows Event Logs and application auditing monitoring. Audit logs are reviewed and archived by systems administrators on a weekly basis. RTLS retains all audit records for a minimum of one year. Information and data containing sources and methods information (SAMI) are retained for five years. All applicable policies are followed with guidance being provided by the National Archives and Records Administration (NARA) General Records Schedules (GRS) federal policy on record retention.

The table (Audit Record Content) below shows the events that the Information System (IS) captures.

Table 36: Audit Record Content

Audit Record Content
User identification (ID)
Unauthorized access attempts to security files
Event date and time
Event type
Event success/failure
Access denial (result of excessive log on attempts)
Successful and unsuccessful log on attempts

Blocked / blacklisted user identity, including terminal, access port, and reason for access withdrawal
Identification of all activities that have the potential to modify, bypass, or negate system safeguards.
Follow CDW best practices and policies for Audit trails of the following: • who accessed specific data and the timestamp of when the data was accessed, edited, or deleted • all connection activity to include timestamps, connection attempts, connection success/failure, quantity of data transferred and connection duration

RTLS will follow all guidance in VA Handbook 6300.1 procedures for implementing the records management program per Audit Record Content above. VA Handbook 6300.2 establishes VA procedures for managing the Vital Records Program and implements the policies contained in VA Directive 6300, Records and Information Management. VA Handbook 6300.8, Procedures for Shipment of Records to the RC&V in Neosho, Missouri, provides procedures for transferring records to the RC&V. The handbook implements VA's Vital Records Program, which is an integral component of VA's Emergency Preparedness Plan.

9.3 Restrict Access to Critical Data Items

The RTLS solution provides the ability to flag individual patient records as being with a "confidential" flag which hides any patient identifiable information on the user interface. Users of the system that do not have permission to view specific information such as Patients or Staff are not able to view any query results that return any records of these types.

Identified Schemas/Accounts/Role based access controls at the application level and database level exist to limit the access to data. Based on the privilege assignments only those users associated with the enumerated roles and in relation to the system privileges above have rights at the database/table level to modify critical data. Only those with these identified privileged assignments have rights to the data. These privileged assignments are audited annually per accreditation requirements.

The RTLS solution creates integrations to synchronize data maintained in these external systems to insure data integrity.

The same is true for RTLS data received from sensors. Location information is received from these systems to maintain accurate data integrity relating tag location to assets, staff, and patients. The rules engine execution assesses changes in the environment and triggers events as appropriate when rule conditions are met. Together these processes work to insure data integrity.

The NDR will restrict access to Protected Health Information (PHI)/Personally Identifiable Information (PII) data to only authorized users of that data.

10 Appendix A

Attach any addition information that supplements the design specification.

10.1 Requirements Traceability Matrix

Please see the Requirements Traceability Matrix spreadsheet.

10.2 Packaging and Installation

Installation guides will be available for the various components/deployments as they are developed for the RTLS Enterprise System. Links to these Install guides will be added as they are completed and verified in the PMAS process.

10.3 Design Metrics

Not Applicable

10.4 Glossary of Terms

The following table is a table of terms (and definitions) that establish meaning within the context of the plan.

Table 37: Glossary of Terms

Term	Meaning
Active Tags	An RFID tag that is equipped with a battery that can be used as a partial or complete source of power for the tag's circuitry and antenna.
Business Intelligence (BI)	Business intelligence is a set of theories, methodologies, processes, architectures, and technologies that transform raw data into meaningful and useful information. BI can handle large amounts of information to help identify and develop new opportunities.
Catheterization Lab	A catheterization laboratory or cath lab is an examination room in a hospital or clinic with diagnostic imaging equipment used to support the catheterization procedure. A catheter is inserted into a large artery, and various wires and devices can be inserted through the body via the catheter which is inside the artery.
Data Warehouse	A Data Warehouse is a system used for reporting and data analysis. Integrating data from one or more disparate sources creates a central repository of data. Data warehouses store current and historical data and are used for creating trending reports for senior management reporting such as annual and quarterly comparisons.
Enterprise Service Bus	An ESB is a software architecture for middleware that provides fundamental services for more complex architectures. In a general sense, an ESB can be thought of as a mechanism that manages access to applications and services (especially legacy versions) to present a single, simple, and consistent interface to end-users via Web- or forms-based client-side front ends. An ESB has a set of rules and principles for integrating numerous applications together over a bus-like infrastructure.

