System Requirements Specification for the Nuclear Smuggling Detection and Deterrence (NSDD) Central Alarm Station (CAS)  
v4.3 (2020-08)

Configuration Control—Record of Changes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VERSION**  **NUMBER** | **DATE** | **NUMBER OF**  **FIGURE, TABLE,**  **OR PARAGRAPH** | **A\***  **M**  **D** | **BRIEF DESCRIPTION** | **CHANGE**  **REQUEST**  **NUMBER** |
| 1 | Dec 20, 2005 | All | A | Created |  |
| 2 | Feb 20, 2006 | Multiple | M | Incorporated DOE comments |  |
| 3 | Sep 8, 2006 | All | M | Incorporated new standard requirements and RTM-rlf |  |
| 4 | December  2007 | All | M | Removed vendor-specific design notes,  updated to accommodate new requirements, and refined previous requirements |  |
| 4.1 | May 2008 | All | M | Minor typographical changes  Removed references to N.25 |  |
| 4.2 | January 2009 | All | A,  M | Minor typographical corrections and clarifications. Introduced Activated and Configured requirements. Added Section 1.3 (References); Appendices B (Event Types, Priorities, and States), C (User Roles); D (Use Cases); and E (Data Dictionary). |  |
| 4.3 | August 2020 | All | A, M,  D | Consolidated documents: Core Standard CAS SRS 4.2, SLD Program Notice 32 – SLD CAS System Anti-Virus Policy, SLD CAS Software Graphing Examples R1.0, SLD CAS Software Graphing Requirement R1.0, SLD Core Standard CAS Disposition Codes R1.0, SLD Data Retention Policy SRS Requirements Addendum  **No new requirements added, but others deleted** |  |

\* N= NEW A=ADDED M=MODIFIED D=DELETED

**Table of Contents**

[Configuration Control—Record of Changes ii](#_Toc49152110)

[1. Introduction 1](#_Toc49152111)

[1.1 Background 1](#_Toc49152112)

[1.2 Purpose and Scope of Document 1](#_Toc49152113)

[1.3 References 1](#_Toc49152114)

[2. CAS System Overview 1](#_Toc49152115)

[2.1 NSDD CAS System Anti-Virus Policy 4](#_Toc49152116)

[2.1.1 Anti-Virus Implementation Strategy 4](#_Toc49152117)

[2.1.2 NSDD Anti-Virus Implementation Strategy for New DICCE SOWs 4](#_Toc49152118)

[2.1.3 NSDD Anti-Virus Implementation Strategy for Sites in Transition and Post Transition Engagement 5](#_Toc49152119)

[3. Design Overview 5](#_Toc49152120)

[3.1 Standard Design Approach 5](#_Toc49152121)

[3.2 Operating Environment 6](#_Toc49152122)

[3.3 Environmental Conditions 6](#_Toc49152123)

[3.4 Operating Conditions 6](#_Toc49152124)

[3.5 Constraints 6](#_Toc49152125)

[3.5.1 Design Constraints 6](#_Toc49152126)

[3.5.2 Implementation Constraints 7](#_Toc49152127)

[3.6 Assumptions and Dependencies 7](#_Toc49152128)

[3.6.1 Capacity Assumption 7](#_Toc49152129)

[3.6.2 Physical Assumptions about Site Operations 7](#_Toc49152130)

[3.6.3 User Assumptions 7](#_Toc49152131)

[3.7 User Roles 7](#_Toc49152132)

[4.0 Requirements 8](#_Toc49152133)

[4.1 Requirement Groupings 8](#_Toc49152134)

[4.2 Software Requirements 9](#_Toc49152135)

[4.2.1 External Interfaces 9](#_Toc49152136)

[4.2.2 Functional Requirements 9](#_Toc49152137)

[4.2.3 Nonfunctional Requirements 9](#_Toc49152138)

[4.3 System Requirements 10](#_Toc49152139)

[4.3.1 External Interfaces 10](#_Toc49152140)

[4.3.2 Functional Requirements 10](#_Toc49152141)

[4.3.3 Nonfunctional Requirements 10](#_Toc49152142)

[Appendix A: Requirements Details 11](#_Toc49152143)

[A.1 Software Requirements 11](#_Toc49152144)

[A.1.1 Software External Interfaces 11](#_Toc49152145)

[A.1.2 Software Functional Requirements 12](#_Toc49152146)

[A.1.3 Software Nonfunctional Requirements 18](#_Toc49152147)

[A.2 System Requirements 19](#_Toc49152148)

[A.2.1 System External Interfaces 19](#_Toc49152149)

[A.2.2 System Functional Requirements 20](#_Toc49152150)

[A.2.3 System Nonfunctional Requirements 21](#_Toc49152151)

[A.3 Requirements Traceability Matrix Description 21](#_Toc49152152)

[Appendix B: Event Types, Priorities, and States 23](#_Toc49152153)

[B.1 Event Types and Priorities 23](#_Toc49152154)

[B.2 Event States 23](#_Toc49152155)

[Appendix C: Use Cases 25](#_Toc49152156)

[C.1 Use Case Diagram and Scenarios 25](#_Toc49152157)

[Appendix D: Version Control 32](#_Toc49152158)

[D.1 Configuration Management 32](#_Toc49152159)

[D.1.1 Version Identification 32](#_Toc49152160)

[D.1.2 Quality Check 32](#_Toc49152161)

[Appendix E: NSDD CAS Software Graphing Requirements 33](#_Toc49152162)

[Overview 33](#_Toc49152163)

[Definitions 33](#_Toc49152164)

[References 33](#_Toc49152165)

[Graphing Requirements 33](#_Toc49152166)

[Vertical Scale 34](#_Toc49152167)

[Data Trace Value Plotting 34](#_Toc49152168)

[Graph Elements 36](#_Toc49152169)

[Appendix F: NSDD CAS Graphing Examples 37](#_Toc49152170)

[Appendix G: NSDD Standard Disposition Codes 42](#_Toc49152171)

[Data Dictionary 43](#_Toc49152172)

[Glossary 44](#_Toc49152173)

**List of Figures**

**Figure 1. Basic NSDD CAS system2**

**Figure 2. Multi-workstation configuration of a NSDD system3**

**Figure B1. Event state diagram24**

**Figure C1. Use case diagram26**

**List of Tables**

**Table 1. User Roles Descriptions8**

**Table B1. Event Priority/Video/Graphing Summary23**

**List of Acronyms and Abbreviations**

|  |  |
| --- | --- |
| CAS | Central Alarm Station |
| ConOps | Concept of Operations |
| DOE | Department of Energy |
| EI | External Interface |
| FR | Functional Requirement |
| G | Gamma Alarm |
| HH | Handheld |
| I/O | Input/Output |
| ICD | Interface Control Document |
| LAS | Local Alarm Station |
| LMP | Local Maintenance Provider |
| N | Neutron Alarm |
| NCS | National Communications System |
| NFR | Nonfunctional Requirement |
| NG | Neutron Gamma Alarm |
| NNSA | National Nuclear Security Administration |
| PC | Personal Computer |
| RDS | Radiation Detection System |
| RID | Radioisotopic Identification Device |
| RPM | Radiation Portal Monitor |
| RTM | Requirements Traceability Matrix |
| SIS  SIT | Secondary Inspection Station  Site Inspection and Testing |
| SO | Software |
| SOH | Status of Health |
| SOW  SPM | Statement of Work  Spectroscopic Portal Monitor |
| SRS | System Requirements Specification |
| SSQ | Site Survey Questionnaire |
| SWS | Secondary Workstation |
| SY | System |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| UC  UI | Use Case  User Interface |
| UPS | Uninterruptible Power Supply |
| USG | United States Government |

# Introduction

* 1. Background

The U.S. Department of Energy/National Nuclear Security Administration’s (DOE/NNSA’s) Office of Nuclear Smuggling Detection and Deterrence (NSDD) plays a critical role in the U.S. government’s (USG’s) effort to prevent nuclear or radiological terrorism. NSDD enhances U.S. national security by forming partnerships to strengthen the capabilities of partner countries to detect, disrupt, and investigate the smuggling of nuclear and radiological materials before those materials can be used against the U.S. or its interests.

Throughout its more than 20-year history, NSDD has focused not only on deploying technologies, but also on ensuring that partners have the capability to operate tools to fulfill their law enforcement responsibilities while systems remain fully functional and operational and that international partnerships endure and global capacities to combat nuclear smuggling risks continue to grow. The NSDD Program provides an integrated, sustainable system to monitor international trade routes and minimize the risk of nuclear proliferation and nuclear materials–related terrorism. This system includes stationary radiation portal monitors (RPMs), mobile detection units (including hand-held, vehicle-based detectors and relocatable RPMs), radioisotopic identification devices, and computer systems to integrate the detection and identification equipment into a Central Alarm Station (CAS).

1.2 Purpose and Scope of Document

This document outlines and describes NSDD CAS system requirements, hardware requirements, interface requirements, and functional and nonfunctional requirements for the software. Additional requirements are provided in the documents referenced in the CAS Communications System statement of work (SOW) and other documents as noted in Section 1.3. All requirements must be tracked by the contractor through the testing and acceptance of the NSDD CAS software. The system requirements are intended to minimize the need for country-specific requirements. Any additional requirements identified outside the scope of this document must be approved by the NSDD Program.

1.3 References

NSDD Guidelines for Naming and Formatting Daily Files

NSDD Data Management Document

Core\_Standard\_CAS-RTM\_R4.2 – Requirements Traceability Matrix

# CAS System Overview

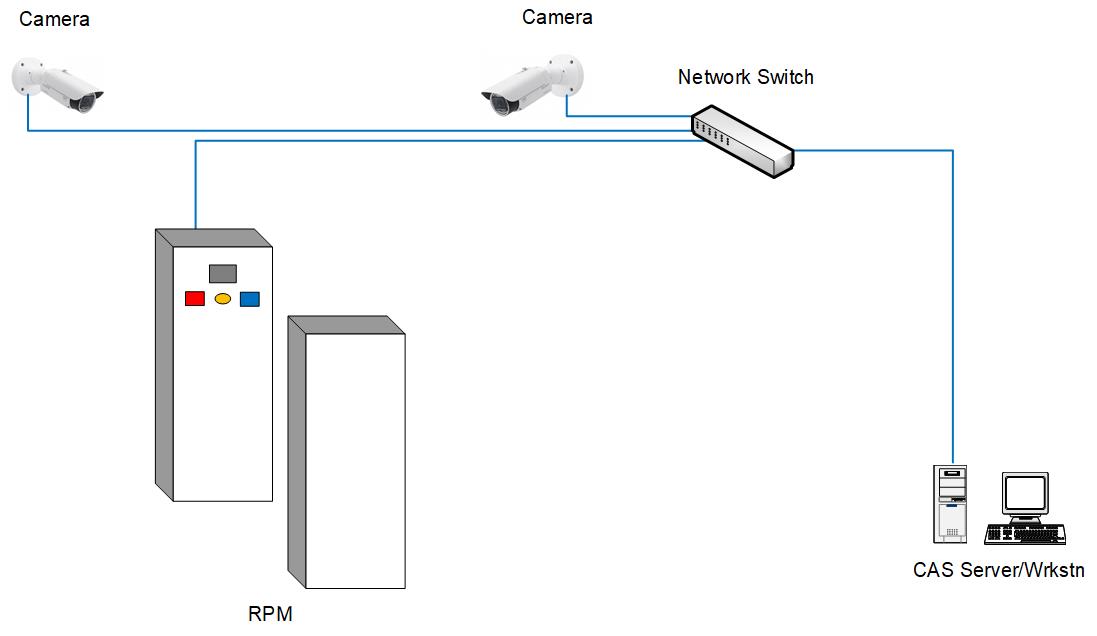
A CAS is the primary location where alarm-based decisions are made by system operators. The term CAS is used to refer to both the physical location where the main system computer is located and the CAS communications system, which includes the hardware, software, and interfaces. The purpose of the CAS system is to tie all data points that are inclusive of occupancies and background to a central database and associated workstation(s) for the purpose of announcing, adjudicating, and recording detection events. In addition, the CAS is required to have functionality that supports various forms of data analysis.

