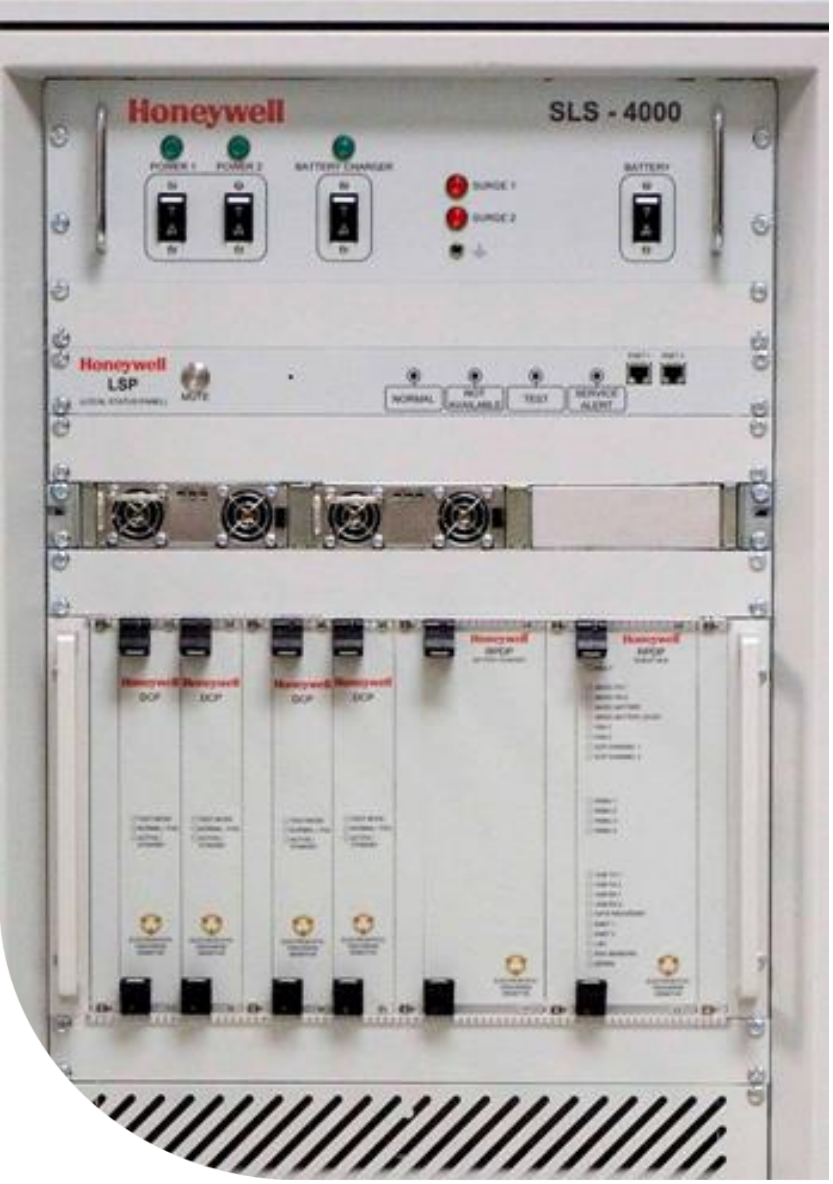
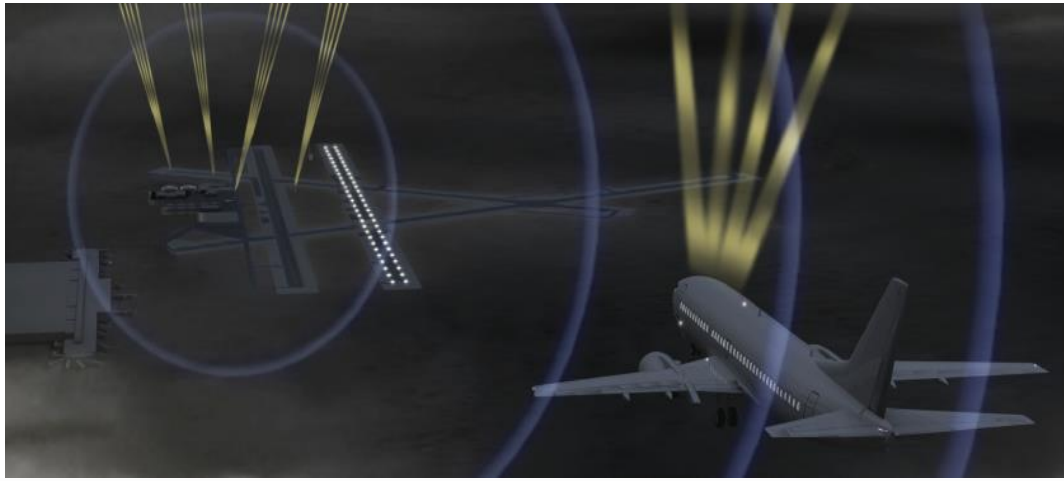




Seoul, Korea
3-5 June 2019

GBAS DESIGN SAFETY ASSURANCE

ICAO GBAS/SBAS Implementation Workshop

Honeywell SmartPath® SLS-4000 complies with the following Requirements and Standards

- ICAO SARPS International Civil Aviation Organization (ICAO) Annex 10, Volume I, Radio Navigation Aids, Sixth Edition (including amendments 1-87), July 2006
- EUROCAE/ED-109 Guidelines for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) System Software Integrity Assurance, 2002
- ICAO Doc. 8071 Volume II, Manual on Testing of Radio Navigation Aids, Fifth Edition, 2007
- FAA-E-3017 Category I Local Area Augmentation System Ground Facility, Non-Fed Specification, dated 29 September 2009
- FAA-E-AJW44-2937A Category I Local Area Augmentation System Ground Facility, Non-Fed Specification, dated 21 October 2005
- ICD-GPS-200C NAVstar GPS Space Segment/Navigation User Interfaces
- RTCA/DO-178B Software Considerations in Airborne Systems and Equipment Certification
- RTCA/DO-245A Minimum Aviation System Performance Standards for the Local Area Augmentation System (LAAS)
- RTCA/DO-246C GNSS-Based Precision Approach Local Area Augmentation System (LAAS) Signal-in-Space Interface Control Document (ICD)
- RTCA/DO-254 Design Assurance Guidance for Airborne Electronics Hardware
- RTCA/DO-278 Guidelines for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) System Software Integrity Assurance, 2002
- SAE/ARP-4754 Certification Considerations for Highly Integrated or Complex Aircraft Systems
- SAE/ARP-4761 SAE Aerospace Recommended Practice, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, December 1996

Honeywell

FAA GBAS Certification Phases

System Design Approval (SDA) – Manufacturer

- Ground station system design meets requirements
- Developed to appropriate design assurance levels

Facility Approval – Owner/ANSP/Airport

- Ground station installed
  - Safety Case for Installation (extrapolation of SDA safety case)
- Maintenance technicians trained, certified

Service Approval – Operator/Airline

- Aircraft equipped
- Pilot crews trained

Honeywell

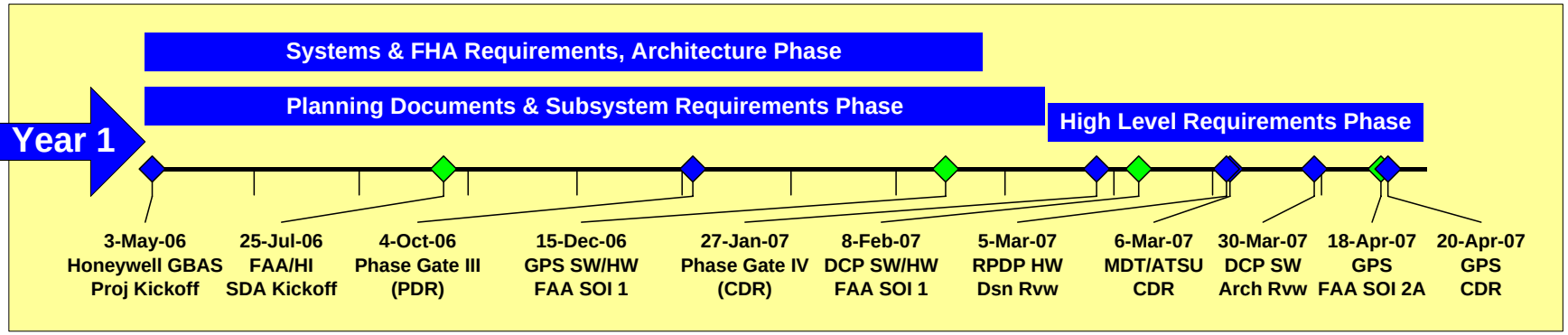
Dual-focus of SDA

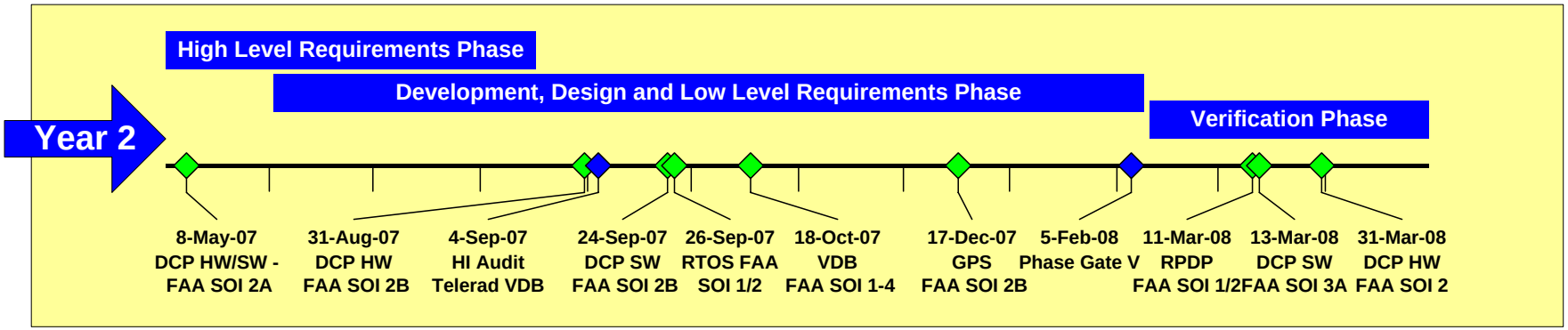
- Technical Correctness
  - Integrity of pseudorange correction, broadcast sigma
  - Fault modes, hazard mitigations, monitor perform (Pmd, Pfd)
    - Error source behavior, statistical distribution
  - Requirements correct, traceability, implemented correct
- Process Rigor
  - RTCA/DO-178B/278,-254, SAE/ARP 4754
  - Plan, Process, Summary
    - Approval (System level), Software, Hardware
  - Process compliance, artifact review
  - Configuration control, change management

