

STPA and Requirement Decomposition for Assurance

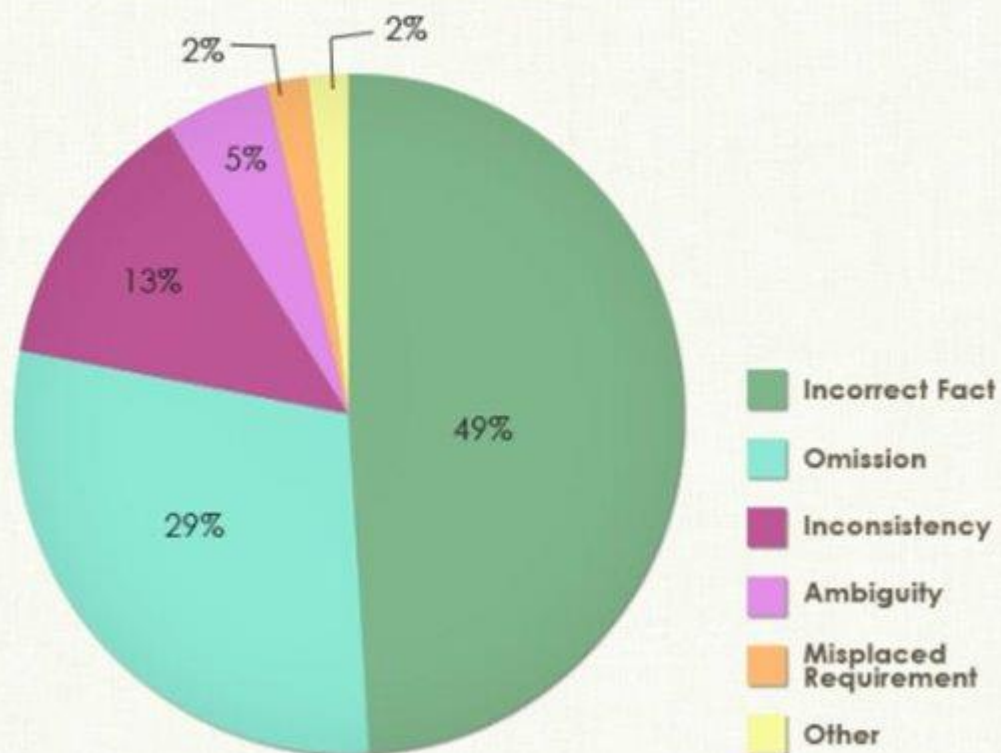
STAMP Workshop 2026

Steven King
Colby Van Orden
Anthony Waters
STPA Engineering Department

March 2026

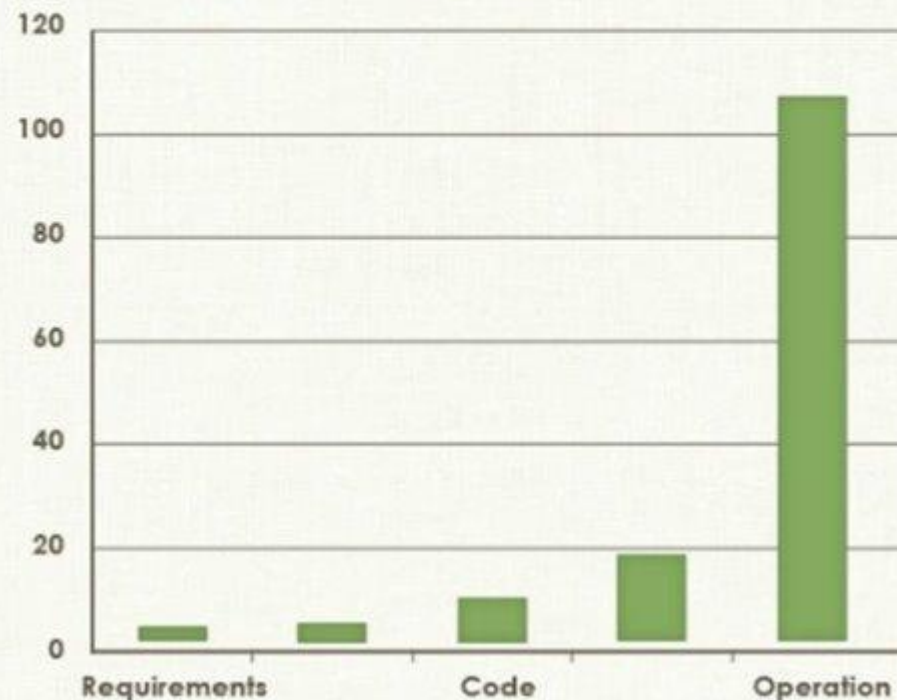
Majority of defects originate in requirement definition Improved Requirements = Big Savings