To meet these objectives, the CAS must be able to receive, process, and associate/integrate data from all equipment composing in the RDS, including, but not limited to, RPMs, hand-held equipment, and cameras. The CAS must be able to display data to system operator use through a user-friendly, interactive interface that supports the interdiction of alarm-causing objects and post event and general trend monitoring analysis. This system must be able to support multiple user role-based configurations under a range of response scenarios. However, the system must also be scalable and flexible to accommodate the required functionality with the smallest possible footprint. Some sites may require a single computer workstation to accomplish all functions. The system must be able to accommodate future growth and/or downsizing with little or no modification.

Basic functional requirements include radiation alarm notification and processing features, fault handling logic, image capture processing, data collection, data storage, and data cataloging. In its simplest configuration, the CAS consists of a single workstation with integrated database/server.

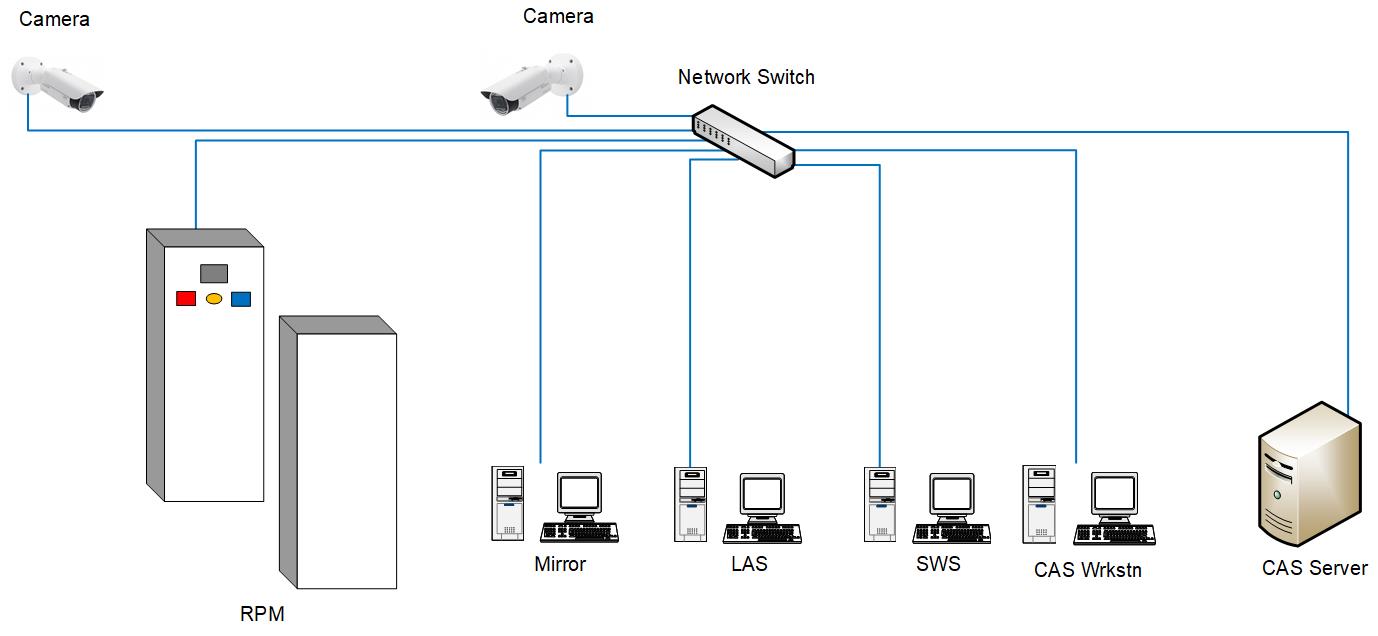
In larger, more complex configurations, the system may consist of a separate workstation and/or server that integrates one or more additional dispersed local workstations. These local workstations are termed Local Alarm Stations (LAS’s). In this configuration, the CAS performs a supervisory function. The CAS, in turn, may be integrated through a national communication system to a national alarm center and/or regional alarm center.

Figure 1 shows the most basic NSDD CAS system.



**Figure 1. Basic NSDD CAS system.**

A diagram of a complex, multi-workstation configuration (appropriate for larger sites) is shown in Figure 2.



**Figure 2. Multi-workstation configuration of an NSDD system.**

The LAS may provide a full or limited subset of CAS functionality to an operator who is physically located at the control point(s) of interest. The primary purpose of a LAS workstation is to alert the local operator of an alarm event so that immediate response actions may occur and subsequently to provide any additional information requested by the CAS Operator. Control of actions (Stop-Go decisions) and the ability to enter supplementary information (such as assessment observations, manifest, or other documentation data) is shared between the CAS and LAS. In such instances where work is distributed between multiple stations, a mechanism must be incorporated to alert the supervisory and subordinate systems to overdue or unresolved actions. A LAS Operator will be responsible for monitoring an assigned set of lanes/RPMs and receiving and carrying out instructions from the CAS Operator to ensure that conveyances, objects, or persons causing alarms are either released or directed to Secondary Inspection.

The LAS Operator may be required to complete logic steps as displayed on the LAS workstation. A LAS Operator may be restricted to applicable portions of alarm assessment and may only be viewing and responding to alarms for RPMs located in the immediate area. In such instances where work is distributed between multiple stations, a mechanism must be incorporated to alert the supervisory and subordinate systems to overdue or unresolved actions.

Some sites may require a Mirror CAS. A Mirror CAS is a workstation with viewer-only privileges. This is an unidirectional station that allows other local stakeholders, such as members of another agency within the host country, to view the same information seen by the main CAS, but it does not allow for interaction, adjudication, or input.

In addition, larger sites or those with a physically separated secondary inspection station (SIS) may require a secondary workstation (SWS). The purpose of a SWS is to display primary alarm details for review by the SIS Operator before performing a secondary inspection and allowing for input of secondary inspection data into the CAS software. Some CAS systems may be configured so primary and secondary data are input into the same workstation with full functionality. Some LAS workstations may also allow for inputting secondary inspection data.

2.1 NSDD CAS System Anti-Virus Policy

NSDD uses a comprehensive and phased approach to protect all deployed IT-based systems against vulnerabilities. These vulnerabilities include computer viruses, malicious attacks, unauthorized use, and catastrophic failures such as fire, flood, hardware, or other software failures.

**NSDD requires that every site will have an anti-virus solution installed for the CAS System.** An up-to-date anti-virus solution is critical to ensuring the continued functionality of systems deployed by NSDD.

The NSDD Program recognizes that some countries may have a preferred or existing anti-virus capability in place. Therefore, while the installation of an anti-virus solution is required, it is appropriate to work with the partner agency and provide the partner agency's preferred anti­virus solution, contingent on there being no USG policy prohibiting use of the system. For countries that do not currently have an anti-virus preference or capability, it is NSDD policy that the CAS vendor’s recommended solution for the site be used.

2.1.1 Anti-Virus Implementation Strategy

Common NSDD anti-virus implementation elements that will be executed in all deployment cases are outlined below.

* Project teams will work with the partner agency and the local system administrator/LMP to select an anti-virus solution.
  + If the site or partner agency has a preferred anti-virus solution, the project team should accommodate this preference, contingent on there being no USG policy prohibiting use of that system.
  + If the site or partner agency has no preferred solution, the project team should coordinate with the local system administrator/LMP to procure the CAS vendor's recommended anti-virus solution. Installation and maintenance (including updates) should be conducted by a local system administrator/LMP where possible. In the event this is not possible, NSDD Technical Services is available to assist with installation and updates.
* Before the installation of anti-virus solution, the installer must consult the relevant CAS manuals to ensure that any CAS vendor-specific instructions are followed.
* Maintenance of anti-virus solution (including updates) should be conducted by a local system administrator/LMP where possible. In the event this is not possible, NSDD Technical Services is an option to assist with updates.

The NSDD anti-virus implementation strategy will vary slightly depending on the current phase of an NSDD project at the time of this policy's publication. These variations are outlined below.

2.1.2 NSDD Anti-Virus Implementation Strategy for New DICCE SOWs

* Information regarding partner agency preferred anti-virus solution should be collected during the site survey and, if available, included in the request for proposal.
* Compatibility of the anti-virus solution with CAS software will be tested during site-specific continental United States testing.
* If the site or partner agency has no preferred solution, the project team will coordinate with the DICCE vendor to procure the CAS vendor’s recommended anti-virus solution.
* Anti-virus installation should be conducted before site inspection and testing (SIT) where possible. In the event this is not possible, the NSDD Help Desk will assist with installation and updates after SIT.

2.1.3 NSDD Anti-Virus Implementation Strategy for Sites in Transition and Post Transition Engagement

* Currently installed CAS communications systems will be tested for compatibility with the chosen anti-virus solution by NSDD personnel at the time of anti-virus installation.
  + Compatibility testing for basic CAS functionality will consist of using sources to confirm all alarms and fault conditions.
  + Load testing for CAS operability will consist of running a system function, which typically consumes a large amount of processor effort while conducting an anti-virus full system scan.

1. Design Overview

The following requirements are derived from the overall approach and philosophy of the NSDD system concept. They are the general parameters that bind the CAS system and must be exhibited by the CAS system. Any measurable quality of these requirements must be incorporated into the CAS system test plans so compliance can be demonstrated.

