# For Cause Review
# Performance Degradation of the Advanced Mixed Waste Treatment Facility Fissile Tracking System – RWC-2004-94


**William McQuiston**

**October 2004**

## INTRODUCTION

On September 1, 2004, BNFL Inc. notified the NE-ID Facility Representative of a performance degradation of a Safety Significant System – The Fissile Tracking System (FTS) at the Advanced Mixed Waste Treatment Facility (AMWTF). BNFL Inc. discovered a problem which would allow the transport of a fissile waste container with potentially invalid assay results past interlocks designed to prevent exceeding fissile mass control limits.

On September 7, 2004, NE-ID EM management requested a focused review of this event and previous software problems experienced at the Advance Mixed Waste Treatment Project to better understand the seriousness and potential vulnerabilities of these issues on safety and operations. The purpose of this review was to identify causal factors for those events, if a common cause can be identified, and root cause as appropriate.

Causal factors are defined as the events or conditions necessary and sufficient to produce or contribute to the unwanted event. A number of causal factors were identified in this review. Causal factors fall into three categories: Direct Cause, Contributing Cause and Root Cause.

The Direct cause is defined as the immediate events or conditions that caused the unwanted event. The Direct Cause of this incident was:

- The Fissile Tracking System software was not built as designed.

Root Causes are causal factors that, if corrected, would prevent recurrence of this, or similar events. Two Root Causes were identified:

- Root Cause 1: The BNFL Software Quality Assurance Program was not implemented at a level of detail to assure changes to, and deviations from design requirements were identified, understood and corrected in a controlled manner.
- Root Cause 2: Acceptance testing of the Fissile Tracking System was not written or conducted in a manner that assured all parties involved understood the basis for expected system response and acceptable performance.

Contributing Causes are those events or conditions that collectively with other causes increased the likelihood of the event but that individually did not cause the unwanted event. The Contributing Factors identified were:

- The operational readiness reviews conducted by BNFL and NE-ID were not conducted at a level of detail sufficient to assure the Fissile Tracking System software was developed, deployed and tested in a manner which assured proper response to assay data, in accordance with the design specification, and prevent facility operations in an unanalyzed condition.
- The URS, DCN-I-0082/OPSDCN-EE-0154, and OPSDCN-EE-0235 all contained diagrams depicting “assay flow.” None of the flow diagrams showed all functions required to be handled by the FTS software (calibrations container status, process container status, high FGE containers, etc.).

## BACKGROUND

The Advanced Mixed Waste Treatment Project retrieves, characterizes, treats if necessary, and ships to WIPP, TRU contaminated waste from various DOE sites that was shipped to and stored at the Radioactive Waste Management Complex (RWMC). The Advanced Mixed Waste Treatment Facility is owned and operated by BNFL Inc., under contract to the Department of Energy Idaho Operations Office (NE-ID).

The Advanced Mixed Waste Treatment Facility is a Category 2 nuclear facility, owned and operated by BNFL Inc. under contract to DOE Idaho. The Fissile Tracking System (FTS) is one of several systems that comprise the AMWTP Data Management System. The FTS is designated as a Q-Listed, Class 1, Safety Significant System. The FTS (and associated software) must function as part of the control strategy to ensure that an accidental nuclear criticality cannot occur when container contents are sorted, re-packaged, and compacted during treatment facility operations.

The automated systems used at the AMWTF to characterize, assay and control the processing flow and treatment of waste items, comprise a complex integration of computer-based data generation, storage and control systems. Overall the system is typical of a distributed control system, however, integrating specialized and one-of-a-kind processes. Of interest to this review is the Fissile Tracking System (FTS). The FTS is used to independently allow (or deny) the movement of fissile bearing containers and items into areas controlled to prevent inadvertent criticality.

Several different companies developed the software used in the AMWTF tracking and control systems. The RDAS was purchased from Canberra. The RBAS and SCWPAS were purchased from BNFL Instruments, Inc. (BII). The FTS was developed and delivered by Aeroflex Altair Cybernetics, Inc.

The WTS comprises several software modules. The key modules relevant to this review are 1) the Waste Characterization module, developed by Contemporary Technologies Inc. (CTi), 2) the Off-Site Shipping Module developed by Insei, LLC, and 3) the Facility Module, developed by Insei, LLC. Some coincidental (minor) in-house development and patches has also been done by BNFL Idaho, Inc.

The FTS interacts with other systems in the Characterization and the Treatment Facilities. Chiefly: the Retrieval Box Assay System (RBAS), Retrieval Drum Assay System (RDAS), Special Case Waste Packet Assay Monitor System (SCWPAS), two Facility Drum Assay Systems, the Integrated Control System (ICS), and its specific associated barcode readers and programmable logic controllers.

The event that initiated this review was the *"Discovery Of A Potentially Inadequate Safety Analysis Regarding The Recording Of Assay Results, ID—BNFL-AMWTF-2004-0011*." Investigation into that anomaly by BNFL revealed the software used to implement the FTS controls was not developed as designed by the vendor, Aeroflex Altar Cybernetics, Inc. A programming loop implemented by the vendor to meet a design requirement had an unintended, and unidentified, consequence, that may have allowed drums with "failed assays" to be re-

designated as “acceptable,” allowing them to pass through the Treatment Facility. The programming error was not identified by BNFL during the FTS system acceptance test. Subsequently, following discussions with NE-ID, BNFL Inc. determined the software anomaly represented an Unreviewed Safety Question on October 7, 2004 (Ref: USQ-S-04-701 and USQ-D-04-073).

The chronology of events and conditions leading to this event is listed in Attachment A.

**AMWTP Facility System Descriptions and Relationships** (See Attachment B)
**Assay Systems -**
The assay systems are commercially available units used to interrogate waste containers and identify the presence and quantity of fissile materials. The assay systems generate a Fissile Gram Equivalent (FGE) value representative of the container being assayed. Three systems are used by AMWTP. Two units, the Retrieval Drum Assay System (RDAS) and the Retrieval Box Assay System (RBAS) are located in the in the Characterization Facility. The RBAS was manufactured by BNFL Instruments Inc. (BII), and the RDAS was manufactured by Canberra Corporation. The third unit, the Special Case Waste Packet Assay System (SCWPAS), is located in the Treatment Facility, and was manufactured by BII. All three of these systems are Safety Significant Systems.

**Fissile Tracking System (FTS)**
The FTS is a Safety Significant System required for adequate criticality control in the Treatment Facility (WMF-676). The FTS is a backup to the WTS for tracking fissile gram equivalent (FGE) values of waste containers and items. The overall design of the FTS is intended to allow safe movement of fissile bearing items into controlled areas. The system provides the enable signal to conveyor motors to allow movement of an item. The FTS receives data for drums, boxes or packets directly from the assay systems in WMF-634 and WMF-676. FTS uses its own barcode readers, independent of the WTS. Interlocks and/or alarms are used to inhibit the movement of boxes or drums into five fissile material control areas: North Box line, South Box Line, Supercompactor Glovebox, Drum Waste Handling Enclosure and the Special Case Waste Glovebox. The normal state of the FTS is to “inhibit” movement of containers. A positive action (signal) is required to energize transport conveyors.

**Waste Tracking System (WTS)**
The core role of the WTS is to record and store information relating to all waste containers. The system provides a complete real-time record of information associated with each container dispatched to Waste Isolation Pilot Plant (WIPP) in Carlsbad, NM. The information held by WTS forms the lifetime history of the waste that was processed at the site, prior to transport to WIPP for long-term storage. The WTS uses its own barcode readers to identify and locate waste items. The WTS works in conjunction with the Integrated Control System (ICS) to move waste items within the Treatment Facility.

The WTS employs two software modules used to identify waste containers, store characterization and visual examination information, monitor and display container locations and facilitate preparation of documents for off-site shipments to WIPP. These software modules were developed and delivered to BNFL by two vendors. BNFL Inc. was responsible for

acceptance testing of each of the modules when delivered to assure they functioned properly and interfaced correctly with the other various modules as required by formal design requirements documents.

**AMWTP Facility Integrated Control System (ICS)**
The AMWTF ICS is used to provide control, monitoring, and intercession of AMWTF systems from one or more workstations. ICS controls plant equipment in the following plant areas:

A. 300A, Box Reduction
B. 300B, Drum Assay, Central Conveying, and Box Import
C. 400, Super Compaction
D. 600, Utilities (only partial control)
E. 700, Ventilation

Area 200, Characterization, has its own ICS, which is not addressed by the FICS AMWTP System Description, FAC-SD-26, Rev 0.

The ICS was installed by Washington Group International, Inc. (WGI). WGI was responsible to install the physical components of the ICS – limit switches, barcode readers, conveyors, etc., and turn over those systems to BNFL Inc. when completed. BNFL Inc. was responsible for acceptance testing to assure compliance with design requirements.

**Software Developers**
**Box and Drum Assay Equipment** –
All three assay units are commercial, off-the-shelf units. The box assay and the special case waste assay units were purchased from BNFL Instruments, Inc. The drum assay unit was purchased from Canberra. Each of these companies provides continuing support to BNFL Inc. in support of overall system operation and maintenance.

**WTS development –**
Contemporary Technologies, Inc., (CTi) developed and delivered the initial Retrieval Characterization module used in WTS. That software module was used to accept and store the characterization information for each container for the lifetime of the waste. In the early stages of the WTS contract with CTi, BNFL Inc. QA manager noted some issues with CTi's software quality assurance process and imposed a finding on CTi. CTi addressed this QA finding and design and coding of the WTS continued until delivery in March 2003. At this time, BNFL Inc. changed the contract arrangements with CTi from a time and material effort to a staff augmentation role within the project. CTi's staff subsequently remained on the AMWTP site until most recently when their work was completed.

