4) Functional / SAFETY Goals of INTEROPERABLE ITEM stated as INTEROPERABLE ITEM SSEPOS; and

5) INTEROPERABLE ITEM-level Context/INTEROPERABLE ITEM Interactions (Use Cases).

b) RISK MANAGEMENT File (updated from initial versions created in Management Processes)

1) Notions of hazardous control actions and data relevant to this Item; and

2) Preliminary definitions of EXTERNAL MEASURES made by the item and mitigations performed by the component to avoid hazardous control actions and data.

E1.2 Development of item requirements and external interoperability specifications

E1.2.1 Specification of item boundary

E1.2.1.1 A specification of the boundary for the INTEROPERABLE ITEM shall be developed following the guidelines of Annex O. The boundary shall be specified at a level of detail sufficient for supporting all item-level RISK MANAGEMENT and ASSURANCE activities.

E1.2.1.2 The INTEROPERABLE ITEM BOUNDARY specification shall document any variabilities in the INTEROPERABLE ITEM BOUNDARY due to variations in CONSTITUENT INTEROPERABLE ITEMS that are able to be used in the INTEROPERABLE ITEM.

E1.2.1.3 The compliance of the specified INTEROPERABLE ITEM BOUNDARY to the REFERENCE ARCHITECTURES in all INTEROPERABLE ITEM-aligned INTEROPERABILITY FRAMEWORKS shall be documented and appropriate traceability established.

E1.2.2 Development of INTEROPERABLE ITEM requirements

E1.2.2.1 The requirements for the INTEROPERABLE ITEM shall be developed with traceability to the INTEROPERABLE ITEM SSEPOS, the Item-level Context/System Interactions, and the INTEROPERABLE ITEM BOUNDARY Specification.

E1.2.2.2 The INTEROPERABLE ITEM requirements shall be specified in accordance with the INTEROPERABLE ITEM'S Use Specification. The guidance in Annex M relevant to the INTEROPERABLE ITEM SSEPOS should be considered.

E1.2.2.3 The INTEROPERABLE ITEM requirements should consider the technical and functional SAFETY guidance in Annex P relevant to the INTEROPERABLE ITEM SSEPOS.

E1.2.2.4 The INTEROPERABLE ITEM requirements shall include any requirements from aligned INTEROPERABILITY FRAMEWORKS that are necessary for the appropriate use of INTEROPERABILITY FRAMEWORK assets, SAFETY/SECURITY controls, and ASSURANCE arguments and evidence.

E1.2.2.5 The INTEROPERABLE ITEM requirements specification shall account for any variabilities in the INTEROPERABLE ITEM due to variations in CONSTITUENT INTEROPERABLE ITEMS that may be used in the INTEROPERABLE ITEM realization.

E1.2.2.6 The INTEROPERABLE ITEM requirements shall clearly indicate the assumptions about the INTEROPERABLE ITEM'S usage and externally realized controls that are necessary for the INTEROPERABLE ITEM implementation to satisfy its requirements.

E1.2.3 INTEROPERABLE ITEM level analysis and RISK MANAGEMENT activities

E1.2.3.1 Data/Control flow analysis

E1.2.3.1.1 A data/control flow analysis that documents the expected flows of data and control signals from the INTEROPERABLE ITEM'S inputs to outputs shall be performed.

E1.2.3.1.2 The analysis results shall document data/control flows that originate within the INTEROPERABLE ITEM as INTEROPERABLE ITEM-source information flows and shall indicate the interfaces in the INTEROPERABLE ITEM Architecture Specification through which the information flows across the INTEROPERABLE ITEM BOUNDARY to entities external to the INTEROPERABLE ITEM.

E1.2.3.1.3 The analysis results shall document data/control flows that terminate within the INTEROPERABLE ITEM as INTEROPERABLE ITEM-sinked information and shall indicate interfaces in the Item Architecture Specification through which the information flows across the INTEROPERABLE ITEM BOUNDARY from external entities into the INTEROPERABLE ITEM.

E1.2.3.1.4 The analysis results shall document data/control flows through the INTEROPERABLE ITEM in terms of the input and output interfaces in the INTEROPERABLE ITEM Architecture Specification through which the information flows across the INTEROPERABLE ITEM BOUNDARY from and to external entities. The flows shall be presented in a manner that captures the dependence relationships between item outputs and inputs.

