DO-331 Model Based Development and Verification Supplement to DO-178C and DO-278A

L. Alford

APT Research, Inc

Objectives

- **Objectives for DO-178C suite of documents, including the Supplements:**
  - Promote safe implementation of aeronautical software
  - Provide clear and consistent ties with the systems and safety processes
  - Address emerging software trends and technologies
  - Implement an approach that can change with the technology
  - Industry-accepted guidance for satisfying airworthiness requirements for avionics equipment

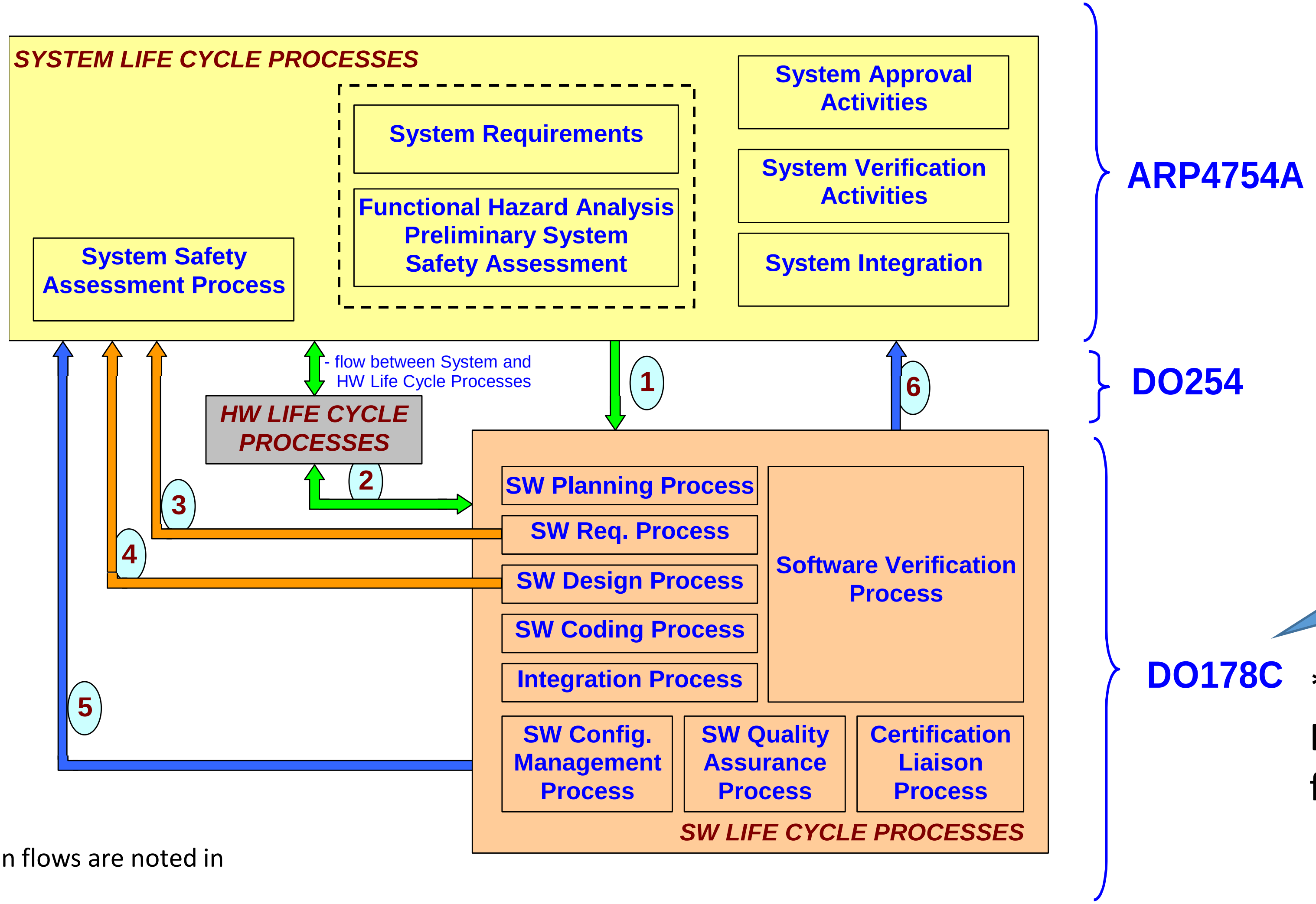
Purpose

- **Industry-accepted guidance for satisfying airworthiness requirements for avionics equipment**
  - To provide guidelines for software to comply with
    - Proof of no intended function
    - Proof of performance in an avionics LRU installation
  - To provide agreed criteria consistent with civil certification authorities
  - By treaty agreement, this applies to NATO nations and any other countries recognizing this set of guidelines for aviation software

