ESBWR
Instrumentation & Controls Systems

JULY 26 – 27, 2006

Lungmen Digital Control Room Simulator

imagination at work

July 26-27, 2006
Richard E. Miller
Thomas W. Jenkins

ESBWR I&C SYSTEMS
Agenda

- Wednesday, July 26
  - > 0800 – GE - Check-In
  - > 0830 – GE - Internal Discussions
  - > 0900 – Entrance Meeting – Introductions
  - > 0915 – Agenda Overview
  - > 0930 – Software Plans Overview
  - > 1400 – Proprietary Discussions – Software Management Plans

- Thursday, July 27
  - > 0800 – GE - Check-In
  - > 0830 – GE - Internal Discussions
  - > 0900 – Entrance Meeting – Introductions

ESBWR I&C SYSTEMS
Agenda (Continued)

- Thursday, July 27 (cont.)
  - > 0930 – DCIS Agenda
    - – Distributed Control & Information Systems (DCIS)
      - DCIS Platform Families
    - – Commercial Grade Dedication for DCIS
    - – I&C Systems Factory Test Program and Interface with COL Applicant's Acceptance Test Program
    - – Fault Tolerant Digital Control System – Mark VIe
    - – RAI 7.0-2 Discussion
    - – RAI 14.3-4 Discussion
    - – N-2 Design Discussion
  - > 1400 – Proprietary Discussions
    - – DCIS Platform Families
    - – Software Plans
  - > 1700 – Exit Site (Day 2 of 2)

ESBWR I&C SYSTEMS – SOFTWARE PLANS

- Software Plans Overview –
  - Man-Machine Interface System & Human Factors Engineering (MMIS&HFE) Implementation Plan
  - Software Management Plan (SMP)
  - Software Quality Assurance Plan (SQAP)
  - Software Configuration Management Plan (SCMP)
  - Software Development Plan (SDP)

ESBWR I&C SYSTEMS – SOFTWARE PLANS

- Software Plans Overview (cont.) –
  - Software Integration Plan (SIntP)
  - Software Verification and Validation Plan (SVVP)
  - Software Safety Plan (SSP)
  - Software Installation Plan (SIP)
  - Software Training (STrngP)
  - Software Operation and Maintenance (SOMP)

ESBWR I&C SYSTEM DESIGN PROCESS

Planning Phase Output Documents

Phase Output Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Software Management Plan (SMP)								
Software Configuration Management Plan (SCMP)								
Software Verification and Validation Plan (SVVP)								
Software Quality Assurance Plan (SQAP)								
Software Safety Plan (SSP)								
Software Installation Plan (SIP)								
Software Integration Plan (SIntP)								

LEGEND
- Document Generation
- Document Used

ESBWR I&C SYSTEM DESIGN PROCESS

Planning Phase Output Documents (cont.)

Phase Output Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Software Operation and Maintenance Plan (SOMP)								
Software Training Plan (STrngP)								
Software Development Plan (SDP)								
Planning Baseline Review Record								

LEGEND
- Document Generation
- Document Used

Man-Machine Interface System & Human Factors Engineering (MMIS&HFE) Implementation Plan

- Describes the methodology used to implement the ESBWR Human Factors Engineering (HFE) and Human Systems Interface (HSI) Design activity.
- Describes the methodology used to implement the Hardware and Software Design Implementation activity compliant with the requirements of Chapter 7 Appendix B of the ESBWR Design Control Document (BTP 14).
- Describes the Human Factors Engineering compliant with the requirements of Chapter 18 of the ESBWR Design Control Document (NUREG 0711).
- Describes the methodology to utilize the detailed design information available from the ABWR reference plant and US standard plant design.
- Provides a systems design approach to ensure that the overall ESBWR I&C is designed, implemented, tested and constructed in an HFE integrated manner within a structured software quality assurance program.

Software Quality Assurance Plan (SQAP)

Defines Software Project Engineering Organization

Describes the SQA standards and principles

Defines minimum qualifications of personnel in SPE

Provides methods of executing various SQA activities

Defines metrics to measure adherence and success

Established organizational and budget independence of verification and validation activities