Insei, LLC., developed and delivered the "Facility" and "Off-Site Shipping" modules of the WTS software. The Facility module was used to identify, monitor and display the location of waste containers in the Treatment Facility. The Off-Site Shipping module was used to facilitate the automated document preparation of waste containers for packaging and transport to WIPP.

## FACTS AND ANALYSIS

### Description of Event

On September 1, 2004, the Quality Assurance Manager for the BNFL Inc. V&V group notified NE-ID that a performance degradation was discovered in the AMWTF Fissile Tracking System (FTS) software that might allow the transport of a fissile waste container, with potentially invalid assay results, past interlocks designed to prevent exceeding fissile mass control limits. The FTS software and interlocks are designated as a "safety significant system," in the facility Documented Safety Analysis (DSA). Failure of the interlocks to prevent the entry of a waste container with invalid assay results into a controlled area could potentially lead to inadvertently exceeding nuclear material safety limits.

Investigation by BNFL Inc. revealed Aeroflex had not built the FTS software exactly as designed. Whereas the design would have required containers marked as a "failed assay" to maintain that status until administrative controls of expert assay reviews were completed, the software vendor built a loop into the software logic that could allow those results to be held in the database until two trailing calibration checks were subsequently passed. Passing of the calibration checks would then have designated those containers as "acceptable," allowing them to continue through the treatment processes. This anomaly could occur irrespective of any corrective maintenance that may have occurred on the assay systems, without regard to time span between the calibration checks, and without regard to the expert assay review process.

The immediate action taken was to put the interlocks controlled by FTS in "suspension," a safe mode of operation that inhibited movement of waste containers through the treatment process. Waste containers currently in the process were verified not to exceed fissile mass control limits and had valid assay results.

### FTS System Development

BNFL Inc. issued *Specification For Retrieval Assay Data System and AMWTF Fissile Tracking System, 16784-1* (URS) for “tender purposes” in February 2001. The URS was issued for “contract purposes” in September 2001. The URS initially identified container status results of Indeterminate, Approved and Rejected. As originally issued, the URS did not include a time limit associated with achieving a valid calibration for calibration items or valid assay for process items, in either the URS text or *Figure 5, Flow Chart for Item Processing.*

The FTS URS includes requirements to have RADS/FTS raise alarms if drum assay results in excess of 200 FGE or boxes assay in excess of 325 FGE. The Aeroflex SDD includes these limits.

Design Change Notice DCN-I-0082 was issued on January 24, 2002 to provide clarification and instructions to the FTS software for the processing of assay samples and calibration samples in FTS. This DCN included a flow diagram “ASSAY FLOW DIAGRAM” that altered the original flow diagram provided in the URS (Figure 5, Flow Chart for Item Processing). DCN-I-0082 also included the following additional FTS requirements and prerequisites in narrative format:

1. A “PASSED” calibration is required to accept results
2. Results must be received within a predefined time from a “PASSED” calibration
    a. Packet Assay results must be within 24 hours

b. Drum/Box Assay results must be within 8 hours
c. The time values shall be adjustable for each assay instrument

3. Abnormal failures will be handled through operational procedures

Block (12) of the DCN, "DESIGN REVERIFICATION REQUIRED," is marked "No."

In February 2002 Aeroflex requested clarification of alarm syntax as a result of adding the status of "FAILED" to process items (Request For Information ID01I.0243-031, *Indeterminate Container Alarm Message Syntax Clarification*, February 15, 2002). The response provided by BNFL Inc. (February 25, 2002) agreed with the approach proposed by Aeroflex for annunciating the alarm message. BNFL Inc. also included an attachment to show their understanding of how the process flow logic would be implemented. The time limits for acceptable trailing calibrations, items 2.a and 2.b in the above paragraph, were included, and if implemented as described, would not be adjustable but would be hard coded into the process logic. There was no discussion of the time limit values being adjustable. This RFI did not generate a Design Change Notice, or cause the URS to be updated.

As the chosen supplier, Aeroflex Altair Cybernetics (Aeroflex) delivered to BNFL Inc., the *RADS/FTS System Design Description* (SDD), for preliminary design review on September 28, 2001. The SDD was last updated September 19, 2002 (Version 1.4). URS Section 1.7.D.4.i, lists requirements the SDD must address regarding the Detailed Software Design Description. This review identified the following deficiencies in the Aeroflex SDD provided for this review, against the URS:

- The SDD Sections are miss-numbered so as to have two sections 3, 4, and 5 (an editorial issue).
- The SDD Section for *Detailed System Design Description* does not include a "traceability matrix" as required in the URS Section 1.7.D.4.i, to link the functional design requirements (section 1.5.2) to the actual design and provide test cases that validate the design.
- Contrary to the requirements of the URS, the SDD states "The choice of Altairis™ as the control system solution of RADS/FTS obviates the need for a detailed software design." A detailed software design description, as described in the URS was not included.
- The SDD does not reference or fully implement IEEE Std. 1016, *Software Design Descriptions* as required in URS Section 1.7.D.4.i.
- The SDD Version 1.4, issued seven months after DCN-I-0082 and RFI-031 were issued, did not include those design change requirements, specifically, the requirement for container assay results to be within specified time constraints (refer to SDD Section *Description of System Functions* "Safety Significant Common Normal Function: Manage container assay data results") to be considered valid.
- The URS states: "A Mean Time Between Failure of at least 10,000 hours is required." And, "A Mean Time to Repair (MTTR) shall be 1 hour or less." The SDD states "By specifying components from well known vendors we believe the [sic] our design will satisfy the following Mean Time Between Failure (MTBF) and Mean Time to Repair (MTTR) requirements.
    - MTBF of at least 10,000 hours
    - MTTR of one hour or less"

"Upon procurement of the specified components, comprehensive testing and analysis will be performed to verify system Reliability and Availability requirements."

The stated testing to confirm system reliability and availability was not completed as described in the SDD and BNFL did not document an alternate approach to confirm and accept the FTS reliability and availability.

The URS, DCN-I-0082/OPSDCN-EE-0154, and OPSDCN-EE-0235 all contained diagrams depicting "assay flow." None of the flow diagrams showed all functions required to be handled by the FTS software (calibrations container status, process container status, high FGE containers, etc.).

BNFL Inc. Quality Assurance did not identify and assure correction of the above noted deficiencies in the SDD prepared by Aeroflex for the software design and implementation of the FTS.

The Retrieval Assay Data System/Fissile Tracking System, System Design Description completed by Aeroflex (September 19, 2002) did not incorporate the time limits and adjustability identified in DCN-I-0082 (1-24-02) or RFI-031 (2-19-02).

Assuring compliance to the stated requirement to use IEEE Std. 1016, *Software Design Descriptions* may have aided in the early identification and correction of the SDD not addressing all requirements contained in the URS and follow-on Design Change Notices and Requests for Information.

DCN-I-0105, approved August 26, 2002, contained ten design change items which were affected or changed. Principally affected were XML file format changes for box, drum and packet assay interfaces, handheld barcode reader feedback, failover notification, vulnerabilities identified during failover, and ICS interfaces. "ITEM 10, URS DOCUMENT UPDATES," states "The FTS URS shall be updated to incorporate the requirements affected by this DCN." The URS provided for this review did not contain those changes. This reviewer asked for and did not receive a URS so updated.

BNFL Inc. did not update the URS as stated in DCN-I-0105, to maintain its configuration current, reflecting the changes brought about by Design Change Notices and Requests For Information that were implemented during the design and implementation phases prior to operation.

Following the September 4, 2004 FTS software event, OPSDCN-EE-0235 (September 7, 2004) again altered the time requirement before a process item container status could be promoted to APPROVED. In this new case, a valid trailing calibration assay must occur "within a predefined time from an initial 'PASSED' check calibration assay." This design change essentially added the requirement for the trailing calibration check to be within a specific time limit, removed the hard-coded time requirements of 8 and 24 hours for packet and drum/box assay respectively and made the time limitations adjustable by local actions.

Acceptance testing was conducted in several phases during the development, implementation and installation of the FTS. Principally, a three phase approach was used. First, a Facility Acceptance Test (FAT) was conducted at the Aeroflex facility in Bowie, MD. That test phase was completed in April 2002. The Site Acceptance Test (SAT) was conducted August 21 – 24, 2002. That test appears to be a repeat of the FAT.

The Facility Acceptance Test and the Site Acceptance Test did not confirm that assay data was processed as specified by the URS, DCN-I-0082 and RFI-031. Further, the test scenario used for "DRUMA" in FAT 3.1 was virtually the same scenario that was later identified by BNFL and reported as a degradation of a Safety Significant SSC, resulting in a positive USQ-D.

**BNFL Oversight of RADS/FTS Software Design**

BNFL Inc. conducted an evaluation of Aeroflex Altair Cybernetics (Aeroflex) on September 4, 2001, as the supplier of the FTS. The evaluation Scope stipulated "No software code development will be included within the scope of this procurement." Also, that "A QA Program meeting 10 CFR 830 requirements will not be required." No justification is provided in the evaluation as to why the requirements of 10 CFR 830 would not apply. As a result, Aeroflex was not required by BNFL Inc. to implement a Software Quality Assurance Program meeting the requirements of 10 CFR 830. BNFL Inc. stated Aeroflex was not capable of implementing such a program and took other actions, as identified in the QA Evaluation, to assure the quality of the FTS. That evaluation resulted in Aeroflex being added to the AMWTP Approved Supplier List

The evaluation included two actions to be taken by BNFL INC. to assure the FTS would meet Specification 16784-1 requirements. 1 - "A Commercial Grade Survey will be conducted to review the implementation of the vendor's application modeling/design, work control and validation methods," and 2 - "Critical Characteristics and Special Tests and Instructions identified in the Technical Specification will be required for acceptance." No deficiencies were identified in the evaluation.