- **Results Needed**
  - Agreed criteria for airworthiness certification requirements for software that doesn’t differ from one person or certification authority to another
  - Allows for recognition of an aircraft model capability by air traffic control for airspace access and interoperability
    - This last is an issue for all military aircraft

Information flow between System & SW life cycle processes

Context for use of DO-331 MBD


SYSTEM LIFE CYCLE PROCESSES
System Requirements
Functional Hazard Analysis Preliminary System Safety Assessment
System Approval Activities
System Verification Activities
System Integration
System Safety Assessment Process
- flow between System and HW Life Cycle Processes
HW LIFE CYCLE PROCESSES
1
2
3
4
5
6
SW Planning Process
SW Req. Process
SW Design Process
SW Coding Process
Integration Process
Software Verification Process
SW Config. Management Process
SW Quality Assurance Process
Certification Liaison Process
SW LIFE CYCLE PROCESSES
ARP4754A
DO254
DO178C

DO-331* is used with DO-178C

*It adds and modifies DO-178C objectives for MBD aspects

More detailed information flows are noted in backup charts

DO-331 MBD Fundamentals - 1

- **Its about identifying the “safe-subset” use of MBD technology to be used in safety related applications**
  - Same role as the suite of DO-178C documents
  - It applies “error class analysis” to determine *what needs to be considered* for MBD projects to confirm best known practices and proof of safety

- **Its about using suitable graphical engineering methods to design a software system**
  - The ability create graphic representations of requirements, architecture and designs has existed for some time
  - Visual format promotes better understanding of the system and its interactions
  - The use of graphics has been refined with semantics of notations with more rigorous syntax and less ambiguity – leading to the use of analysis techniques on models within the modelling environment to remove errors early in the lifecycle

DO-331 MBD Fundamentals - 2

- **Clear distinctions are made between 2 types of graphical models:**
  - Specification Models – Defining high level requirements without implementation, software architecture, or data flow and/or control flow

  - Design Models – Defining architecture and design (low level requirements)
    - If code can be written from the model, then it is considered a Design Model
    - A Design Model must have parent requirements in scope of the DO-178C development process

  - Note that Systems Engineering may be the author of a Specification Model and therefore subject to meeting the objectives of DO-331 for that model

DO-331 MBD Fundamentals - 3

- **Determining which artifacts will be in a model drives the determination of applicable objectives and activities**
  - If the model is defining requirements without indicating how it will be accomplished, then the Software Requirements Document (SRD) becomes the location for that model
  - Detailed architecture, data and control flow, implementation and performance form the content of the Software Design Document (SDD)
  - A MBD area of a system will continue to include:
    - Full requirement traceability and model traceability
    - Configuration control including the models and elements used
    - Verification of the models, libraries, and model elements

Model Usage Examples

1. Example 1: Simplest and common use of MBD; the Design Model goes into the Software Design Document (SDD)

2. Example 2: the Design Model is developed from the requirements contained in the Specification Model.

3. Example 3: the textual description refers to LLR and possibly architecture: DO-178C guidance is applicable to these.

4. In examples 4 and 5, separating system and software life cycle data may be difficult: the artifacts may serve for both the systems and software groups. Use the guidance in DO-331 as the compliance criteria for the artifact(s). The MBD guidance for HLR applies to system and software Specification Models, while the MBD guidance for Low-Level Requirements (LLR) applies to software Design Models.

5. Examples 6 and 7 are evolving now and are added to provide guidance. These are not currently represented in DO-331, though the planning, activities, artifacts, and relationships are defined in DO-331.