Term	Meaning
Extract Transform Load	Extract Transform Load (ETL) is a technique used to transfer data from a source system to a target system. ETL is performed in the following steps: • Extracts data from source systems • Transforms the data to operational needs, which can include quality levels Loads data into the end target (database, more specifically, operational data store, data mart, or data warehouse)
Java Quartz Scheduler	Quartz is a full-featured, open source job scheduling service that can be integrated with, or used alongside any Java application. Quartz can be used to create simple or complex schedules for executing tens, hundreds, or even tens-of-thousands of jobs; jobs whose tasks are defined as standard Java components that may execute virtually anything you may program them to do. The Quartz Scheduler includes many enterprise-class features, such as support for JTA transactions and clustering.
JavaScript Object Notation (JSON)	JSON is a text-based open standard designed for human-readable data interchange. It is derived from the JavaScript scripting language for representing simple data structures and associative arrays, called objects. The JSON format is often used for serializing and transmitting structured data over a network connection. It is used primarily to transmit data between a server and web application, serving as an alternative to XML.
Keyboard Wedge Device	A keyboard wedge device is an interface that lets a non-keyboard device plug into a computer like it's sending keyboard data
National Data Repository (NDR)	The RTLS solution has a national view (as well as more limited views) of the data stored at the facility and/or regional levels. The NDR shall house sophisticated business intelligence, predictive analytics, and reporting capabilities used for workflow analysis, as well as medical research and analysis purposes.
Passive Tags	A passive tag is an RFID tag that does not contain a battery; the power is supplied by the reader. When radio waves from the reader are encountered by a passive RFID tag, the coiled antenna within the tag forms a magnetic field. The tag draws power from it, energizing the circuits in the tag. The tag then sends the information encoded in the tag's memory.

Term	Meaning
RESTful Web Service	A RESTful web service is a web service implemented using the principles of HTTP. It is a collection of resources, with four defined aspects: • the base URI for the web service, such as http://example.com/resources/ • The Internet media type of the data supported by the web service. • The set of operations supported by the web service using HTTP methods (e.g., GET, PUT, POST, or DELETE). • The API must be hypertext driven.
RFID Reader	An RFID tag is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked. "RFID" stands for Radio Frequency Identification. The tag's antenna picks up signals from an RFID reader or scanner and then returns the signal, usually with some additional data (like a unique serial number or other customized information).
RTLS Data Model	The database schemas that shall will used for across the VA RTLS Enterprise.
Service Oriented Architecture (SOA)	SOA is an architecture approach that packages functionality as interoperable, loosely-coupled units, or services, made accessible over a network and communicating by passing data independent of operating system or programming language.
SOAP Web Service	SOAP is form of a Web Service that provides a basic messaging framework. This XML based protocol consists of three parts: an envelope, which defines what is in the message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing procedure calls and responses.
Wi-Fi	Wi-Fi is a technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network.
VistA	VistA is an enterprise-wide information system built around an Electronic Health Record, used throughout the United States Department of Veterans Affairs (VA) medical system. It consists of nearly 160 integrated software modules for clinical care, financial functions, and infrastructure.