The Process Assures System Safety

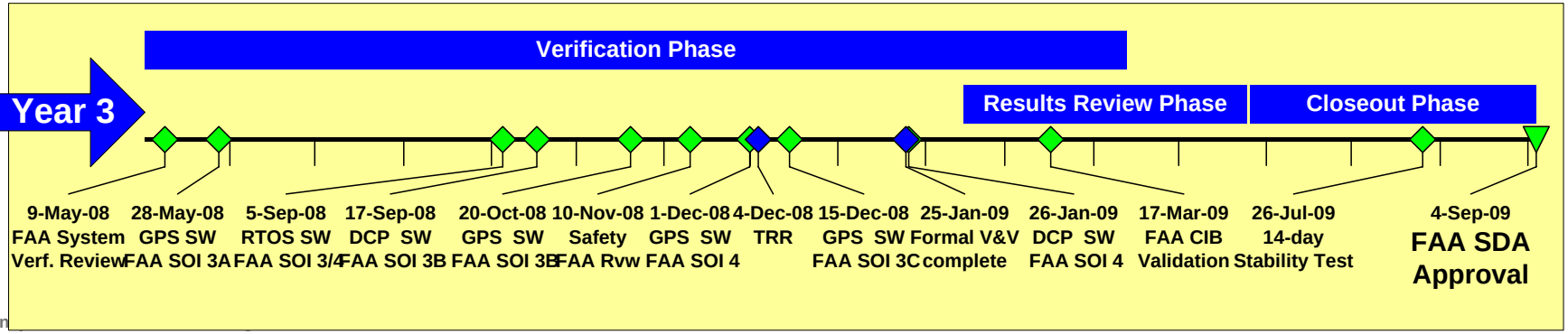
Honeywell

SmartPath™ SDA Development Milestones





FAA Audit Review Honeywell Design Activity



A Thorough Process with Predefined Checkpoints

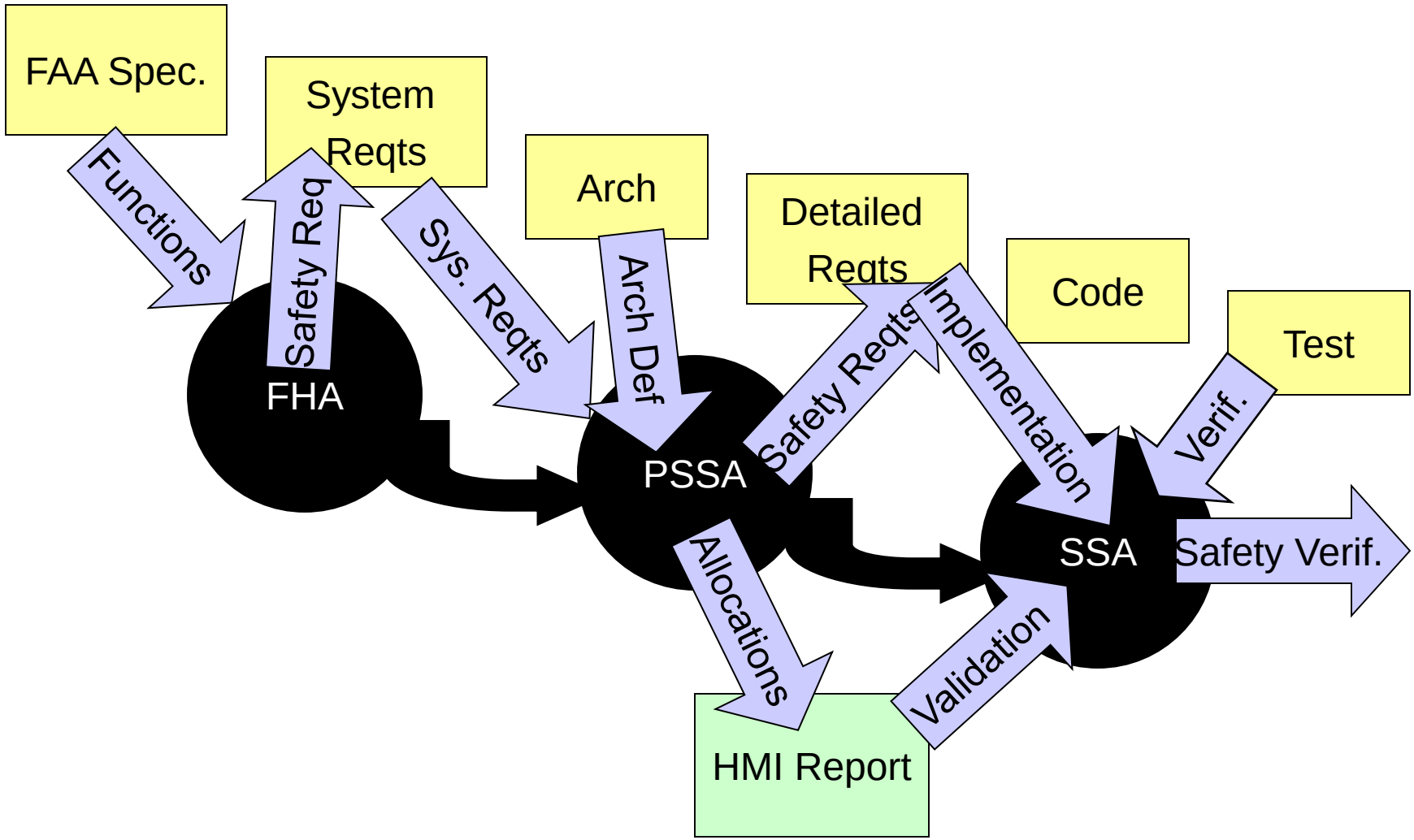
Safety Assurance Process

- The FAA's SDA Plan [14] recommends the safety process follows guidelines provided in SAE/ARP-4754 [21] and SAE/ARP-4761 [22].
- Honeywell's process relative to SLS-4000 defined in "LGF System Safety Assurance Program Plan" [2]
- Safety process is characterized by systematic evaluations performed at progressively lower levels of system abstraction
  - Functional Hazard Assessment (FHA) – Evaluates system functions
  - Preliminary System Safety Assessment (PSSA) – Evaluates proposed architecture
  - System Safety Assessment (SSA) – Evaluates final design