BNFL Inc. QA conducted the Commercial Grade Survey of Aeroflex on November 6, 2001 (QA Surveillance Report 2001-26). Neither the Evaluation Report nor the Surveillance Report identified that IEEE Std 1016, *Recommended Practice for Software Design Descriptions*, was not referenced or used as required by Specification 16784-1. The Commercial Grade Survey conducted identified no specific criteria by which to judge acceptable performance of the Supplier (Aeroflex).

NE-ID believes the Fissile Tracking System design and implementation is subject to the requirements of a Quality Program meeting 10 CFR 830, due to the nature of its intended function.

The BNFL QA Evaluation did not assure the requisite level of justification or compensatory actions commensurate (expected) with the design and manufacture of a Q-Listed, Category 2, Nuclear Facility Safety Significant System.

BNFL Inc. stated a "Traceability Testing Matrix" was required to be supplied by Aeroflex. That matrix was to provide a one-for-one match showing how the requirements in the Specification were addressed in the FTS development and implementation. BNFL Inc. did not demonstrate a formal, independent check was conducted to assure the Critical Characteristics of the FTS were addressed in the vendor's application modeling/design. The *Inspection and Test Plan and Procedures* (FTS_VV-01_001, Version 1.3, 4-12-2002), did include *Appendix B, Requirements Verification Matrix*. That matrix addressed testing during the "Factory Acceptance Test (FAT)." However, the method in which Aeroflex constructed these tables does not allow for a one-for-one check of all requirements.

BNFL Inc. initiated *an FTS System Component Verification and Compliance Matrix* in August 2004. This document attempts to identify requirements from the URS and identify where/how the requirements are satisfied in the final FTS system implementation. In some cases the matrix does not identify where/how a requirement was satisfied because alternate approaches were used. For example, the barcode readers were to use an RS-485 interface. Because the actual implementation used an RS-232, twisted pair connection, no verification was completed. This matrix is not a formal document under configuration control.

The URS was written in narrative fashion and included no table or other organized matrix that identified processing requirements in a detailed fashion. This manner of documentation makes it difficult to assure each requirement in the URS has been addressed in the development of the FTS software and hardware. It is not possible to back track from the Requirements Verification Matrix to the URS, or trace forward from the URS to the final product, requirement for requirement. The less than rigorous approach in establishing a detailed system design description resulted in a failure to detail the specific steps required in the container "promotion" process. This approach did not assure a one-for-one matrix with all requirements was constructed to assure all requirements were implemented as intended and tested to assure functionality.

Testing of the FTS was conducted in three phases. A Factory Acceptance Test (FAT) was conducted at the Aeroflex facility in Bowie, MD. Site Acceptance Testing was conducted at the AMWTF after installation of the major components. Since some portions of the facility were not operational, some of the testing intended to occur as part of the SAT was deferred to a later time. Specifically, those were the regression testing Sections 4.2 and 5.2. Testing of those functions was carried out during the Commissioning Phase of the facility readiness under procedure CP-SO-F27 on March 11, 2004.

A detailed review was conducted of the April 16, 2002 FAT test 3.1, *Assay Interface System Verification and Data Processing*. An analysis of the assay data processing sequences is shown in Attachment C. This analysis resulted in the following observations:

- The sequence of events used in the "DRUMA" scenario in this test is a virtual representation of the anomaly identified by BNFL on September 1, 2004 and reported on ID—BNFL-AMWTF-2004-0020. That event was later determined to be an Unreviewed Safety Question. The processing steps in the test scenario allowed containers marked as FAILED (and should have remained so based on the processing criteria) to be changed to

INDETERMINATE and subsequently to APPROVED, following two trailing PASSED calibration assays.

BNFL did not recognize the incorrect response as a deviation from the criteria specified in DCN-I-0082 when the test was conducted and accepted the test as proof of proper operation.

- The test includes "Requirements Addressed" as part of the documentation. However, the list as written does not correlate the steps of the test to specific requirements.
- Although the listed requirements do not include the time limits for valid processing (< 8 hours for drum and box assay and < 24 hours for packet assay) as identified in DCN-I-0082 and OPSDCN-EE-0150 and RFI-031, Test 3.1 did check these functions successfully in Step 7. BNFL Systems Engineer was not aware this function was tested successfully as part of this test.
- Test 3.1 did not check the following processing paths identified in DCN-I-0082:
    - "The time values shall be adjustable for each assay instrument."
    - For both normal processing, "the cycle will repeat using the "PASSED" calibration (4) in step E as the starting point. The processing loop will continue."
    - For both normal processing and failure processing – "The system must receive a "PASSED" calibration sample prior to enable [sic] normal assay samples to be collected (2)." No sample collections were attempted after a FAILED calibration instrument status on BOXC and DRUMC after calibration failures.
    - The test scenario of a FAILED trailing calibration followed by a second FAILED trailing calibration was not tested.
- Step 14 of the test did not use the test file specified for this step (SEQ 7). Instead, the testers used the file from sequence 6 (SEQ 6), Step 13 again. This had the effect of using two PASSED trailing calibrations with the same time stamp to change the status the containers to INDETERMINATE (Step 13) and then to APPROVED (Step 14). This also invalidated the ability to check that the calibration pass time was recorded correctly in Step 14, as it should have changed from Step 13. The performers of test noted the substitution on the test form and accepted the results. There is no indication in the test file that BNFL QA agreed with the use of the substitute files for SEQ 7 testing.
- In the data file provided for this review, the Calibration Containers data decimal precision varies from one to two places for the same container FGE high limit and FGE Low limit in the data string. The consequence of this change is not known. BNFL stated, however, the present FTS design does not use this value in any calculations.
- The algorithm used to check for valid barcodes was not shown. While barcodes of single character length were not processed in the test, recent problems have occurred in which non-numeric characters were passed to the FTS that caused the system to halt.
- In Step 7, the Expected Results stated in part "Open all the files and verify all files except BOXC and DRUMC have PASSED calibration." The actual state for BOXC and DRUMC was not specified nor verified. The reason for not passing is not specified in the test. (BOXC should have failed on high FGE, DRUMC should have failed on low FGE. These values were neither checked nor verified in the test procedure.)

An analysis of the assay data processing sequences is shown in Attachment C.

BNFL Inc. needs to conduct a comprehensive review of the requirements identified in Specification 16784-1 and associated Document Change Notices and Requests for Information to assure that all requirements have been included in the FTS software design as intended and tested for satisfactory performance. This review should include developing a requirements verification matrix as a formal, controlled document.

The FTS System Description (FAC-SD-35, Rev 0) Section 4.1.1 discusses the major components of the FTS. In the introductory paragraph, the statement is made "The WTS and FTS are separate and independent, thereby helping to satisfy the requirements for double contingency per DOE O 420.1." Because the data used by both WTS and FTS is commonly generated (data is received from the same assays systems) this redundancy approach is not in keeping with the intent of DOE O420.1, and therefore credit cannot be given for double contingency as discussed in this context.

## DOE AND CONTRACTOR OVERSIGHT AND ASSESSMENT OF TREATMENT FACILITY READINESS

BNFL initiated its Contractor Operational Readiness Review (CORR) on April 15, 2004. After three days, of review, the General Manager withdrew his assessment of readiness due to problems encountered with the Facility Ventilation System and other hardware and operational issues. The CORR was again initiated on June 16, 2004 and conducted through June 24, 2004. None of the 22 Findings from the CORR identified any issues with the Software Quality Assurance Program or other issues related to the Data Management Systems in general.

The Idaho Operations Office (NE-ID) conducted a Line Management Assessment (LMA) of the AMWTF June 16-23, 2004. The LMA was conducted using Criteria and Review Approach Documents (CRADS), including Software Quality Assurance (SQA). The LMA identified two Post-Start Findings and two Observations relative to this review: RWC-2004-35.1, Lack of Complete Software Inventory (Post-Start Finding), and RWC-2004-35.49, Requirements Traceability Matrix Not Controlled (Observation), RWC-2004-35.50, FTS Alarm Condition (Observation), and RWC-2004-35.51, FTS Response to Key Press Post-Operational Test Not Performed (Post-Start Finding).

NE-ID conducted an Operational Readiness Review (ORR) of the AMWTF in August 2004. The DOE ORR included CRADS for Safety Envelope Verifications (SE) and Software Quality Assurance (SQA) programs. Those CRADS contained criteria relevant to the control of Safety Significant Systems, such as FTS, and the development, implementation and maintenance of software. The SE review resulted in one Post-Start Finding relative to computer messages generated by the drum assay system not conforming to the DSA/TSR requirement (SE.1.2). The SQA review resulted in no issues being identified.

The NE-ID LMA and ORR reviewed many of the same documents as this review. However, because of the way in which the LMAs and ORRs were intended to function, the review process focused more generally at ensuring software quality assurance program procedures were

established to control design, development and change of software systems. Those reviews were more of a "horizontal slice" of how the program was established and functioned, using known issues to test the program implementation.

In contrast, none of the FTS-related reviews for readiness for operations conducted a "vertical slice" type of assessment. Such an assessment would have followed the FTS system development from concept, through design, assembly, construction and testing, to assure the SQA programmatic controls (software quality assurance programs) put into place actually functioned as intended to assure a quality and reliable product.