Describes treatment of Previously Developed Software

Describes treatment of Third Party vendors

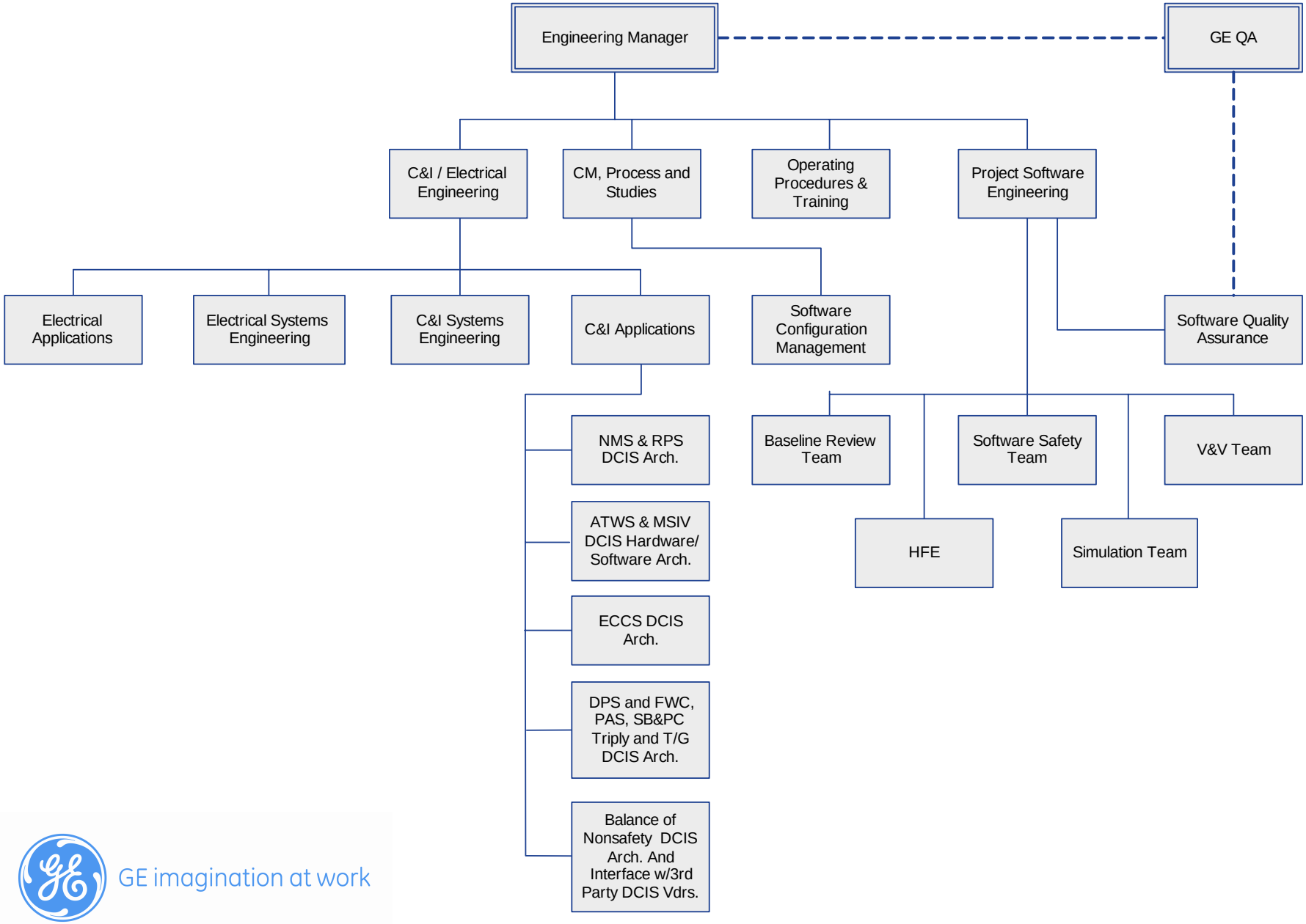
Defines SPE responsibility for Risk Mitigation Monitoring and Management

Establishes Software Rejection Authority in SPE

Software Management Plan (SMP)

- Establishes the standards, methodologies, tools and quality assurance procedures to be used during the software design and development process,
- Defines Organizational units
- Describes the ESBWR Software Engineering Process
- Defines the design activities performed at each level of the software development process and how those activities are verified,
- Defines Life Cycle Phases and measurable outputs from each phase
- Describes the software plan interrelationships
- Defines requirements flow of data and specifications through the engineering process
- Defines software quality classes
- Outlines design document structure
- Describes treatment of Previously Developed Software
- Describes treatment of Third Party Software

ESBWR C&I and Electrical and Software Project Engineering



GE imagination at work

Software Configuration Management Plan (SCMP)

Establishes standards and methodology for configuration control of software

Defines organizational responsibilities

Defines Configuration Items subject to this plan

Defines management of all forms of software artifacts(Source, Object codes, data bases etc.)

Defines Change Control processes within GEEN procedures

Addresses third party vendor software products and maintains the relationship to procurement documents and procedures

Software Development Plan (SDP)

Establishes the program management procedures to be followed

Defines program risk profiling and mitigation

Addresses staffing plans for the software development

Establishes software development budgets, scheduling and progress monitoring

Provides connectivity to the overall ESBWR project plans

Software Integration Plan (SIntP)

- Defines the hardware/software integration test management approach
- Describes a multi-tiered integration and testing echelon
- Establishes compliance procedures and management reporting mechanisms
- Describes roles and responsibilities of the test organizations
- Addresses schedule development, security management, risk and contingency planning
- Describes the anomaly and problem reporting
- Describes module and integration test scope and acceptance criteria
- Defines the boundaries and interface to independent validation activities
- Defines documentation types and test deliverables

Software Verification and Validation Plan (SVVP)

- Establishes the standards, methods and procedures for Independent Verification and Validation
- Verifies software design and test artifacts throughout the process
- Traces requirements from source to validated implementation
- Assesses quality of outputs
- Facilitates timely detection of errors
- Addresses third party vendor requirements
- Provides V&V of the software implementation of HFE design requirements (HSI implementation)
- Defines qualifications of V&V personnel, including HFE representation
- Provides periodic management V&V status reviews
- Establishes V&V activities associated with software safety analysis

Software Safety Plan (SSP)

Establishes the methods, procedures and standards supporting the software safety analysis

Evaluates architectural system level design appropriateness to support the required safety functions

Evaluates the interfaces, safety to safety and safety to non-safety.

Verifies HFE System Functional Requirements and PRA inputs are captured in the software requirements

Describes the deterministic hazard analysis approach

Provides verification of system timing and sizing analysis

Verifies Defense in Depth and Diversity basis is maintained throughout the software development cycle

Verifies the scope of the integration and module tests

Verifies Security is addressed

Verifies safety analysis basis is maintained through implementation, including third party development

Software Installation Plan (SIP)

- Establishes the methods, procedures and standards supporting the software installation phase
- Defines Installation and turnover activities to maintain configuration control of all software, manuals and training material
- Establishes requirements for documenting the results of the installation
- Verifies site installation tests are executed and anomalies resolved
- Verifies issuance of operations and maintenance manuals
- Verifies on going security requirements are accepted by the licensee
- Verifies training manuals are delivered
- Establishes a documentation record for future field modification

Software Training (STrngP)