3.1 Standard Design Approach

1. The system shall be based on commercially available operating systems, use standard commercially available development languages, and any database used shall be commercially available and relational.
2. The use of commercially available unmodified components shall be maximized.
3. The system shall be expandable so future features can be added without major redesign of the software.
4. The user shall be able to access all information associated with any data related to a single event.
5. To the extent possible, the system shall be able to recognize new components and auto-configure components for use. Where this is not possible, tools shall be provided to assist the System Administrator with configuring new or replaced hardware.
6. All optional features may be selected or deselected at the time of installation depending on mission requirements.
7. Software installations and updates shall be installable by trained local System Administrators. (See SONFR-003-01.)
8. Software must be open-architected to facilitate the integration of additional equipment into the RDS as required.
9. The system should implement prudent computer and network security practices to make the system resistant to hackers, unauthorized software modifications, and downloading of unauthorized software onto the system (e.g., games).
10. Communications lines should be supervised or encrypted where possible. Audit trails should be maintained to discourage insiders from changing settings and sensitivities.
11. Interfaces requiring additional software development and/or specific data exchange protocols must be recorded in an interface control document (ICD) that is mutually agreed upon by the relevant stakeholders (NSDD Program, the software developer, and the external system or component developer).
12. The system shall be capable of continuous operation in remote environments and at points of entry.
13. The system design shall minimize the hardware footprint.

3.2 Operating Environment

The system operating environment will encompass both environmentally protected (indoor) and unprotected (outdoor) locations. The RPMs and the communication equipment (including the LAN and any supporting signal conversion electronics) will be installed outdoors and must be adequately protected from ambient weather conditions. The more sensitive hardware (where applicable), such as the servers, storage arrays, network switches, and the Operator’s workstation, will be indoors to provide adequate environmental protection. LAS stations at control points and the SWS’s at SIS locations will be required to operate in a wide range of ambient conditions. Unusual operating parameters (temperature and environmental conditions) for each type of device will be specified in the site survey report. Equipment chosen by the vendor must be compatible with the field conditions and be approved by the NSDD Program.

3.3 Environmental Conditions

When possible, communications equipment shall be installed in an environmentally controlled facility capable of maintaining an environment suitable for equipment operation. Communications equipment required to connect lane side equipment and other required systems, such as those associated with a LAS or SWS, may be installed outside. This communication equipment shall be rated for the operating environment. Direct and indirect factors may reduce the functional capabilities of imaging systems supporting RPMs.

Systems are deployed to multiple foreign countries where temperatures range from -40 degrees Celsius to 55 degrees Celsius and environments are humid, temperate, and arid. Where applicable, the NSDD Program may provide air conditioners, heaters, and back-up generators in workstation and server locations. Nevertheless, all system components must be able to operate effectively and constantly in these environments. The contractor is responsible for identifying locations where additional environmental controls are required and for making subsequent recommendations.

3.4 Operating Conditions

Standard operating conditions for all RPMs (vehicle, pedestrian, conveyor, and rail) require only one occupant within the portal at any given time, with sufficient time/space between occupancies for the RPM to determine the end of occupancy and the beginning of the next occupancy. If the RPM cannot determine when the occupancy begins or ends, then a combination of modified imaging system parameters and operational procedures is required to associate a particular occupant with an alarm event. In addition, sufficient time/space between occupancies is required so that (a) background radiation levels can be updated for the next occupancy and (b) license plates, container numbers, or pedestrian images are not blocked by previous and/or following occupants. Cameras and related imaging equipment shall be located by the contractor, in cooperation with host partners, to provide unobstructed views of objects entering and exiting the RPMs. Systems should be designed assuming 24/7 operations.

3.5 Constraints

3.5.1 Design Constraints

The design environment for the CAS is as follows:

* Modern, currently supported, Windows-compatible Workstation Operating System
* Modern, currently supported, Server Operating System
* Modern, currently supported Server development languages (e.g., C#)
* Modern, currently supported user interface (UI) development languages (e.g., .Net)
* Industry standard network and communications protocols (transmission control protocol/internet protocol [TCP/IP])
* Versions of these licenses must be compliant with U.S. Technology Export regulations
* Language—English for the Standard Design
  + Support partner agency’s specific language
* U.S. power configurations for the Standard Design
  + Support partner agency and site-specific power
* Ambient temperature and humidity constraints, per manufacturer’s specifications for equipment

3.5.2 Implementation Constraints

A LAN may not exist at all sites or be accessible and shareable. In such cases, a LAN shall be designed for integration of the detection equipment at each site. The LAN shall provide connectivity to ensure the requirements in these specifications are satisfied.

3.6 Assumptions and Dependencies

3.6.1 Capacity Assumption

The system must be scalable to accommodate a higher capacity if and where required. The system must also be open-architected so it can be integrated with a National Communications System (NCS) and other new or non-NSDD provided detection equipment if and when necessary.

3.6.2 Physical Assumptions about Site Operations

**RPM Traffic Flow:** Site personnel will control traffic through a portal such that the portal will have sufficient time following the occupancy by a single object to re-establish Gamma and Neutron background levels before another object occupies the portal space. The time, at minimum, is two seconds. Objects must not stop between the monitor pillars. Vehicle and rail speed through the portals should not exceed 8 kilometers per hour.

**Network:** The NSDD network shall never have a direct connection with outside networks. Separate, external machines located in the CAS office by the partner government agency for its own use shall remain separate from the system.

3.6.3 User Assumptions

It is assumed that a local System Administrator will have the necessary computer skills to perform computer system maintenance and will have the training necessary to make configuration changes and do backups, but s/he may or may not be fluent in English.

It is assumed that all other operators will receive CAS and workstation training for the assessment and adjudication of alarms and will operate the systems during times at which the location where the radiation detection system is installed is operating.

3.7 User Roles

The following descriptions are based on the functions performed, not the geographic location of or name given to the workstation at which the user might sit.

**Table 1. User Roles Descriptions**

|  |  |  |  |
| --- | --- | --- | --- |
| **User Role** | **Description** | **Rights** | **Notes** |
| System  Administrator | Sets up all user accounts and privileges for the different users. Sets up system configurations and system parameters. Performs any necessary system maintenance, such as database maintenance and regular system backups. This is generally intended to be a principal role (i.e., the only role assigned to an individual user ID). | System  Administrator Functions | Windows Admin functions require a Windows Admin Account. |
| Supervisor | Manages the CAS (Primary and Secondary) Operators, establishes and manages event queues, distributes and manages event logic, etc.  Also has all the privileges of an Evaluator and Primary Operator. | All Operator Functions | The Supervisor queue shall also display all alarms owned by the other Operators. |
| Evaluator | The operator making decisions on events (where oversight function is assigned to a CAS over LANs and/or SWS’s) who determines whether a secondary inspection is required and determines when additional response agencies need to be contacted (e.g., investigations need to be conducted). | Limited  Operator  Functions | The events displayed in the various event queues displayed on the Operator screens shall be dictated by which (if any) custom event  queues are assigned to the  Operator. |
| Primary  Operator | Monitors an assigned set of lanes. Receives and carries out instructions. The Local User Display provides the radiation profile and images associated with an alarm. | Limited  Operator  Functions | Only one authorized Operator can control a particular LAS site at one time. The LAS shall be assigned to a particular CAS site. |
| Secondary Operator | Performs secondary inspections as directed by the Supervisor and Evaluator. Updates the NSDD CAS system using the SWS/CAS UI. | Limited  Operator  Functions | Can only read and write messages with the CAS Operator and upload radionuclide identification device (RID)/HH data. |
| Observer | This role may be assigned to a third-party agency (e.g., another onsite agency working alongside the agency that operates the CAS system) with viewing and reporting performed through a Mirror CAS.  This role provides access to screens and reports. | Limited  Operator  Functions | Has no update privileges. |

4.0 Requirements

4.1 Requirement Groupings

The following section defines functional requirements for the CAS software and the system. All requirements are grouped by major functional areas and organized by logical usage. This organization supports development of use cases for the design document and test cases for the test plans. The requirement sub-groups are shown in Sections 4.2 and 4.3.

Each requirement has a unique alphanumeric identifier; for example, SOEI-001-01a. The numbering convention is as follows:

* the first letter sequence represents the requirements major functional grouping, followed by a dash;
* the next three digits represent the requirement sub-group, followed by a dash;
* the next two digits represent the requirement number; and
* the last letter identifies a requirement detail item.

The major functional groups are identified as follows:

* the first two letters differentiate software (SO) requirements from system (SY) requirements;
* the remaining letters indicate the requirement type, which include
  + external interface (EI) requirements,
  + functional requirements (FR), and
  + nonfunctional requirements (NFR).

4.2 Software Requirements

The following sections include lists of requirements for the software. The Requirements

Traceability Matrix (RTM) and Appendix A include detailed descriptions of these requirements.

4.2.1 External Interfaces

|  |
| --- |
| SOEI-001-00. Cameras |
| SOEI-002-00. RPMs |
| SOEI-003-00. RIDs |
| SOEI-004-00. National Communications System |

4.2.2 Functional Requirements

|  |
| --- |
| SOFR-001-00. Events |
| SOFR-002-00. Displays |
| SOFR-003-00. Data |
| SOFR-004-00. Users |
| SOFR-005-00. Multi-mode |
| SOFR-006-00. Status of health (SOH) alarm closure |

4.2.3 Nonfunctional Requirements

|  |
| --- |
| SONFR-001-00. Availability |
| SONFR-002-00. Security |
| SONFR-003-00. Maintainability |
| SONFR-004-00. Recoverability |
| SONFR-005-00. Exportability |
| SONFR-006-00. Performance |
| SONFR-007-00. TCP/IP |
| SONFR-008-00. Serverless (stand-alone desktop core processing unit) |

4.3 System Requirements

The following sections include a list of requirements for the system. The Requirements Traceability Matrix and Appendix A include detailed descriptions of these requirements.

4.3.1 External Interfaces

|  |
| --- |
| SYEI-001-00. Communication Infrastructure |
| SYEI-002-00. Power |
| SYEI-003-00. RIDs |
| SYEI-004-00. RPMs |
| SYEI-005-00. Cameras |
| SYEI-006-00. VoIP |
| SYEI-007-00. Video Image Real Time Viewing |

4.3.2 Functional Requirements

|  |
| --- |
| SYFR-001-00. Hardware |
| SYFR-002-00. Storage |

4.3.3 Nonfunctional Requirements

|  |
| --- |
| SYNFR-001-00. Archive |
| SYNFR-002-00. Downtime |
| SYNFR-003-00. Auto Shutdown |
| SYNFR-004-00. System Security |