Types of Requirement Errors

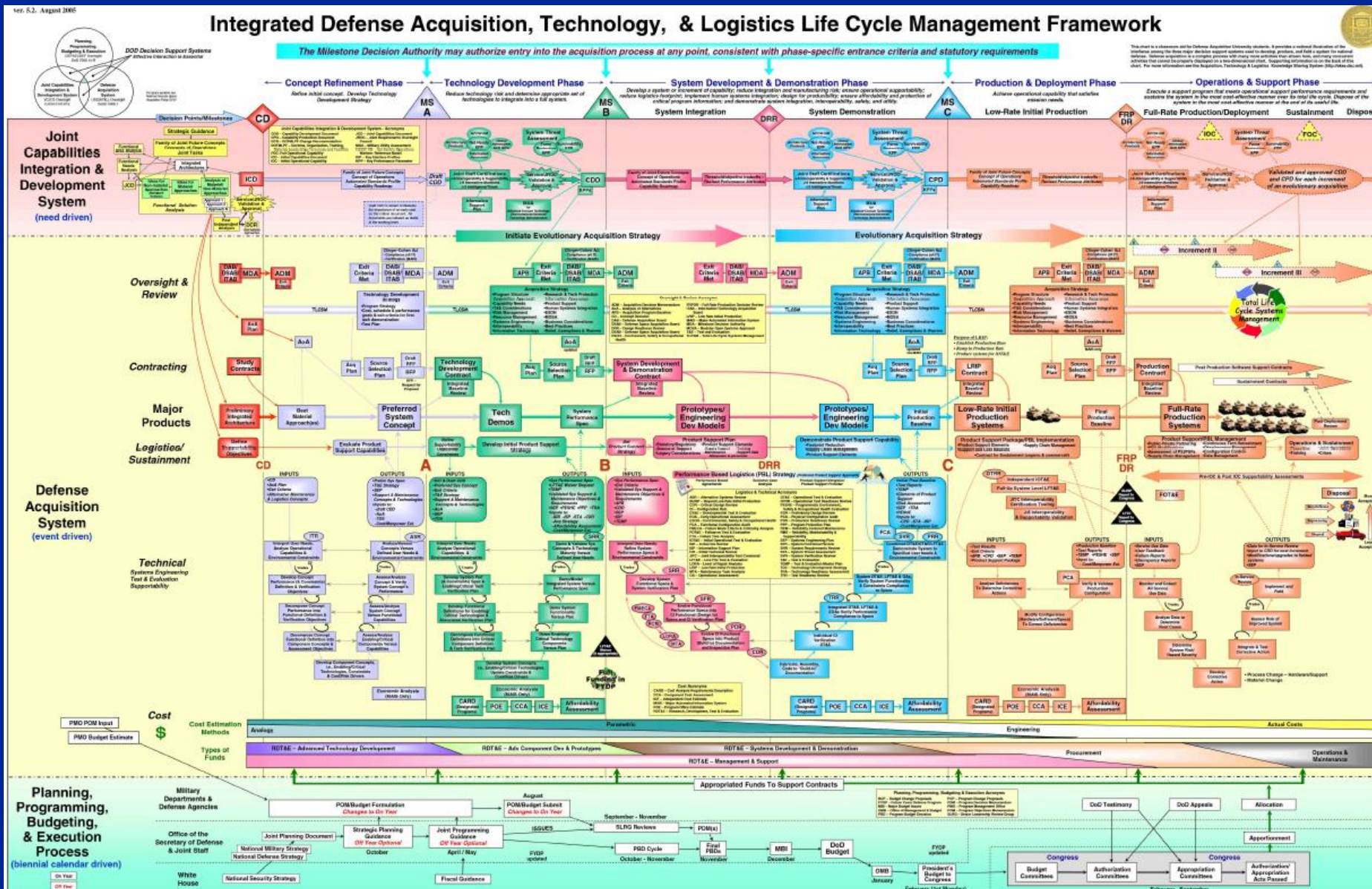


Source: "Customer Centered Products" Ivy Hooks and Kristin Farry