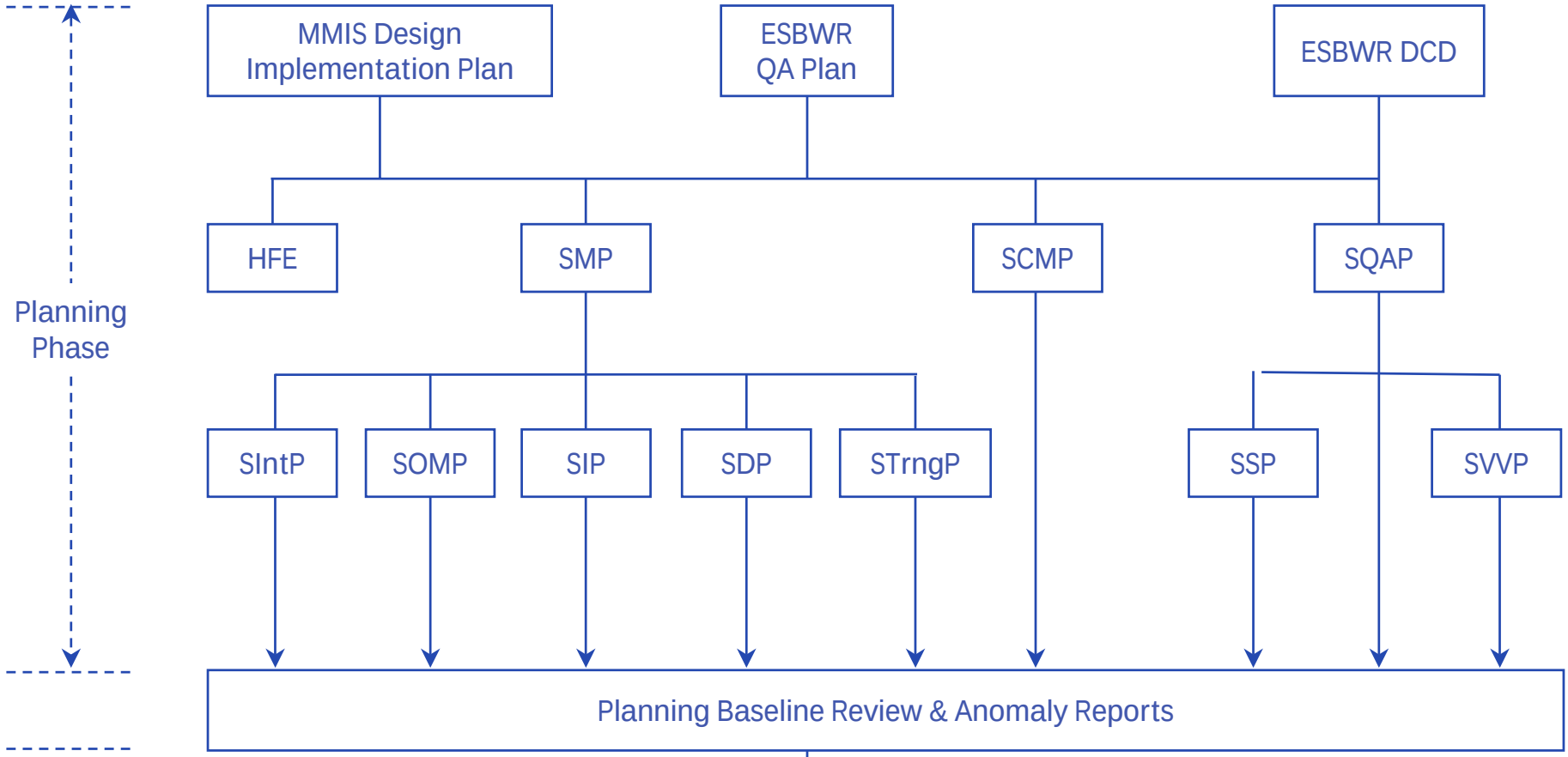
- Establishes the methods, procedures and standards supporting the software training activities during all phases of the project
- Defines training organization responsibility
- Defines training personnel qualifications
- Establishes the scope of training
- Requires a methodology to capture problem reporting associated with the training materials

Software Operation and Maintenance (SOMP)

- Establishes the methods, procedures and standards supporting software activities during Operation and Maintenance Phases
- The Software Installation Plan (SIP) and SOMP define requirements for development of the System Operations & Maintenance Manual
- Defines maintenance procedures for modification of software once it is placed in service
- Defines required documentation for Operation and Maintenance Phases
- Defines that Maintenance activities shall use the entire life cycle to modify software

ESBWR I&C SYSTEM DESIGN PROCESS

Planning Phase



DCD – Design Control Document
HFE – Human Factors Engineering
MMIS – Man-Machine Interface System
SCMP – Software Configuration Management Plan
SDP - Software Development Plan
SIP – Software Installation Plan
SIntP – Software Integration Plan

SMP – Software Management Plan
SOMP – Software Operation & Maintenance Plan
SVVP - Software Verification and Validation Plan
SQAP – Software Quality Assurance Plan
SSP – Software Safety Plan
STrngP – Software Training Plan