Safety discipline involved throughout development and verification processes

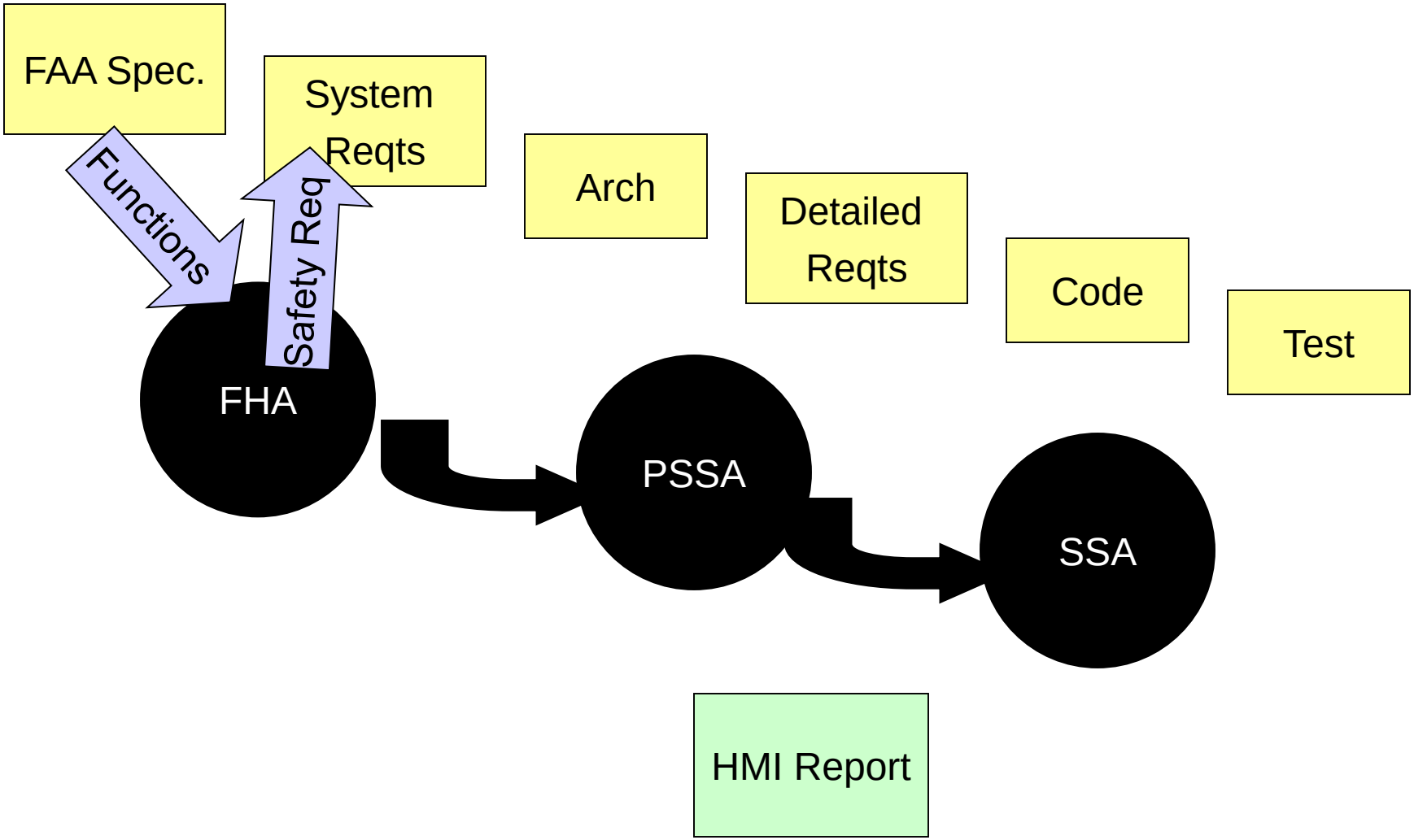
Honeywell

Safety Assurance Process



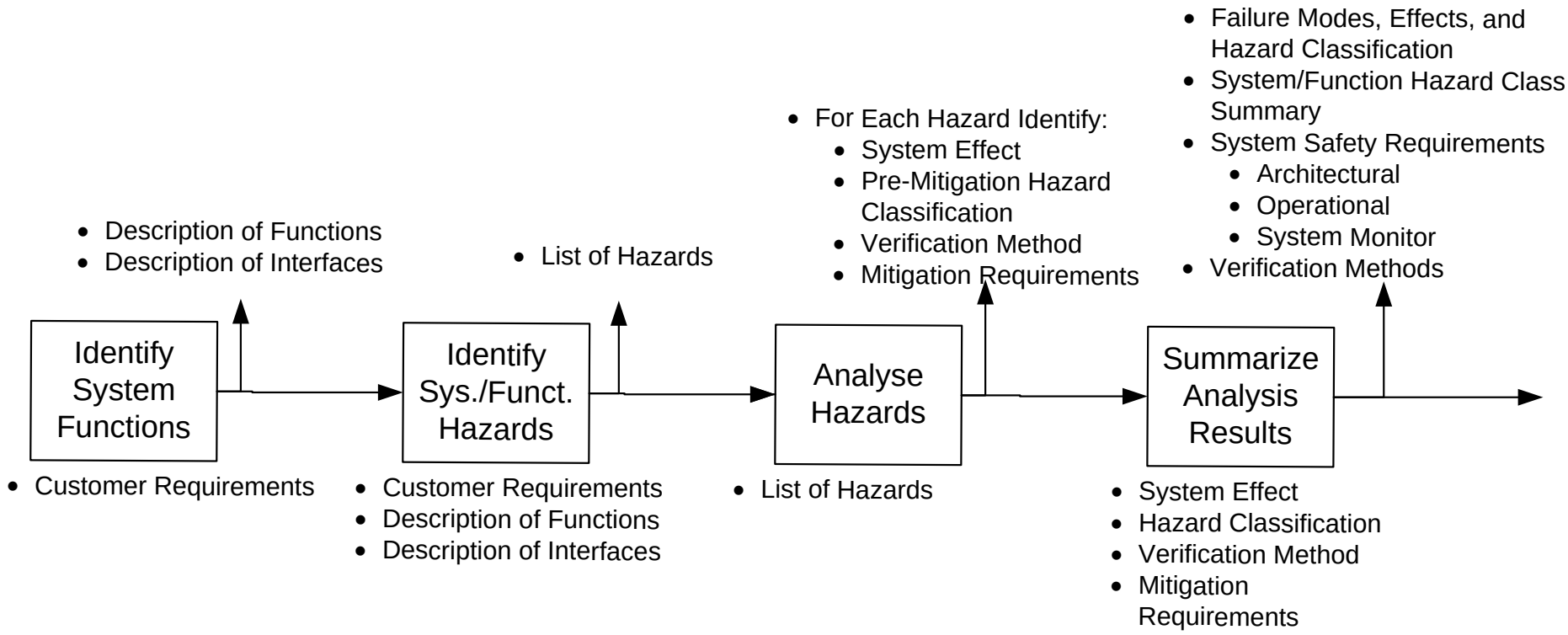
Honeywell

Safety Assurance Process - FHA



As an Example—Later Slides Show Process, not Details

Safety Assurance Process - FHA



For Each Assessment There is a Process Map

Safety Assurance Process - FHA

DATE: _____ SYSTEM FUNCTIONAL HAZARD ASSESSMENT (FHA) PREPAREDBY: _____

SYSTEM: LAAS REVIEWED BY: _____

Function	Failure Condition (Hazard Description)	Effect of Failure Condition on System	Hazard Classification	Reference to Supporting Material	Verification Method

HAZARD CLASSIFICATION

Class I: Catastrophic Class II: SevereMajor Class III: Major

Class IV: Minor Class V: No Effect

Forms to be Completed for Each Assessment

Safety Results - FHA

- Safety Definitions
  - Integrity – The probability of transmitting out-of-tolerance navigation data for 3-seconds or longer in any 150-second interval
  - Continuity – The probability of an unscheduled interruption of the VHF transmission for 3-seconds or longer in any 15 second interval
  - Availability – The proportion of time during which service is provided, computed over a long period (typically a year)

Safety Results - FHA

- Severe-Major Hazard Classification
  - Approach Integrity due to LGF failure, anomalous environmental or atmospheric effects – 1.5×10^{-7} in 150-seconds
  - Approach Integrity under fault free or no more than Reference Receiver fault – 5×10^{-8} in 150-seconds
- Minor Hazard Classification
  - Unscheduled interruption of VDB transmission (Loss of Continuity) – 1.0×10^{-6} in 15-seconds
  - Unscheduled loss of sufficient Reference Receivers or Ranging Sources (Loss of Continuity) – 2.3×10^{-6} in 15-seconds
  - Availability – 0.99

LGF Specification safety requirements validated

Results are Classified by Severity

Safety Results - FHA

- Minor Hazard Classification
  - VDB Operates in a manner that could interfere with nearby LGF system for 1 second – 5.0×10^{-7} in 30-seconds. This encompasses:
    - VDB Power 3 dB above assigned power level (LGF Requirement)
    - VDB transmission outside of TDMA time slots (LGF Requirement)
    - VDB transmission outside of assigned frequency (Derived Requirement)
  - VDB transmission exceeds unwanted or adjacent channel emissions for 1-second – 1.0×10^{-2} in 30-seconds (Derived Requirement)
  - VDB Power 3 dB above assigned power level for 1 second – 2.0×10^{-7} in 30-seconds
  - VDB transmission outside of TDMA time slots for 1-second – 1.0×10^{-7} in 30-seconds

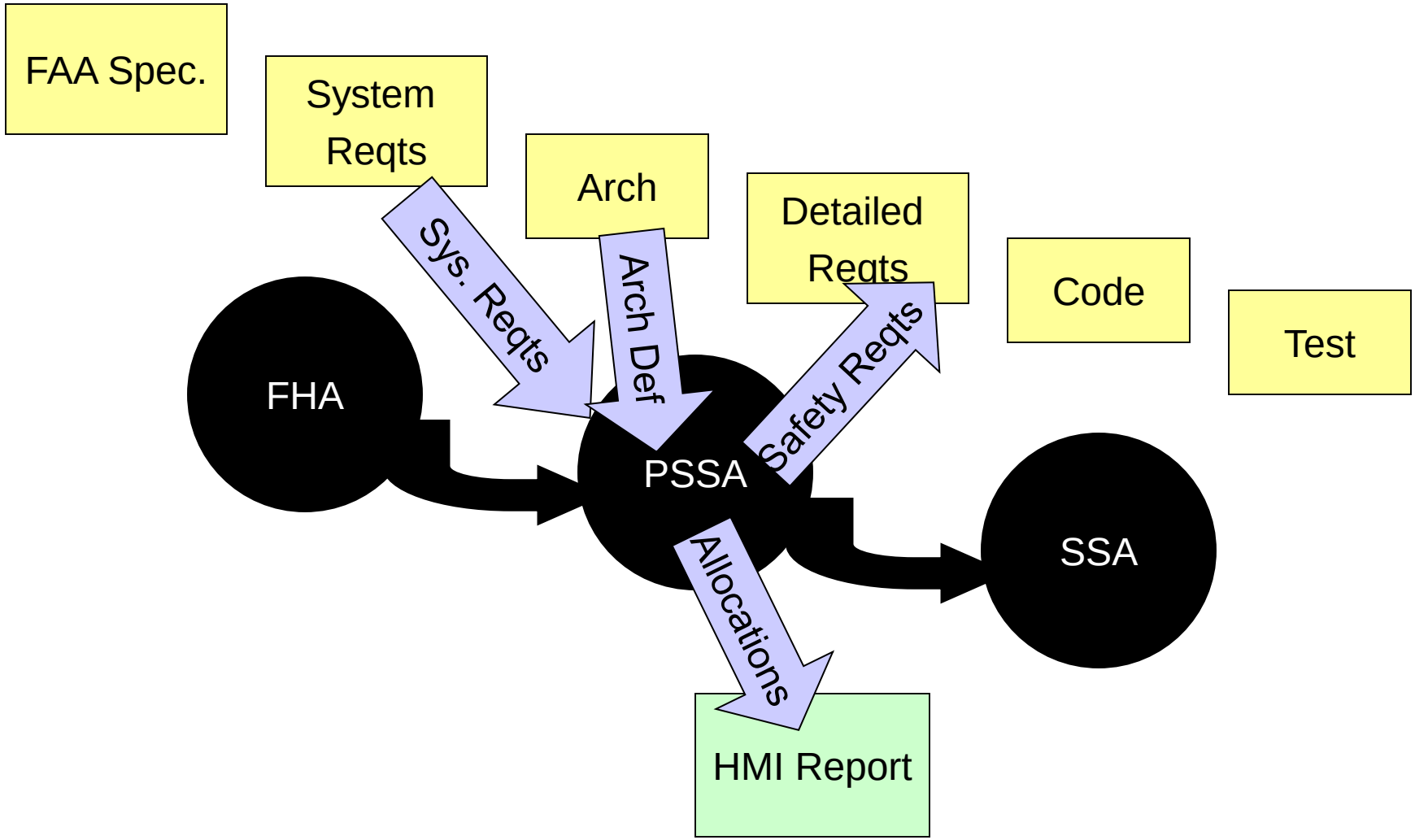
Derived Safety Requirements

Honeywell

Safety Results - FHA

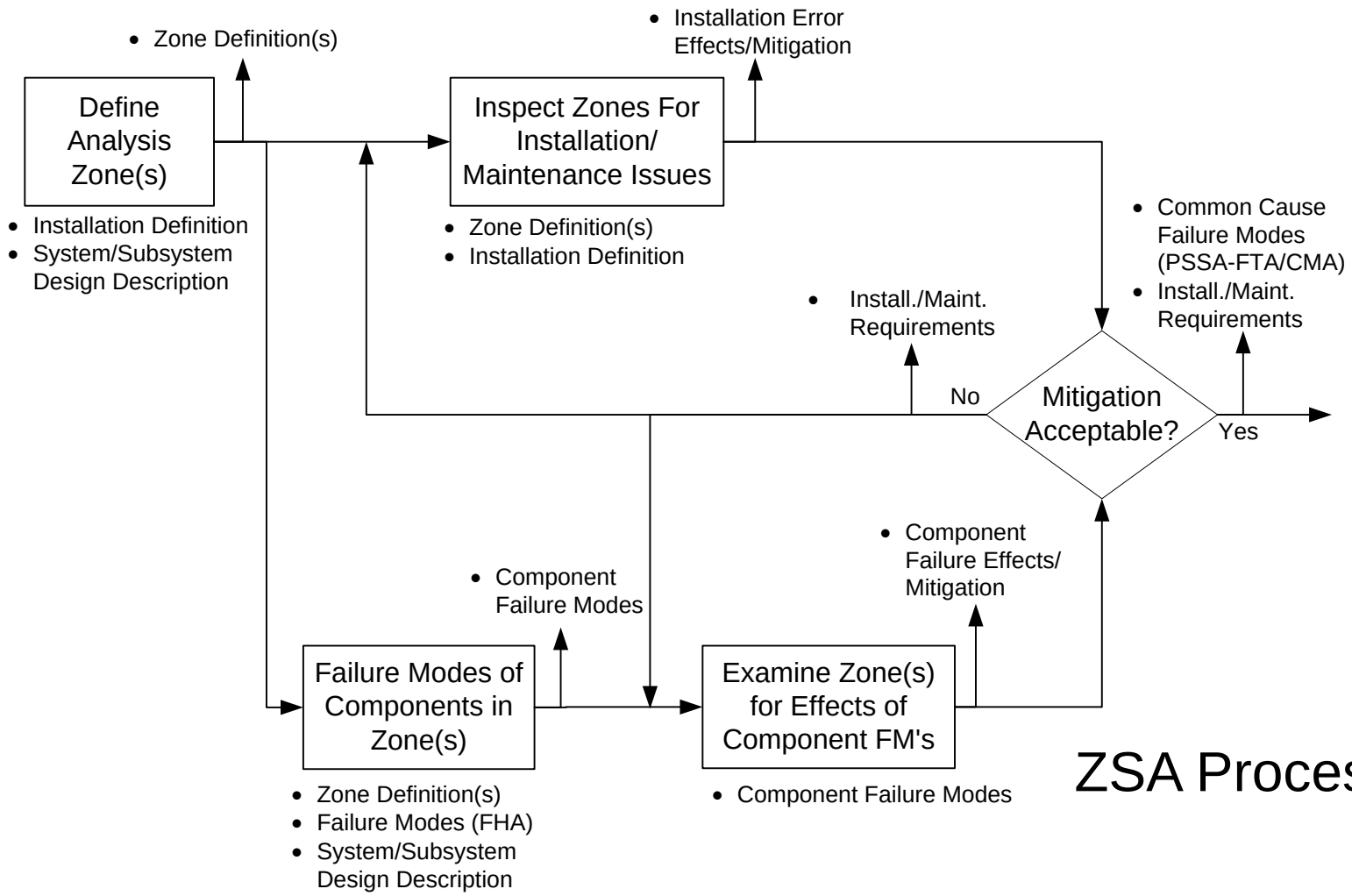
- LGF Hazard Classifications by System Function:
  - Primary/Secondary Power (Severe-Major)
  - LGF Correction Processor/Integrity Monitor (Severe-Major)
  - Reference Receiver (Severe-Major)
  - VDB Transmitter (Minor)
  - VDB Monitor (Minor)
  - VDB Antenna (Severe-Major)
  - LSP (Minor)
  - MDT (Severe-Major)
  - ATSU (Minor)
  - Data Recorder (No Effect)
  - Environmental Sensor (Minor)