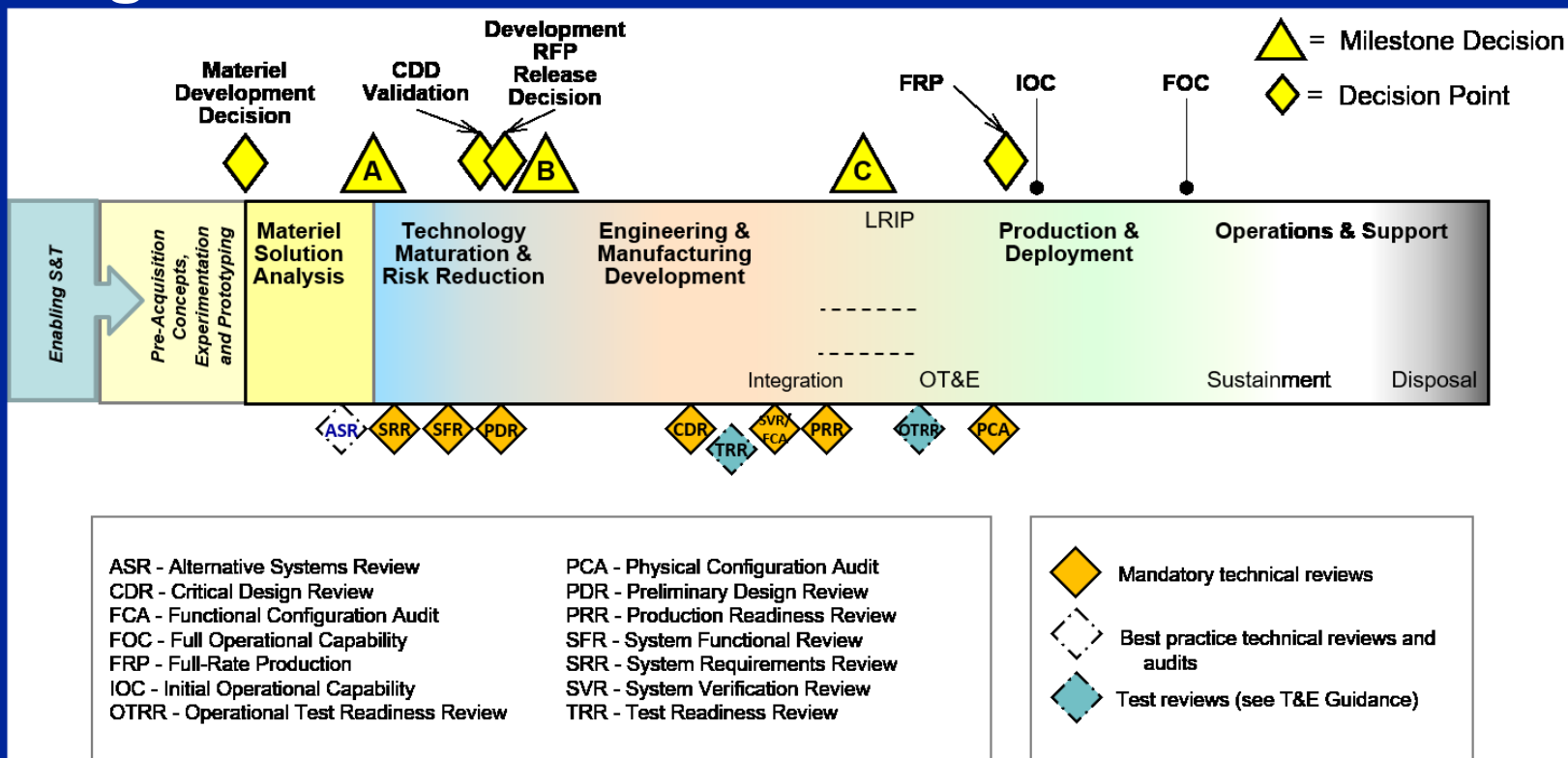
Relative cost to correct a requirement defect depending on when it is discovered