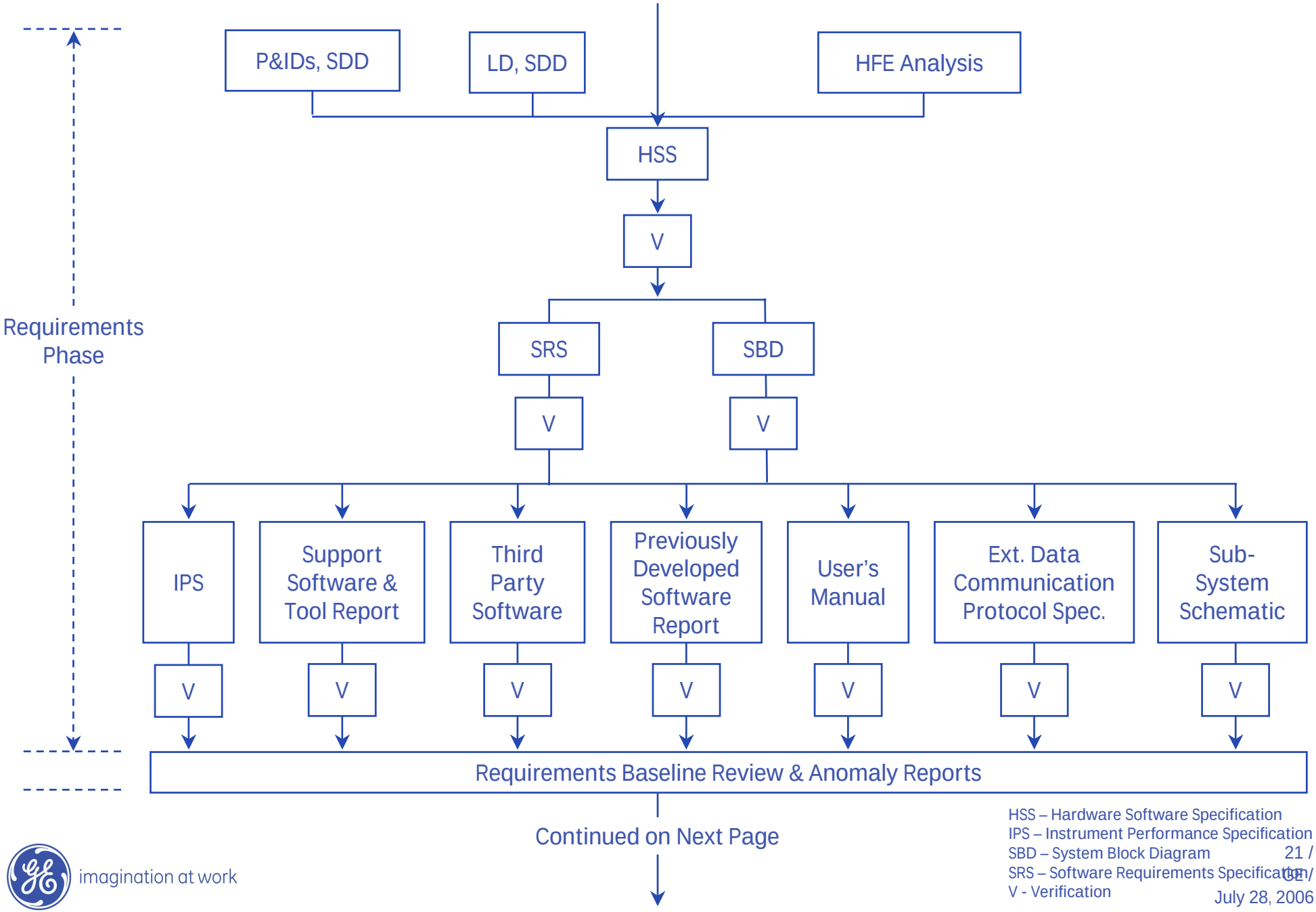
Continued on Next Page

imagination at work

ESBWR I&C SYSTEM DESIGN PROCESS

Requirements Phase

Continued from last page



Continued on Next Page

HSS – Hardware Software Specification
IPS – Instrument Performance Specification
SBD – System Block Diagram
SRS – Software Requirements Specification
V - Verification

ESBWR I&C SYSTEM DESIGN PROCESS

Requirements Phase Output Documents

Requirements Phase Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Hardware/Software System Specification (H/SSS)		═══	═══	═══				
System Block Diagram (SBD)		═══	═══	═══				
Software Requirements Specification (SRS)		═══	═══	═══	═══	═══		
Instrument Performance Specification (IPS)		═══	═══	═══	═══	═══		
Subsystem Schematic		═══	═══	═══				
External Data Communication Protocol Specification		═══	═══	═══	═══			
User's Manuals		═══				═══	═══	═══
Support Software/Tool and its documentation package		═══		═══	═══	═══	═══	═══

NOTE: An SRS is used for software-based systems, while an IPS is used for a microprocessor-based system. Both an IPS and SRS are not required for a single system.

LEGEND
═══ Document Generation
═══ Document Used

ESBWR I&C SYSTEM DESIGN PROCESS

Requirements Phase Output Documents (cont.)

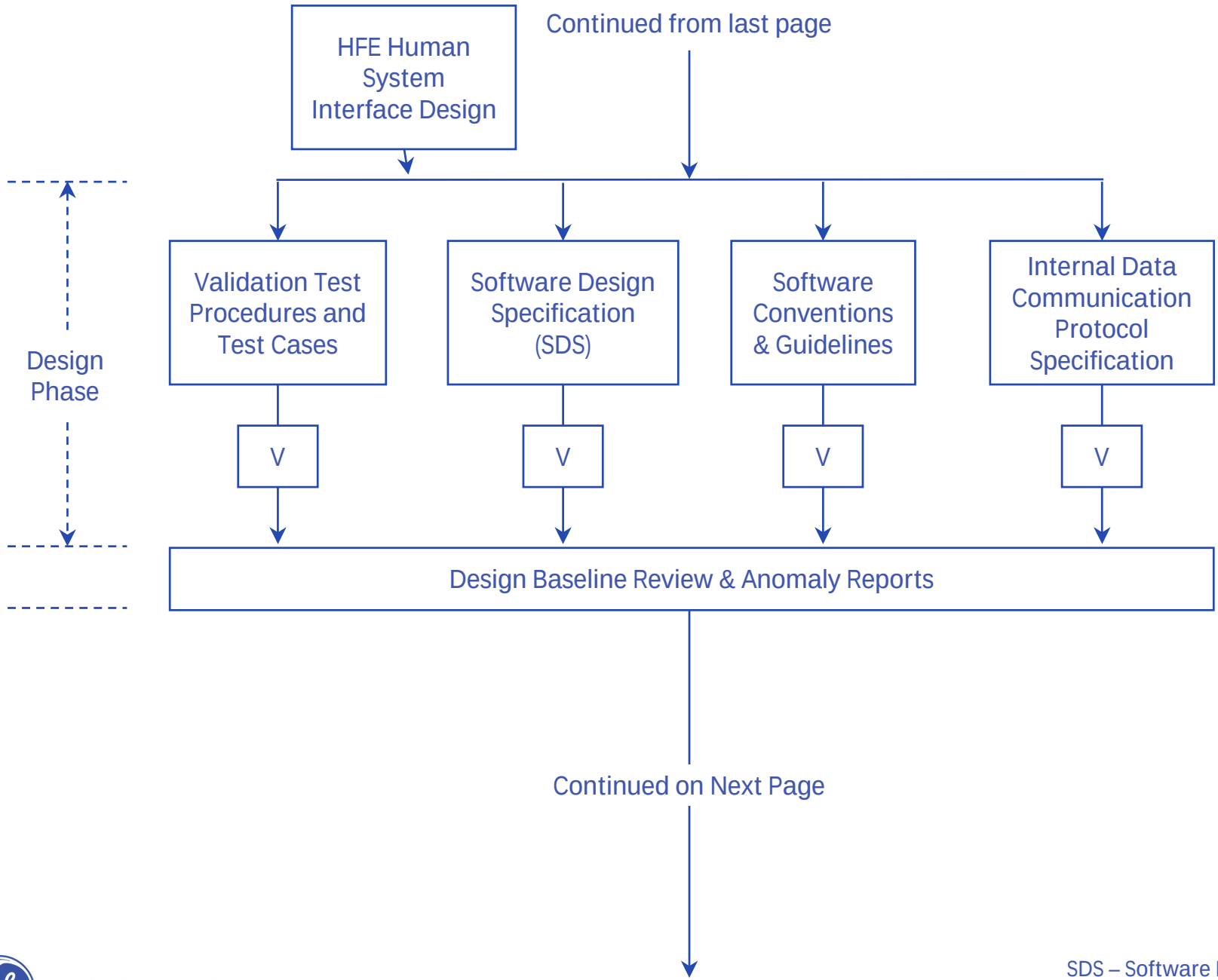
Requirements Phase Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Third Party Software and its documentation package.								
Previously Developed Software Evaluation Report								
Supplemental documentation for Previously Developed Software								
Requirements Baseline Review Record								