E1.2.3.1.5 For each flow, the following information shall be provided:

a) The types of data associated with the flow as reflected in the INTEROPERABLE ITEM'S INFORMATION VIEW Data Dictionary.

b) An indication of the INTEROPERABLE ITEM modes in which the flows may be active or controlled to be inactive.

c) Changes in the INTEROPERABLE ITEM'S modes and states associated with the flow that are necessary for reasoning about the INTEROPERABLE ITEM'S medical function or technical SAFETY.

d) Traceability information linking the flow to INTEROPERABLE ITEM-Context Interactions that exercise the flow.

e) Anticipated entities in the INTEROPERABLE ITEM'S context that may provide data or control information that may be the source or sink of data/control information associated with the flow.

f) Traceability to operations on and transformations of data within the component as captured in the INTEROPERABLE ITEM'S INFORMATION VIEW.

g) Indications of when the INTEROPERABLE ITEM serves as a conduit for information but its function is not affected by the content of the information.

E1.2.3.2 Fault and ERROR propagation analysis and specification

E1.2.3.2.1 An enumeration of the different categories of faults and ERRORS considered in item-level hazard analysis shall be specified in a Fault/Error Categorization. The Fault/Error Categorization shall consider the common fault/error types related to INTEROPERABLE MEDICAL SYSTEMS provided in Annex I. Each fault/error type shall be accompanied by:

a) Nomenclature for uniquely identifying the fault/error type,

b) A human readable semantic interpretation of the fault/error type, and

c) Example descriptions of situations in which the fault/error type may arise and potential methods for generating the fault as part of fault injection testing.

E1.2.3.2.2 The INTEROPERABLE ITEM Fault/Error Categorization shall be aligned with Fault/Error Categorizations provided by INTEROPERABLE ITEM-aligned INTEROPERABILITY FRAMEWORKS.

E1.2.3.2.3 For each INTERFACE operation in the INTEROPERABLE ITEM'S Architecture Specification, the possible inwardly propagating ERRORS that have been considered in the INTEROPERABLE ITEM'S analysis shall be specified and disclosed as part of the INTEROPERABLE ITEM'S ERROR PROPAGATION SPECIFICATION. The ERROR PROPAGATION SPECIFICATION shall state the expected likelihood of inwardly propagating ERRORS. Arguments addressing the completeness and appropriateness of the specification as related to the INTEROPERABLE ITEM'S use specification shall be provided as part of the INTEROPERABLE ITEM'S RELEASE CRITERIA.

E1.2.3.2.4 The inwardly propagating ERRORS and associated likelihoods captured in the INTEROPERABLE ITEM'S ERROR PROPAGATION SPECIFICATION shall address interoperability and system context related ERRORS specified in the ERROR PROPAGATION SPECIFICATION of any INTEROPERABLE ITEM-aligned INTEROPERABILITY FRAMEWORKS.

E1.2.3.2.5 The failure modes of the INTEROPERABLE ITEM shall be specified, including the following causality-related information:

a) Inwardly propagating data, control, or ERRORS that may cause the INTEROPERABLE ITEM to transition into a failure mode;

b) Faults within the component that may cause the INTEROPERABLE ITEM to transition into a failure mode; and

c) For each failure mode, ERRORS that may propagate out of the INTEROPERABLE ITEM through its INTERFACES and associated likelihoods shall be specified.

E1.2.3.2.6 Fault mitigation and recovery mechanisms associated with mitigating inwardly propagation ERRORS and recovering from failure modes shall be specified.

E1.2.3.3 Control loop analysis

E1.2.3.3.1 The control loop analysis results of E1.1.6.3 shall be refined to address the detailed INTEROPERABLE ITEM INTEROPERABILITY ARCHITECTURE and INTERFACES. The specific interfaces, operations, and data associated with each point at which a path in the control loop crosses the INTEROPERABLE ITEM BOUNDARY shall be specified.

E1.2.3.3.2 For each control loop, the system theoretic notions of sensing, actuating, controlling, and controlled process shall be allocated to the INTEROPERABLE ITEM or to entities in the context of the INTEROPERABLE ITEM. In situations where a notion is allocated to an external entity, one or more representative entities shall be described as appropriate for achieving coverage of the INTEROPERABLE ITEM'S Use Specification.