Source: "An Economic Release Decision Model: Insights into Software Project Management" Grady, Robert B. 1999



DoD Major Program Milestones with SETR Events



Notes:

- Derived from DoDI 5000.85, Major Capability Acquisition Model

Technical Reviews and Audits | www.dau.edu. (2017). Dau.edu. <https://www.dau.edu/tools/dau-systems-engineering-brainbook/technical-reviews-and-audits>

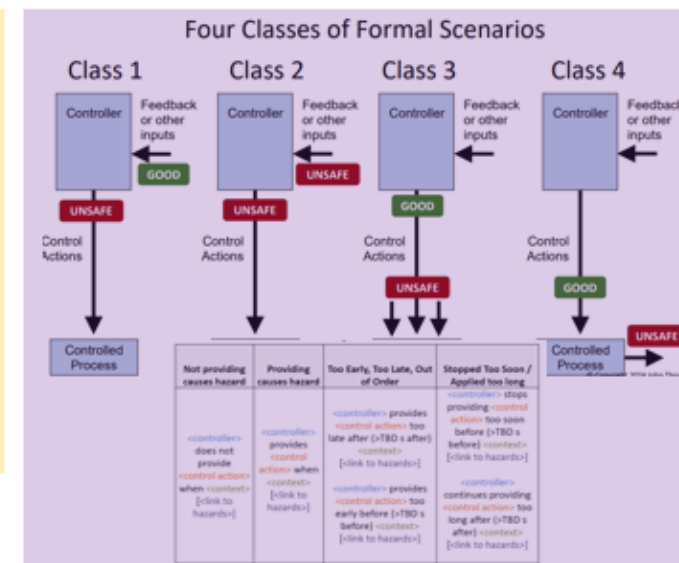
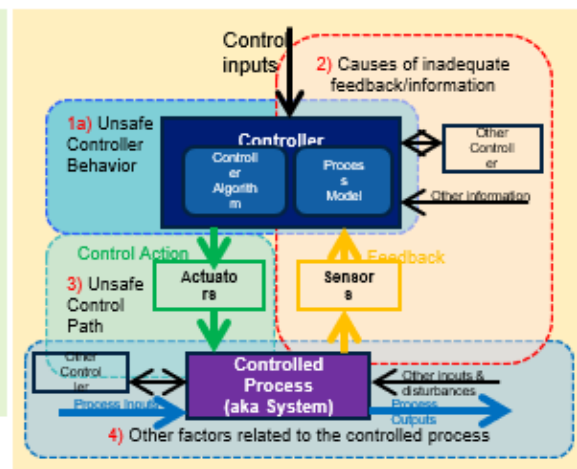
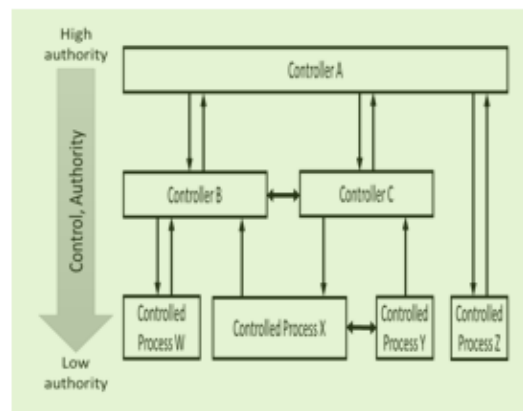
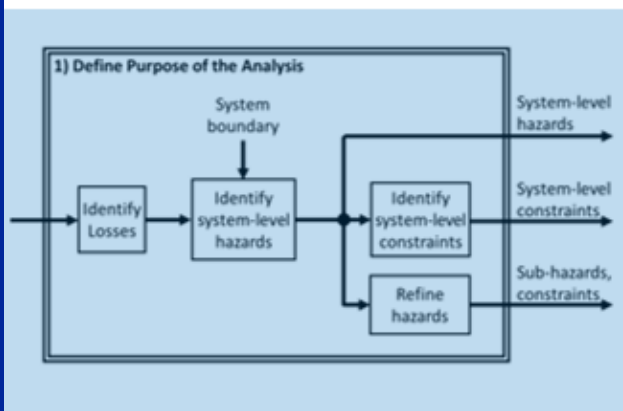
STPA Analysis 4-Steps