Preliminary System Safety Assessment (PSSA)



PSSA/System Requirements→Detailed Requirements

Safety Process – PSSA/ZSA



ZSA Process Map

Honeywell

Safety Process – PSSA/ZSA

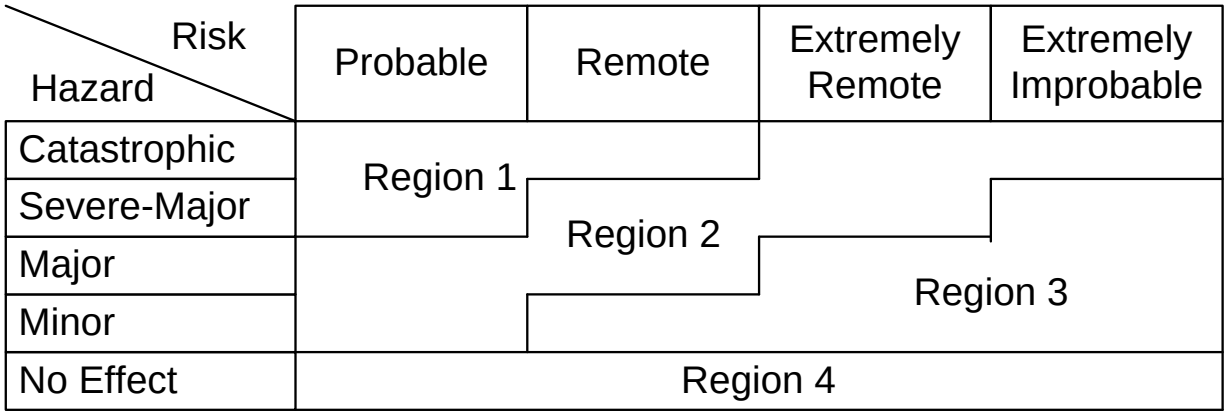
ZSA Form

SYSTEM:			ZONE:	ANALYST:
ID #	Source	Hazard	Effect	Mitigation
1-1				
1-2				
1-3				
1-4				
1-5				
1-6				

Honeywell

Safety Process – PSSA/PRA

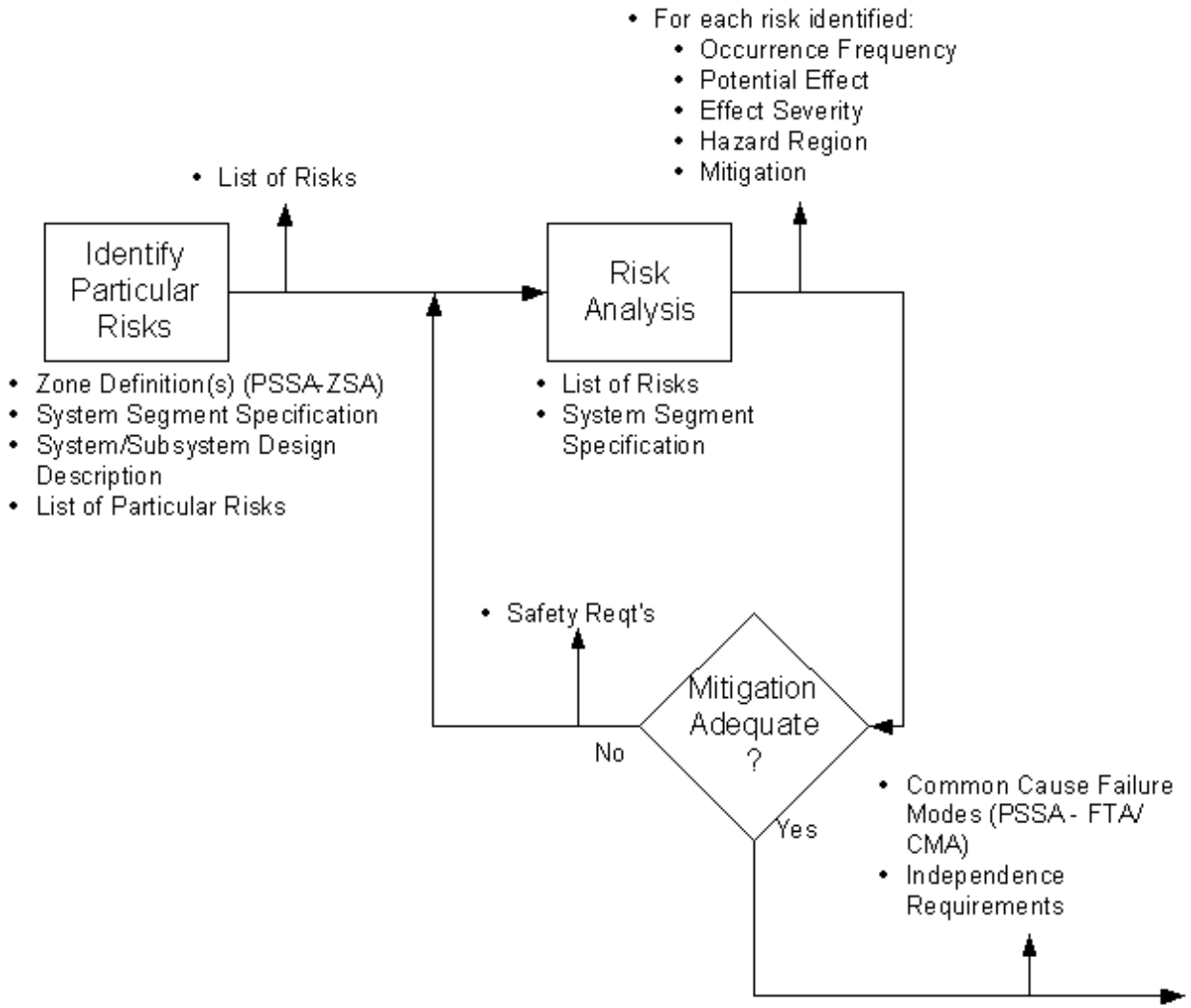
- Analysis
  - Assess pre and post mitigation against hazard/risk index



  - Region 1: Design action required to eliminate or control hazard
  - Region 2: Hazard must be controlled or hazard probability reduced
  - Region 3: Hazard control desirable
  - Region 4: Hazard control not necessary

Honeywell

Safety Process – PSSA/PRA



Process Map

Honeywell

Safety Process – PSSA/PRA

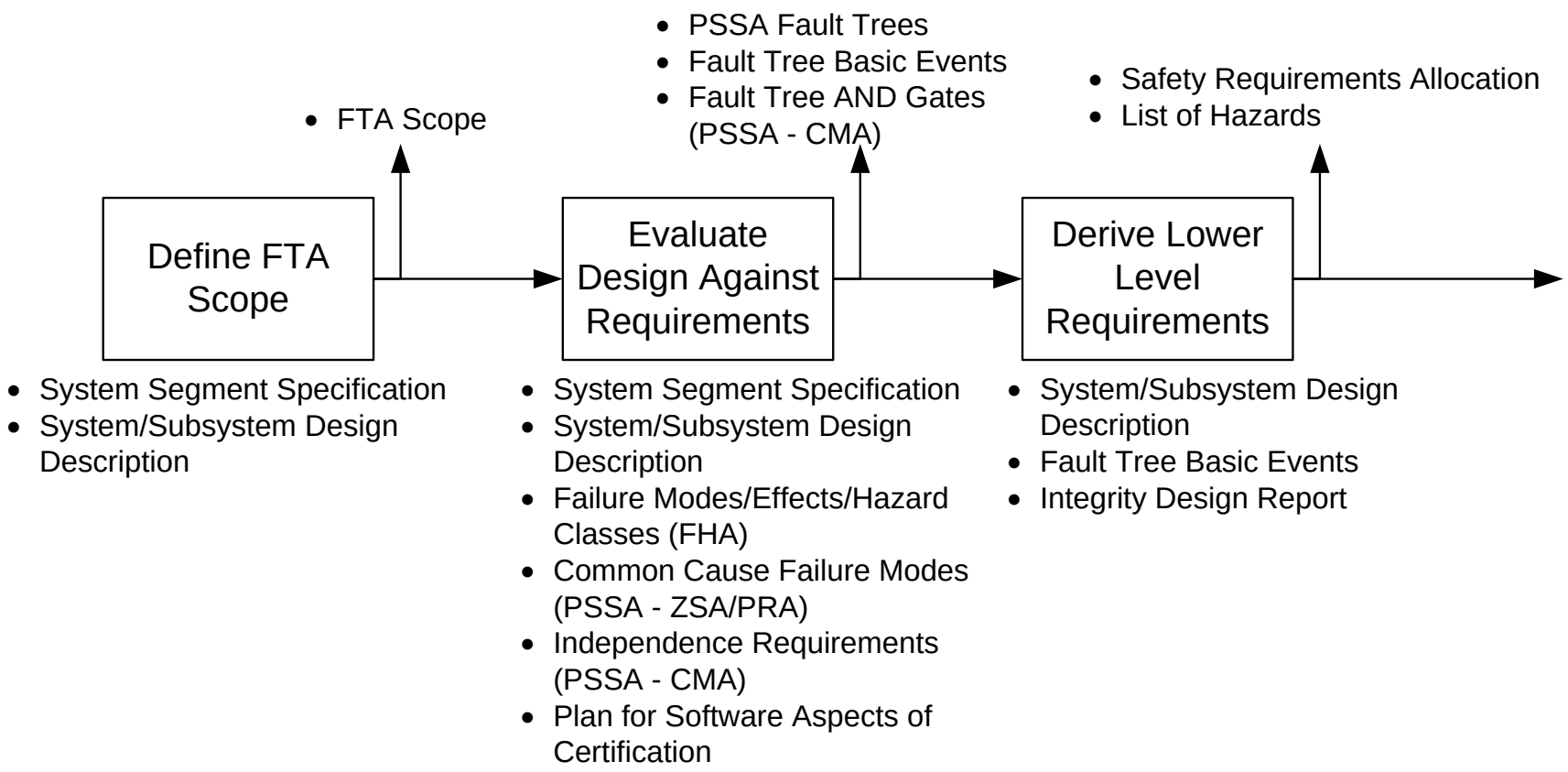
PRA Form

Particular Risk Analysis - DGPS (Zone 1)									
RISK ID NO.	PARTICULAR RISK DESCRIPTION	FREQ. RANK	EFFECT OF RISK ON SYSTEM	SEV. RANK	HAZ. REGION	SYSTEM MITIGATION	FREQ. RANK	SEV. RANK	HAZ. REGION
1-1									
1-2									