Initiating Process for Life Cycle Data	Model Example 1	Model Example 2	Model Example 3	Model Example 4[1]	Model Example 5[1]	Model Example 6[4]	Model Example 7[4]
System Requirements Process	Textual source requirements allocated to software	Textual source requirements for the model(s)	Textual source requirements for the model(s)	Textual source requirements for the model(s)	Textual source requirements for the model(s)	Textual source requirements for the models	Specification Model(s)
System Design Process					Design Model(s)	Specification Model(s)	Textual source requirements for the model(s)
Software Requirements Process	Textual source (SRS) requirements for the model(s)	Specification Model(s)[2]	Specification Model(s)	Design Model(s)		Design Model(s)	Model examples 1 - 5
Software Design Process	Design Model(s)	Design Model(s)	Textual Design Description (SDD)[3]				
Software Coding Process	Source Code	Source Code	Source Code	Source Code	Source Code	Source Code	Source Code

DO-331 MBD Fundamentals - 4

- **MBD Data Items (beyond the normal items) to be expected in a program:**
  - Model Planning
    - How it will be used and how and where it fits into the lifecycle; what Model Standards will be used; the verification approach; simulation - if used for credit
  - Model Standards and Techniques
    - The guides for both Specification and Design models, including constraints, instructions, language, symbols used, model element libraries
  - Model Element Libraries
    - Each element must be assured to meet the required Software Level as it is a set of executable code that generates a symbol and associated action. A full data package for each library is necessary
    - Unused elements should be removed from the library, unless the standard includes instructions prohibiting use, particularly for unassured elements