Appendix A: Requirements Details

A.1 Software Requirements

A.1.1 Software External Interfaces

| **ReqID** | | | **Req Name** | **Description** | **Functionality** |
| --- | --- | --- | --- | --- | --- |
| SOEI-  001-00 |  |  | Cameras | The software shall include the ability to interface with networked cameras using TCP/IP. | Provides still frame images of portal area. |
|  | SOEI-  001-01 |  | Video Image Collection | The software shall include the ability to collect video images and automatically associate these images with an alarm or fault event. | Allows operator to view images associated with an alarm or fault event. |
|  | SOEI-  001-02 |  | Video Image Viewing | The software shall include the ability to view camera images or video associated with an alarm or fault event from an IP camera with the following capabilities.  Cameras shall, at a minimum, be capable of delivering the following:  - 640x480 pixels at 5 frames/second or better  - JPEG compressed still frame images  - MJPEG, H.264, H.265 streams | Allows operator to view images or video associated with an alarm or fault event. |
|  | SOEI-  001-04 |  | Video Image Storage | Software shall store video or images for later retrieval in accordance with SYFR-002-01, SYFR-002-02, SYFR-002-03, SYFR-002-04, and SYFR-002-05. | During the entire event or first 30 seconds of event (configurable). |
|  | SOEI-  001-05 |  | Event Video  Image  Configuration | Image collection times shall be adjustable with default requirements settings of:  - **2** seconds pre-event  - Duration (entire event/first **30** seconds)  - **2** seconds post-event  **URLs to collect single images (JPG) or streams shall be configurable in the software by an Administrator.** | Allows the system to be flexible based on site specific video viewing needs.  Allows for the URL for image requests to be configurable to support different camera models. |
|  | SOEI-  001-06 |  | Frame Rate Configuration | The frame rate of images saved per occupancy shall be configurable without recompilation of the code. | Frame rate should be sufficient to ensure adequate coverage of event (note: not all images will be usable). |
|  | SOEI-  001-07 |  | Camera  Configuration | The software shall include the ability to configure the association of at least **2** cameras with each RPM lane. |  |
| SOEI-  002-00 |  |  | Portal Monitors | The software shall include the ability to interface with RAPISCAN RPMs (and any others as required by the NSDD program) through TCP/IP communications. | Provides radiation measurement data. |
|  | SOEI-  002-01 |  | RPM Data  Collection | The software shall include the ability to automatically collect and store RPM data. | Association of RPM data with event. |
|  | SOEI-  002-02 |  | RPM Data Viewing | The software shall include the ability to view RPM data in real time. | Allows operator to view event associated RPM data. |
|  | SOEI-  002-03 |  | RPM Monitor  Settings | The software shall include the ability to collect and store the RPM configuration settings. | Storage of RPM configuration settings. |
| SOEI-  003-00 |  |  | RID | The software shall include the ability to interface with a RID and other handheld detection devices. | Provides interface with RID and other handheld detectors. |
|  | SOEI-  003-01 |  | RID/Handheld Download | The software shall be able to upload, associate, and store data from handheld detection devices RIDs natively or with the vendor provided software and associate this data with an alarm. | Collection of data files from RID and association with event. |
|  | SOEI-  003-02 |  | RID View and  Print | The software shall include the ability to view and print RIDs data associated with an alarm natively or with the vendor provided software. | View/print data from RID. |
| SOEI-  004-00 |  |  | National  Communications  System | The software shall include the ability to interface with an NCS. | Interface with NSDD NCS system. |

A.1.2 Software Functional Requirements

| **ReqID** | | | **Req Name** | **Description** | **Functionality** |
| --- | --- | --- | --- | --- | --- |
| SOFR-  001-00 |  |  | Events | The software shall support events and messages. |  |
|  | SOFR-  001-01 |  | Event Types | Event types include Alarms, Faults, and Messages. (Appendix B) |  |
|  |  | SOFR-001-01a | Alarm Events | Alarm events are radiation alarms and include:   * Gamma Alarms (G) * Neutron Alarms (N) * Neutron Gamma Alarms (NG Pair) |  |
|  |  | SOFR-001-01b | Fault Events | Fault events are system or device events indicating the system or device may be operating in a degraded state.  Faults include:  - Gamma High  - Gammy Low  - Neutron High  - RPM communications  - Extended occupancy (software generated)  - Tamper  - Camera communications loss |  |
|  |  | SOFR-001-01c | Messages | Messages are all other communications from devices, such as RPMs. Messages are not annunciated and do not require disposition. The software shall include the ability to display device messages. | This event type allows the software to accept and display non-fault messages from the system or from devices on the network. |
|  | SOFR-  001-02 |  | Event States | Event states include:  - Open Active: Event has not been closed.  - Unreviewed: Event has entered the queue but has not been reviewed.  - Unacknowledged: Event has entered the queue but has not be acknowledged.  - Closed: Event has had all required disposition information entered and has been closed. |  |
|  | SOFR-  001-03 |  | Event  Handling  Process | Alarm and Fault Events require closure. Messages do not require closure. | The event handling process is also referred to as "disposition." |
|  |  | SOFR-001-03a | Event  Annunciation | For Alarm and Fault Events, the software shall provide unique visible and audible indications of events within 5 seconds of the time the event occurred on all CAS and LAS workstations configured to monitor the lane. |  |
|  |  | SOFR-001-03b | Priority | Alarm and Fault Events shall be displayed, by default, in order of the event priority identified in Appendix B. |  |
|  |  | SOFR-001-03c | Concurrent Event  Processing | When a new Alarm or Fault Event with a higher priority enters the queue, processing of a current event shall not be interrupted, but the operator shall be notified that a higher priority alarm is in the queue. |  |
|  |  | SOFR-001-03d | Event Audio | When a new event enters the queue, an audible sound file shall be played. When multiple events with different priorities are annunciating, the audio file associated with the highest event priority shall be played. Audio files shall be in standard .WAV or .MP3 format. Specific audio files shall be configurable by event type. Event annunciation shall be provided regardless of application window state. |  |
|  |  | SOFR-001-03e | Event  Acknowledge | The software shall provide the operator with the ability to acknowledge (silence) one or several currently annunciating events. New events entering the queue will be annunciated. |  |
|  |  | SOFR-001-03f | Unreviewed  Event Display | The software shall provide a visual indicator of events that have been added to the queue but not reviewed. |  |
|  |  | SOFR-001-03g | Logic | The software shall provide the ability to configure logic functionality at different event states to support site specific concept of operations (ConOps) without recompilation. Each logic step shall include a mandatory/optional setting. |  |
|  |  | SOFR-001-03h | Closing | The software shall require the following to be completed prior to closing:  - All mandatory logic steps   * Disposition code * Authorization validation (password) |  |
|  |  | SOFR-001-03i | Event responsibility record | The software shall record which operator closed each event. |  |
|  |  | SOFR-001-03j | Closed Events | The software shall allow authorized users to search for and view closed events, including assessment information. The software shall allow authorized users to add comments and attach additional RID/HH data files. No existing data will be modifiable. |  |
|  |  | SOFR-001-03k | Archived Events | The software shall allow authorized users to search for and view archived events, including assessment information. Archived events will not be modifiable. |  |
|  | SOFR-  002-01 |  | Workstations | The software shall support multiple alternate simultaneous control stations.  Functionality shall be available on different workstation displays based on site-specific ConOps. Available functionality shall be controlled using a configuration file or system administration interface permitting modification without recompilation of the code. | This feature set addresses the need for multiple types of workstations based on permissions and logic steps. |
|  |  | SOFR-002-01a | CAS  Workstation | The software shall provide a UI and include all logic functionality. Specific functions shall be available based on role-based security. |  |
|  |  | SOFR-002-01b | LAS  Workstation | The software shall provide a well-defined subset of CAS functionality. |  |
|  |  | SOFR-002-01c | Secondary  Inspection  Workstation | The software shall provide a UI for entering data at a secondary inspection location. |  |
|  |  | SOFR-002-01d | Mirror CAS | The software shall provide a view-only version of the CAS workstation display. |  |
|  | SOFR-  002-02 |  | User Interfaces | The software shall provide the following UIs:   * Site map * New/active events * Closed/archived events * Event details * RPM and camera SOH * Lane details * Live camera view |  |
|  |  | SOFR-002-02a | Event Details Presentation | Display alarm or fault type and all pertinent data are time synchronized and associated together (e.g., alarm or fault data, video and other pertinent data are associated and presented together with alarm or fault type and time of event).    Alarms shall be presented with unique color and sound and in the priority order described in Table B1 in Appendix B. |  |
|  |  | SOFR-002-02b | Event Details Assessment | Provide an interface/form to facilitate the operator in assessing an alarm and fault. Assessment allows the operator to enter details about the alarm or fault as well as the final disposition. See Table B1 in Appendix B. |  |
|  |  | SOFR-002-02c | Event Count Graph | The software shall display RPM event data in the form of traces, including Gamma (Sigma), Neutron (Counts), and Background (Counts). The Gamma and Neutron trace displays shall be viewable simultaneously and be displayed on the same time scale. |  |
|  |  | SOFR-002-02d | Active Events  Queue | The software interface shall display alarms and faults requiring attention. |  |
|  |  | SOFR-002-02e | Video to support  alarm/fault assessment | For all alarms and faults, provides video images that allow the operator to determine the alarm or fault cause.  In the case of a single alarm event per occupancy, the software shall include the ability to limit the number of seconds of image collection to the first 30 seconds (configurable parameter), plus (configurable) pre and post number of seconds of image data. |  |
|  |  | SOFR-002-02f | Force Disposition prior to event closure | The software shall require assessment entry for events (alarms and faults) before they can be closed. |  |
|  |  | SOFR-002-02g | Disposition  Codes | The software shall allow an Operator to select from a set of allowable disposition codes such that it allows for modification without recompilation of the software code. | Refer to the Core Standard Disposition Codes baselined document. |
|  |  | SOFR-002-02h | SOH Display | The software shall provide an interface to display SOH for all monitored system devices. |  |
|  | SOFR-  002-03 |  | Language | The software shall permit the UI to be translated into the language of the partner agency. |  |
|  |  | SOFR-002-03a | Language  Entry | The software shall permit the UI to accept data entry in the language of the partner agency. |  |
|  |  | SOFR-002-03b | Language  Selection | The UI menu shall include the ability to change the display language (e.g., from English to partner agency language and vice versa). |  |
|  |  | SOFR-002-03c | Language  Display  Persistence | In the event of workstation software restarting, the UI shall restart in the language of the last user on the system. |  |
| SOFR-  003-00 |  |  | Data | The software shall include the ability to record various data sets in files as required by the NSDD Program and other users and transmit that data in multiple formats to multiple sets of stakeholders. Data acquisition and retention parameters shall be configurable. |  |
|  | SOFR-  003-01 |  | Data Types | The software shall support several categories of data. The SRS includes a data dictionary (see Data Dictionary) with detailed descriptions of these data types. |  |
|  |  | SOFR-003-01a | Event Data | The software shall include support for all event data from devices, including RPM data, camera videos/images, and RID/HH data files. |  |
|  |  | SOFR-003-01b | Disposition Data | The software shall include support for all disposition data, including comments, disposition codes, and user ID. |  |
|  |  | SOFR-003-01c | Configuration Data | The software configuration settings allow for customization without recompilation. The configurable settings are in the requirements specification. |  |
|  |  | SOFR-003-01d | User Data | The software shall include the ability to track users, including authentication and authorization information. | Audit log of user login and logout attempts and password changes. |
|  |  | SOFR-003-01e | Administration Data | The software shall track successful and unsuccessful authorization attempts (SOFR-003-05). |  |
|  | SOFR-  003-03 |  | Daily File | The software shall include the ability to record  RPM data in accordance with the NSDD Guidelines for Naming and Formatting Daily Files. |  |
|  | SOFR-  003-05 |  | Logs | The software or operating system shall log:  - Successful authentication attempts  - Unsuccessful authorization attempts  - User password changes  - RPM and camera events  - Changes to the configuration files  - Software component failures  - System failures (including interface faults and software failures)  - System restarts |  |
|  | SOFR-  003-06 |  | Print | The software shall support the ability to print reports, logs, and screenshots. |  |
|  | SOFR-  003-07 |  | Reports | The software shall include the ability to create reports. |  |
|  | SOFR-  003-08 |  | Transmission | The UI shall provide the ability to package information from an alarm event into a file so it can be forwarded to another party for viewing. |  |
|  | SOFR-  003-09 |  | Event Data Association | The software shall associate all event data and disposition data with a unique event record. |  |
| SOFR-  004-00 |  |  | Users | The software shall implement role-based authentication and authorization. Each user shall have a unique password. Passwords are required to meet Administrator-defined length and complexity requirements. Each user may be assigned to one or more roles. |  |
|  | SOFR-  004-01 |  | Roles | The software shall support the user roles described in Section 3.7, User Roles. |  |
| SOFR-  005-00 |  |  | Multi-mode (number of alarms per occupancy) | The software shall include a configuration setting to support the association of one or multiple alarms during a given occupancy. Default shall be that multiple alarms from a portal during a single occupancy shall be reported as a single alarm event.  Configurability shall be by RPM lane. | For anticipated extended occupancies, this feature allows the software to treat each alarm within an occupancy as a separate event, to be dispositioned independently. Frequently used for rail lanes. |
| SOFR-  006-00 |  |  | SOH Fault Closure | SOH events should not be able to be cleared/closed until after the SOH event in question is no longer in an active state (for example, communications restored, camera repaired). | This feature prevents SOH faults from being cleared until the state of the device has returned to normal. |

