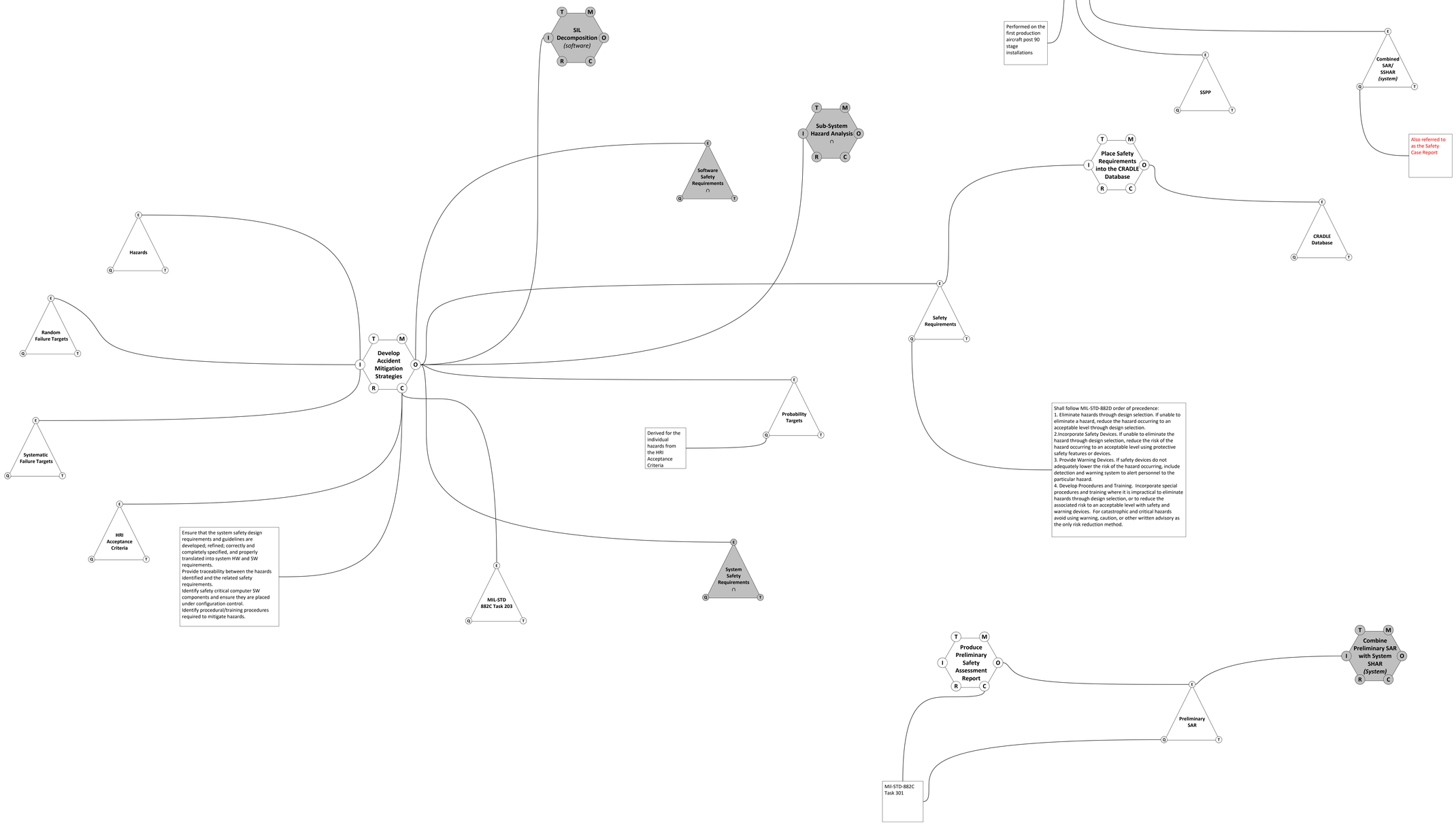
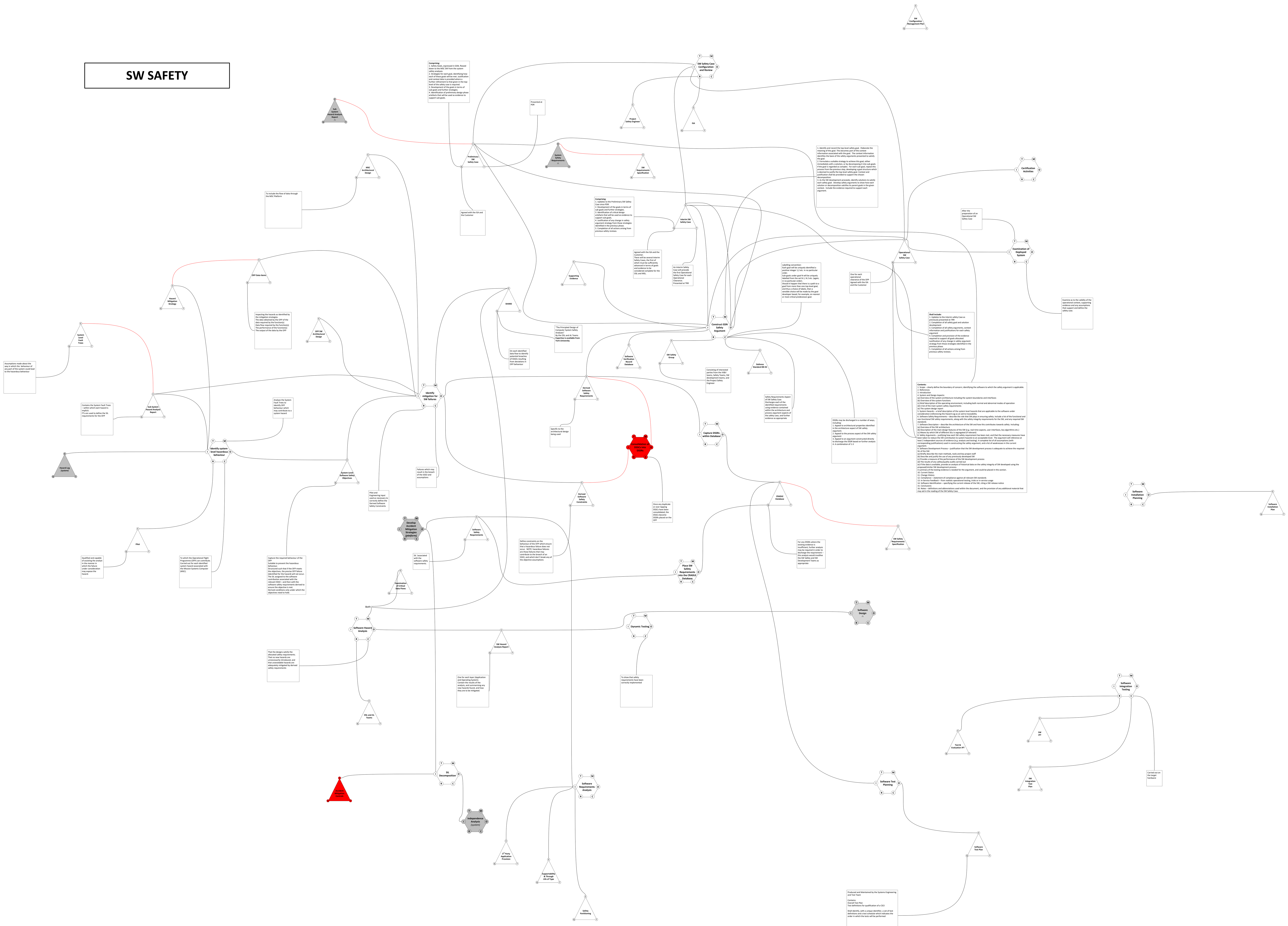
PLATFORM