During the development and implementation of the FTS, no NE-ID oversight activities were conducted specific to the progress of the design, building and testing of the FTS. The lack of early involvement by NE-ID with the FTS provided a lost opportunity for NE-ID to fully understand the FTS design, design changes, implementation and testing. Early involvement by NE-ID may have aided in identification of unsatisfactory performance of the FTS.

The operational readiness reviews conducted by BNFL and NE-ID were not conducted at a level of detail sufficient to assure the Fissile Tracking System software was developed, deployed and tested in a manner to assure proper response to assay data in accordance with the design specification and did not result in entering an unanalyzed condition.

The lack of early involvement by NE-ID with the FTS provided a lost opportunity for NE-ID to fully understand the FTS design, design changes, implementation and testing.

**CAUSAL ANALYSIS**

Causal factors are defined as the events or conditions necessary and sufficient to produce or contribute to the unwanted event. A number of causal factors were identified in this review and are shown in Attachment D. These causal factors are used in conjunction with the Events and Causal Factors Charting (Attachment E) to determine the Direct Cause, Contributing Causes and Root Causes.

The Direct cause is defined as the immediate events or conditions that caused the unwanted event. The Direct Cause of this incident was:

The Fissile Tracking System software was not built as designed.

Root Causes are causal factors that, if corrected, would prevent recurrence of this, or similar events. Two Root Causes were identified:

- Root Cause 1: The BNFL Software Quality Assurance Program was not implemented at a level of detail to assure changes to, and deviations from design requirements were identified, understood and corrected in a controlled manner.
- Root Cause 2: Acceptance testing of the Fissile Tracking System was not written or conducted in a manner that assured all parties involved understood the basis for expected system response and acceptable performance.

Contributing Causes are those events or conditions that collectively with other causes increased the likelihood of the event but that individually did not cause the unwanted event. The Contributing Factors identified were:

- The URS, DCN-I-0082/OPSDCN-EE-0154, and OPSDCN-EE-0235 all contained diagrams depicting "assay flow." None of the flow diagrams showed all functions required to be handled by the FTS software (calibrations container status, process container status, high FGE containers, etc.).
- The operational readiness reviews conducted by BNFL and NE-ID were not conducted at a level of detail sufficient to assure the Fissile Tracking System software was developed, deployed and tested in a manner which assured proper response to assay data, in accordance with the design specification, and prevent facility operations in an unanalyzed condition.
- The lack of early involvement by NE-ID with the FTS provided a lost opportunity for NE-ID to fully understand the FTS design, design changes, implementation and testing.

**Documents Reviewed**

1. FACT SHEET - Performance Degradation of Safety Significant System SSC at the AMWTP, Julie Finup, 09-01-2004
2. Fissile Tracking System, AMWTF System Description, FAC-SD-35, 3-29-2004
3. Facility Integrated Control System, AMWTF System Description, FAC-SD-26, 3-18-2004
4. OPS Design Change Notice EE-0235, FMP-193, 9-7-04
5. NCR 9832, Fissile Tracking System Incorrectly Promoting Calibration Status Based, 8-31-2004
6. NCR 3444, System Design Deficiencies, 9-3-2003
7. Facility Modification Proposal 182, WTS, ICS, FTS Facility Merge with 634 Characterization, SCR 532, completed 8/12/2004
8. AI No. 4754, Integration of the Characterization data with the Treatment Fac [sic] is incomplete, 4-14-2004
9. Facility Modification Proposal 167, Permanent Connection of WMF 676 to WMF 634 Production Networks, completed 8/12/2004
10. Documented Safety Analysis, Section 2.5, Process Description
11. Specification 16784-1, RADS and AMWTF FTS, 9/18/2001
12. Design Change Notice DCN-I-0082, 01-24-2002
13. Design Change Notice DCN-I-0105, 08-27-2002
14. Retrieval Assay Data System/Fissile Tracking System, System Design Description, Aeroflex Altair Cybernetics Corporation, FTS_TD-02_002, Version 1.4, 9/19/2002
15. RADS/FTS Operations and Maintenance Manual, Version 2.2, FTS_UD-08_001, 3/18/2003
16. FTS System Component Verification And Compliance Matrix (informal document)
17. Inspection and Test Plan and Procedures, FTS_VV-01_001, Version 1.3, 4/12/2002
18. Request For Information (RFI) ID01I.0243-031, Approved 2-26-02
19. Factory Acceptance Test 3.1 XML Data Files produced from the "TestGen" tool. Test files generated on 9/21/2004.

20. BNFL Quality Program Evaluation Report: Aeroflex Altair Cybernetics/Fissile Tracking System, 9/14/2001.
21. BNFL Quality Program Surveillance Report, 2001-26, 11/6/2001.
22. Advanced Mixed Waste Treatment Facility DOE Operational Readiness Review, September 2004
23. Treatment Facility Commissioning System Operability Testing Results Report, BNFL-5232-CTRR-02-Rev 1, July 2004
24. Line Management Assessment AMWTP Treatment Facility, 9/21/2004 (OIMS RWC-2004-35)
25. BNFL letter, A. J. Dobson to M. L. Adams, Submittal of the Evaluation of the Safety of the Situation (ESS) corresponding to RPS-ID-BNFL-AMWTF-2004-0020 (AJD-201-2004, dated September 15, 2004)
26. Contract No. DE-AC07-97ID13481, Advanced Mix Waste Treatment Facility Project (AMWTP), Review of Evaluation of the Safety of the Situation (ESS) and Unreviewed Safety Question Determination (USQD) for the Fissile Tracking System (EM-AMWTP-04-165), dated September 28, 2004
27. Contract No. DE-AC07-97ID13481, Advanced Mix Waste Treatment Facility Project (AMWTP), Submittal of the Revised Evaluation of the Safety of the Situation corresponding to ORPS-ID-BNFL-AMWTF-2004-0020 – AJD-218-2004, dated October 5, 2004
28. BNFL Corrective Action Report 8125, FTS Alarm Condition
29. BNFL Corrective Action Report 8126, FTS Response to Key Press
30. NTS-ID—BNFL-AMWTF-2003-0002, Software Issues Affecting Pre delivery testing of the BNFL Inc. Retrieval Box Assay
31. ID—BNFL-AMWTF-2003-0001, WTS programming error allowed high FGE drum to move, May 2003
32. ID—BNFL-AMWTF-2004-0011, Bar code reader reporting incorrect drum number, April 2004
33. Fact Sheet - Barcode reader passed non-numeric character (not reportable), September 2004
34. Fact Sheet - Non-reportable: Bar code reader passed an alpha character ($) causing the FTS to halt processing, September 2, 2004

**Personnel Contacted**

- Julie Finup, NE-ID
- Ivan Thomas, BNFL
- Ian Milgate, BNFL
- Daren Brock, BNFL
- Phil Atkinson, BNFL
- Brian Anderson, NE-ID
- Tony LaRosa, BNFL
- Elvin Dumas, BNFL
- Kay Emanuelson, BNFL
- Steve Somers, NE-ID
- Jaqualine Carrozza, NE-ID

- Robert Blyth, NE-ID
- Steve Westenzweig, BNFL
- Bryan Swinson, BNFL

# ATTACHMENT A
## Chronology of Events

| Date/Time | Events | Conditions |
|---|---|---|
| 02/28/2001 | URS 16784-1 issued for "tender" purposes | |
| 09/14/2001 | BNFL Quality Program conducts evaluation of Aeroflex | • FTS is a "Q-listed system.<br>• "A QA program meeting 10 CFR 830 requirements will not be required."<br>• Aeroflex added to Approved Supplier List as "Commercial Grade Software" product supplier.<br>• Critical Characteristics and Special Tests and Instructions in the Tech Specs will be required for acceptance. |
| 09/18/2001 | Specification 16784-1 approved for contract purposes. | • Approval follows QA evaluation of Aeroflex<br>• Includes requirement to use IEEE 1016.89, Software Design Description, as a guide to developing the Detailed Software Design Description. |
| 10/19/2001 | RADS/FTS SDD, Revision A issued by Aeroflex | |
| 11/06/2001 | BNFL conducts Surveillance of Aeroflex (Surveillance No. 2001-26) | • No specific acceptance criteria established or defined<br>• Specification 16784-1 requires IEEE 1016.89, Software Design Description. No rational was provided to justify equivalency of IEEE 730 XXXXX…. |
| 11/2001 | Software Issues Affecting Pre delivery testing of the BNFL Inc. Retrieval Box Assay (Reported in NTS-ID—BNFL-AMWTF-2003-0002, 10-21-2003) | • A physics algorithm in the RBAS software was not producing expecting results.<br>• The algorithm, used to determine fissile content, was replaced with a software patch to allow testing other functions of the RBAS<br>• The RBAS was released for delivery and installation without the correct software |
| 1/24/2002 | Design Change Notice DCN-I-0082 issued against URS 16784-1 | • Time limits established for valid calibration results on process containers<br>• Time limit values were to be adjustable |
| 2/28/2002 | RFI ID01I.0243-031 from Aeroflex is approved by BNFL. Subject: Indeterminate Container Message Syntax Clarification. | • Change was required due to added container status value of "FAIL."<br>• BNFL attachments of resolution includes time limit for containers to "PASS" following calibration run and requirement for the time limits to be adjustable |
| 4/16/2002 | Factory Acceptance Test 3.1, Assay Interface System Verification and Data Processing, was conducted. | • Assay data was processed beyond "Procedural Review Required."<br>• Test Objective: Verify proper receipt and processing of assay data records<br>• Test must be accomplished within three hours of generating test files<br>• 8-hour and 24-hour time limits were tested, and not understood by BNFL<br>• No comprehensive check of DCN and RFI requirements can be demonstrated<br>• |