A.1.3 Software Nonfunctional Requirements

| **ReqID** | | | **Req Name** | **Description** | **Functionality** |
| --- | --- | --- | --- | --- | --- |
| SONFR-  001-00 |  |  | Availability | The software shall minimize downtime and support 24/7 operation. No normal system operation and administration functions shall require the CAS to be unavailable. This includes backups. The software shall also permit offline restoration of configuration and data files. |  |
| SONFR-  002-00 |  |  | Security | The software shall limit access to functionality by means of role-based security. |  |
| SONFR-  003-00 |  |  | Maintainability | The software shall allow standard system administration functions. |  |
|  | SONFR-  003-01 |  | Installation  and Upgrade | The CAS software and associated applications and operating systems shall be capable of being installed and updated by a trained System Administrator. | Installation of CAS software shall be performed through a single automated installation wizard.  The operating system and applications shall be able to be upgraded to support patches and fixes. |
| SONFR-  004-00 |  |  | Recoverability | The software shall provide the ability to recover the following:  - Database: most recent backup  - Operating system or system image  - Image files or any other CAS-related data |  |
| SONFR-  005-00 |  |  | Exportability | The software shall allow data to be exported to a standard file format to permit offline viewing using a readily available viewer. |  |
| SONFR-  006-00 |  |  | Performance | The software shall be capable of handling the maximum number of device event messages from all devices in all lanes without noticeable degradation in responsiveness at the server or client workstation. |  |
| SONFR-  008-00 |  |  | Serverless | Sites shall not require a separate server rack where the number of occupancies is few enough to allow a single CPU CAS system. | CAS System (server and  Workstation applications) shall be capable of running on a single Personal Computer (PC) system. |

A.2 System Requirements

A.2.1 System External Interfaces

| **ReqID** | | | **Req Name** | **Description** | **Functionality** |
| --- | --- | --- | --- | --- | --- |
| SYEI-  001-00 |  |  | Communication  Infrastructure | The system shall support the ability to communicate through a TCP/IP network. |  |
| SYEI-  002-00 |  |  | Power | All components of the system shall support the power specifications of the partner agency. |  |
|  | SYEI-  002-01 |  | Power  Protection | The system shall include UPS with power conditioning and regulation for protection of workstations, servers, and networking equipment. At minimum, the UPS shall provide **15** minutes of backup power for any connected device that generates, stores, or transmits data. UPS devices located in a server room or closet shall be connected to the network. UPS’s in a server room shall also include temperature and relative humidity monitoring. |  |
| SYEI-  003-00 |  |  | RIDs and handheld detectors | The system shall include the ability to associate to events and display any RID data deployed by the NSDD Program. |  |
| SYEI-  004-00 |  |  | Radiation  Portal Monitors | The system shall include the ability to connect to any RPMs as required by the program. |  |
| SYEI-  005-00 |  |  | Cameras | The system shall include the ability to connect to TCP/IP-based cameras. |  |
| SYEI-  007-00 |  |  | Video Image  Real Time  Viewing  (Streaming  Video) | The system shall provide the ability to view “real time” video from a selected camera at any time. Cameras shall be capable of delivering the following or better:  - 640x480 pixels at 30 frames per second  - (JPEG, MJPEG, H.264, H.265) | Provides the ability to monitor the portal lane remotely. This video shall never be saved. |
|  | SYEI-  007-01 |  | Streaming  Video Interface | The system shall provide an interface to display the streaming video from any selected camera. | The interface may be provided in either the CAS workstation application or a separate application. |

A.2.2 System Functional Requirements

| **ReqID** | | | **Req Name** | **Description** | **Functionality** |
| --- | --- | --- | --- | --- | --- |
| SYFR-  001-00 |  |  | Hardware | The system shall include computer and communications equipment sufficient to meet the needs of this requirements specification. |  |
|  | SYFR-  001-01 |  | Printers | Printers must be modern, PC-compatible, multifunctional, and networkable. Printers and their associated consumables shall be available locally in the host country. |  |
|  | SYFR-  001-02 |  | Screens | Screens must be modern, flat-panel displays sufficient to meet the needs of this requirements specification. |  |
|  | SYFR-  001-03 |  | Bandwidth | Network capacity shall be sufficient to support throughput requirements of connected equipment with minimal network latency. | **Ensure LAN and WAN connections can provide adequate bandwidth and latency for the system.** |
| SYFR- 002-00 |  |  | Storage |  |  |
|  | SYFR- 002-01 |  | Data Retention Type | The system shall not store non-alarming-occupancy data if this feature can be disabled through configuration settings. |  |
|  | SYFR- 002-02 |  | Data Retention Length | The system shall store daily files, alarm data, fault data, and SOH data for six months and/or until the disk space reaches 80% full. |  |
|  | SYFR- 002-03 |  | Data Retention Deletion Order | The system shall automatically delete daily files, alarm data, fault data, and SOH data based upon age and/or disk space. |  |
|  | SYFR- 002-04 |  | Data Retention Monitoring | The system shall automatically monitor age of data and/or disk space. |  |
|  | SYFR- 002-05 |  | Data Retention Rules | The system shall not archive daily files, alarm data, fault data, or SOH data. All daily files, alarm data, fault data, and SOH data shall remain in the active database or file system until deleted in accordance with SYFR-002-01, SYFR-002-02, SYFR-002-03, and SYFR-002-04. |  |

A.2.3 System Nonfunctional Requirements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ReqID** | | | **Req Name** | **Description** | **Functionality** |
| SYNFR-  003-00 |  |  | Auto  Shutdown | The system shall include components necessary to allow for automatic shutdown of computing equipment in the event of extended power loss or a high humidity or temperature alarm. | Ungraceful shutdowns may have a negative impact on system stability.  UPS devices shall perform a graceful shutdown on computing equipment if the temperature is above 27 C, below 17 C, less than 20% relative humidity, or above 70% relative humidity. |
|  | SYNFR-  003-01 |  | Auto Shutdown  Notification | The system shall include a notification to the local user of impending shutdown of workstations or servers. |  |
| SYNFR-  004-00 |  |  | System Security | The system shall include security features necessary to limit access to the system components to authorized personnel. | Physical access to system components may introduce security risks. |

A.3 Requirements Traceability Matrix Description

The RTM uniquely identifies and describes each requirement.

For reverse traceability, the RTM provides the source for each requirement. For forward traceability, each requirement allows for entry of design entity and test case identifiers.

To support scalability and flexibility, the RTM also includes a site survey questionnaire (SSQ). These questions can be answered by the relevant expert during or after the site survey and provide the ability to activate, configure, and clarify many of the requirements. Most of the requirements are universal to all installations and are indicated with the word “(Standard)” in the SSQ field.

SSQ field tags include:

* (Activation)—True/False question. If true, the requirement and the test case become active
* (Configuration)—Variable setting or parameter
* (Clarification)—Explanation or amplification
* (Standard)—Universal requirement, always active
* (Default)—Typical setting or entry

Appendix B: Event Types, Priorities, and States

Event types include Alarms, Faults, and Messages. Alarm events are radiation alarms and include Gamma alarms, Neutron alarms, and Neutron-Gamma alarms. Fault events are system or device events indicating the system or device may be operating in a degraded state. Faults include RPM communications fault, extended occupancy fault (software generated), tamper fault, and camera communications fault. Messages are all other communications from devices, such as RPM messages. Messages are not enunciated and do not require disposition.

B.1 Event Types and Priorities

The events that shall be displayed on all systems are contained in Table B1, in highest to lowest priority order.

**Table B1. Event Priority/Video/Graphing Summary**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Event** | **Event Type** | **Sound\*** | **Color\*** | **Video Provided** | **Graphing Provided** |
| 1 | NG Alarm | RPM Alarm | A | A | Yes | Yes |
| 2 | N Alarm | RPM Alarm | B | B | Yes | Yes |
| 3 | G Alarm | RPM Alarm | C | C | Yes | Yes |
| 4 | Gamma Hi | RPM Fault | D | D | No | No |
| 5 | RPM Connection Loss | RPM Fault | D | D | No | No |
| 6 | Gamma Lo | RPM Fault | D | D | No | No |
| 7 | Neutron Hi | RPM Fault | D | D | No | No |
| 8 | Camera Fault | SOH Fault | D | D | No | No |
| 9 | Extended Occupancy Fault | Software-generated  RPM Fault | D | D | Yes (SSQ) | No |
| 10 | Tamper | RPM Fault | D | D | Yes (SSQ) | No |
| 11 | SOH Fault (Other) | SOH Fault | D | D | No | No |

\*Note: The letters A, B, C, and D represent unique sounds and associated colors that shall correspond to events.

\*\* It is noted that for some software vendors, priorities 5 and 6 are switched. These are minimum standards and software that exceeds these standards is acceptable.

B.2 Event States

Each Alarm or Fault event will be in one of several distinct states: Open, Closed, or Archived.

When an event is initiated, it enters the Open: Active state.

The event will also be tagged as unacknowledged and unreviewed.

While unacknowledged, the system will provide an audible indicator (sound file).

Acknowledging an event will silence the audible indicator (and will also acknowledge all other unacknowledged events).