First Representative Aircraft Assessment ZHA
Hazard Log (system)
Performed on the first production aircraft post 90 stage installations
SSPP
Combined SAR/ SSHAR (system)
Also referred to as the Safety Case Report
SIL Decomposition (software)
Sub-System Hazard Analysis
Software Safety Requirements
Place Safety Requirements into the CRADLE Database
CRADLE Database
Hazards
Safety Requirements
Random Failure Targets
Develop Accident Mitigation Strategies
Probability Targets
Derived for the individual hazards from the HRI Acceptance Criteria
Systematic Failure Targets
Shall follow MIL-STD-882D order of precedence:
1. Eliminate hazards through design selection. If unable to eliminate a hazard, reduce the hazard occurring to an acceptable level through design selection.
2.Incorporate Safety Devices. If unable to eliminate the hazard through design selection, reduce the risk of the hazard occurring to an acceptable level using protective safety features or devices.
3. Provide Warning Devices. If safety devices do not adequately lower the risk of the hazard occurring, include detection and warning system to alert personnel to the particular hazard.
4. Develop Procedures and Training. Incorporate special procedures and training where it is impractical to eliminate hazards through design selection, or to reduce the associated risk to an acceptable level with safety and warning devices. For catastrophic and critical hazards avoid using warning, caution, or other written advisory as the only risk reduction method.
HRI Acceptance Criteria
Ensure that the system safety design requirements and guidelines are developed; refined; correctly and completely specified, and properly translated into system HW and SW requirements.
Provide traceability between the hazards identified and the related safety requirements.
Identify safety critical computer SW components and ensure they are placed under configuration control.
Identify procedural/training procedures required to mitigate hazards.
MIL-STD 882C Task 203
System Safety Requirements
Produce Preliminary Safety Assessment Report
Combine Preliminary SAR with System SHAR (System)
Preliminary SAR
Mil-STD-882C Task 301