# ATTACHMENT A
## Chronology of Events

| Date/Time | Events | Conditions |
|---|---|---|
| 8/27/2002 | DCN-I-0105 issued against URS 16874-1 | • XML file format and other changes identified.<br>• Logic for establishing valid calibration changed<br>• "The logic for using calibration item within FTS/RADS shall remain as described in the URS and DCN-I-0082." |
| 9/19/2002 | RADS/FTS SDD Revision 1.4, issued by Aeroflex | • "Updated system architecture to as builts."<br>• SDD did not incorporate requirements of DCN-I-0082 or RFI-031.<br>• Detailed Software Design Description as described in IEEE 1016, was not included in SDD |
| 5/14/03 | High Fissile Content Drum Released by Control system after Assay<br><br>ID—BNFL-AMWTF-2003-0001 | • Cause determined to be "incorrect programming of the WTS software."<br>• Incorrect "trigger" level (380 FGE) was written into the software.<br>• Actual assay value used for comparison against trigger level rather than actual value +2 sigma. |
| 6/9/2003 | RADS Time limit change for WMF-634 requested, SCR 846-002 | • "Change batch time limit in RADS from 8 hours to 24 hours to coincide with requirement for daily calibration checks on Assay systems."<br>• Change requested to improve production schedule<br>• Time limits still not "adjustable" as required in DCN-I-0082, 1-24-2002 |
| 9/3/2003 | NCR 3444 Opened to correct software problems identified through an unplanned observation. | • RADS/FTS contains data that is indicated with a status of PASS, when the results are technically indeterminate pending ETR activity<br>• RADS/FTS contains data that has been reworked in WTS, however, date has not been performed to the parallel data in RADS/FTS<br>• Waste containers can be moved out of or within WMF-634 with assay data that has changed within WTS without an update to RADS/FTS. This issue will become a Safety Significant issue if not corrected prior to Operations activities in the Treatment Facility<br>• Although WTS should identify and prohibit container movements that fall outside of Criticality Working Requirements, RADS/FTS is designed to be a secondary system and does not currently have the functionality to perform as such |
| 12/15/2003 | 846-SCR002, written to change batch time limits, was "placed into production for testing." | • Treatment Facility not yet "Operational" |
| 3/11/2004 | Commissioning Test CP-SO-F27, AMWTF Treatment Facility Fissile Tracking System (846) Area Operability Test is conducted | • |

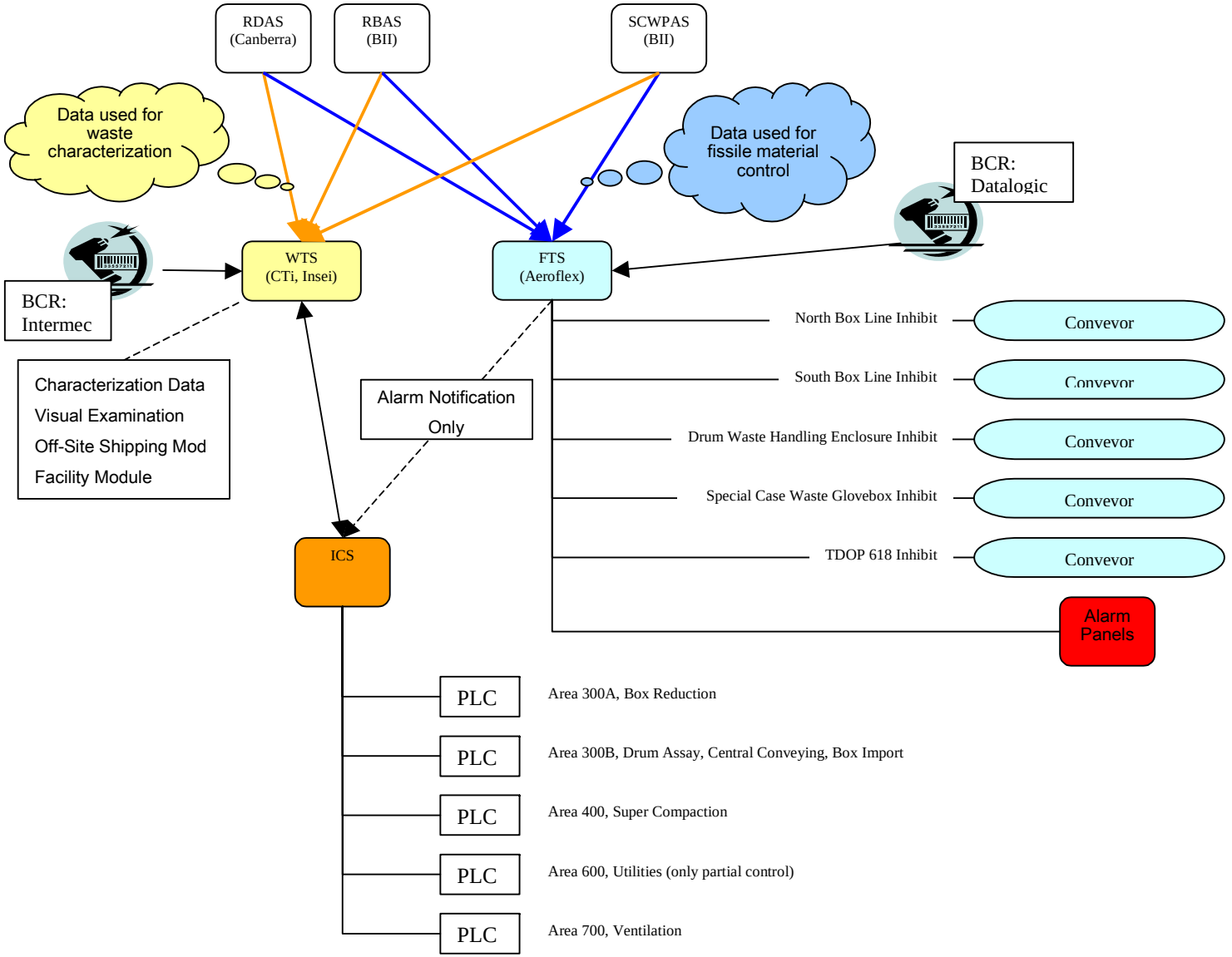
# ATTACHMENT A
## Chronology of Events

| Date/Time | Events | Conditions |
|---|---|---|
| 4/14/2004 | AMWTP Action Item 4754 – Integration of the Characterization DMS data with the Treatment Facility is incomplete | • Integration of data is in coordination with NCR-3444<br>• Requires "Modify the software associated with Box Assay, Drum Assay, and Fissile Tracking Systems such that any box or drum that requires an expert review remains at the "indeterminate" state until the expert review has been completed and the appropriate state is changed to "accept" or "reject."<br>• Generated FMMP-167, |
| 4/14/2004 | OPSDCN-EE-0154 issued against URS 16784-1 for, "Clarification for the processing of Assay samples and Calibration samples in FTS (Fissile Tracking System)" | • This was a "re-issue" of DCN-I-0082<br>• This DCN included a facsimile of DCN-I-0082 and a new flow chart "Assay Flow Diagram" not included in DCN-I-0082 |
| 4/15-18/2004 | BNFL conducts Management Self Assessment for Treatment Facility | • Assessment of Readiness withdrawn by General Manager |
| 4/24/2004 Reported 4-26-04 | Discovery of a Potentially Inadequate Safety Analysis Regarding the Recording of Assay Results [Barcode reader malfunction] ID—BNFL-AMWTF-2004-0011 | • Drum assay barcode reader misread a drum barcode<br>• Incorrect barcode passed to WTS and FTS<br>• Software fault may have allowed data in FTS to be over-written with FGE data of a lower value |
| 6/16-23/2004 | NE-ID conducts Line Management Assessment for Facility Startup | • Issue RWC-2004-35.1, Lack of Complete Software Inventory (Post-Start Finding)<br>• Issue RWC-2004-35.49, Requirements Traceability Matrix Not Controlled (Observation). |
| 6/2004 | BNFL initiates Management Self Assessment for Facility Readiness | |
| 6/24/2004 | BNFL conducts contractor ORR | • Report BNFL-5232-RPT-OPS-022, issued 6-24-2004. |
| 8/2/2004 | DOE conducts ORR for Facility Startup | • Software Quality Assurance CRAD results in no issues. |
| 8/9/2004 | BNFL ordered software modification from Canberra for RDAS | • BNFL developed JAVA code as an interim measure<br>• Eleven month delay since deficiency was noted on NCR 3444. |
| 8/9/2004 | BNFL ordered software modification from BII for RBAS | • BNFL developed JAVA code as an interim measure<br>• Eleven month delay since deficiency was noted in NCR 3444. |
| 8/11-12/2004 | BNFL installs JAVA code "patches" for RDAS and RBAS | • Change needed to address "Operations_Code=0" field change |
| 8/17/2004 | Treatment Facility becomes "Operational." | • |
| 8/31/2004 | NCR 9832 opened. Fissile Tracking System incorrectly Promotes Calibration Status | • FTS allows successful trailing Q/C check container results of a subsequent batch to promote containers in a previous batch<br>• Root cause code of "Software Design or Other." |