NOTE: An SRS is used for software-based systems, while an IPS is used for a microprocessor-based system. Both an IPS and SRS are not required for a single system.

LEGEND
- Document Generation
- Document Used

ESBWR I&C SYSTEM DESIGN PROCESS

Design Phase



ESBWR I&C SYSTEM DESIGN PROCESS

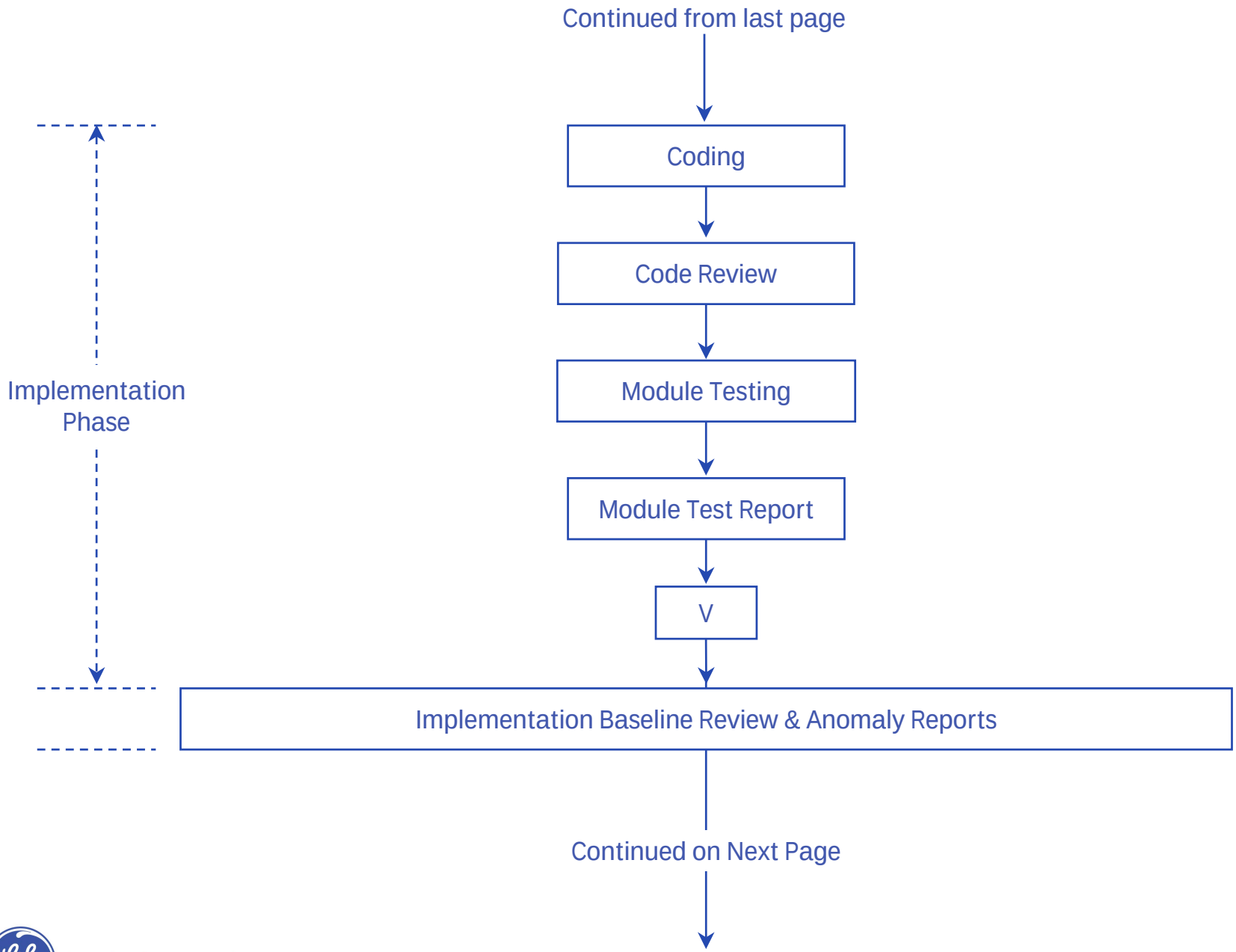
Design Phase Output Documents

Design Phase Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Software Design Specification (SDS)								
Validation Test Procedures and Test Cases Specification								
Software Conventions and Guidelines Document								
Internal Data Communication Specification Protocol								
Support Software/Tool and its documentation package								
Third Party Software and its documentation package.								
Supplemental documentation for Previously Developed Software								
Design Baseline Review Record								