SYSTEM


System Test Plan
System Test Planning
Test & Evaluation IPT
Independence Analysis
SIL Decomposition (software)
Non Functional Requirements
Human Factors
Functional Requirements
SIL Allocation
Hazards (platform)
Sub System Engineers
Safety Requirement Allocation to Sub-Systems
Safety Requirement Partitioning to HW & SW
System Engineers
SW Requirements Specification
System Safety Requirements
Develop Accident Mitigation Strategies (platform)
Aircrew O&SHA Report
Ground Crew O&SHA Report
SMART Health Hazard Assessment
Operating and Support Hazard Analysis
Health Hazard Assessment
Failure Mode Effects and Criticality Analysis
FMEAs from Equipment Suppliers
EMC & Lightning Protection Assessments
Aircraft Structural Integrity Activities
EMC & Lightning Protection Assessment
Design Phase Zonal Hazard Analysis
ZHA Report
Safety Requirement Verification
Historical and Past In-Service Experience
System/Sub-System Architectural Design
Hazard Checklist Reports
Preliminary System Hazard Identification
Preliminary System Hazard Analysis
Sub-System Hazard Analysis
Functional Failure Analysis Reports
System Safety Engineers
Sub System Hazard Analysis Report
Preliminary SW Safety Case
Hazard Log
Preliminary Hazard List
Manage the Hazard Log
Preliminary System Hazard Analysis report
Combine Preliminary SHA with System SHAR
Preliminary SHA (platform)
Manage Changes to Safety Requirements
Combined SAR/SSHA
Update the Hazard Log
Standard Configuration Mgmt Procedures
Project Safety Engineer
System Engineers
Hazard Logging and Tracking Procedure
'System' level Hazard Analysis Reports
Updated Hazard Log
Change Request

SW SAFETY



SW Safety Case Configuration and Review
Comprising:
1. Safety Goals, expressed in GSN, flowed down to the MSC SW from the system safety analyses.
2. Strategies for each goal, identifying how each of these goals will be met. Justification and context data is provided where a further refinement to that given in the top-level of the safety case is required.
3. Development of the goals in terms of sub-goals and further strategies.
4. Identification of preliminary design phase artefacts that will be used as evidence to support sub-goals.
Presented at PDR
Project Safety Engineer
ISA
Preliminary SW Safety Case
System Safety Requirements
SW Requirements Specification
Agreed with the ISA and the Customer
Comprising:
1. Updates to the Preliminary SW Safety Case since PDR.
2. Development of the goals in terms of sub-goals and further strategies.
3. Identification of critical design artefacts that will be used as evidence to support sub-goals.
4. Justification of any change in safety argument strategy from those strategies identified in the previous phase.
5. Completion of all actions arising from previous safety reviews.
Interim SW Safety Case
Agreed with the ISA and the Customer.
There will be several Interim Safety Cases, the first of which must be sufficiently advanced in terms of goals and evidence to be considered complete for the OSL and MSL.
An Interim Safety Case will precede the first Operational Safety Case for each Operational Clearance.
Presented at TRR
Supporting Evidence
The data obtained by the OFP of the data required by the function(s)
Data flow required by the function(s)
The performance of the function(s)
The output of the data by the OFP
OFP SW Architectural Design
Sub-System Hazard Analysis Report
Analyse the System Fault Trees to identify OFP behaviour which may contribute to a system hazard
Identify mitigation for SW failures
Identify system-level hazardous behaviour
System-Level Software Safety Objectives
Failures which may result in the breach of the SSSO and assumptions
Pilot and Engineering input used as necessary to correctly define the Derived Software Safety Constraints
Develop Accident Mitigation Strategies (platform)
Software Safety Requirements
SIL 'associated with the software safety requirements.
Pilot
To which the Operational Flight Programme (OFP) can contribute. Carried out for each identified system hazard associated with the Mission Systems Computer (MSC).
Capture the required behaviour of the OFP
Suitable to prevent the hazardous behaviour.