# ATTACHMENT A
## Chronology of Events

| Date/Time | Events | Conditions |
|---|---|---|
| 9/1/04, 1230 | Potentially Inadequate Safety Analysis results from Software Implementation Anomaly<br>ID—BNFL-AMWTF-2004-0020<br><br>[EVENT UNDER REVIEW] | • Software might allow transport of a fissile waste container past interlocks<br>• Software was not built exactly as designed |
| 9/2/2004, 1800 | NE-ID informed of problem with FTS Server #1. Barcode reader failure (non-reportable) | • Barcode reader misread a digit "9" transmitting an alpha character "$" causing the Unix server to halt, awaiting a variable.<br>• Drum reads 0.64 FGE<br>• FTS Server #1 alarmed "Overspec and reject at char drum storage."<br>• FTS Server #1 has no flag to prevent alarm. |
| 9/7/2004 | OPSDCN EE-0235 (and FMP-193) issued to correct PISA. | • Requirement for 8-hour/24-hour limits was removed. (Time limits may now be set to > 24 hours – contrary to TSR Surveillance Requirements)<br>• Trailing calibration check is now included in time limits for valid calibration checks.<br>• Calibration Status for containers exceeding the time limit is set to "REJECTED."<br>• FAILED trailing calibrations now causes status of FAILED. Subsequent PASSED calibration will not promote status of containers. |
| 9/14/2004 | 846-SCR002 - Parameters for valid calibration period for drum, box and packet were found set at 48, 24 and 24 hours respectively. | • Parameters set to 24 hours and tested under TC-FMP-193.<br>• FTS Version was 2.5.0.5.<br>• Previous data to be evaluated under NCR 9832.<br>• NCR 9832 evaluates the impacts on FTS Version 2.5.0.2. |
| 9/24/2004 | Inattention to Detail Causes Management Concern<br>ID—BNFL-AMWTF-2004-0022 | A series of events in the past seven months created concern on senior management's part that the required attention to detail may be lacking at many levels of the organization most notably within the Operations and Waste program departments. |

# ATTACHMENT B
# AMWTF Data Management System (control systems only)



# ATTACHMENT C
## NE-ID Analysis of the Factory Acceptance Test 3.1 Assay Data Processing Sequences

### FAT TEST PLAN 3 - SYSTEM PERFORMANCE UPON RECEIPT OF ASSAY DATA

| | | Box Assay | | | Drum Assay | | | Packet Assay | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sequence | | BoxA | BoxB | BoxC | DrumA | DrumB | DrumC | PacketA | PacketB | PacketC |
| SEQ1 | | | | | | | | | | |
| | Item | 99999991 | 99999992 | 99999997 | 99999993 | 99999994 | 99999998 | 99999995 | 99999996 | 99999999 |
| | Date/Time | 9-21/08:40:00 | 9-21:01:24:59 | 9-21/06:40:00 | 9-21/8:40:00 | 9-21/01:24:59 | 9-21/06:40:00 | 9-21/08:40:00 | 9-20/09:24:59 | 9-21/06:40:00 |
| | Condition | | | **FGE>FGE Limit** | | | **FGE<FGE Limt** | | | |
| | Results | CAL PASSED | CAL PASSED | **CAL FAILED** | PASSED | PASSED | **CAL FAILED** | CAL PASSED | CAL PASSED | CAL PASSED |
| NOTE: | Files 66666661, 66666662 and 66666663 were copied into the system and the files were not processed presummably based upon not having a valid barcode. | | | | | | | | | |
| SEQ2 | | | | | | | | | | |
| | Item | 10000001 | 20000001 | | 10000002 | 20000002 | | 10000011 | 20000005 | |
| | Date/Time | 9-21/09:25:00 | 9-21/09:25:00 | | 9-21/09:25:00 | 9-21/09:25:00 | 9-21/09:25:00 | 9-21/09:25:00 | 9-21/09:25:00 | |
| | Condition | **FGE>FGE limit** | FGE>FGE LIMIT, >8 HOURS | | **FGE>FGE LIMIT** | **FGE>FGE LIMIT, >8 HOURS** | | | **>24 HOURS** | |
| | Results | **REJECTED** | **REJECTED** | | **REJECTED** | **REJECTED** | | APPROVED | **NO RECORD UPDATE** | |
| | Item | 10000003, 10000004, 10000005, 10000006 | 20000003 | | 10000007, 10000008, 10000009, 10000010 | 20000004 | | | | |
| | Date/Time | 9-21/09:25:00 | 9-21/09:25:00 | | 9-21/09:25:00 | 9-21/09:25:00 | | | | |
| | Condition | | **> 8 HOURS** | | | **>8 HOURS** | | | | |
| | Results | INDETERMINATE | **NO RECORD UPDATE** | | INDETERMINATE | **NO RECORD UPDATE** | | | | |
| SEQ3 | | | | | | | | | | |
| | Item | 99999991 | | | 99999993 | | | | | |
| | Date/Time | 9-21/09:55:01 | | | 9-21/09:55:01 | | | | | |
| | Condition | CAL CHECK | | | FGE>200 | | | | | |
| | Results | CAL PASSED | | | **CAL FAILED** | | | | | |
| | Item | 10000003, 10000004, 10000005, 10000006 | | | 10000007, 10000008, 10000009, 10000010 | | | | | |
| | Results | APPROVED | | | FAILED | | | | | |
| SEQ4 | | | | | | | | | | |
| | Item | | | | 999999993 | | | | | |
| | Date/Time | | | | 9-21/10:10:01 | | | | | |
| | Condition | | | | | | | | | |
| | Results | | | | CAL PASSED | | | | | |
| | Item | | | | 10000007, 10000008, 10000009, 10000010 | | | | | |
| | Results | | | | INDETERMINATE | | | | | |

# ATTACHMENT C
## NE-ID Analysis of the Factory Acceptance Test 3.1 Assay Data Processing Sequences

### FAT TEST PLAN 3 - SYSTEM PERFORMANCE UPON RECEIPT OF ASSAY DATA

| | Box Assay | | | Drum Assay | | | Packet Assay | | |
|---|---|---|---|---|---|---|---|---|---|
| Sequence | BoxA | BoxB | BoxC | DrumA | DrumB | DrumC | PacketA | PacketB | PacketC |
| SEQ5 | | | | | | | | | |
| Item | | | | 99999993 | | | | | |
| Date/Time | | | | 9-21/10:16:01 | | | | | |
| Condition | | | | **FGE<FGE LIMIT** | | | | | |
| Results | | | | **CAL FAILED** | | | | | |
| Item | | | | 10000007, 10000008, 10000009, 10000010 | | | | | |
| Results | | | | FAILED | | | | | |
| | | PROCEDURAL REVIEW OF ASSAY DATA REQUIRED PER ASSAY FLOW DIAGRAM | | | | | | | |
| | | | Containers should not be updated past this point. | | | | | | |
| SEQ6 | | | | | | | | | |
| Item | | | | 99999993 | | | | | |
| Date/Time | | | | 9-21/10:22:01 | | | | | |
| Condition | | | | | | | | | |
| Results | | | | CAL PASSED | | | | | |
| Item | | | | 10000007, 10000008, 10000009, 10000010 | | | | | |
| Results | | | | INDETERMINATE | | | | | |
| SEQ7 | | | | | | | | | |
| Item | | | | 99999993 | | | | | |
| Date/Time | | | | 9-21/10:28:01 | | | | | |
| Condition | | | | **SEQ6 files used in lieu of SEQ7 files** | | | | | |
| Results | | | | CAL PASSED | | | | | |
| Item | | | | 10000007, 10000008, 10000009, 10000010 | | | | | |
| Results | | | | APPROVED | | | | | |
| | | | | **END** | | | | | |

# ATTACHMENT D
# Causal Analysis

Causal factors are defined as the events or conditions necessary and sufficient to produce or contribute to the unwanted event. Causal factors fall into three categories: Direct Cause, Contributing Cause and Root Cause.

The Direct cause is defined as the immediate events or conditions that caused the unwanted event. The Direct Cause of this incident was:

| |
|---|
| The Fissile Tracking System software was not built as designed. |

Root Causes are causal factors that, if corrected, would prevent recurrence of this, or similar events. Two Root Causes were identified and are shown in the table below.