1) Define Purpose of the Analysis

2) Model the Control Structure

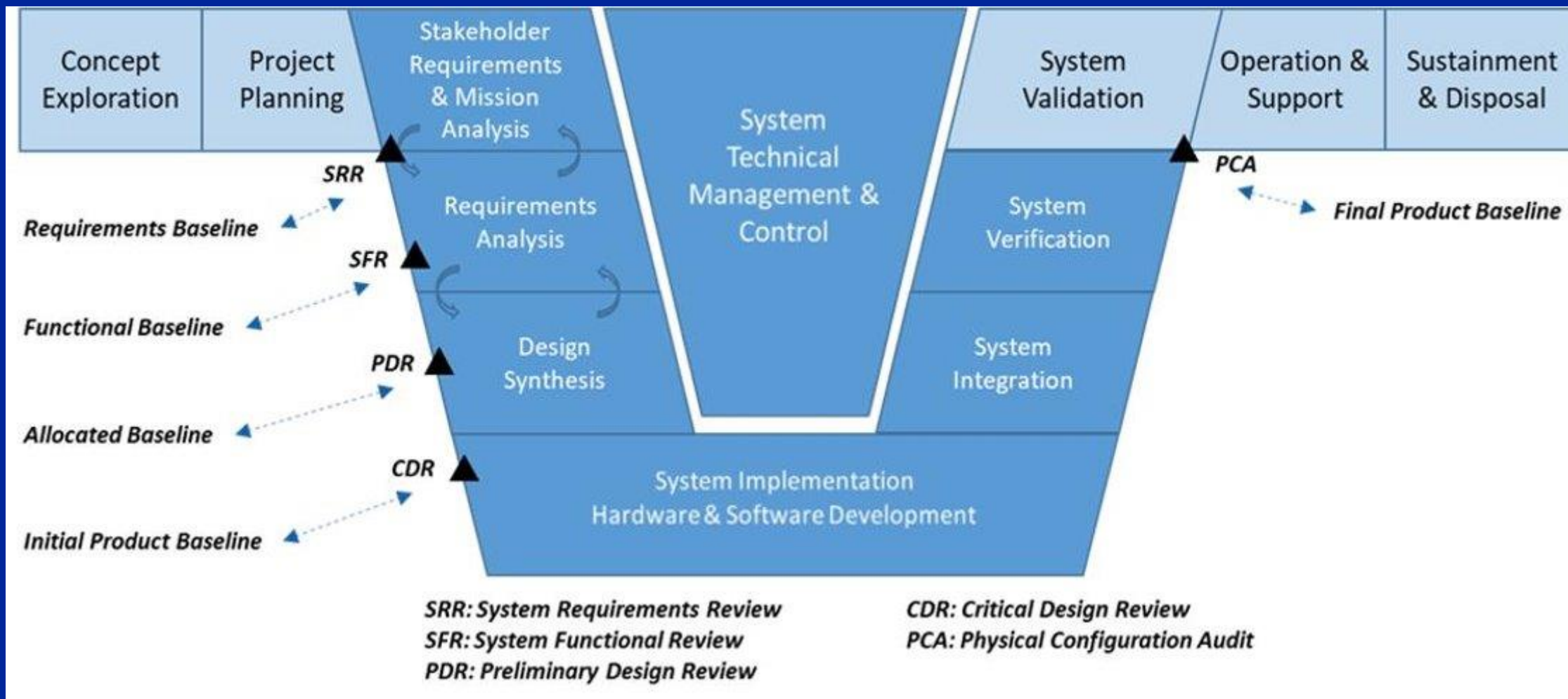
3) Identify Hazardous Control Actions (HCA)