Honeywell

Safety Process – PSSA/FTA

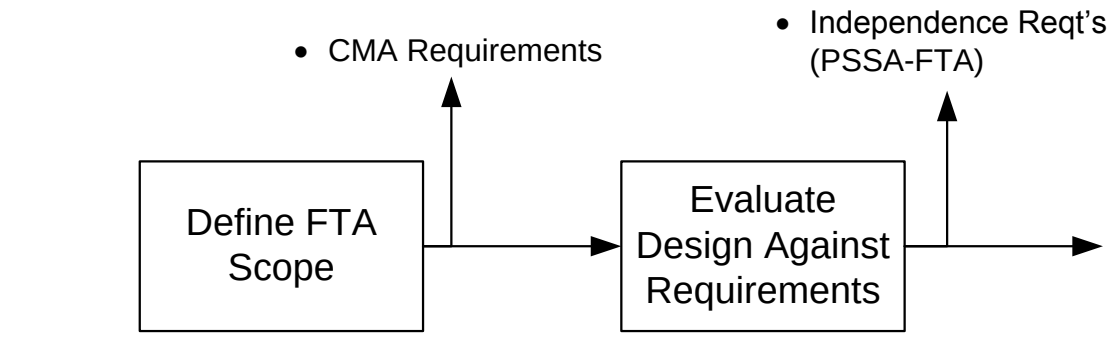
FTA Process Map



Honeywell

Safety Process – PSSA/CMA

CMA Process Map

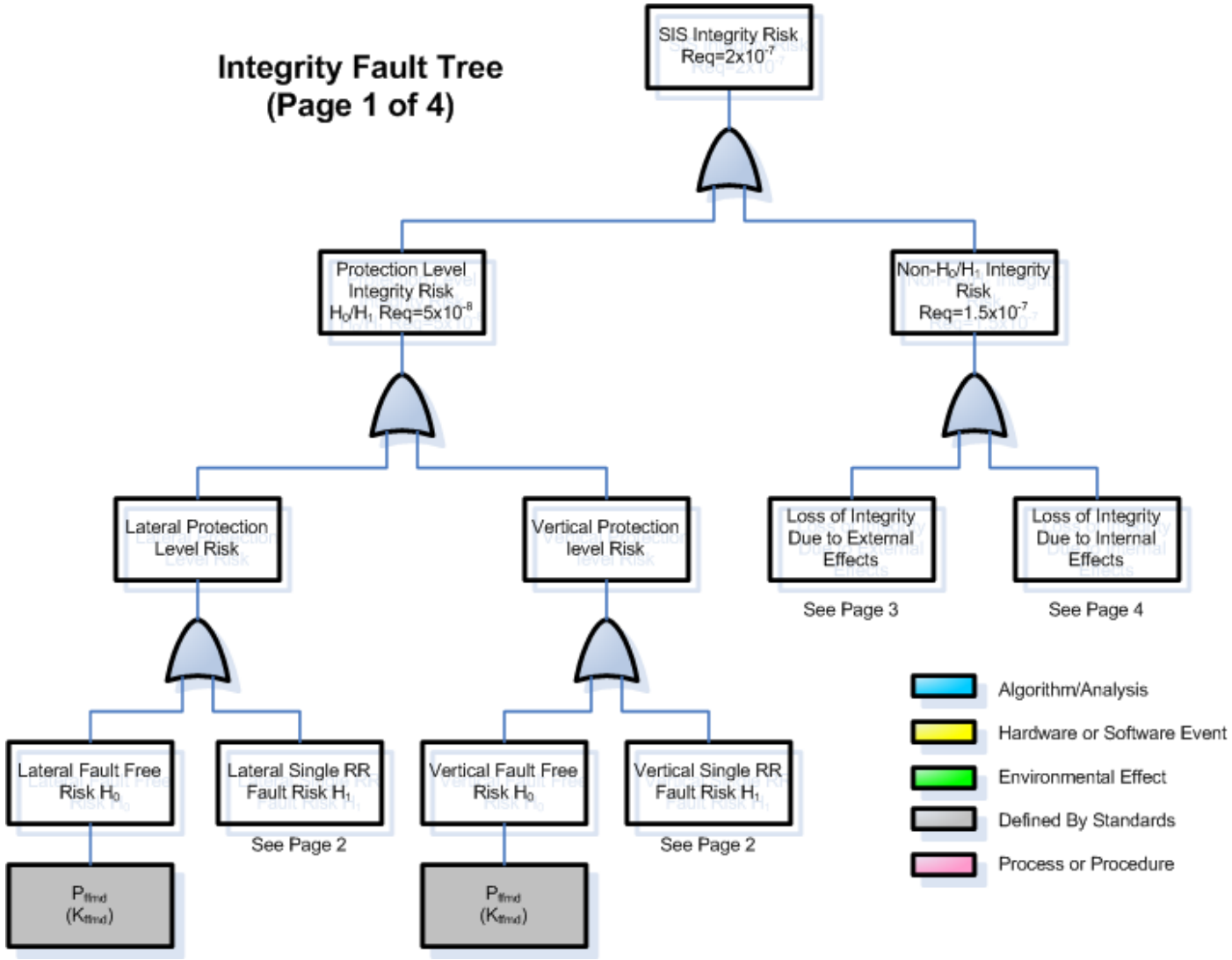


- System Segment Specification
- System/Subsystem Design Description
- Fault Tree AND-Gates (PSSA-FTA)
- CMA Checklist

- CMA Requirements
- System Segment Specification
- System/Subsystem Design Description
- Common Cause Failure Modes (PSSA-ZSA/PRA)