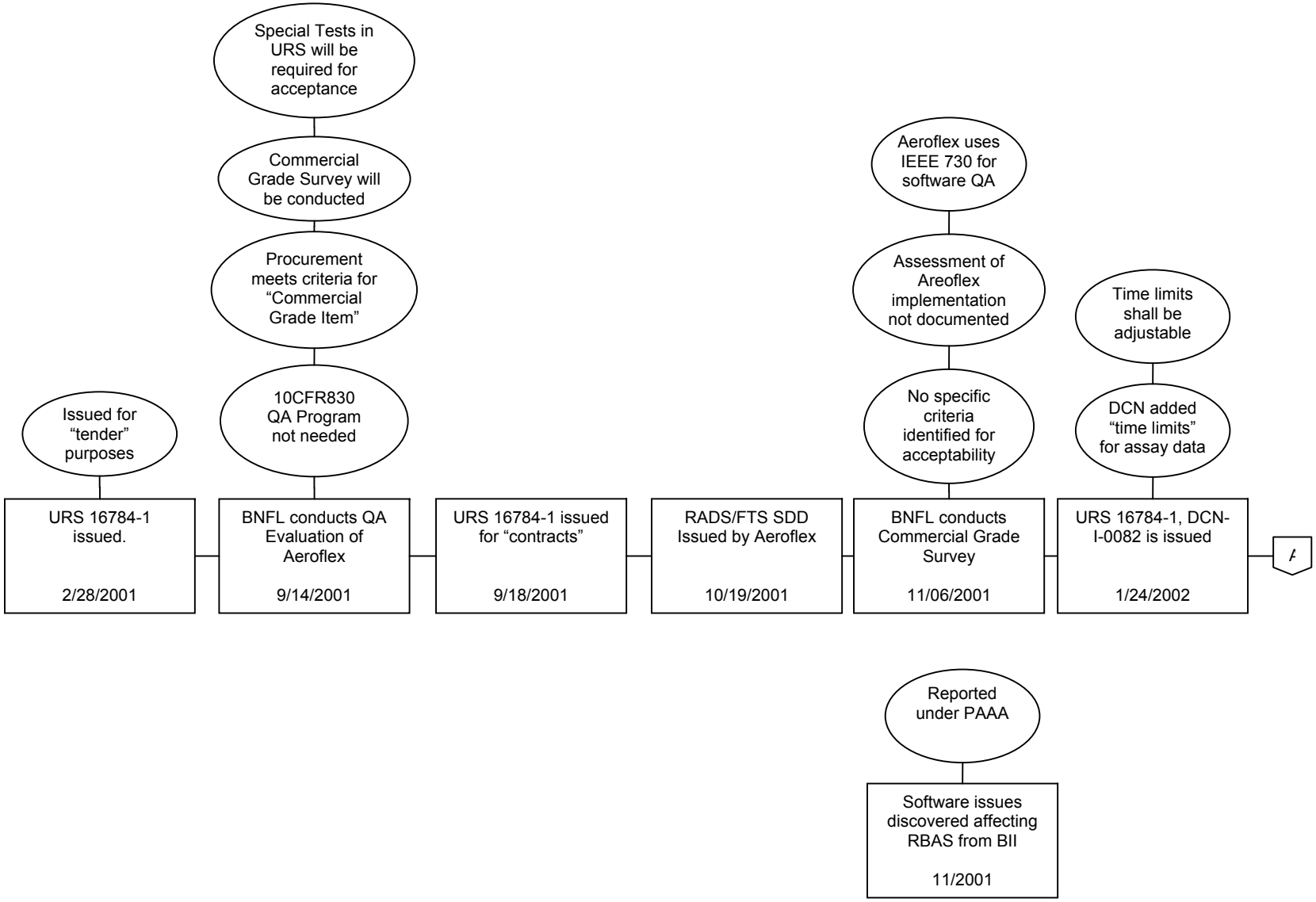
| Root Causes | Causal Factors |
|---|---|
| Root Cause 1: The BNFL Software Quality Assurance Program was not implemented at a level of detail to assure changes to, and deviations from design requirements were identified, understood and corrected in a controlled manner. | • NE-ID believes the Fissile Tracking System design and implementation is subject to the requirements of a Quality Program meeting 10 CFR 830, due to the nature of its intended function.<br>• The BNFL QA Evaluation did not assure the requisite level of justification or compensatory actions commensurate (expected) with the design and manufacture of a Q-Listed, Category 2, Nuclear Facility Safety Significant System.<br>• The Retrieval Assay Data System/Fissile Tracking System, System Design Description completed by Aeroflex (September 19, 2002) did not incorporate the time limits and adjustability identified in DCN-I-0082 (1-24-02) or RFI-031 (2-19-02).<br>• BNFL Inc. Quality Assurance did not identify and assure correction of deficiencies in the SDD prepared by Aeroflex for the software design and implementation of the FTS.<br>• BNFL Inc. did not update the URS as stated in DCN-I-0105, to maintain its configuration current, reflecting the changes brought about by Design Change Notices and Requests For Information that were implemented during the design and implementation phases prior to operation.<br>• The stated testing to confirm system reliability and availability was not completed as described in the SDD and BNFL did not document an alternate approach to confirm and accept the |

| Root Causes | Causal Factors |
|---|---|
| | FTS reliability and availability.<br>• Assuring compliance to the stated requirement to use IEEE Std. 1016, *Software Design Descriptions* may have aided in the early identification and correction of the SDD not addressing all requirements contained in the URS and follow-on Design Change Notices and Requests for Information. |
| Root Cause 2: Acceptance testing of the Fissile Tracking System was not written or conducted in a manner that assured all parties involved understood the basis for expected system response and acceptable performance. | • BNFL did not recognize the incorrect response as a deviation from the criteria specified in DCN-I-0082 when the test was conducted and accepted the test as proof of proper operation.<br>• The Facility Acceptance Test and the Site Acceptance Test did not confirm that assay data was processed as specified by the URS, DCN-I-0082 and RFI-031. Further, the test scenario used for "DRUMA" in FAT 3.1 was virtually the same scenario that was later identified by BNFL and reported as a degradation of a Safety Significant SSC, resulting in a positive USQ-D. |

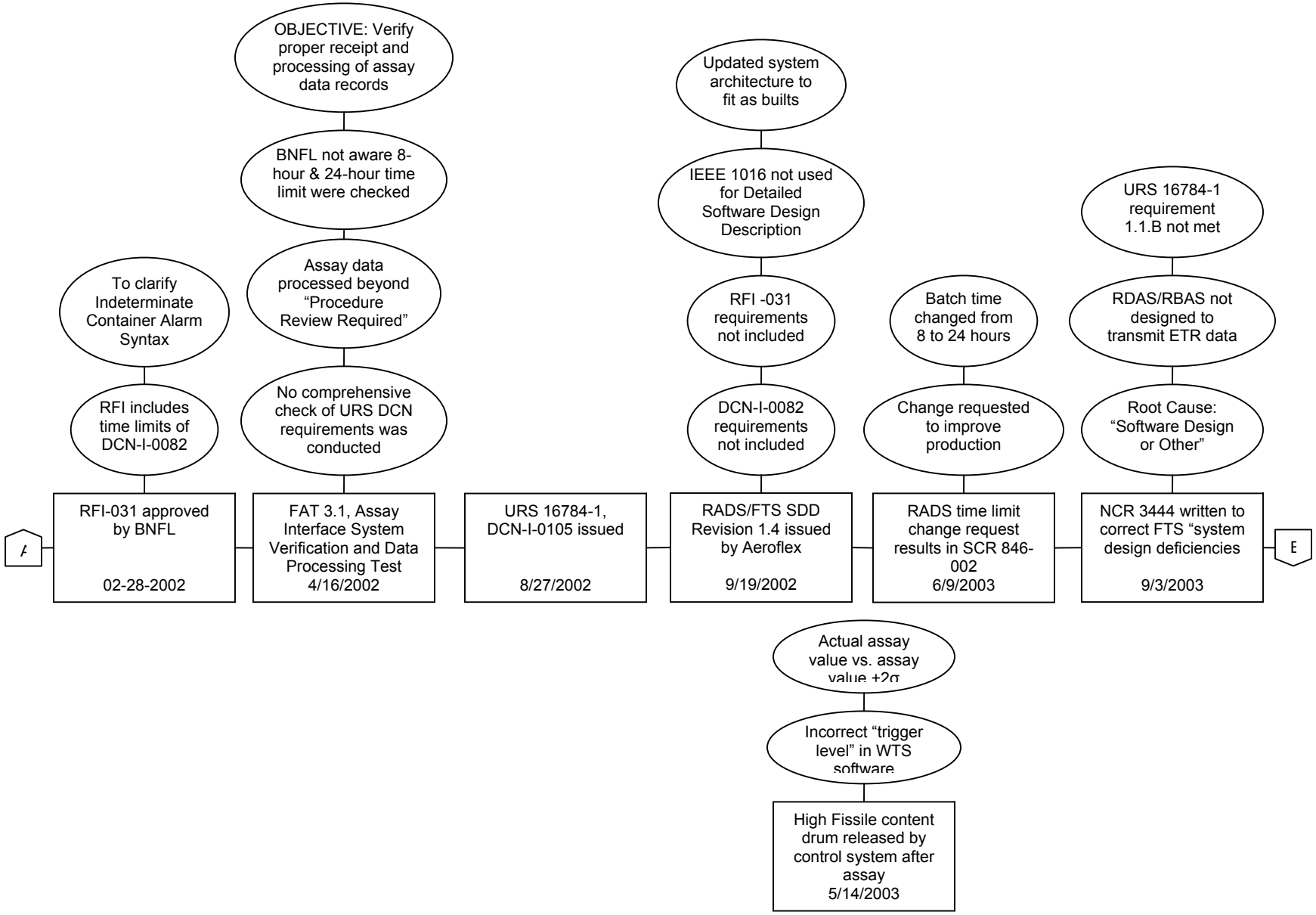
Contributing Causes are those events or conditions that collectively with other causes increased the likelihood of the event but that individually did not cause the unwanted event.

| Contributing Causes |
|---|
| • The URS, DCN-I-0082/OPSDCN-EE-0154, and OPSDCN-EE-0235 all contained diagrams depicting "assay flow." None of the flow diagrams showed all functions required to be handled by the FTS software (calibrations container status, process container status, high FGE containers, etc.).<br>• The operational readiness reviews conducted by BNFL and NE-ID were not conducted at a level of detail sufficient to assure the Fissile Tracking System software was developed, deployed and tested in a manner to assure proper response to assay data in accordance with the design specification and did not prevent facility operations in an unanalyzed condition.<br>• The lack of early involvement by NE-ID with the FTS provided a lost opportunity for NE-ID to fully understand the FTS design, design changes, implementation and testing. |