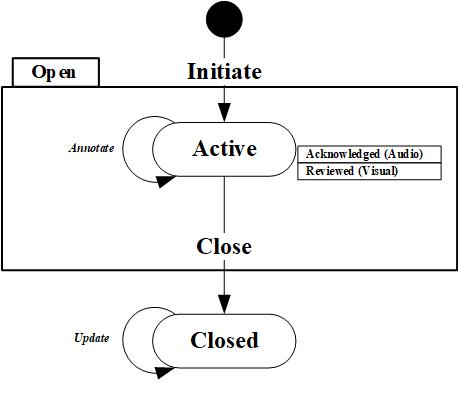
While unreviewed, the system will provide a visual indicator (e.g., record entry is flashing).

Opening the event details will disable the visual indicator.

While Open: Active, the event may be annotated. This self-transition requires the entry of event information and may include comments and RID/HH file pointers.

Transitioning from the Open: Active state to the closed state requires the operator to close the event. This transition requires completion of all mandatory adjudication entries, the selection of a disposition code, and a user authentication and authorization check.

When closed, an event can be updated by addition of comments and RID/HH file pointers based on installation configuration settings.

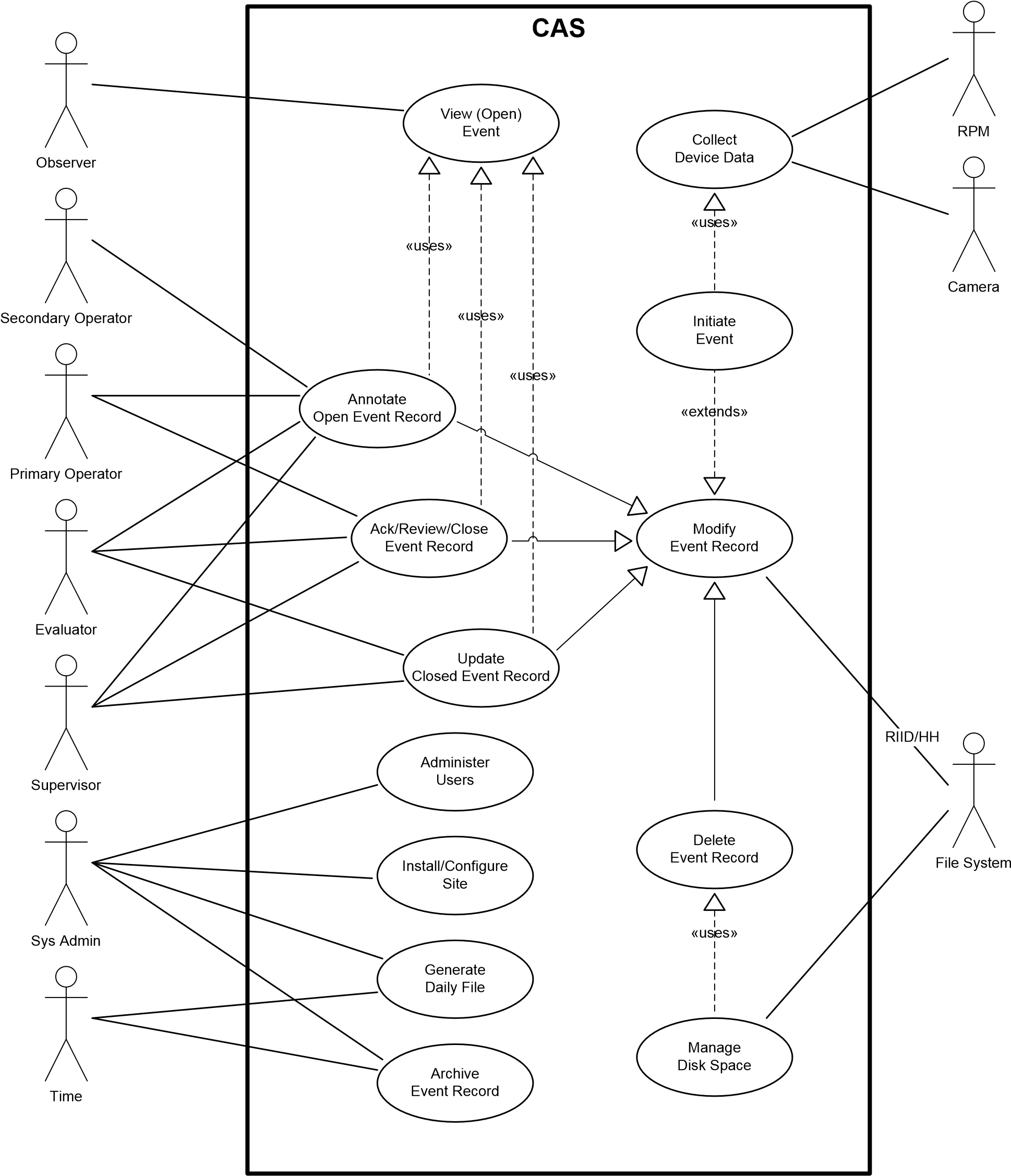


**Figure B1. Event state diagram.**

Appendix C: Use Cases

C.1 Use Case Diagram and Scenarios

The use case diagram (Figure C1) shows which actors interact with which use cases and how the different use cases are related. The use case diagram and following scenarios cover only the most common interactions with the CAS software system.



**Figure C1. Use case diagram.**

| **C.1.1 View Event** | |
| --- | --- |
| **Use Case ID** | UC-1.1 |
| **Use Case Name** | View Event |
| **Actors** | Observer, Secondary Operator, Primary Operator, Evaluator, Supervisor |
| **Description** | Allows authorized user to search for and display event details |
| **Preconditions** | User has been authenticated  User has been authorized |
| **Postconditions** | UI displays event details |
| **Normal Course** | 1. User identifies event record to be displayed 2. User selects event from Active/Closed/Archived event list 3. User enters query information into search interface 4. System performs search for event record and retrieves data from data store 5. System displays event record in UI |
| **Alternative Course** | **3.A.1 Event data time synchronization (after step 3)**   1. User modifies event time control 2. User scrolls trace (graph) time controller 3. User activates video playback controller 4. System updates video with synchronized image and updates trace (graph) display with synchronized time indicator |
| **Exceptions** | **2.E.1 Search returns zero records (at step 2)**   1. System displays message indicating no records found |
| **Includes** | None |
| **Associated Requirements and Business Rules** | SOEI-001, SOEI-003-02, SOEI-002-02, SOFR-002-02 |
| **Special Requirements** | Graph trace display, video image display |
| **Assumptions** | None |

| **C.1.2 Annotate Open Event Record** | |
| --- | --- |
| **Use Case ID** | UC-1.2 |
| **Use Case Name** | Annotate Open Event Record |
| **Actors** | Secondary Operator, Primary Operator, Evaluator, Supervisor |
| **Description** | Allows authorized user to add/modify disposition data in open event record |
| **Preconditions** | Event is open  Event record has been selected for viewing using UC-1.1 View Event Record  User has been authenticated  User has been authorized |
| **Postconditions** | Event workflow data has been added/updated in event record |
| **Normal Course** | 1. User adds/modifies disposition data in active event record 2. User adds/modifies comment 3. User identifies RID/HH file as associated data 4. System updates event record to include added/modified disposition data |
| **Alternative Course** | None |
| **Exceptions** | **1.b.E.1 File input/output (I/O) error. File is corrupt or not found.**   1. System displays descriptive error message |
| **Includes** | Uses UC-1.1 View Event Record |
| **Associated Requirements and Business Rules** | SOFR-003-01b Disposition Data, SOFR-003-09 Event Data Association |
| **Special Requirements** | File selection dialog |
| **Assumptions** | Event has been silenced |

| **C.1.3 Ack/Review/Close Event Record** | |
| --- | --- |
| **Use Case ID** | UC-1.3 |
| **Use Case Name** | Ack/Review/Close Event Record |
| **Actors** | Primary Operator, Evaluator, Supervisor |
| **Description** | Allows authorized user to silence annunciating event and close an event. This use case describes the behavior of the event state engine while the event is in the open state and during operator-system interaction. |
| **Preconditions** | Event is open  For event closed, user is viewing open event record (UC-1.1)  User has been authenticated  User has been authorized |
| **Postconditions** | Event attribute has been modified to match the resultant event state, and system silences or displays event record in UI accordingly |
| **Normal Course** | 1. User opens event details screen 2. System modifies state of event record 3. System stops visually identifying event as unreviewed 4. User acknowledges event 5. System modifies state of event record 6. System stops playing audio file 7. User closes event 8. System prompts user for credentials 9. User enters credentials 10. System modifies state of event record 11. System displays event record in closed event list |
| **Alternative Course** | **2.A.1 Alternate acknowledgement methodologies (step 2)**   1. User opens event record 2. (Optional) User selects event record(s) and selects UI “acknowledge” control |
| **Exceptions** | **3.E.1 Close: Required workflow data has not been entered**   1. System displays message indicating that a required disposition data entry has not been completed (UC-1.2).   **3.E.2 User not authorized**   1. System displays message indicating that user is not authorized to close event   **3.E.3 SOH Fault Closure. (Activation SSQ SOFR-006-00) SOH of device has not returned to normal condition.**   1. System displays message indicating that Fault Event cannot be closed |
| **Includes** | Uses UC-1.1 View Event Record |
| **Associated Requirements and Business Rules** | SOFR-001-02 Event States, SOFR-001-03 Event Closure, SOFR-002-00 Displays, SOFR-00301b Disposition Data, SOFR-006-00 Fault Closure |
| **Special Requirements** | Silence: System audio sub-system  Close requires that required disposition data entry (UC-1.2) has been completed |
| **Assumptions** | Close event assumes event has been silenced |

| **C.1.4 Update Closed Event Record** | |
| --- | --- |
| **Use Case ID** | UC-1.4 |
| **Use Case Name** | Update Closed Event Record |
| **Actors** | Evaluator, Supervisor |
| **Description** | When a record has been closed, certain types of workflow data may still be appended to the event record. |
| **Preconditions** | Event record has been closed  Event record has been selected for viewing using UC-1.1 View Event Record  User has been authenticated  User has been authorized |
| **Postconditions** | Additional data is appended to closed event record |
| **Normal Course** | 1. User adds additional data to closed event record 2. User adds comment 3. User identifies RID/HH file as associated data 4. System prompts user for credentials 5. User enters credentials 6. System updates closed event record to include added data |
| **Alternative Course** | None |
| **Exceptions** | **1.b.E.1 File I/O error. File is corrupt or not found.**   1. System displays descriptive error message   **3.E.2 User not authorized**   1. System displays message indicating that user is not authorized to update event |
| **Includes** | Uses UC-1.1 View Event Record |
| **Associated Requirements and Business Rules** | SOFR-001-03i Closed Events |
| **Special Requirements** | File selection dialog |
| **Assumptions** | None |

Appendix D: Version Control

D.1 Configuration Management

When this document is approved and baselined, modifications shall be initiated and approved using a change request (as described in the Configuration Management Plan). Change requests are approved by a configuration control board.

D.1.1 Version Identification

The document version identification is in the following format:

A capital letter “R,” followed by the major revision number, followed by a period, followed by the minor revision number, followed by an optional sub-revision letter.