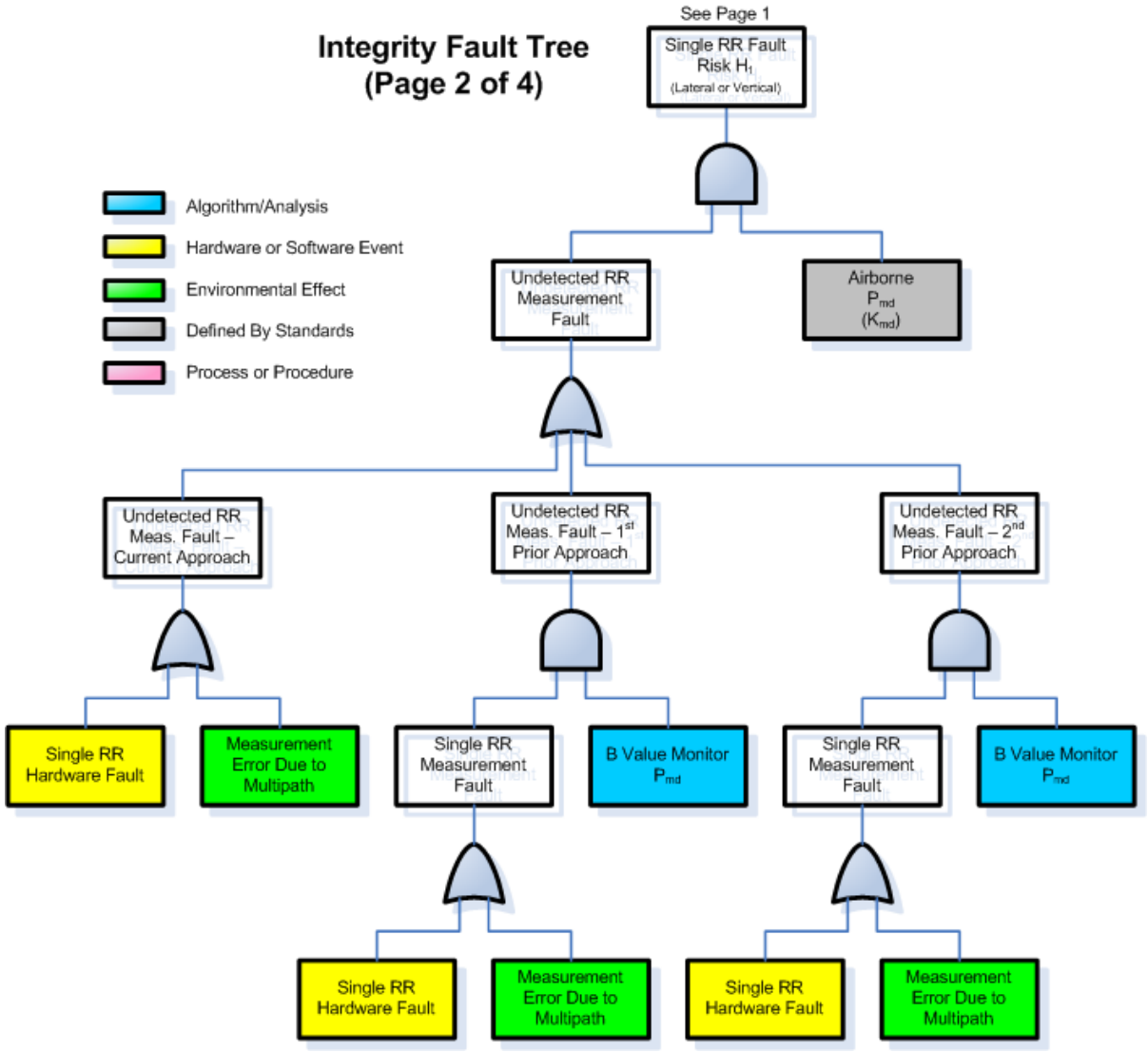
Honeywell

Safety Results – PSSA



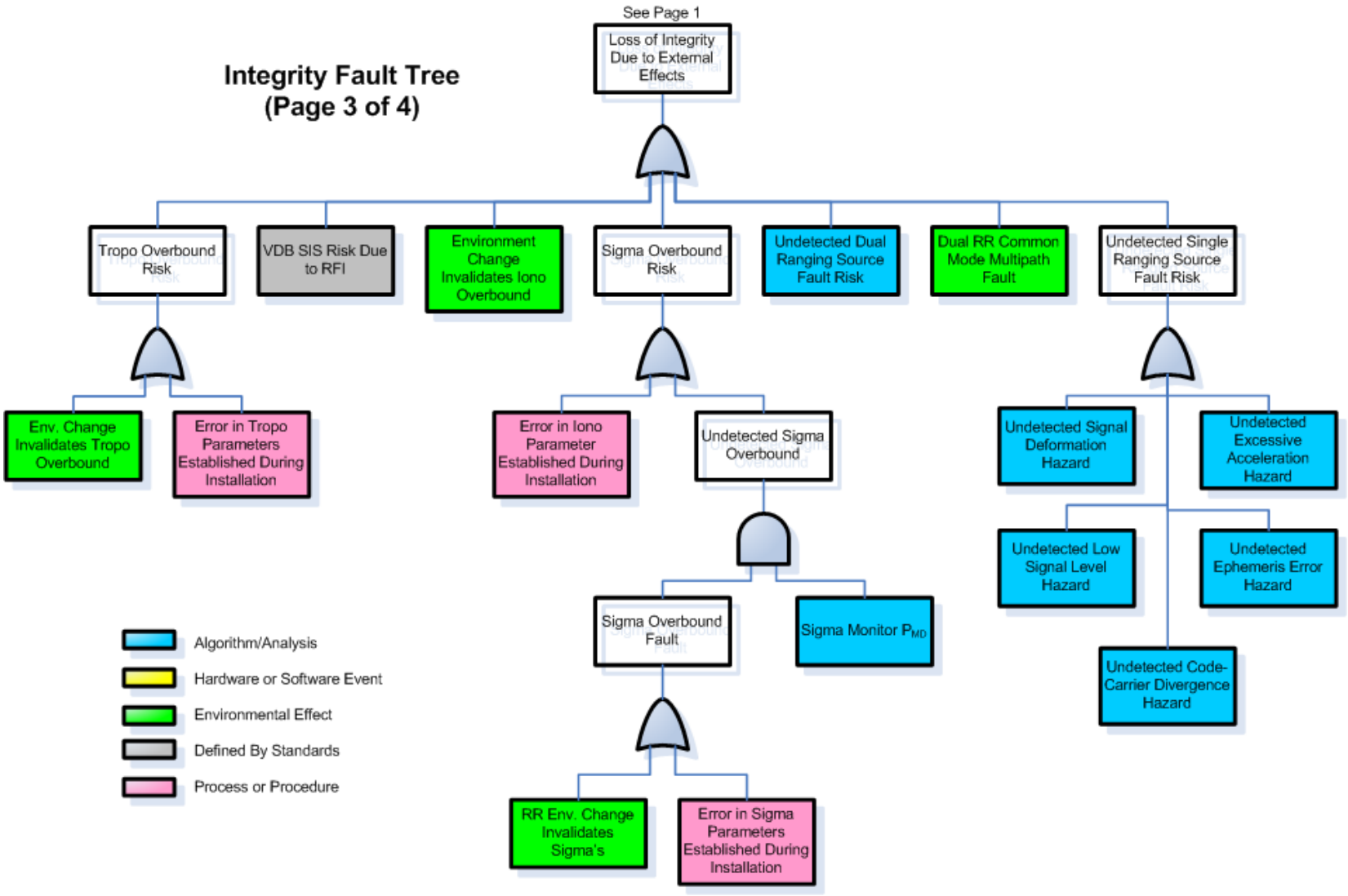
Assessment Results are Published and Reviewed