E1.2.3.3.3 The allocation of system theoretic notions shall be mapped to the generic control loop analysis provided by INTEROPERABLE ITEM-aligned INTEROPERABILITY FRAMEWORKS.

E1.2.3.3.4 An analysis shall be performed to determine the potential impacts of the ERROR behavior of the INTEROPERABLE ITEM (as reflected in its disclosed Error Specification) on the ability of the INTEROPERABLE ITEM or its context to SAFETY/SECURITY objectives related to the control goals of each control loop. In situations where the item itself is performing a direct actuation on the environment entities or is providing information through OPERATOR interfaces that will be used to make care-giving situations, the HAZARDOUS SITUATIONS that the actuation (or information display) is able to generate shall be documented.

E1.2.3.4 RISK CONTROL and FUNCTIONAL SAFETY CONCEPT design

E1.2.3.4.1 A FUNCTIONAL SAFETY CONCEPT shall be specified to indicate controls necessary to achieve the INTEROPERABLE ITEM SSEPOS. For each functional SAFETY objective, the specification shall indicate how the

following FUNCTIONAL SAFETY CONCEPT dimensions are allocated to the INTEROPERABLE ITEM or entities anticipated to be present in its operational context:

a) Sensing – gathering information about a phenomena of within the item or its context that may lead to a HAZARDOUS SITUATION;

b) Detecting/Analyzing – processing the information collected by sensory dimension of the FUNCTIONAL SAFETY CONCEPT for the purpose of detecting a problematic state (or history of states) within the item or its context that could lead to a HAZARDOUS SITUATION;

c) Determining Response – Determine the actions to be taken to respond to a reported problematic state for the purpose of realizing a control; and

d) Response – implementing the actions to be taken to effect a control for a HAZARDOUS SITUATION. Common notions of response include logging the occurrence of the problematic state, notifying an OPERATOR or INTEROPERABLE ITEM in the INTEROPERABLE ITEM'S context, moving the INTEROPERABLE ITEM to a safe state, and actuating entities in the environment to avoid or reduce harm associated with the HAZARDOUS SITUATION.

E1.2.3.4.2 The FUNCTIONAL SAFETY CONCEPT and the allocation of dimensions within the concept shall be aligned with REFERENCE ARCHITECTURE FUNCTIONAL SAFETY CONCEPT for any INTEROPERABLE ITEM-aligned INTEROPERABILITY FRAMEWORKS.

E1.2.3.4.3 The responsibilities of the INTEROPERABLE ITEM for the INTEROPERABLE ITEM-allocated FUNCTIONAL SAFETY CONCEPT dimensions shall be reflected in the INTEROPERABLE ITEM'S requirements.

E1.2.3.4.4 The assumptions that INTEROPERABLE ITEM makes concerning FUNCTIONAL SAFETY CONCEPT dimensions allocated to entities in its context shall be reflected in the INTEROPERABLE ITEM'S disclosed labelling and instructions for use.

E1.2.4 Development of RELEASE CRITERIA plan

E1.2.4.1 The RELEASE CRITERIA used to confirm that the INTEROPERABLE ITEM realization meets its ITEM SPECIFICATION shall be planned and detailed in the RELEASE CRITERIA Plan taking into consideration the guidance in Annex F.

E1.2.4.2 The RELEASE CRITERIA Plan for the INTEROPERABLE ITEM shall be aligned with those provided by all aligned INTEROPERABILITY FRAMEWORKS.

E1.2.4.3 The RELEASE CRITERIA Plan shall indicate how the responsibilities for generating ASSURANCE evidence are assigned to development and operating stakeholders and how plans for generating required evidence are accounted for in the INTEROPERABLE ITEM VERIFICATION Plan, INTEROPERABLE ITEM VALIDATION Plan, and Deployment Plan / Operating Instructions.

E1.2.5 Initiation of INTEROPERABLE ITEM VERIFICATION plan

E1.2.5.1 An INTEROPERABLE ITEM VERIFICATION Plan shall be initiated to support that construction of evidence demonstrating that the INTEROPERABLE ITEM realization meets its ITEM INTEROPERABILITY SPECIFICATION according to the RELEASE CRITERIA.