4) Identify Loss Scenarios



Leveson, N. G., & Thomas, J. P. (2018). *STPA Handbook*. (March 2018 ed.). MIT Partnership for Systems Approaches to Safety and Security. Psas.scripts.mit.edu

System Engineering V with SETR Events and INCOSE/IEEE Baselines



SRR

- Mission Hazards
- Control Structure

PDR

- UCAs Driving Architecture and Interfaces

CDR

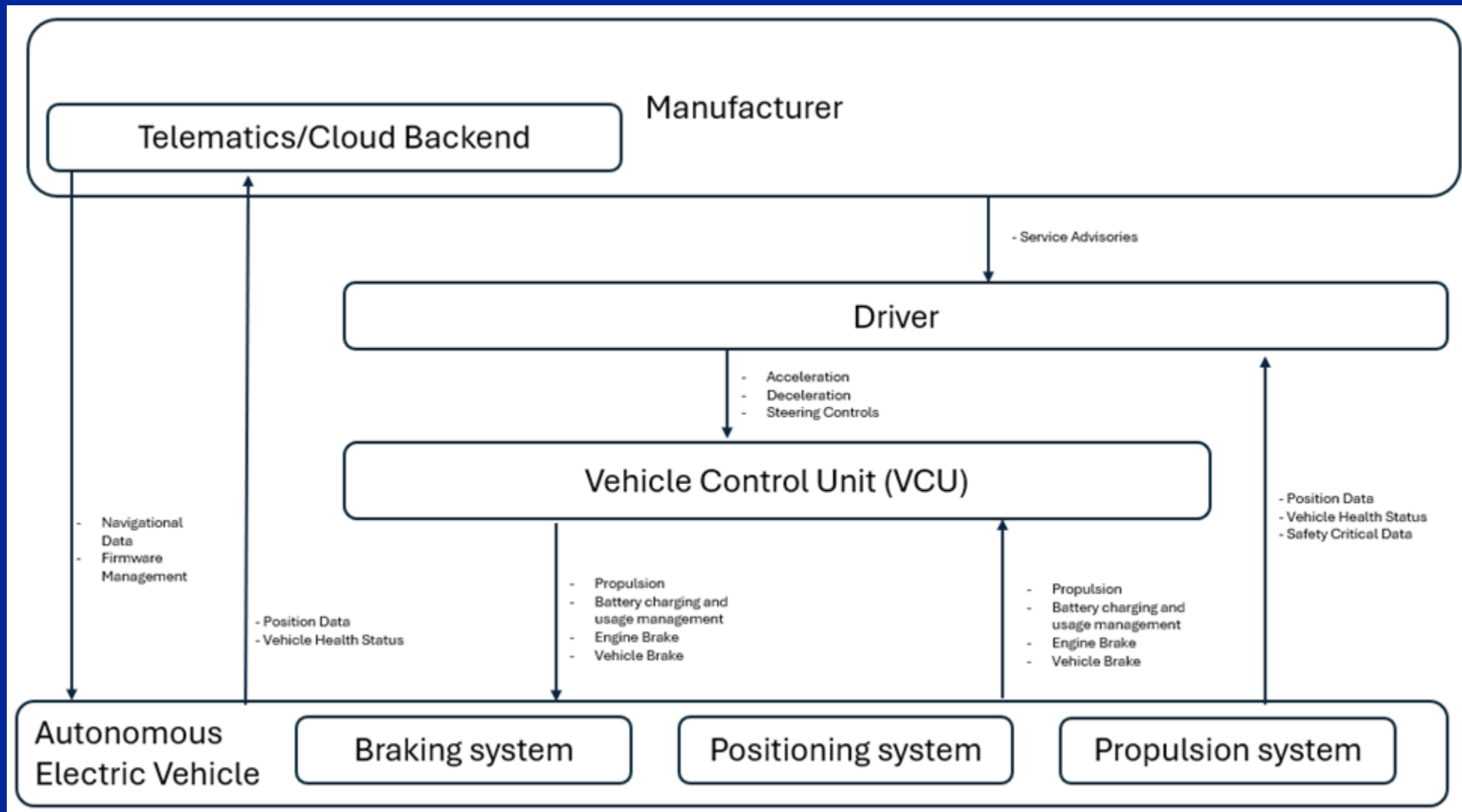
- Allocated Requirements and Design Constraints