10.5 Glossary of Abbreviations/Acronyms

Abbreviations/Acronyms	Definition
ACT	Access Control Templates
AD	Active Directory
AEMS-MERS	Automated Engineering Management System /Medical Equipment Reporting System

Abbreviations/Acronyms	Definition
API	Application Programming Interface
ATO	Authority to Operate
BI	Business Intelligence
BIS	Microsoft Business Intelligence Suite
BISL-OI&T	Business Integrated Service Line – Office of Information and Technology
BPEL	Business Process Execution Language
C&A	Certification and Accreditation
CART-CL	Clinical Assessment, Reporting, and Tracking Catheterization Lab
CBOC	Community-Based Outpatient
CCX	Cisco Compatible Extensions
CDC	Change Data Capture
CDW	Corporate Data Warehouse
CE	Conformité Européenne
CFR	Code of Federal Regulations
CMOP	Consolidated Mail Outpatient Pharmacies
COM	Component Object Model
COOP	Continuity of Operations Plan
COTS	Commercial Off the Shelf
CRC	Cyclic Redundancy Check
CPRS	Computerized Patient Record System
CRUD	Create, Retrieve, Update, and Delete
DB	Database
DBMS	Database Management System
DDL	Data Definition Language
DEK	Data Encryption Key
DM	Data Mart
DQS	Microsoft SQL Server Data Quality Services
DR	Disaster Recovery
DW	Data Warehouse
EDA	Enterprise Data Architecture
EDW	Enterprise Data Warehouse
EG	Enterprise Guide
EHR	Electronic Health Record
EiRTLS	Enterprise Inventory Real Time Location System
EMR	Electronic Medical Record
EP	Electrophysiology Lab
EPC	Engineering, Procurement, and Construction
ePHI	Electronic Protected Health Information
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
ETL	Extract Transform Load
ETS	Econometric Time Series
FCC	Federal Communications Commission
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GIP	Generic Inventory Package

Abbreviations/Acronyms	Definition
GMS	Global Monitoring System
GRS	General Records Schedules
GUI	Graphical User Interface
HCE	Health Care Efficiency
HD	Hemodynamic monitoring system
HID	Human Interface Device
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7
HPC	High Performance Computing
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HWSC	HeatlheVet Web Services Client
IC	Ion Chromatography
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
iEHR	Integrated Electronic Health Record
IETF	Internet Engineering Task Force
IFCAP	Integrated Funds Distribution, Control Point Activity, Accounting, and Procurement
IIS	Internet Information Services
iLO	Integrated Lights Out
IP	Internet Protocol
IPT	Integrated Project Team
IR	Infrared
ISM	Institute for Supply Management
ISO	International Organization for Standards
IT	Information Technology
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
JDBC	Java Database Connectivity
JEE	Java Enterprise Edition
JMS	Java Message Service
LAN	Local Area Network
LED	Light Emitting Diode
LLRP	Low Level Reader Protocol
LWAP	Lightweight Access Points
LWAPP	Lightweight Access Point Protocol
KPI	Key Performance Indicator
MAC	Media Access Control
MBI	Moderate Background Investigation
MD5	Message Digest Algorithm
MDM	Master Data Management
MDS	Master Data Services
MMIS	Medicaid Management Information Systems
MOM	Message Oriented Middleware
MOSS	Microsoft Office SharePoint Server
MRN	Medical Record Number
MSE	Mobility Services Engine