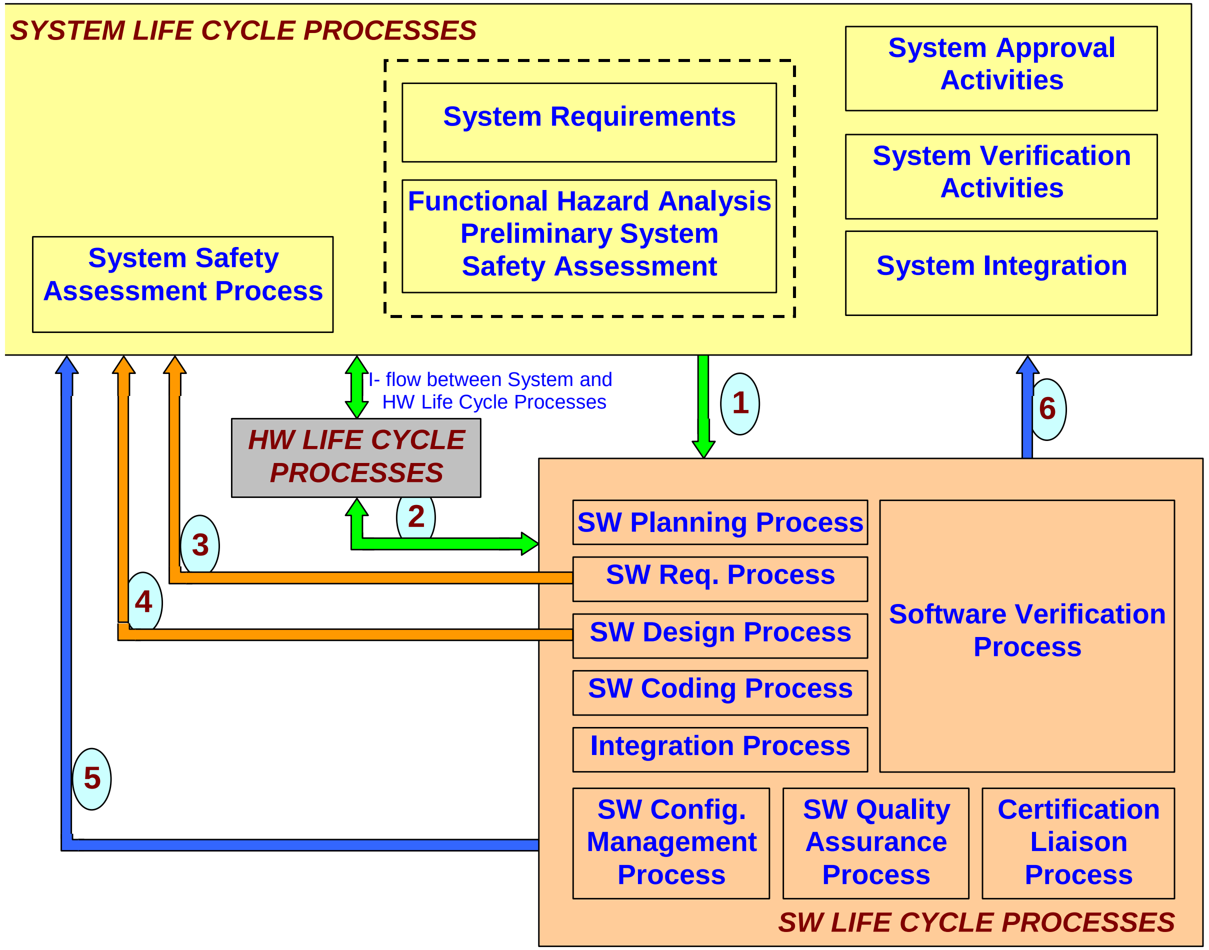
DO-331 MBD Fundamentals - 5

- **MBD Data Items to be expected in a program, continued:**
  - Model Coverage
    - Analysis which identifies requirements in a Design Model not verified by requirements testing;
    - This may identify unintended functionality
    - Criteria for this analysis and resolution of issues found must be defined in the planning document
  - Model Simulation
    - This activity exercises the model behavior using a simulator
    - If used for credit, the simulation cases, procedures and results are necessary

Backup Charts

Context required between Systems and Software/Hardware processes

Information flow between System & SW life cycle processes


SYSTEM LIFE CYCLE PROCESSES
System Requirements
Functional Hazard Analysis
Preliminary System
Safety Assessment
System Approval Activities
System Verification Activities
System Integration
System Safety Assessment Process
I- flow between System and HW Life Cycle Processes
HW LIFE CYCLE PROCESSES
1
2
3
4
5
6
SW Planning Process
SW Req. Process
SW Design Process
SW Coding Process
Integration Process
Software Verification Process
SW Config. Management Process
SW Quality Assurance Process
Certification Liaison Process
SW LIFE CYCLE PROCESSES