E1.2.5.2 For each INTEROPERABLE ITEM behavioral requirement, the INTEROPERABLE ITEM VERIFICATION Plan shall indicate appropriate Conformance Points for observing the conformance of the INTEROPERABLE ITEM realization to the requirement selected from among the Reference Points declared in the COMPUTATIONAL VIEW of the Item.

E1.2.5.3 The INTEROPERABLE ITEM VERIFICATION Plan shall be aligned with INTEROPERABLE ITEM testing requirements provided by all aligned INTEROPERABILITY FRAMEWORKS.

E1.2.5.4 The INTEROPERABLE ITEM VERIFICATION Plan should consider the requirements of Annex G.

E1.2.6 Initiation of item VALIDATION plan

E1.2.6.1 An INTEROPERABLE ITEM VALIDATION Plan shall be initiated to support that construction of evidence demonstrating that an INTEROPERABLE ITEM realization fulfills the expectations of each INTEROPERABLE ITEM-IDENTIFIED user in the DEVELOPMENT CONTEXT OF USE and the DEPLOYMENT CONTEXT OF USE.

E1.2.6.2 The INTEROPERABLE ITEM VALIDATION Plan shall include objectives and plans for demonstrating that the INTEROPERABLE ITEM performs as expected and can be configured and used as expected in the context of all aligned INTEROPERABILITY FRAMEWORKS. The plan shall include arguments that appropriate coverage is achieved of different framework compliant contexts that may exercise the item in different ways and expose different SAFETY issues.

E1.2.6.3 The INTEROPERABLE ITEM VALIDATION Plan shall include objectives and plans for demonstrating that the INTEROPERABLE ITEM performs as expected and can be configured and used as expected in the context of care-giving scenarios within the scope of the item's Use Specification. The plan shall include arguments that appropriate coverage is achieved of different care-giving scenarios that may exercise the item in different ways and expose different SAFETY issues.

E1.2.7 Initiation of INTEROPERABLE ITEM operating procedures, labeling, and DISCLOSURES

E1.2.7.1 A plan for documenting the INTEROPERABLE ITEM'S statement of EXTERNAL MEASURES and other assumptions about its context in the form of operating procedures, labeling, and DISCLOSURES shall be initiated. For each EXTERNAL MEASURE, the provided documentation shall include:

a) The entities in the INTEROPERABLE ITEM'S context constrained by the EXTERNAL MEASURE;

b) The points in the life-cycle of the INTEROPERABLE ITEM when the EXTERNAL MEASURE is achieved; and

c) Entities responsible for ensuring that the EXTERNAL MEASURE is adhered to.

E1.2.7.2 The plan shall be aligned with associated the Operating Procedures, Labeling, and Disclosure plan of all aligned INTEROPERABILITY FRAMEWORKS.

E1.2.7.3 The plan shall account for all assumptions needed to support the INTEROPERABLE ITEM ASSURANCE and shall be aligned with the INTEROPERABLE ITEM RELEASE CRITERIA Plan.

E1.2.7.4 The plan shall account for all assumptions concerning allocation of the INTEROPERABLE ITEM FUNCTIONAL SAFETY CONCEPT.

E1.2.7.5 The plan shall account for all assumptions reflected in the INTEROPERABLE ITEM INTERFACE CONTRACTS in the INTEROPERABLE ITEM INTEROPERABILITY ARCHITECTURE.

E1.2.7.6 The plan shall document the potential impacts on SAFETY and SECURITY if the EXTERNAL MEASURES are not adhered to.

E1.2.8 Work products

E1.2.8.1 The activities in the preceding sections shall lead to the following work products:

a) ITEM INTEROPERABILITY SPECIFICATION (updated):

1) INTEROPERABILITY ARCHITECTURE (extended with detailed architecture description of item boundary);

2) INTEROPERABLE ITEM Requirements.

b) INTEROPERABLE ITEM RELEASE CRITERIA Case Plan;

c) INTEROPERABLE ITEM VERIFICATION Plan;

d) INTEROPERABLE ITEM VALIDATION Plan;

e) Operating Procedures, Labeling, Disclosures (initiated);

f) RISK MANAGEMENT File (updated):

1) Data Flow Analysis (updated to reflect the detailed interface description);

2) Control Loop Analysis (updated to reflect the detailed interface description);

3) Specification of Error Propagations in terms of interfaces;

4) INTEROPERABLE ITEM FUNCTIONAL SAFETY CONCEPT.