LEGEND
- Document Generation
- Document Used

ESBWR I&C SYSTEM DESIGN PROCESS

Implementation Phase



ESBWR I&C SYSTEM DESIGN PROCESS

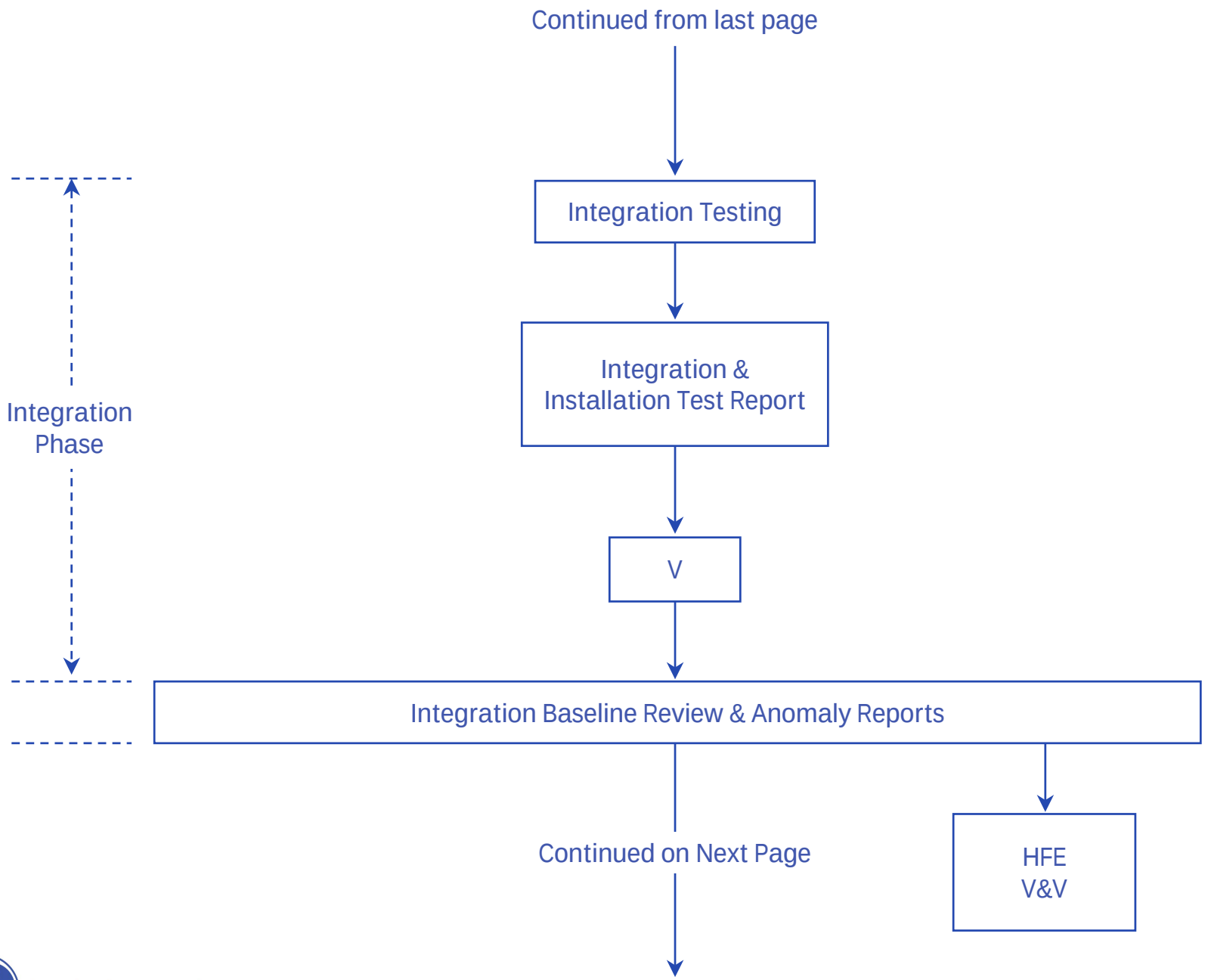
Implementation Phase Output Documents

Implementation Phase Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Source Code								
Executable Code								
Module Test Report								
Support Software/Tool and its documentation package								
Third Party Software and its documentation package.								
Supplemental documentation for Previously Developed Software								
Implementation Baseline Review Record								