Safety Results – PSSA



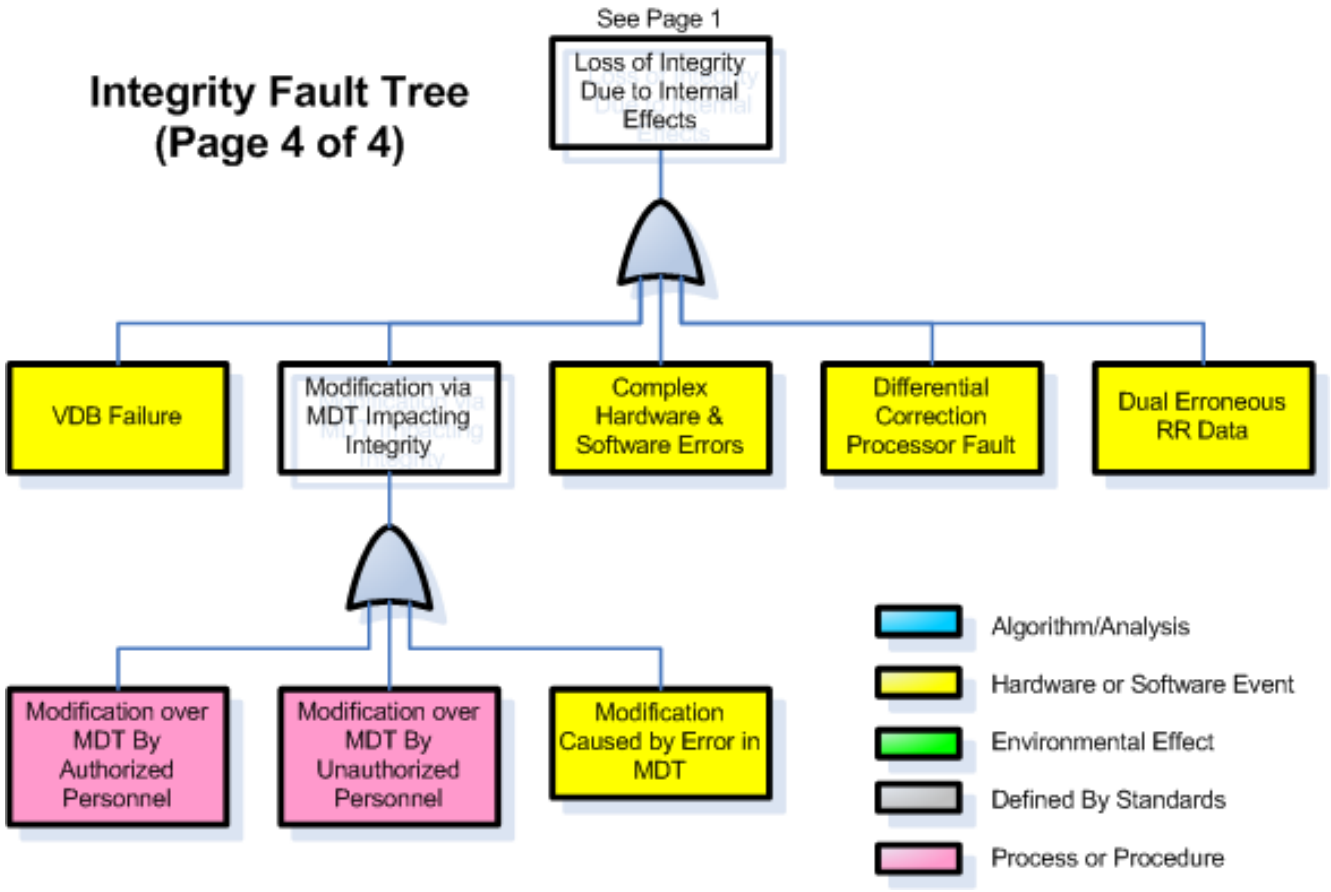
Honeywell

Safety Results – PSSA



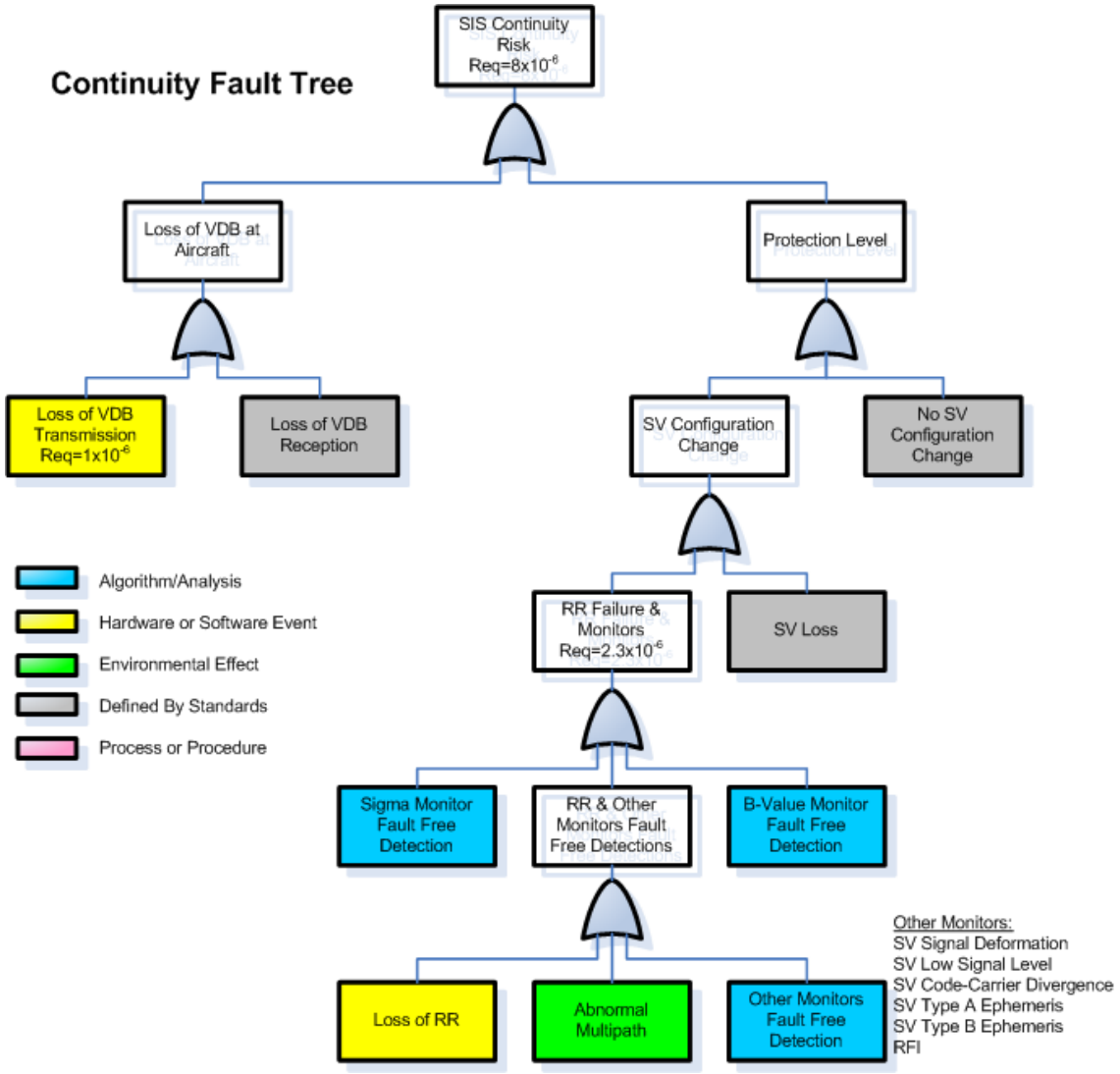
Honeywell

Safety Results – PSSA



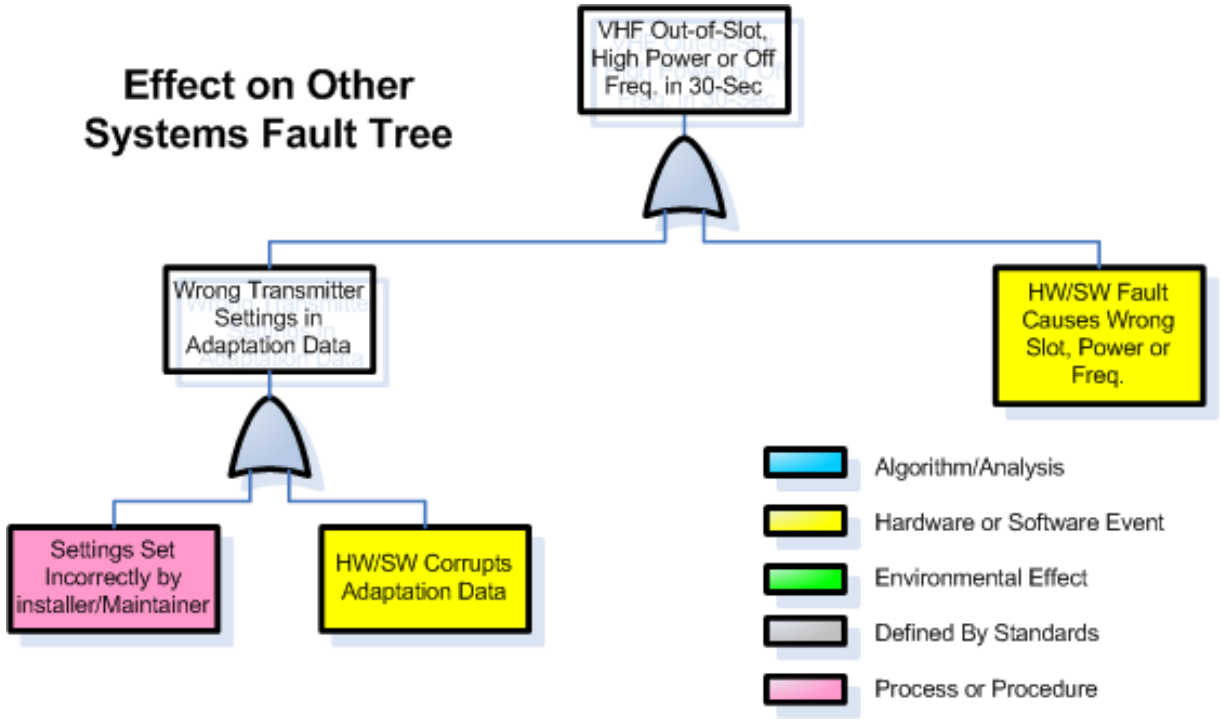
Honeywell

Safety Results – PSSA



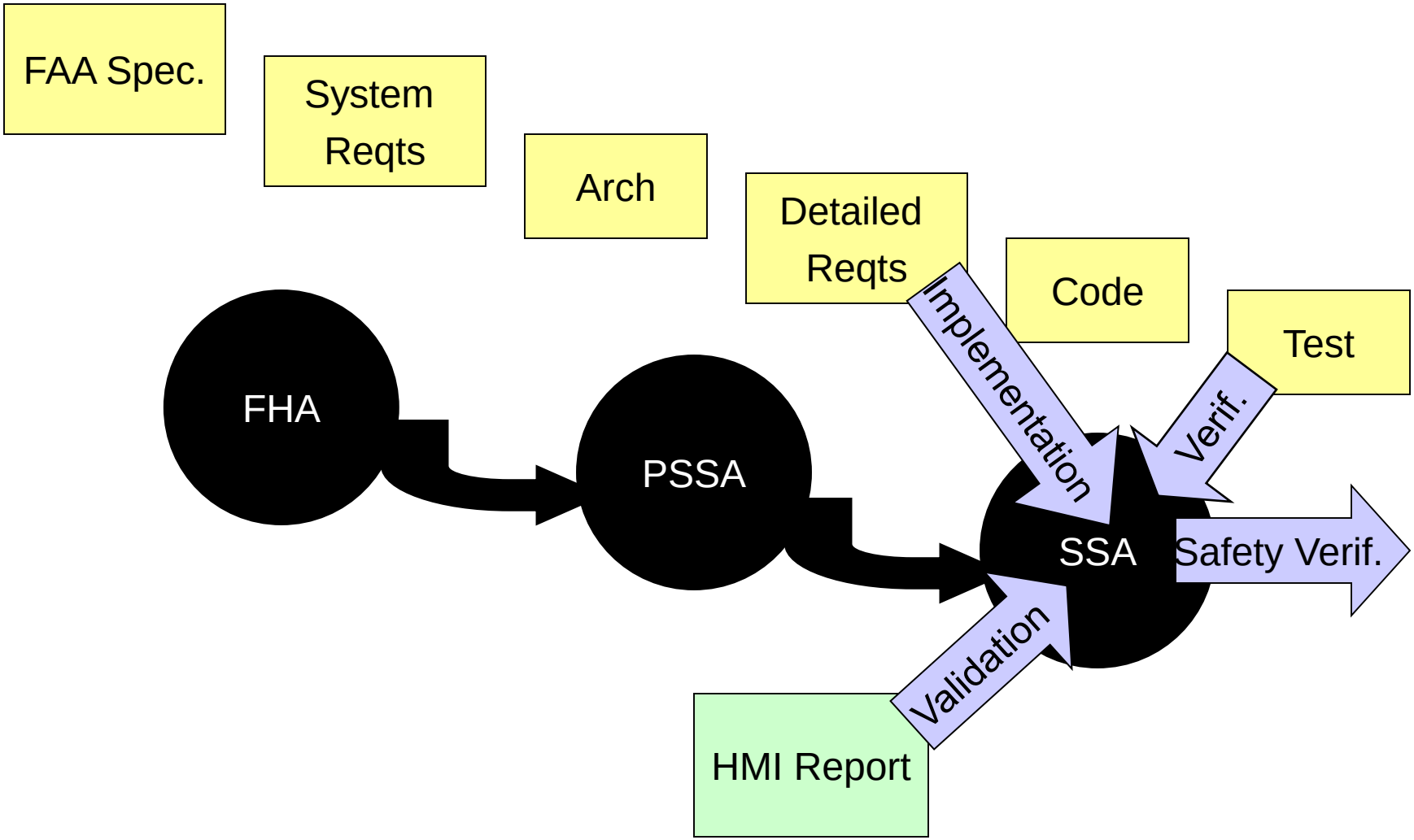
Honeywell

Safety Results – PSSA



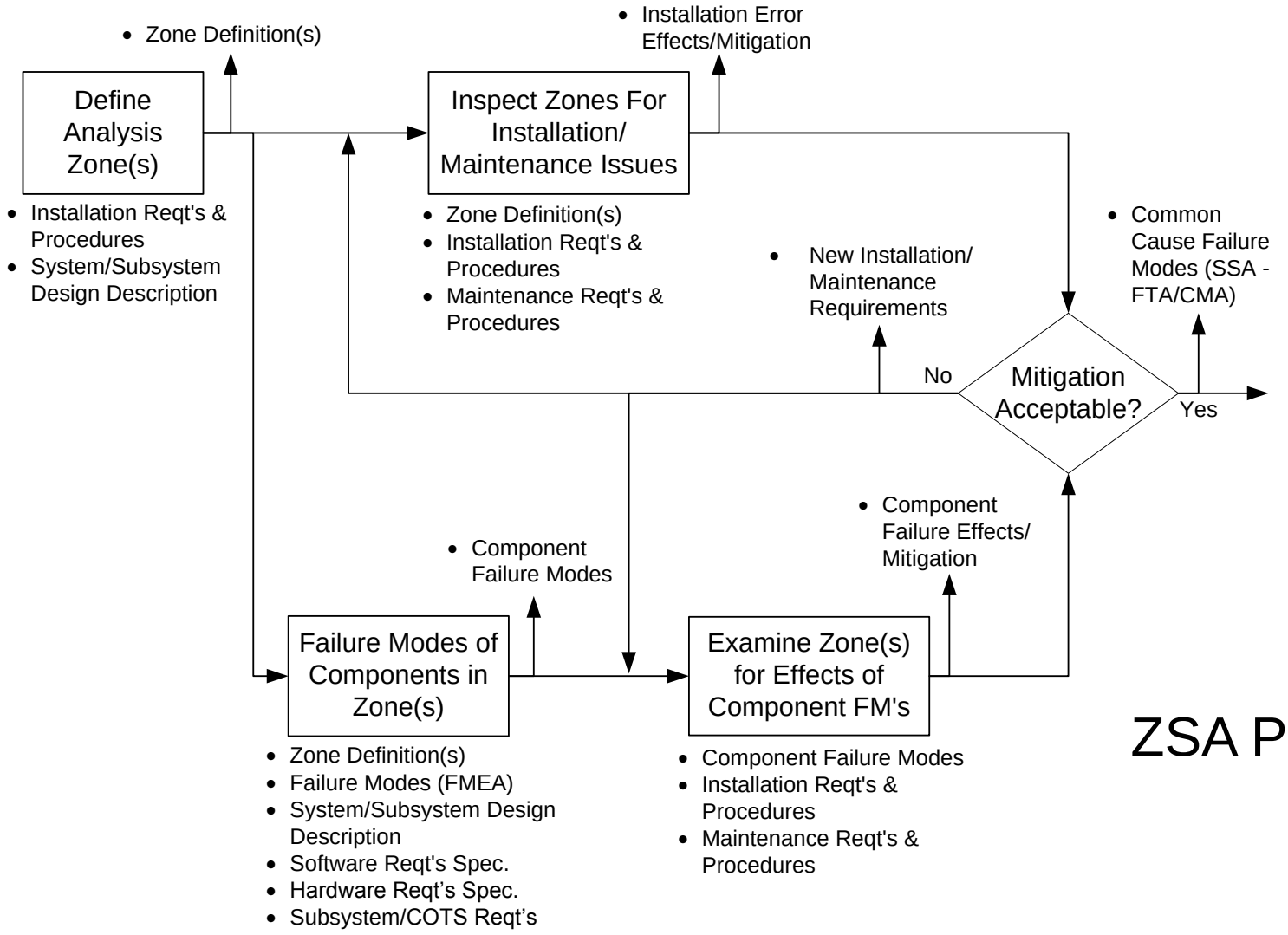
Honeywell

Safety Process - SSA



System Safety Analysis based on Detailed Requirements

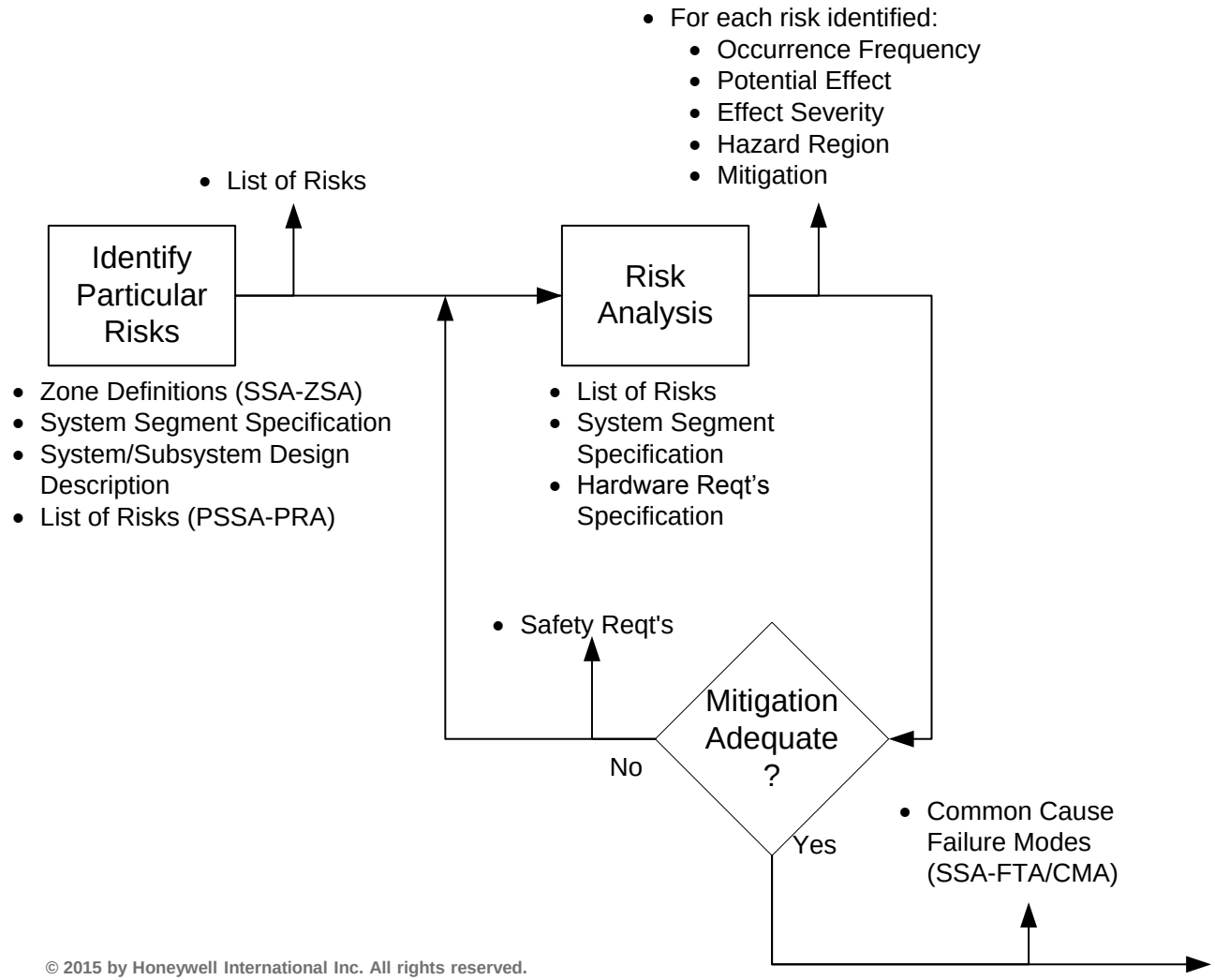
Safety Process – SSA/ZSA



ZSA Process Map

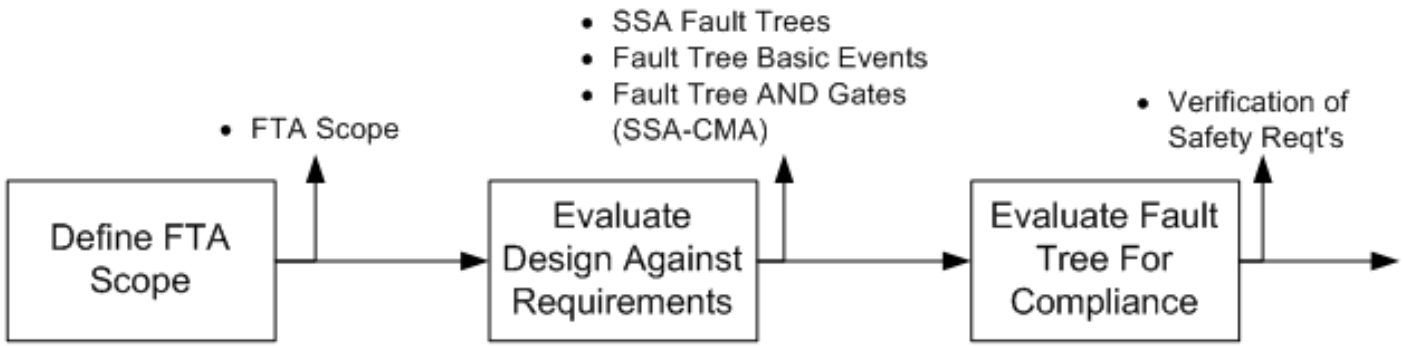
Honeywell

Safety Process – SSA/PRA



As in PSSA, Each SSA Assessment has a Process Map

Safety Process – SSA/FTA



- System Segment Specification
- System/Subsystem Design Description
- System Level Safety Reqt's (FHA, PSSA)

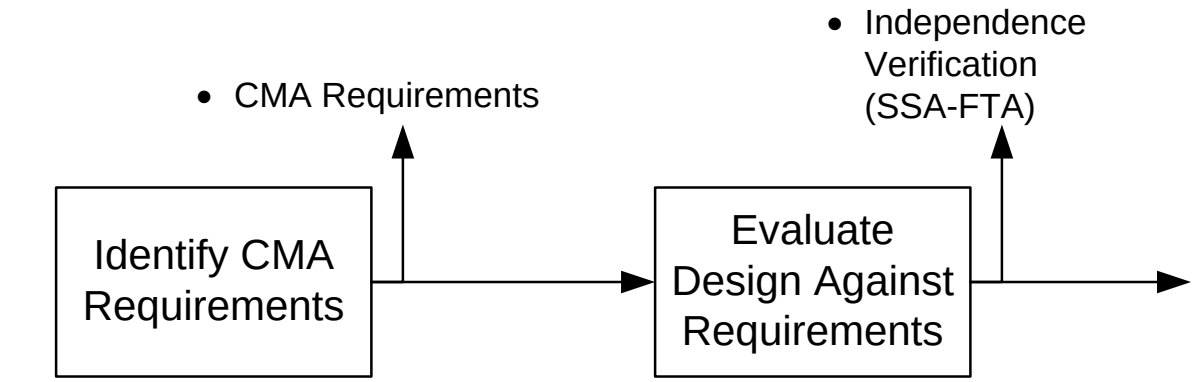
- System Segment Specification
- System/Subsystem Design Description
- Hardware Requirements Spec.
- Software Requirements Spec.
- Software Design Description (SDD)
- Subsystem/COTS Requirements
- Installation Guide
- Maintenance Manual
- Verification Documents
- Fault Trees (PSSA-FTA)
- Failure Modes/Effects/Detection/New Hazards (FMEA)
- Common Cause Failure Modes (SSA-ZSA/PRA)
- Independence Reqt's (SSA-CMA)
- Failure Modes/Failure Rates (FMEA)
- Reliability Prediction Report
- Fault Tree Basic Events
- Integrity Design Verification Analyses

- Minimal Cut Set Tool

FTA Process Map

Honeywell

Safety Process – SSA/CMA



CMA Process Map

Honeywell

Safety Process – Personal Safety

- Purpose: Analyze potential personal hazards with interfaces that could occur throughout the products life cycle including: operator, maintainer, installer and transportability.
- Program Requirements:
  - The FAA specification [15] stipulates that the ground subsystem is to meet the Personal Safety and Health requirements in section 3.3.5 of the Electronic Equipment, General Requirements document [17].
  - Honeywell elected to get a CE mark on the SLS-4000 which stipulates personal safety requirements.
- Approach
  - CE Mark compliance performed by independent party. Due to commonality with FAA requirement for personal safety, elected to include them with compliance being performed by independent party.

Safety Process – Personal Safety

- Requirements Overview (# of requirements)
  - General (7)
  - Electrical Safety (56)
  - Laser Radiation (3)
  - Switches (8)
  - Mechanical Hazards (13)
  - Markings, Signs, Tags and Symbols (46)
  - Hazardous and Restricted Materials (13)
  - Seismic Safety (6)
- Results – All applicable tests Passed
- The Personnel Safety Hazard Analysis Report [4] was prepared as part of the original Block 0 SDA program.

Honeywell

SITING/INSTALLATION & SAFETY

- Many of the derived safety requirements identified in the SSA relate to installation or operational requirements (See SSA results).
- The derived safety requirements trace to an installation requirements book in the requirements database.
- Compliance with these requirements is shown by contents of one or more of the following documents:
  - GBAS Siting Plan [12]
    - Defines the processes for selecting an installation site for the Honeywell SLS-4000.
  - GBAS Measured Site Data (MSD) Process [11]