E1.3 INTEROPERABLE ITEM realization

E1.3.1 Requirements for implementing interoperability related functionality

E1.3.1.1 Alignment of implementation with architectural and INTERFACE SPECIFICATIONS

E1.3.1.1.1 The relation between (a) conformance points IDENTIFIED in the INTEROPERABLE ITEM VERIFICATION Plan and (b) features in the hardware, software, and associated interface implementations where testing can make observations about the INTEROPERABLE ITEM'S behavior shall be specified.

E1.3.1.1.2 It shall be demonstrated that each implementation-manifested conformance points are adequate for achieving the testing observations necessary for supporting the INTEROPERABLE ITEM VERIFICATION Plan.

E1.3.1.1.3 The implementation shall be assessed to determine that there is no other means to interact with and influence the state of the object relative to interoperability and functional SAFETY than through the interfaces declared in the INTEROPERABILITY ARCHITECTURE.

E1.3.1.1.4 For each optional mechanism of interacting with the component and for all variability mechanisms associated with the component, the implementation shall provide a means of disabling or controlling access to the component through those mechanisms that can be applied during the integration and use of the INTEROPERABLE ITEM to prevent UNAUTHORIZED and unplanned for access to the INTEROPERABLE ITEM.

E1.3.2 Implementation of INTEROPERABLE ITEM without internal interoperability

E1.3.2.1 General

E1.3.2.1.1 The requirements in this section shall apply to an INTEROPERABLE ITEM realization that has no internal interoperability in its INTEROPERABILITY ARCHITECTURE.

E1.3.2.2 Realization of the SAFETY concept

E1.3.2.2.1 An Internal Architecture description of the INTEROPERABLE ITEM shall be developed that documents the ORGANIZATION and INTERACTION between the interoperability function of the item and its medical and SAFETY functions. Traceability shall be established between the implementation artifacts and Internal Architecture Description.

E1.3.2.2.2 The allocation of the FUNCTIONAL SAFETY CONCEPT for the INTEROPERABLE ITEM RISK CONTROLS shall be allocated to the INTEROPERABLE ITEM realization to achieve the TECHNICAL SAFETY CONCEPT, and shall be documented in terms of the Internal Architecture Description of the INTEROPERABLE ITEM.

E1.3.2.2.3 The allocation of the FUNCTIONAL SAFETY CONCEPT to the TECHNICAL SAFETY CONCEPT shall be aligned with that of any aligned INTEROPERABILITY FRAMEWORKS.

E1.3.2.3 RISK MANAGEMENT activities

E1.3.2.3.1 The faults in the Fault/Error Categorization in E1.2.3.2 shall be mapped to specific behaviors (associated to the implementation) distinguishable via testing. The construction of the fault categorization shall be refined as necessary to reflect the effects of the failure modes of the implementation. The completeness of the Fault/Error Categorization with respect to implementation behaviors shall be assessed.

E1.3.2.3.2 The expansion of the Fault/Error Categorization to specific implementation oriented behaviors shall be aligned the Fault/Error implementation behaviors of the reusable implementation assets drawn from item-declared INTEROPERABILITY FRAMEWORKS.

E1.3.2.3.3 The INTEROPERABLE ITEM'S ERROR PROPAGATION SPECIFICATION shall be extended to include a mapping of the incoming and outgoing ERRORS documented in the Item's ERROR PROPAGATION SPECIFICATION shall be mapped to specific behaviors (associated to the implementation) distinguishable via testing. The Item VERIFICATION Plan and associated testing infrastructure supporting Fault Injection Testing shall be enhanced to generate inputs associated with incoming ERRORS and provide detection mechanisms for outgoing ERRORS.

E1.3.2.3.4 A bottom-up hazard analysis shall be performed to determine the effects of inward propagating ERRORS or internal failures. The analysis shall evaluate the EFFECTIVENESS of risk controls captured by the TECHNICAL SAFETY CONCEPT.

E1.3.2.3.5 The bottom-up hazard analysis shall address all relevant inward propagating ERRORS and ERRORS propagating from underlying infrastructure resources associated with all item-declared INTEROPERABILITY FRAMEWORKS.

E1.3.2.3.6 The VERIFICATION Plan shall be updated with tests designed to confirm the EFFECTIVENESS of the TECHNICAL SAFETY CONCEPT.