LEGEND
Document Generation
Document Used

ESBWR I&C SYSTEM DESIGN PROCESS

Integration Phase



ESBWR I&C SYSTEM DESIGN PROCESS

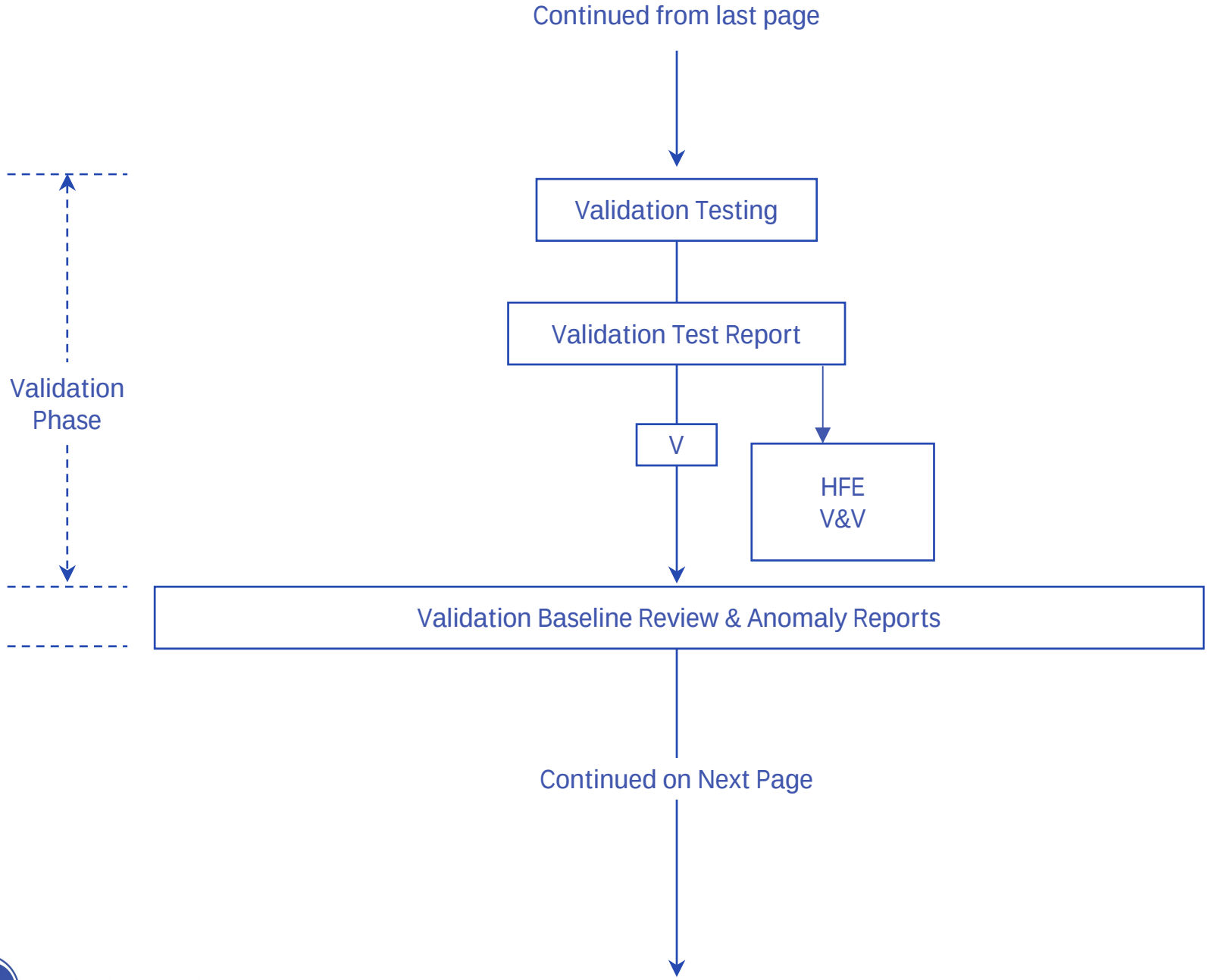
Integration Phase Output Documents

Installation Phase Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Integration and Installation Test Report, including Errors Checklist and system build description								
Support Software/Tool and its documentation package								
Integration Baseline Review Record								