1

System process shall give the following data to SW process

⇒ **To planning process**

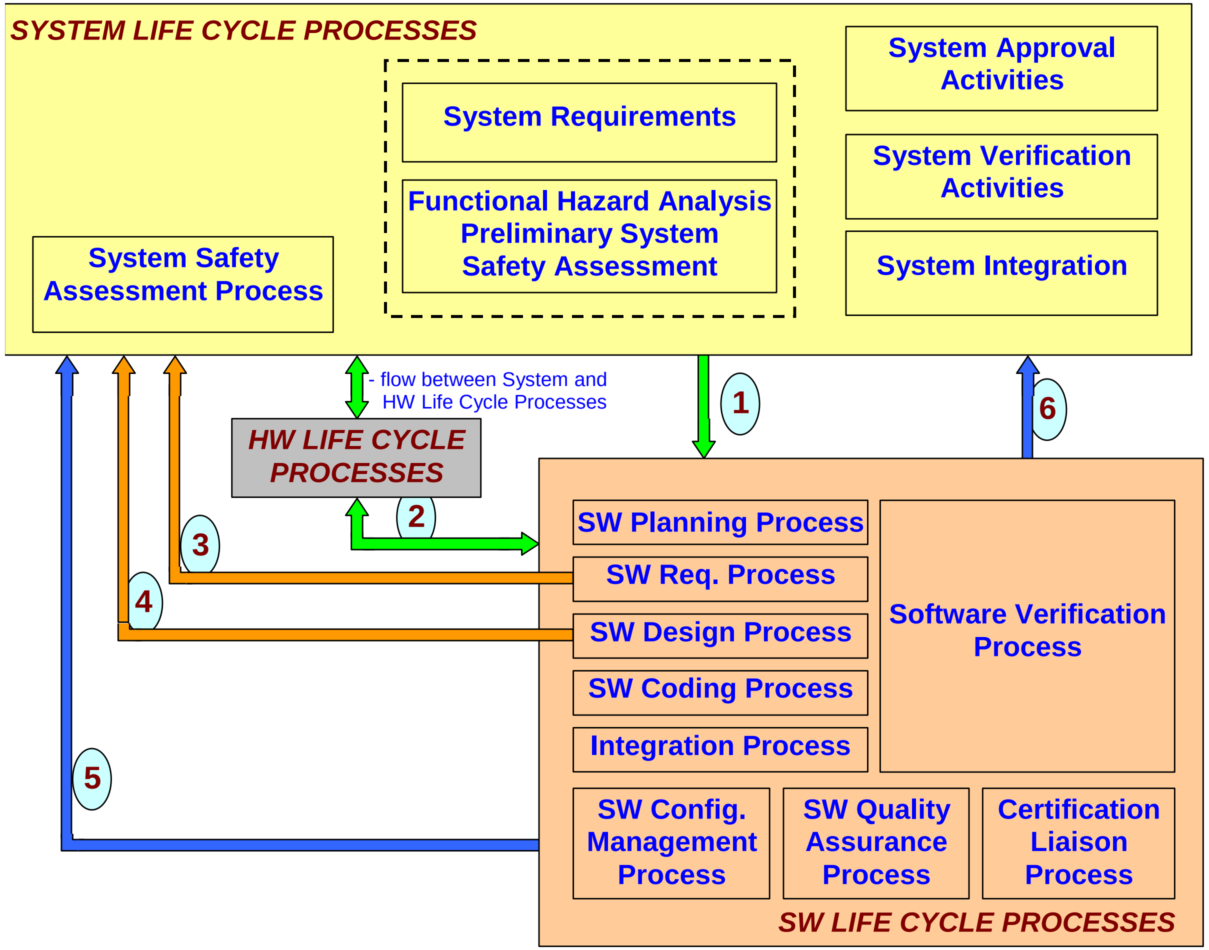
- System Safety Objectives
- Software Level(s)
- System Description and Hardware Definition

⇒ **To development process**

- System Requirements Allocated to Software
- Design Constraints

The data flow between systems, software and hardware are critical to success and should be confirmed

Information flow between System & SW life cycle processes


SYSTEM LIFE CYCLE PROCESSES
System Requirements
Functional Hazard Analysis Preliminary System Safety Assessment
System Approval Activities
System Verification Activities
System Integration
System Safety Assessment Process
- flow between System and HW Life Cycle Processes
HW LIFE CYCLE PROCESSES
1
2
3
4
5
6
SW Planning Process
SW Req. Process
SW Design Process
SW Coding Process
Integration Process
Software Verification Process
SW Config. Management Process
SW Quality Assurance Process
Certification Liaison Process
SW LIFE CYCLE PROCESSES