E1.3.3 Implementation of INTEROPERABLE ITEM with internal interoperability

E1.3.3.1 The requirements in this section shall apply to an INTEROPERABLE ITEM realization that has CONSTITUENT INTEROPERABLE ITEMS in its INTEROPERABILITY ARCHITECTURE.

E1.3.3.2 The implementation of the INTEROPERABLE ITEM in terms of CONSTITUENT INTEROPERABLE ITEMS and their integration shall be achieved following the life-cycle activities in Section E2, Item Integration Life-Cycle Activities.

E1.3.4 Work products

E1.3.4.1 The activities in the preceding sections shall lead to the following work products.

a) INTEROPERABLE ITEM Realization;

b) INTEROPERABLE ITEM Realization to Architecture Specification Mapping;

c) INTEROPERABLE ITEM Security Vulnerabilities Report;

d) INTEROPERABLE ITEM Bill of Materials;

e) RISK MANAGEMENT File (updated):

1) TECHNICAL SAFETY CONCEPT;

2) INTEROPERABLE ITEM Error Categorization (updated to reflect interpretation of fault / error types in terms of implementation);

3) INTEROPERABLE ITEM ERROR PROPAGATION SPECIFICATION (updated to reflect interpretation of ERROR propagation in terms of implementation); and

4) Data Flow and Control Loop Analysis (updated as above).

E1.4 INTEROPERABLE ITEM ASSURANCE

E1.4.1 INTEROPERABLE ITEM VERIFICATION

E1.4.1.1 The INTEROPERABLE ITEM VERIFICATION Plan shall be followed to produce OBJECTIVE EVIDENCE and test results documented in the INTEROPERABLE ITEM VERIFICATION Report that demonstrates that the INTEROPERABLE ITEM conforms to its ITEM INTEROPERABILITY SPECIFICATION.

E1.4.1.2 Testing infrastructure and results shall be AVAILABLE to support compliance.

E1.4.1.3 Discrepancies between testing results and expected results indicated in the INTEROPERABLE ITEM VERIFICATION Plan shall be documented. Corrective actions taken shall be documented, and the impact of failing tests on the Item's Specification, SAFETY Concept, and RISK MANAGEMENT shall be documented, with these activities being iterated as necessary.

E1.4.1.4 Testing infrastructure and results shall be included in DISCLOSURES as necessary to support integration of the INTEROPERABLE ITEM.

E1.4.2 INTEROPERABLE ITEM VALIDATION

E1.4.2.1 The INTEROPERABLE ITEM VALIDATION Plan shall be followed to produce OBJECTIVE EVIDENCE and test results documented in the INTEROPERABLE ITEM VALIDATION Report that demonstrates that the INTEROPERABLE ITEM is suitable for use in DEVELOPMENT CONTEXT OF USE and DEPLOYMENT CONTEXT OF USE.

E1.4.2.2 VALIDATION infrastructure and results shall be AVAILABLE to support compliance.

E1.4.2.3 Failure to achieve VALIDATION objectives shall be documented. Corrective actions taken shall be documented, and the impact of failing tests on the Item's Specification, SAFETY Concept, and RISK MANAGEMENT shall be documented.

E1.4.2.4 VALIDATION results infrastructure and results shall be included in DISCLOSURES as necessary to support integration of the INTEROPERABLE ITEM.

E1.4.3 INTEROPERABLE ITEM Release Criteria Substantiation

E1.4.3.1 Evidence and traceability information substantiating that the RELEASE CRITERIA for the INTEROPERABLE ITEM has been achieved shall be completed according to the RELEASE CRITERIA Plan.

E1.4.3.2 The RELEASE CRITERIA and all associated evidence shall be AVAILABLE to demonstrate compliance.

E1.4.3.3 The portions of the RELEASE CRITERIA necessary to support assurance of the INTEROPERABLE ITEM in its DEVELOPMENT OF CONTEXT OF USE and DEPLOYMENT CONTEXT OF USE shall be included in the INTEROPERABLE ITEM'S DISCLOSURES.

E1.4.4 Work products

E1.4.4.1 The activities in the preceding sections shall lead to the following work products:

a) INTEROPERABLE ITEM VERIFICATION Report;

b) INTEROPERABLE ITEM VALIDATION Report;

c) RISK MANAGEMENT FILE (extended);

d) INTEROPERABLE ITEM RELEASE CRITERIA Report; and

e) INTEROPERABLE ITEM DISCLOSURES.