TRR

- Verification of Safety/Security Mechanisms

FCA/PCA

- Traceability from Hazard → Requirement → Test



Level	WBS Hierarchy	Source / Detail	Suggested Syntax	Generic Template	Example	Notes & Guidance	Level-Fit Check Questions
0	JCIDS (ICD/CDD/CPD)	Capability needs, KPPs/KSAs	"The system shall capability with value"	"The capability shall enable effect in context"	"The system shall enable fully autonomous electric vehicle operations to meet defined safety and efficiency standards."	Aligns mission needs; avoid design; testable at system level.	<ul style="list-style-type: none"> Is it truly capability, not design? Is it measurable and system-level appropriate?
1	System	System Requirements Spec	"The System shall perform under conditions"	"The System shall provide performance within envelope"	"The autonomous electric vehicle shall operate without human intervention under specified environmental conditions."	Allocates KPPs into technical performance.	<ul style="list-style-type: none"> Does it derive from a KPP/KSA? Measurable and not too detailed?
2	Segment	Segment Spec	"The [Segment] shall function to support system req"	"The [Segment] shall provide function at performance"	"The vehicle control unit shall process driver commands and manage vehicle subsystems accordingly."	Functional allocation; no design.	<ul style="list-style-type: none"> Clearly supports system requirement? Functional, not directive design?
3	System within System	System Spec	"The [System] shall perform with criteria"	"The [System] shall provide outcome with accuracy/reliability"	"The propulsion management system shall control vehicle propulsion based on VCU commands."	Environmental/functional allocation.	<ul style="list-style-type: none"> Traceable to segment? Defines what, not how?
4	Subsystem	Subsystem Spec	"The [Subsystem] shall performance"	"The [Subsystem] shall provide performance under conditions"	"The propulsion system shall convert electrical energy into mechanical motion consistent with driver and VCU commands."	Partitioned functional performance.	<ul style="list-style-type: none"> Testable at subsystem level?
5	Assembly	Assembly Spec	"The [Assembly] shall requirement"	"The [Assembly] shall operate within constraint"	"The electric motor assembly shall produce torque outputs within specified limits for propulsion."	Adds SWaP, interfaces.	<ul style="list-style-type: none"> Testable independently? Avoids design mandate?
6	Subassembly	Subassembly Spec	"The [Subassembly] shall parameter ± tolerance"	"The [Subassembly] shall measure/provide parameter within tolerance"	"The motor controller module shall regulate electric motor operation according to VCU commands."	Narrow functional elements.	<ul style="list-style-type: none"> Too detailed? Should it be component level?
7	Component	Component Spec	"The [Component] shall parameter"	"The [Component] shall supply/withstand value"	"The power electronics unit shall switch power devices within specified electrical parameters and timing accuracy."	Lowest contract-level requirement.	<ul style="list-style-type: none"> Procurement-ready? Defines design-driving performance?
8	Subcomponent	Build-to Spec	"The [Subcomponent] shall detail"	"The [Subcomponent] shall operate at parameter under condition"	"The power metal oxide semiconductor field effect transistors (MOSFETs) and insulated gate bipolar transistors (IGBTs) shall handle specified voltage and current loads without failure."	Detailed, may trace to drawings.	<ul style="list-style-type: none"> Is this build-to? Should this be a drawing/spec note?

Thank you!

Questions, discussion or follow-on conversations are welcome.

NORTHROP
GRUMMAN

The logo graphic consists of a thick black horizontal line extending from the end of the word "NORTHROP" to the right, and a thick black vertical line extending downwards from the end of the word "GRUMMAN" to the right, forming an L-shaped corner.