3 SW process shall give the following data to System process

- Derived HLR

4 SW process shall give the following data to System process

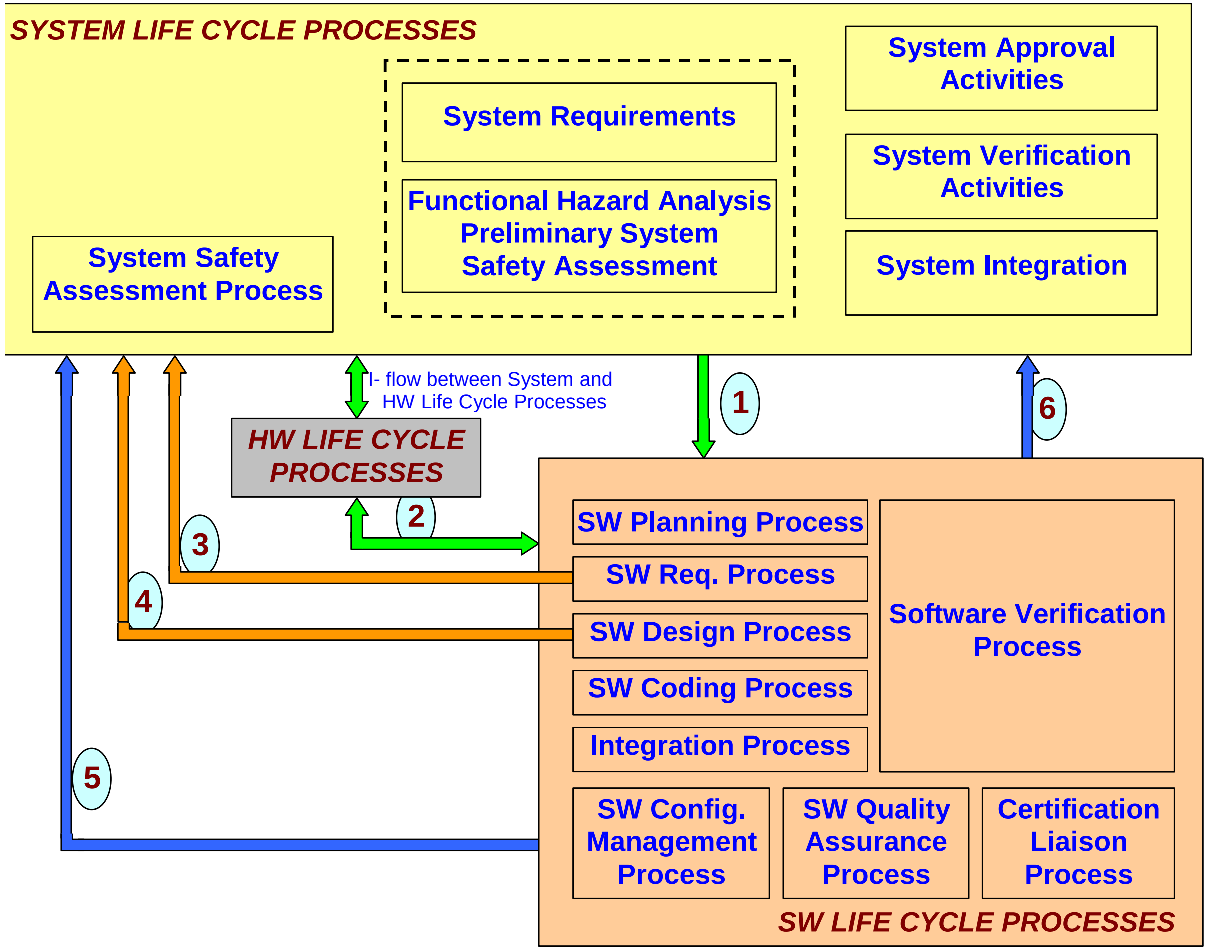
- Derived LLR

1 System process shall give the following data to SW process

- Evidence of Acceptability of Derived Requirements

The data flow between systems, software and hardware are critical to success and should be confirmed

Information flow between System & SW life cycle processes



SYSTEM LIFE CYCLE PROCESSES
System Requirements
Functional Hazard Analysis
Preliminary System
Safety Assessment
System Approval Activities
System Verification Activities
System Integration
System Safety Assessment Process
I- flow between System and HW Life Cycle Processes
HW LIFE CYCLE PROCESSES
1
2
3
4
5
6
SW Planning Process
SW Req. Process
SW Design Process
SW Coding Process
Integration Process
Software Verification Process
SW Config. Management Process
SW Quality Assurance Process
Certification Liaison Process
SW LIFE CYCLE PROCESSES