LEGEND
Document Generation
Document Used

ESBWR I&C SYSTEM DESIGN PROCESS

Validation Phase



ESBWR I&C SYSTEM DESIGN PROCESS

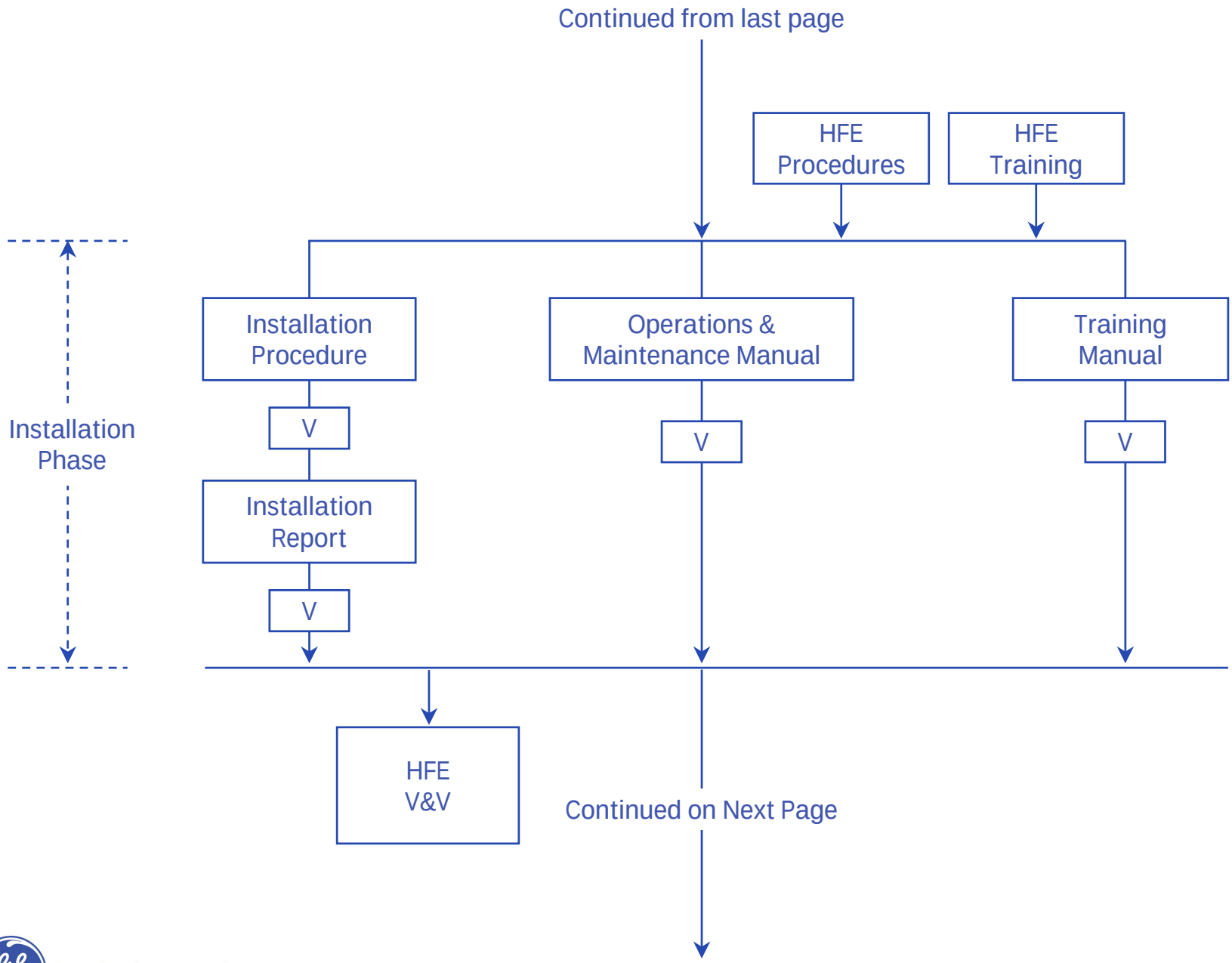
Validation Phase Output Documents

Validation Phase Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Validation Test Report								
Build Release Description								
Support Software/Tool and its documentation package								
Validation Test Baseline Review Record								

LEGEND
Document Generation
Document Used

ESBWR I&C SYSTEM DESIGN PROCESS

Installation Phase



ESBWR I&C SYSTEM DESIGN PROCESS

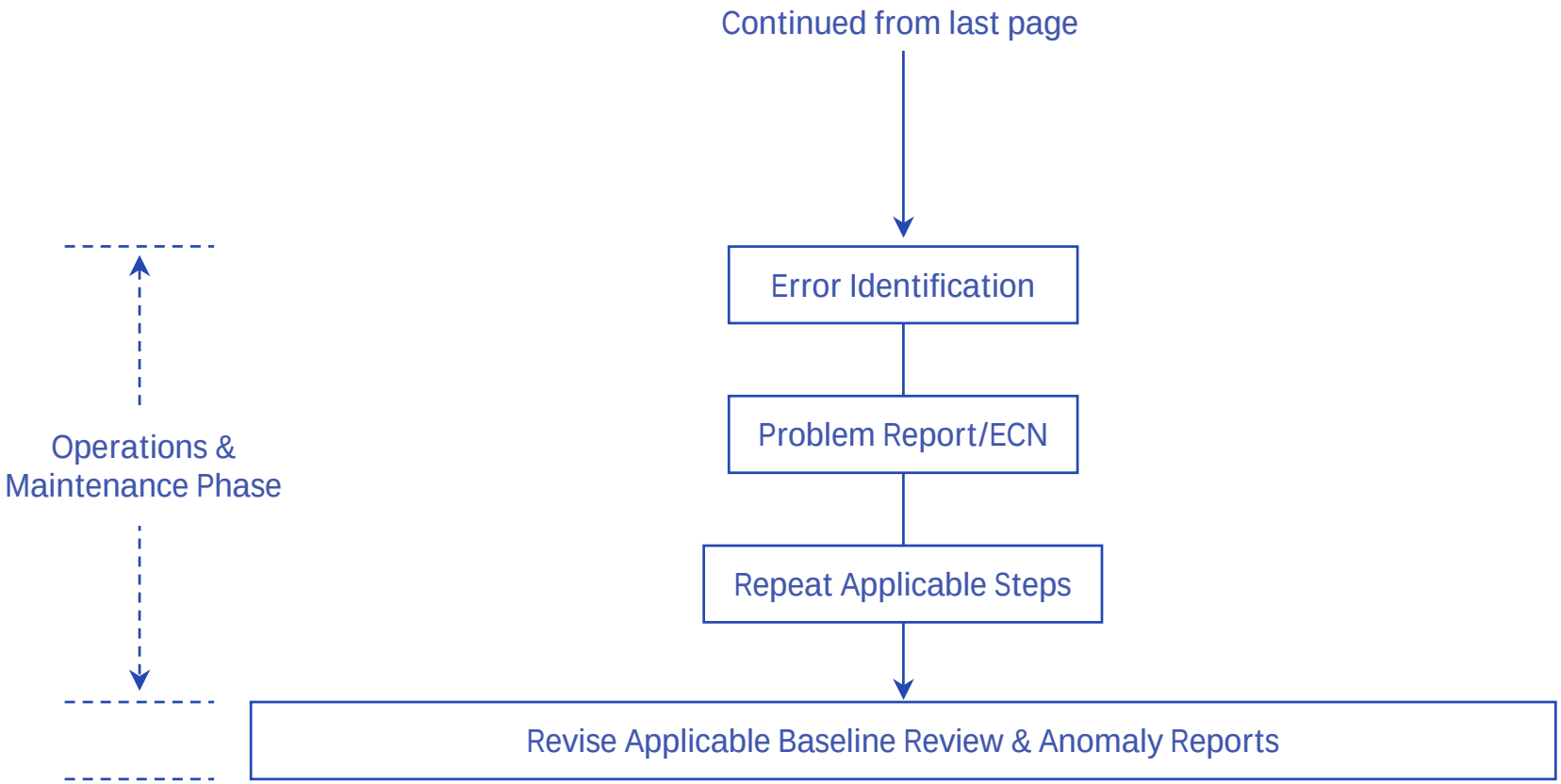
Installation Phase Output Documents

Installation Phase Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Software Installation Procedure								
Software Installation Report								
Installation Configuration Tables								
Operations Manual								
Maintenance Manual								
Training Manual								

LEGEND
Document Generation
Document Used

ESBWR I&C SYSTEM DESIGN PROCESS

Operations and Maintenance Phase



ESBWR I&C SYSTEM DESIGN PROCESS

Operations and Maintenance Phase Output Documents

Operations and Maintenance Phase Document Name	Project Life Cycle (BTP HICB-7-14)							
	Planning Phase	Requirement Phase	Design Phase	Implementation Phase	Integration Phase	Validation Phase	Installation Phase	O&M Phase
Engineering Change Notifications (ECNs)								—
Revised/impacted documentation								—
Revised Source and Executable Code								—
Module Test Report								—
Integration and Installation Test Report								—
Validation Test Report								—
Revised Baseline Review Records								—

LEGEND
— Document Generation
— Document Used