Abbreviations/Acronyms	Definition
NARA	National Archives and Records Administration
NDC	National Data Center
NDR	National Data Repository
NMSP	Network Mobility Services Protocol
NOC	Network Operations Center
ODBC	Open Database Connectivity
ODS	Operational Data Store
OIT	Office of Information Technology
OLAP	Online Analytical Processing
OLEDB	Object Linking Embedded Database
OR	Operations Research
OSHPD	Office of Statewide Health Planning and Development
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
PDW	Parallel Data Warehouse
PHI	Protected Health Information
PII	Personally Identifiable Information
PIMS	Patient Information Management System
PMAS	Project Management Accountability System
PMO	Project Management Office
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks
RDM	RTLS Data Model
RF	Radio Frequency
RFID	Radio Frequency Identification
ROI	Return on Investment
RPC	Remote Procedure Call
RSD	Requirements Specification Document
RSSI	Received Signal Strength Indication
RTLS	Real Time Location System
SAMI	Sources and Methods Information
SAN	Storage Area Network
SEDR	System Engineering Design Review
SEI	Software Engineering Institute
SFTP	Secure File Transfer Protocol
SHA-2	Secure Hash Algorithm
SLA	Service Level Agreement
SMA	Software Management Agreement
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPS	Sterile Processing Service
SSAS	Microsoft SQL Server Analysis Services
SSH	Secure Shell Protocol
SSIS	Microsoft SQL Server Integration Services
SSL	Secure Sockets Layer
SSRS	SQL Server Reporting Services
SSO	Single Sign On

Abbreviations/Acronyms	Definition
SQL	Structured Query Language
TCP-IP	Transmission Control Protocol
TLS	Transport Layer Security
TOC	Table of Contents
TRM	Technical Reference Model
UDP-IP	User Datagram Protocol
UL	Underwriters Laboratories
UOW	Unit of Work
URL	Uniform Resource Locator
VA	Veterans Affairs
VAMC	Veterans Affairs Medical Center
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network
VISTA	Veterans Health Information Systems and Technology Architecture
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
XML	Extensible Markup Language
xPOS	Point of Service Station

10.6 Required Technical Documents

The following documents must be submitted for review to support proper approval:

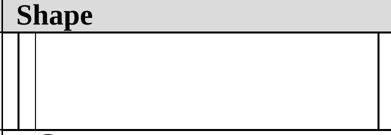
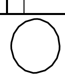
- Product Architecture Document;
- Disaster Recovery Plan;
- Interface Data Mapping
- Security Assurance Strategy

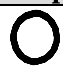
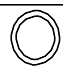
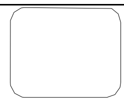
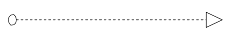
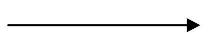
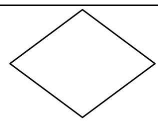
For additional information regarding how to obtain proper approval for this project, refer to the following documents:

- ***IT Infrastructure Standards***
- ***Technical Analysis Review-Technical Analysis Summary (TAR-TAS) process***
- ***Enterprise Architecture Web page***
- ***One-VA TRM***

10.7 Business Process Legend

Figure 125: Business Process Legend

Element	Shape	BPMN Type	Description
Swimlane		Lane	A swim lane represents all activity within a function or role.
Start Event		Event	An event represents something that happens. Start events act as a process trigger.

Element	Shape	BPMN Type	Description
End Event		Event	End events represent the result of a process.
Intermediate Event		Event	Intermediate events represents something that happens between the start and end events. For example, a task could flow to an event that throws a message across to another pool, where a subsequent event waits to catch the response before continuing.
Task		Activity	A task represents a single unit of work.
Message		Connection	A message represents flow of information across organizational boundaries (i.e. between pools).
Sequence		Connection	A sequence shows the order in which activities are performed.
Gateway		Gateway	A gateway represents forking and merging of paths depending on the conditions expressed.

11 Appendix B

11.1 Test Architecture

TBD – this will be created once the test architecture has been decided on.

Attachment A - Approval Signatures

Signed: **Date:**

[redacted]

Director, RTLS Project Management Office

Healthcare Technology Management Office (10NA9)

RTLS Integrated Project Team (IPT) Co- Chair

Signed: **Date:**

[redacted]

Chief Healthcare IT Strategist

Office of the Associate Deputy Assistant Secretary

Enterprise Systems Engineering

RTLS Integrated Project Team (IPT) Co- Chair

Signed: **Date:**

[redacted]

Product development (PD)

RTLS Integrated project team (IPT) Co-Chair