5

SW process shall give the following data to System process

- Problem or change documentation

6

SW process shall give the following data to System process

- Any limitation of use
- Configuration identification data

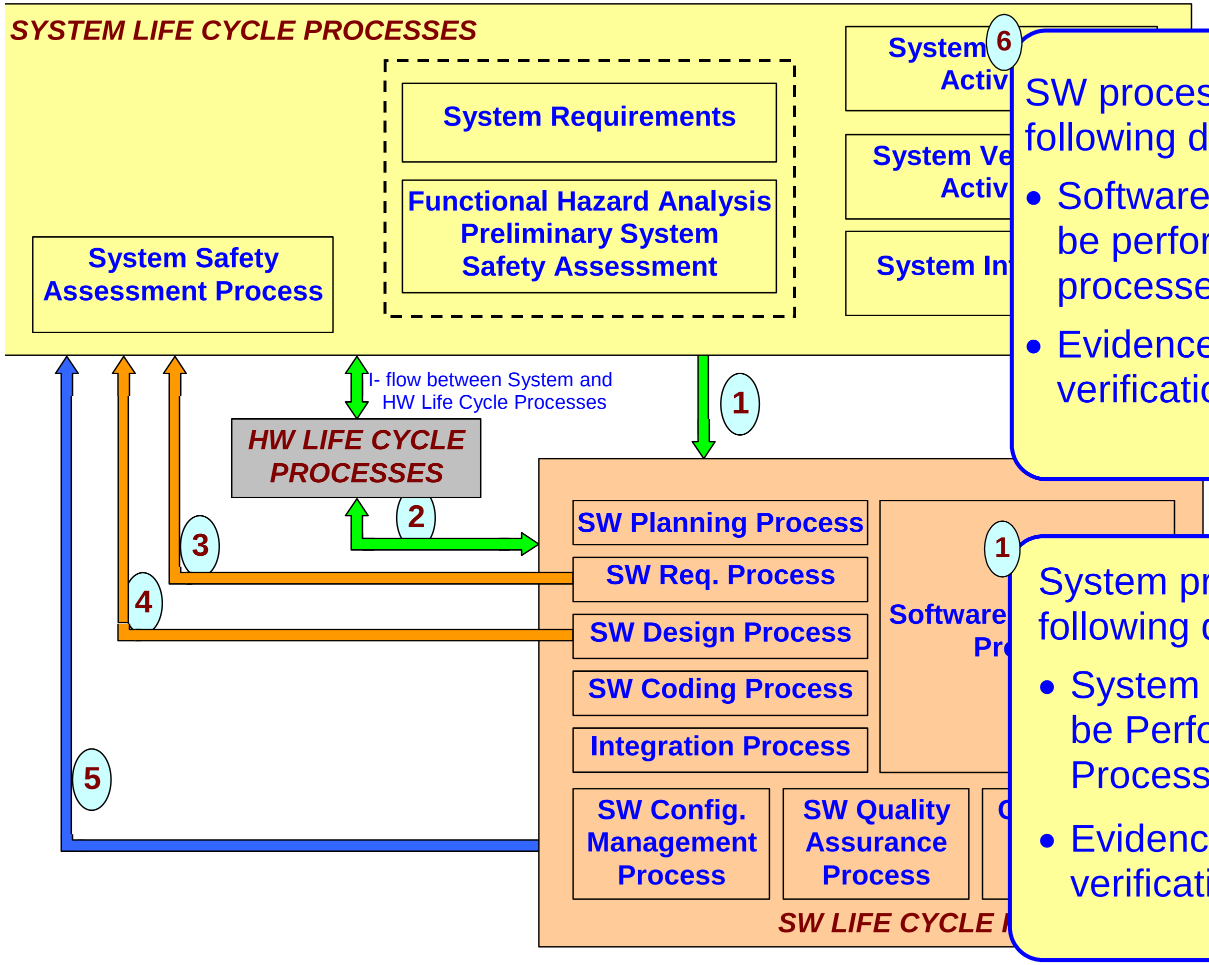
1

System process shall give the following data to SW process

- Evidence of Acceptability of Problem or change documentation

The data flow between systems, software and hardware are critical to success and should be confirmed

Information flow between System & SW life cycle processes


SYSTEM LIFE CYCLE PROCESSES
System Requirements
Functional Hazard Analysis
Preliminary System Safety Assessment
System Safety Assessment Process
System
Activ
6
System Ve
Activ
System In
I- flow between System and HW Life Cycle Processes
HW LIFE CYCLE PROCESSES
1
2
3
4
5
SW Planning Process
SW Req. Process
SW Design Process
SW Coding Process
Integration Process
Software
Pr
1
SW Config. Management Process
SW Quality Assurance Process
C
SW LIFE CYCLE P

SW process shall give the following data to System process

- Software verification activities to be performed by system processes
- Evidence of any system verification

System process shall give the following data to SW process

- System Verification Activities to be Performed by Software Processes
- Evidence of any SW verification activities performed

The data flow between systems, software and hardware are critical to success and should be confirmed