SW DESIGN

Application Layer Detailed Design

Application Layer Design Description

To cover:
Initial Application Manager partition design.
Detailed Design for a generic partition.
Global type definitions for data on the VCs
Detailed definition of VC contents
Details of time budgets for each partition together with schedule for each configuration

Software Design

Software Design Description

Microsoft Word, but UML for CSCI

UML supported by Rational Rose Real Time Studio Professional

One SDD for each functional application

Software Design Decision Log

3-layer software architecture

Use of Object Oriented Development

Software Product Specification

DRAFT version provided for Test Readiness Review

Software Development Plan

Produced in accordance with MA-STD-498 for a CSCI

Software Development

SA Approval

MA-STD-498

Prepare the Version Description

Software Version Document

DRAFT version provided for Test Readiness Review

Comply with the required format specified in MIL-STD-498 DID for an SVD

Contain instructions for the installation

Prepare the Executable Software

Prepare Software for Use

Analyse Source Code

SPARK Analysis

Unit Verification Plan

STMTAS - Which advocates the use of the VectorCAST unit test tool

Dynamic Analysis

Static Analysis

Both

Test

Code Review

Code Review Results

Analyse Code Review Results

STMTAS

STMTAS

Prior to the formal release of the software

Code Walkthrough

Agreed Software Changes

Software Development Team Leader
The Unit author
Around 2-3 reviewers selected from the software development team

STMTAS

Code/Design Review Checklist

Completed Checklist

Software Development File

Signed by the Software Team leader and authorising manager

Configuration Management Group

Software Test Report

Prior to being released for sub system and system qualification

CSCI Qualification Testing

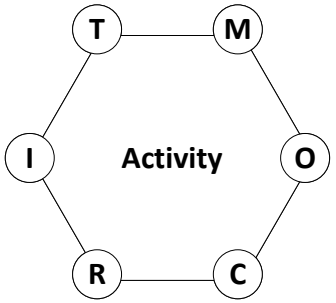
Software Version Document

Software Product Specification

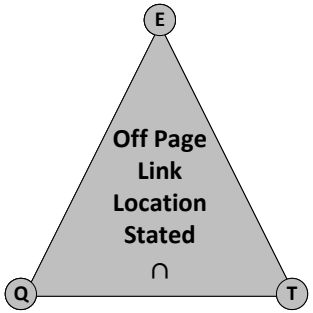
Test Readiness Review

Software Integration

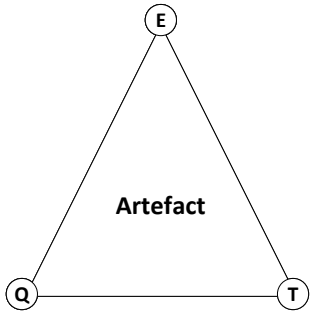
STMTAS



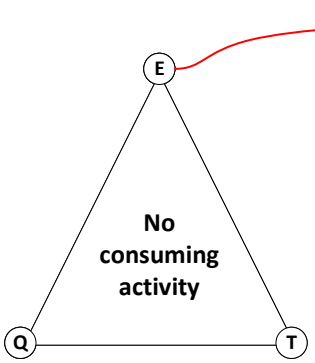
I: Input
T: Time
M: Method/Technique
O: Output
C: Control
R: Resource

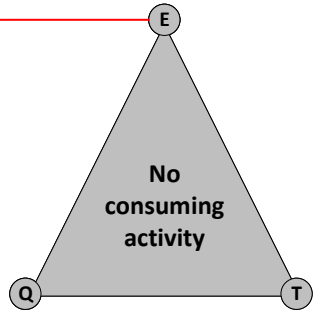


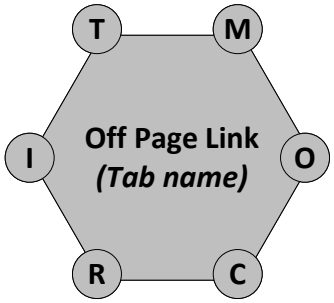
NOTES – when an artefact is not required

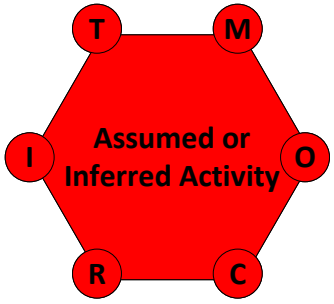


E: Existence
Q: Quality Criteria
T: Time









KEY