    - Defines the procedures and acceptance criteria for creating an installation specific Measured Site Data loadable binary file.
  - GBAS SLS-4000 Commercial Instruction Book [6]
    - Defines all procedures required for installation, operation and maintenance of the Honeywell SLS-4000.

Questions Asked:

- How the key performances requirements (Accuracy, Continuity, Availability, Integrity, Time to Alarm) are demonstrated to the SBAS/GBAS operator for acceptance ? Which means are used : collection of data, simulation,… ?—Please see preceeding pages
- How GBAS is handling ionosphere corrections around equator ? What are the challenges ?
  - Honeywell Block II software Provides Configurability Options
    - Allows for a user-defined iono threat model
      - Enables improved availability in all geographies
    - Allows for automatic user-defined GLS approach procedures for a specific time period
      - Motivated by low latitudes – Set up to broadcast only during specific time periods
- How unavailability of performances is communicated to the users ?
  - Monitor Vertical Protection limits based on threat model (developed from 12-month data collection and analysis)
  - Though no specific monitors to warn in GAST-C system, when number of satellites with acceptable signals drops below 5, SLS-4000 would not transmit an acceptable solution and aircraft will show GLS not available.
  - ATSU will show GBAS unavailable

Acronyms

- AL – Assurance Level
- ARP – Aerospace Recommended Practices
- ASCII – American Standard Code for Information Interchange
- ATSU – Air Traffic Status Unit
- BB – Broadband
- CCD – Code Carrier Divergence
- CE – Conformity European
- CI – Configuration Item
- CIB – Component Instruction Book
- CMA – Common Mode Analysis
- COTS – Commercial Off The Shelf
- CRC – Cyclic Redundancy Check
- DAL – Design Assurance Level
- DCP – Differential Correction Processor

Honeywell

Acronyms

- EA – Excessive Acceleration
- EMI – Electromagnetic Interference
- FCM – Fault Containment Module
- FHA – Functional Hazard Assessment
- FM – Failure Modes
- FMEA – Failure Modes & Effects Analysis
- FT – Fault Tree
- FTA – Fault Tree Analysis
- GBAS – Ground-Based Augmentation System
- GPS – Global Positioning System
- HMI – Hazardously Misleading Information
- HW – Hardware
- ICAO – International Civil Aviation Organization

Honeywell

Acronyms

- Kffmd – Fault Free Missed Detection K-factor
- Kmd – Missed Detection K-factor
- LAAS – Local Area Augmentation System
- LAN – Local Area Network
- LGF – LAAS Ground Facility
- LP – Low Power
- MDT – Maintenance Data Terminal
- Pffmd – Fault Free Missed Detection Probability
- Pmd – Missed Detection Probability
- PRA – Particular Risk Analysis
- PSSA – Preliminary System Safety Assessment
- RFI – Radio Frequency Interference
- RPDP – Robust Power Distribution Panel
- RR – Reference Receiver

Honeywell

Acronyms

- SAE – Society of Automotive Engineers
- SARPS – Standards and Recommended Practices
- SDA – System Design Assurance
- SDM – Signal Deformation Monitor
- SIS – Signal-in-Space
- SLS – Satellite Landing System
- SSA – System Safety Assessment
- SV – Satellite Vehicle
- SW – Software
- TDMA – Time Division Multiple Access
- TX – Transmitter
- VDB – VHF Data Broadcast
- VSWR – Vertical Standing Wave Ratio
- ZSA – Zonal Safety Analysis

Honeywell