Site-specific documents will be identified by the version identifier, followed by an underscore, followed by the country name, a hyphen, and the site name.

For example, a version of “3.2b\_CountryX-SiteY” would indicate the following:

Major Revision = 3; Minor Revision = 2; Sub-revision = b; Country = CountryX; Site = SiteY

Changes to the document that introduce, modify, or remove significant content or concepts require a major revision and re-approval. Typographical corrections and clarifications require only minor revisions or sub-revisions. Re-approval of minor revisions may be required.

D.1.2 Quality Check

To assist the NSDD federal country manager in crafting a requirements specification that is complete, accurate, and satisfies all criteria, a requirements specification review checklist has been attached in Section 4.4, Requirements Specification Review Checklist.

Before releasing this document, a checklist shall be completed by a quality engineer. Completed checklists are configuration nodes and are controlled in accordance with the configuration management plan.

Legend:

P = Passed

A = Passed, but there are suggested improvements to strengthen the document.

F = Failed, inadequate, does not completely satisfy established criteria.

Checklist items evaluated as either “A” or “F” require comments.

Appendix E: NSDD CAS Software Graphing Requirements

Overview

This requirements specification applies to the CAS application. This document includes the requirements and algorithms for generating a graph UI element.

Definitions

* **Alarm**: An event where the RPM has detected a level of radiation in excess of a predetermined threshold.
* **Ceiling**: A function that means to round up to the next larger integer.
* **Event**: A time period during which a condition exists that requires special considerations or response. An event is a general concept and includes alarms, faults, and occupancies.
* **Fault**: An event in which the system has detected an abnormal or degraded operating condition.
* **Graph**: An area of the UI screen that is used to display numerical data as one or more data traces.
* **Occupancy**: An event in which the RPM has detected an object between the RPM pillars.
* **Plot**: The placement of data points on a graph and the connection of data points to produce a trace.
* **Sigma**: The standard deviation from the background. Gamma data for events can be plotted in terms of the difference from the background in units of Sigma.
* **Trace**: A series of plotted data points connected by lines.

References

* Example Graph Data.xls
* RAPISCAN RPM ICD

Graphing Requirements

Messages from the Rapiscan RPM, including structure and timing, are described in the RAPISCAN RPM ICD, which is available for each version of the firmware.

The software shall display RPM event data in the form of traces, including Gamma (Sigma), Neutron (Counts), and Background (Counts). The Gamma and Neutron trace displays shall be viewable simultaneously and be displayed on the same time scale.

**Graph Views**

The CAS application shall provide the following graph views:

* **Standard View**: Sample data from each detector is summed by radiation detector type, and presented as single graph traces. (One trace for Gamma data, one trace for Neutron data.) Appropriate background graphic indicators shall also be shown.
* **Expert View**: Sample data from each individual detector radiation detector type, and presented as single graph traces. (One trace for Gamma data, one trace for Neutron data.) Appropriate background graphic indicators shall also be shown.

**Detector Type Selection**

The CAS application shall include the ability to select/deselect traces based on detector type.

* Only Neutron trace(s)
* Only Gamma trace(s)
* Both Neutron and Gamma traces

**Note**: When displaying both Gamma and Neutron data, traces shall be displayed on the same horizontal time scale.

**Horizontal Scale**

The horizontal scale is in units of time and corresponds to the event period. This is typically in units of seconds.

* **Start Time**: The start time shall be the timestamp of the first data sample or image. Time shall be time relative to the start of the event.
* **Time Zero**: Reference time zero (0) shall be the start of the event. (e.g., RAPISCAN RPM start of occupancy is indicated by receipt of the burst of scan mode messages from the RPM.)
* **End Time**: The end time is the timestamp of the last data sample or image.
* **Pre/Post Video**: Full horizontal time scale will normally include additional pre and post time before and after the plotted data points to support synchronized display of pre and post event video.

### Vertical Scale

* **Vertical Margin**: The graph shall be displayed on a vertical scale from the lower bound to the upper bound with an additional margin below the lower bound and above the upper bound. This is to prevent the plotted values from reaching the extreme vertical edges of the graph area. Total margin space shall be no greater than 5% of the full scale.
* **Gamma Scale**: The system shall allow the operator to select to display the Gamma data in vertical units of either counts per second or multiples of Sigma. The default shall be in counts per second.
  + Counts Lower Bound (γlb)—The Gamma counts lower bound shall be zero (0).
  + Sigma Lower Bound (γlb)—The Gamma Sigma lower bound shall be the minimum plotted value.
  + Upper Bound (γub)—The Gamma upper bound shall be the maximum plotted value.
* **Neutron Scale**: The Neutron vertical scale shall be in units of counts per second.
  + Lower bound (*n*lb)—The Neutron vertical scale lower bound shall be zero (0).
  + Upper bound (*n*ub)—The Neutron vertical scale upper bound shall be the max Neutron plotted value. The Neutron upper bound shall never be less than 15.

### 

### Data Trace Value Plotting

* **Gamma Data**: Plotted data will be a transformed sum of fast count data per the following algorithms.
  + **Timing**: Every 200 milliseconds, the RAPISCAN RPM provides a Gamma fast count reading. The current Gamma fast count reading is referred to as γt. Gamma data points shall be plotted 200 milliseconds apart starting with the first γt message in each occupancy or event. **Note**: At the start of an occupancy, the RAPISCAN RPM provides a burst of five Gamma messages, which include the first γt reading and the previous four readings. The previous reading message values are not plotted. They are used to calculate the first Gamma data point and are rolled out sequentially with subsequent plotted values.
  + **Expert View Gamma Counts**: For expert view, the Gamma counts data for each detector panel (Sd) is the sum of the current sample and the previous 4 samples.
  + **Standard View Gamma Counts**: For standard view, the Gamma counts data (Stotal) is the sum of all the individual detector panel Gamma counts data (Sd). **Note**: This assumes a four detector panel RPM.
  + **Gamma Sigma**: Calculate Gamma Sigma as the square root of the background.
  + Plotted Gamma data (Gσ) in terms of Sigma uses the following formula.

For expert view, use Sd and Bd values. For standard view, use Stotal and Btotal values. **Note**: Negative values can result from this equation.

* Gamma Background
  + **Expert View**: the background for each detector panel (Bd) is taken from the separate field values in the last GB message before the start of the occupancy.
  + **Standard View**: calculate total background (Btotal) as the sum of all detectors of the background data received in the GB message just before occupancy start.
* **Gamma Background Indication**: Gamma background will be indicated on the graph in a manner that does not obscure data traces (e.g., dashed horizontal line in examples). This indicator shall be a provided by a graphic element other than the Gamma data trace. **Note**: By definition, the Gamma background, in units of Sigma, is zero (0).
* **Neutron Data**: During an occupancy, the RAPISCAN RPM provides a Neutron fast count data message every second.
  + **Expert View**: Neutron data is plotted as raw counts from the individual message field values.
  + **Standard View**: Neutron data is plotted as a sum of the individual detector data values.
* **Neutron Background**: Neutron background will be indicated on the graph in a manner that does not obscure data traces. This indicator shall be provided by a graphic element other than the Neutron data trace. **Note**: Newer firmware versions provide the sum Neutron background as a floating point value in the “GX” message (See RAPISCAN RPM ICD). If this is used, the Neutron background indicators in expert view shall be a quarter of this value.

**Threshold Excursion Indication**

The Neutron and Gamma graph area shall clearly indicate all periods when the alarm threshold is exceeded (e.g., different data point icons in Example 1; red rectangle in Example 2.) This is based on alarm messages from the RPM.