E2 INTEROPERABLE ITEM Integration Life-Cycle Activities

E2.1 Architecture and INTEROPERABLE ITEM integration concept development

E2.1.1 ITEM INTEROPERABILITY ARCHITECTURE and domain asset instantiation

E2.1.1.1 The INTEROPERABLE ITEM Boundary Definition shall be extended to document the preliminary ITEM INTEROPERABILITY ARCHITECTURE (including both external and internal interoperability) of the INTEROPERABLE ITEM following the guidance in Section in conformance with O1, Interoperability View Point Guidance.

E2.1.1.2 The preliminary INTEROPERABILITY ARCHITECTURE shall be demonstrated to properly instantiate the REFERENCE ARCHITECTURE of the INTEROPERABLE ITEM'S declared aligned INTEROPERABILITY FRAMEWORK (S) (following the base instantiation guidance specified in Annex O).

E2.1.1.3 The Architecture Variability Report associated with the INTEROPERABILITY ARCHITECTURE shall specify the range of INTEROPERABILITY ARCHITECTURE INSTANCES to be addressed in the INTEROPERABLE ITEM ASSURANCE arguments by documenting planned commonalities and variabilities within the architecture.

E2.1.2 INTEROPERABLE ITEM internal interoperability management

E2.1.2.1 The Interoperability Management Plan shall properly instantiate the Interoperability Management Plans of the aligned INTEROPERABILITY FRAMEWORK(S).

E2.1.2.2 The Interoperability Management Plan shall be extended to address the internal interoperability of the INTEROPERABLE ITEM. For each constituent INTEROPERABLE ITEM in the preliminary INTEROPERABILITY ARCHITECTURE (Interoperability View), it shall be indicated if the INTEROPERABLE ITEM will be internally sourced or externally sourced.

E2.1.2.3 For each internally sourced constituent INTEROPERABLE ITEM implementation, the following shall be specified in the Interoperability Management Plan:

a) An indication if the constituent implementation is a new implementation to be developed, or a previous implementation to be reused; and

b) The INTEROPERABILITY FRAMEWORKS to which the constituent implementation will claim conformance.

E2.1.2.4 For each externally sourced constituent implementation, the following shall be specified in the Interoperability Management Plan:

a) An indication if the CONSTITUENT INTEROPERABLE ITEM implementation is a new implementation to be developed, or a previous implementation to be reused; and

b) An indication if the CONSTITUENT INTEROPERABLE ITEM implementation shall be conformant with one or more INTEROPERABILITY FRAMEWORKS.

E2.1.2.5 The Interoperability Management Plan shall include criteria for selecting suppliers for externally sourced INTEROPERABLE ITEMS. The selection criteria shall provide a basis for determine a supplier's ability to deliver a compliant item implementation at appropriate levels of quality. Development of the criteria shall consider the following:

a) Evidence of the supplier's quality management system and its ability to support products conforming to SSEPOS;

b) The supplier's past performance and quality;

c) Results of previous compliance to; and

d) The supplier's participation in INTEROPERABILITY FRAMEWORKS to which the item MANUFACTURER has declared alignment.

E2.1.3 Internal item interoperable component interactions (use cases)

E2.1.3.1 The INTEROPERABLE ITEM context interactions of E1.1.5 shall be extended to show how achieving the interactions with an INTEROPERABLE ITEM exercises the INTERACTION POINTS of each of the CONSTITUENT INTEROPERABLE ITEMS.

E2.1.3.2 The coverage of the internal interoperability view point INTERACTION POINTS and internal INTEROPERABILITY BINDINGS shall be assessed and the use cases reflected by the interactions shall be extended as necessary to obtain complete coverage of the internal interoperability view point INTERACTION POINTS and internal INTEROPERABILITY BINDINGS declared for use in the INTEROPERABLE ITEM'S Interoperability View.

E2.1.4 Item preliminary hazard analysis – interoperability-related hazard analysis

E2.1.4.1 A preliminary specification shall be developed of the primary failure modes and immediate effects of all constituent implementations and engineering and technology approaches that are used to achieve the internal INTEROPERABILITY BINDINGS in the Item's Interoperability View.