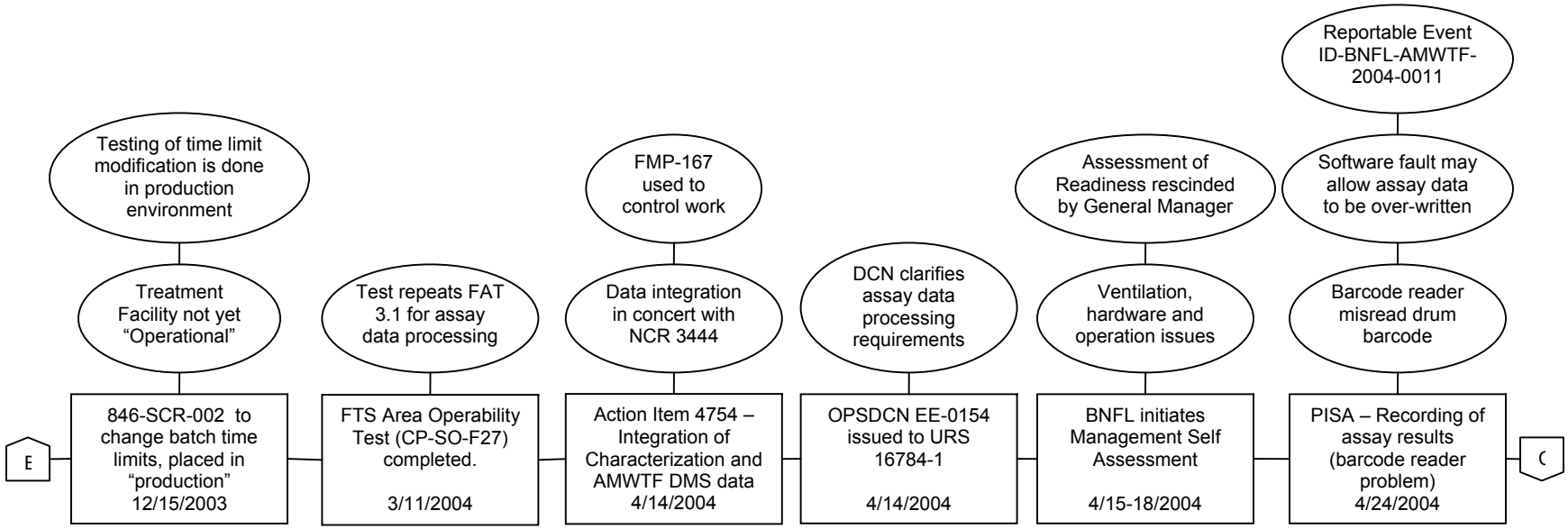
**Attachment E**
**Events and Causal Factors Chart**
**AMWTF RADS/FTS Software Development and Implementation**



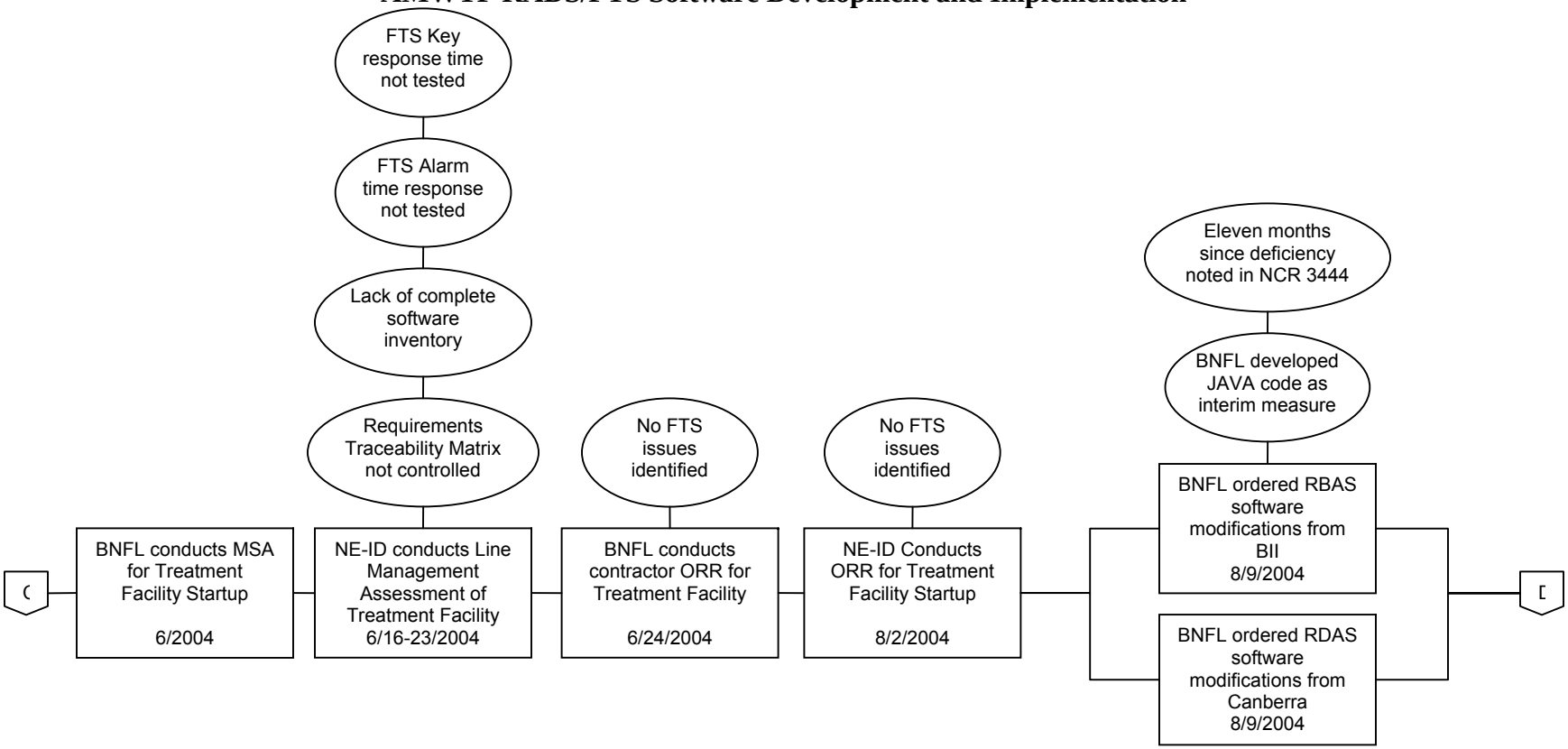
**Attachment E**
**Events and Causal Factors Chart**
**AMWTF RADS/FTS Software Development and Implementation**



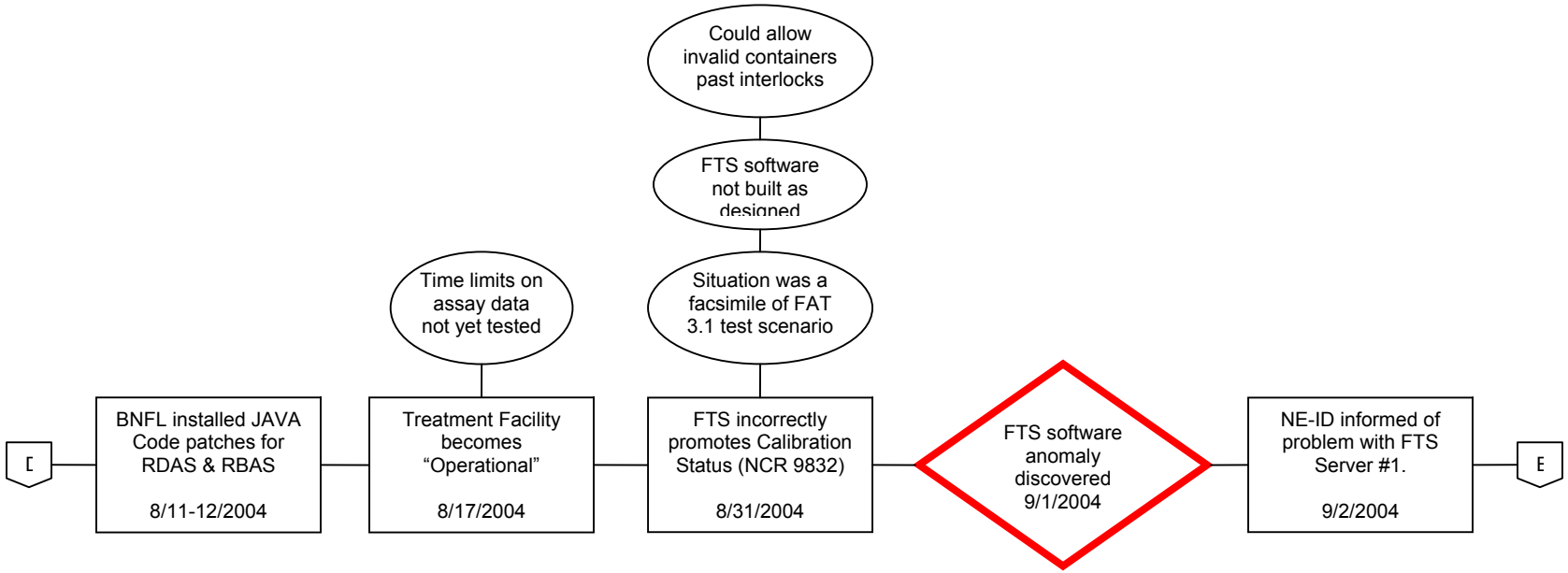
**Attachment E**
**Events and Causal Factors Chart**
**AMWTF RADS/FTS Software Development and Implementation**



**Attachment E**
**Events and Causal Factors Chart**
**AMWTF RADS/FTS Software Development and Implementation**



**Attachment E**
**Events and Causal Factors Chart**
**AMWTF RADS/FTS Software Development and Implementation**



**Attachment E**
**Events and Causal Factors Chart**
**AMWTF RADS/FTS Software Development and Implementation**