**Graph Video Time Synchronization Indication**

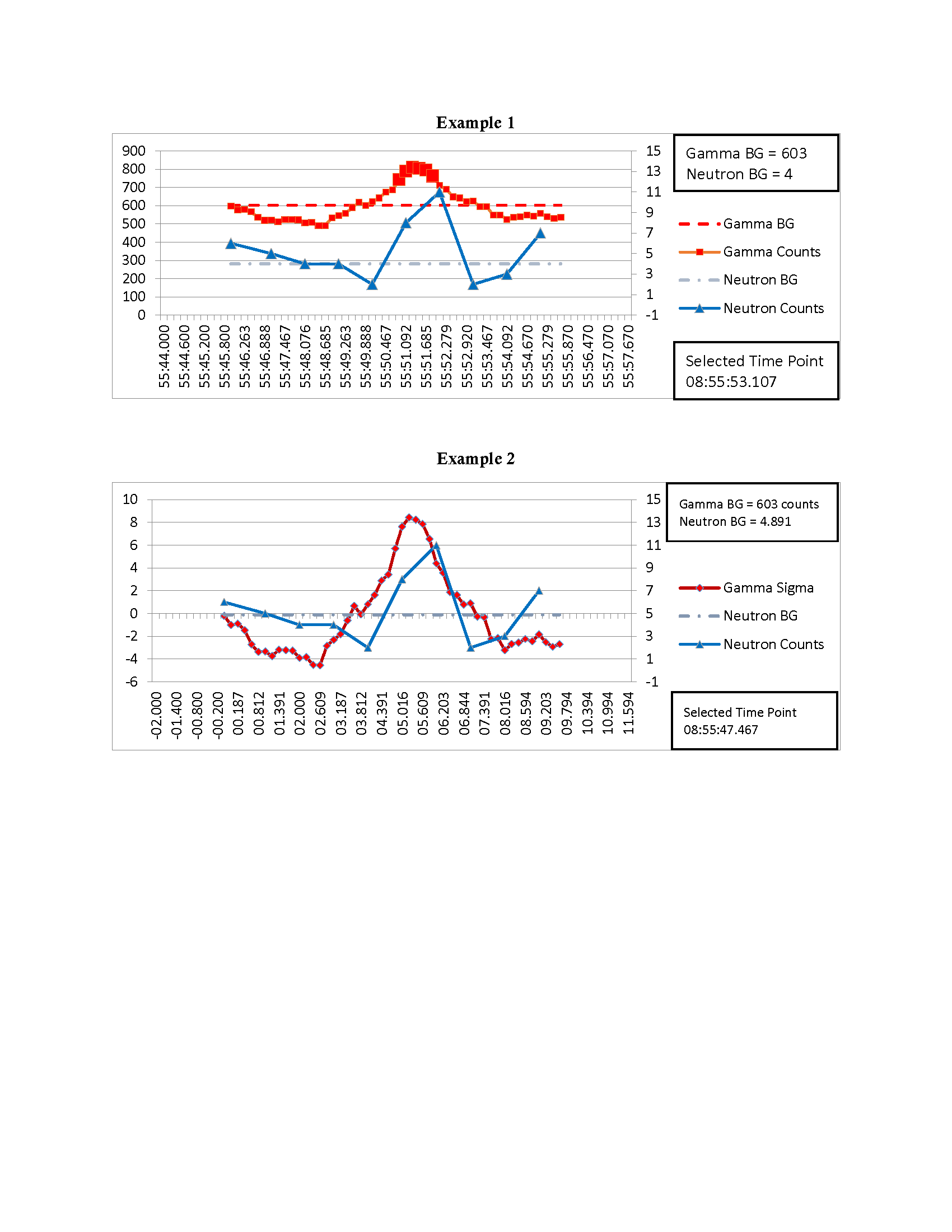
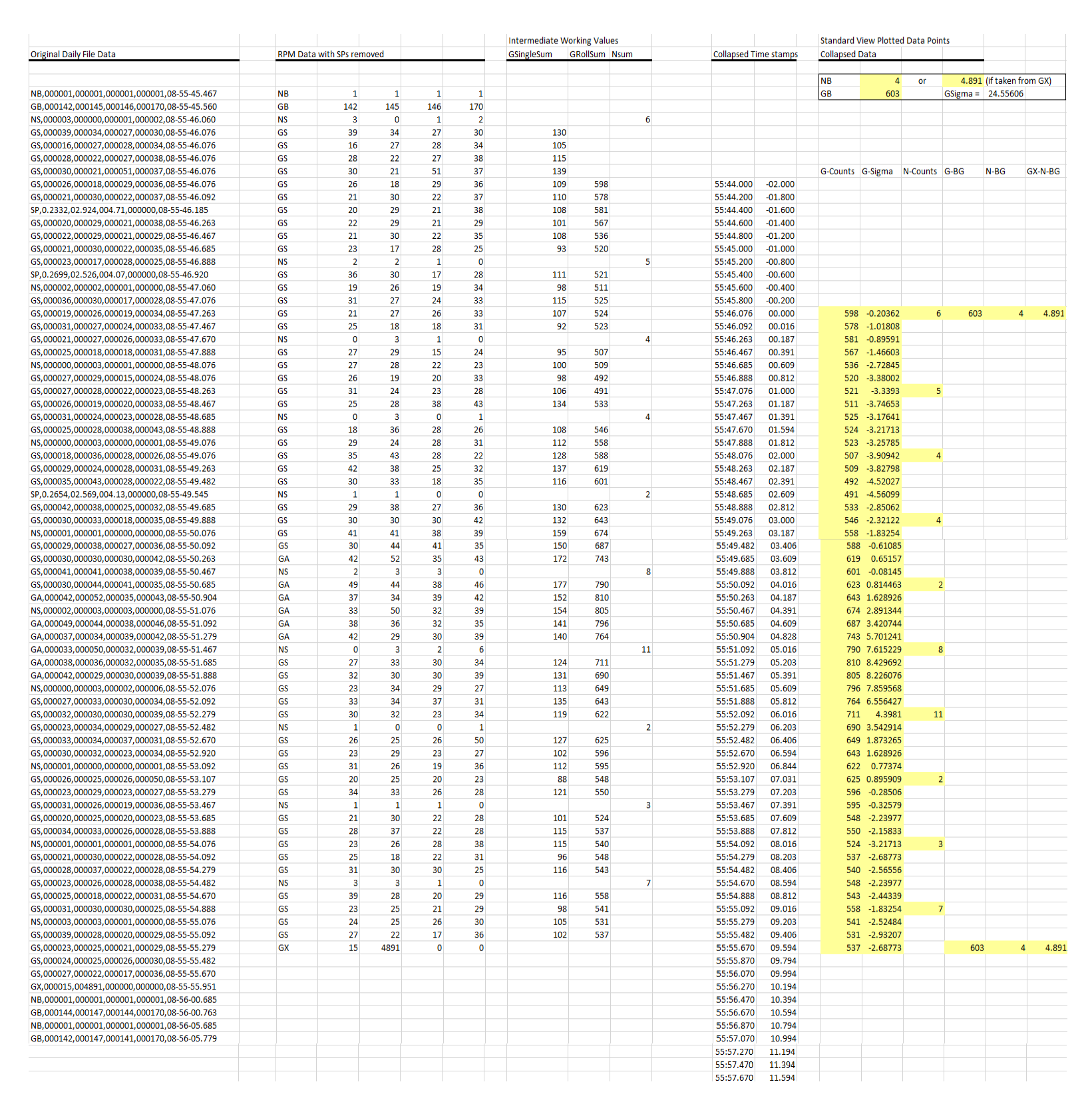
The Neutron/Gamma graphs shall include a method for identifying the time point of the displayed image (e.g., green vertical bar in examples). (This is a clarification of existing requirements, MPI SOFR-002-01, and Core SOFR-002-02a.) If the currently selected time point is not within a video collection period, it is acceptable to display a message indicating that no image is available.

### 

### Graph Elements

* **GAMMA**: The color for Gamma traces shall be red.
* **NEUTRON**: The color for Neutron traces shall be blue.
* **LINE STYLE**: The line style for trace data shall be solid.
* **BACKGROUND**: If backgrounds are indicated as lines, the lines shall be dashed. Data points shall be indicated with different icons to allow the traces to be differentiated on a black and white print-out.
* **GRID**: If grid lines are provided, they shall be drawn so as to be distinguishable from data traces and background indicators and not obscure data traces or background indicators.

Appendix F: NSDD CAS Graphing Examples



**Example 3: Master Upper**

**Example 4: Master Lower**

**Example 5: Slave Upper**

**Example 6: Slave Lower**

Appendix G: NSDD Standard Disposition Codes

The NSDD Standard Disposition Codes will serve as the basic set of disposition codes for all CAS units deployed by the program. These codes were developed with input from technical experts. They do not attempt to address every conceivable cause of alarm. Rather, they reflect typical operational conditions and causes of alarm while allowing for user interaction with and input to the system. While this list of codes serves as the basic standard, it shall remain extensible, with any additions subject to approval by the NSDD Program.

**Note: Exact punctuation and the inclusion of the numbers preceding the disposition codes are required.**

**NSDD Program Standard Disposition Codes**

1. Real Alarm—Contraband Found
2. Real Alarm—Other
3. Innocent Alarm—Medical Isotope Found
4. Innocent Alarm—Naturally Occurring Radioactive Material Found
5. Innocent Alarm—Declared Shipment of Radioactive Material
6. False Alarm—Physical Inspection Negative
7. False Alarm—RID/ASP Indicates Background Only
8. False Alarm—Other
9. Alarm/Tamper/Fault—Authorized Test/Maintenance/Training Activity
10. Tamper/Fault—Unauthorized Activity
11. Other

Data Dictionary

The software shall include the ability to record various data sets in files as required by the NSDD Program and other users and to transmit that data in multiple formats to multiple sets of stakeholders.

**Data Types**: The data domain includes several data types collected and stored during installation, configuration, administration, and daily operations. Data formats are not specified but shall be identified in Design Descriptions.

**Event Data**: Event data includes data from sensor devices corresponding to an alarm or fault. This includes messages from the RPM and images from cameras. This may also include data from other devices, such as RID, optical character recognition, license plate recognition, and spectroscopic portal monitor (SPM) when present.

**Disposition Data**: Disposition data is data collected during event closure, such as comments, RID files, disposition codes, and identification for the user closing the event. Disposition codes are identified in the NSDD Core Standard Disposition Codes baselined document.

**Configuration Data**: Configuration data consists of all settings and parameters that modify the behavior of the CAS software application to meet site-specific or installation requirements.

**User Data**: User data includes authentication and authorization (password) information about each user, including identification, password, and role information. Role information includes specific authorities for each role. User data may also include custom roles if present.

**Administration Data**: Administration data includes log data for system activity and successful and unsuccessful authorization attempts.

Glossary

**Alarm:** An alarm is a radiation detection event generated by an RPM or SPM during an occupancy. The three possible types of alarms are Gamma (G), Neutron (N), and Neutron+Gamma (NGPair).

**Aspect:** Brand of RPMs, RIDs, and hand-held survey meters deployed by the NSDD Program in Russia and some former Soviet Union countries.

**Central Alarm Station (CAS) System:** The CAS System provides the capabilities required to accept, process, display, and store data from fixed RPMs; provides images to support alarm and fault event resolution; and provides a CAS System Operator interface that allows the operator to effectively assess the site status and respond to alarm and fault events.

**Event:** An event in the CAS System occurs when one of the detection devices (i.e., RPMs) sends a message associated with a particular event. In addition, CAS System events can be triggered by a change in status of system components, such as a SOH change. Events can include radiation alarms, radiation faults, tamper faults generated by the RPMs, and SOH events such as camera faults or portal faults.

**Fault:** A fault is an event generated when an unusual equipment condition is detected (e.g., a tamper fault is generated if a pillar door is open; the monitor generates a Gamma high fault if background values exceed threshold and no occupancy is detected).

**Local Alarm Station (LAS):** The LAS provides a limited subset of CAS workstation functions to an operator who is physically local to the control point(s) of interest.

**Monitor:** See Radiation Portal Monitor (RPM).

**National Communications System (NCS):** A communications architecture, with software and equipment, developed by the NSDD Program for the purpose of tying all CAS’s to a regional and central alarm station, providing national oversight and allowing reach-back analysis and alarm resolution support.

**Occupancy:** The period of time during which a detection device is occupied by traffic (rail, vehicle, object, or pedestrian). The RPM detects an occupancy using an ultrasonic, radar, or a break beam sensor. During an occupancy, the RPM collects radiation data at a faster rate. The goal is for the RPM is to detect an occupancy for each individual vehicle, container, object, or rail car rather than a single occupancy for an entire line of traffic.

**Primary Inspection Site:** A primary inspection site is the location where people, vehicles, objects, or railcars pass through portals that detect nuclear and other radiological materials.

**Pillar:** A pillar is the major sub-unit of an RPM. There are Master and Slave pillars.

**Radiation Alarm:** A radiation alarm is generated when the occupant of a portal causes the level of Gamma or Neutron radiation to exceed a threshold level. There are Neutron and Gamma radiation alarm events.

**Radiation Portal Monitor (RPM):** An RPM is a fixed radiation portal monitor. It may have one or two pillars, though it generally has two. The terms “RPM,” “monitor,” and “portal” are used interchangeably. There are Pedestrian, Vehicle, Rail, and Conveyer RPMs.

**Remote Alarm Panels:** Annunciation devices connected directly to the RPM.

**Secondary Inspection Site:** Secondary inspection sites are used to detain people, vehicles, or cargo that generated an Alarm Event and to gather additional information to assess and process the Alarm Event.

**Nuclear Smuggling Detection and Deterrence (NSDD):** NSDD is a cooperative effort between the U.S. DOE/NNSA and other foreign governments to deter, detect, and investigate smuggling of nuclear and other radiological materials.

**Secondary Work Station (SWS):** The SWS provides a limited subset of CAS workstation functions to an operator who is physically located at the secondary inspection site.

**Tamper:** A tamper is a deliberate or inadvertent attempt to gain access to the monitoring equipment and is a specific message type sent by the monitor device. A tamper is a type of fault event.

**RAPISCAN RPM:** A brand of fixed radiation portal monitor, designed by RAPISCAN Systems, Ltd., and deployed by the NSDD Program at points of entry and in mobile detection systems.