E2.1.4.2 In situations where constituent implementations are externally sourced and information about the failure modes and effects of a CONSTITUENT INTEROPERABLE ITEM are unknown, worst-case assumptions about the item shall be used in the analysis or assumptions about the component's risk-related behavior relied on to avoid worse-case assumptions shall be documented.

E2.1.4.3 The specification activity in E2.1.4.1 and E2.1.4.2 shall consider the fault taxonomy and factors to consider in Annex I.

E2.1.4.4 It shall be established that the specification activities in E2.1.4.1 and E2.1.4.2 consider the failure modes and effects IDENTIFIED in the Preliminary Hazard Analysis – Interoperability Related Hazard Analysis of the INTEROPERABILITY FRAMEWORK REFERENCE ARCHITECTURES in aligned INTEROPERABILITY FRAMEWORKS.

E2.1.4.5 Control structures and associated SAFETY and SECURITY objectives for each control structure shall be specified.

E2.1.4.6 A preliminary hazard analysis shall be provided that seeks to determine how component failures and interoperability mechanism failures may lead to violations of the item's goals and may contribute to hazardous control actions and data IDENTIFIED in E1.1.6.2.

E2.1.4.7 It shall be established that the analysis activities in E2.1.4.1 and E2.1.4.2 refine the Preliminary Hazard Analysis – Interoperability Related Hazard Analysis of the INTEROPERABILITY FRAMEWORK REFERENCE ARCHITECTURES in aligned INTEROPERABILITY FRAMEWORKS.

E2.1.4.8 The item's goals specified in E1.1.4 shall be refined to include any risk controls necessary to address causes of goal violations uncovered in the preliminary hazard analysis.

E2.1.5 Refinement of INTEROPERABLE ITEM SSEPOS and development of FUNCTIONAL SAFETY CONCEPT

E2.1.5.1 The SSEPOS of the INTEROPERABLE ITEM developed in E1.1.4 shall be refined to addresses failures and ERRORS that may potentially arise from the INTEROPERABLE ITEM'S internal interoperability communication or CONSTITUENT INTEROPERABLE ITEM implementations.

E2.1.5.2 A FUNCTIONAL SAFETY CONCEPT shall be developed for the INTEROPERABLE ITEM that documents how risk controls necessary to achieve the SSEPOS will be realized across the constituents in the preliminary INTEROPERABILITY ARCHITECTURE. For each HAZARDOUS SITUATION, the FUNCTIONAL SAFETY CONCEPT shall indicate how the following aspects of risk controls are allocated to CONSTITUENT INTEROPERABLE ITEMS:

a) Detection of faults and failures;

b) Decisions about whether or not to act of or notify concerning the fault/failure;

c) Notification functions to operators that are expected to take action on item or entities in its environment to achieve a safe state;

d) Actions performed within CONSTITUENT INTEROPERABLE ITEMS to move the item to a safe state;

e) Goals for response times associated with controls documented in the FUNCTIONAL SAFETY CONCEPT.

E2.1.6 Work products

E2.1.6.1 Work products include the following:

a) INTEROPERABLE ITEM Concept / Interoperability Concept

1) INTEROPERABILITY ARCHITECTURE (preliminary, focusing on Interoperability View / Preliminary);

2) Architecture Variability Descriptions;

3) Item interactions; and

4) Functional / SAFETY Goals of the Item.

b) RISK MANAGEMENT File

1) Preliminary Hazard Analysis – Internal Interoperability-Related Hazard Analysis;

c) Functional SAFETY / SECURITY Concept; and

d) Interoperability Management Plan.

E2.2 Architecture and integration specification

E2.2.1 Development of internal INTEROPERABILITY ARCHITECTURE and INTERFACE SPECIFICATION

E2.2.1.1 The portions of the INTEROPERABILITY ARCHITECTURE capturing of the internal interoperability for the INTEROPERABLE ITEM shall be developed following the guidance of Annex O. The specification shall extend and be integrated with the preliminary ARCHITECTURE SPECIFICATION of the ITEM BOUNDARY developed in E1.2.1. The architecture shall be specified at a level of detail sufficient for supporting all system-level RISK MANAGEMENT and ASSURANCE activities.

E2.2.1.2 Traceability shall be established between the INTEROPERABILITY ARCHITECTURE Specification in E2.2.1.1 and the interoperability view of the internal interoperability defined in E2.1.1.