

STPA RETURN ON INVESTMENT INDUSTRY PERSPECTIVE

LORI SMITH

MARC NANCE

MARK VERNACCHIA



STAMP
ENGINEERING
SERVICES, LLC

INTRODUCTIONS



LORI SMITH
RETIRED BOEING
23 YEARS AEROSPACE
CURRENTLY STAMP ENGINEERING SERVICES VP SYSTEMS ENGINEER



MARC NANCE
RETIRED BOEING
35 YEARS AEROSPACE & AUTOMOTIVE
CURRENTLY STAMP ENGINEERING SERVICES COO

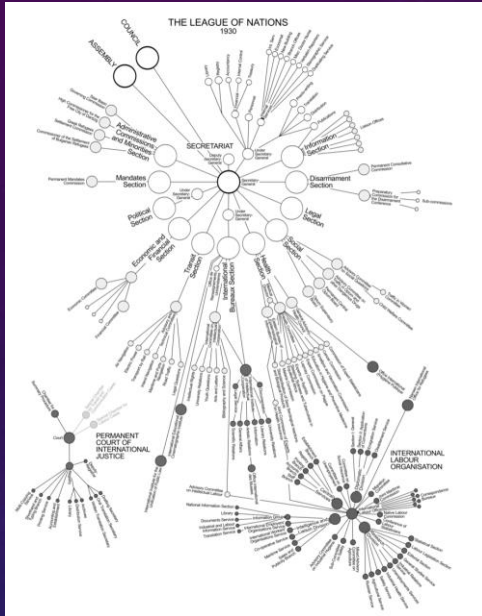


MARK A. VERNACCHIA
GENERAL MOTORS COMPANY
TECHNICAL FELLOW – PRINCIPAL SYSTEMS SAFETY ENGINEER
35 YEARS AUTOMOTIVE

AGENDA

- BACKGROUND AND ASSUMPTIONS
- FINDINGS AND RECOMMENDATIONS
- EXAMPLES

BACKGROUND



ORGANIZATIONAL
DESIGN



PRODUCTION SYSTEMS



MANNED VEHICLES



TEST PLANNING



UNMANNED VEHICLES

ROI ASSUMPTIONS



“FORESIGHT IS NOT ABOUT PREDICTING THE FUTURE; IT’S ABOUT MINIMIZING SURPRISE”

FUTURIST KARL SCHROEDER

ROI ASSUMPTIONS

- STPA ANALYSIS CONDUCTED EARLY IN CONCEPT / REQUIREMENTS DEVELOPMENT PHASE
- IDENTIFIED LOSSES ARE CORRECTED
- SYSTEM LEVEL COST IMPACTS
- LARGER SYSTEMS HAVE MORE INTERACTIONS AND INTERFACES WITH GREATER COST RISK
- LARGER SYSTEMS REQUIRE MORE ANALYSIS (LABOR)

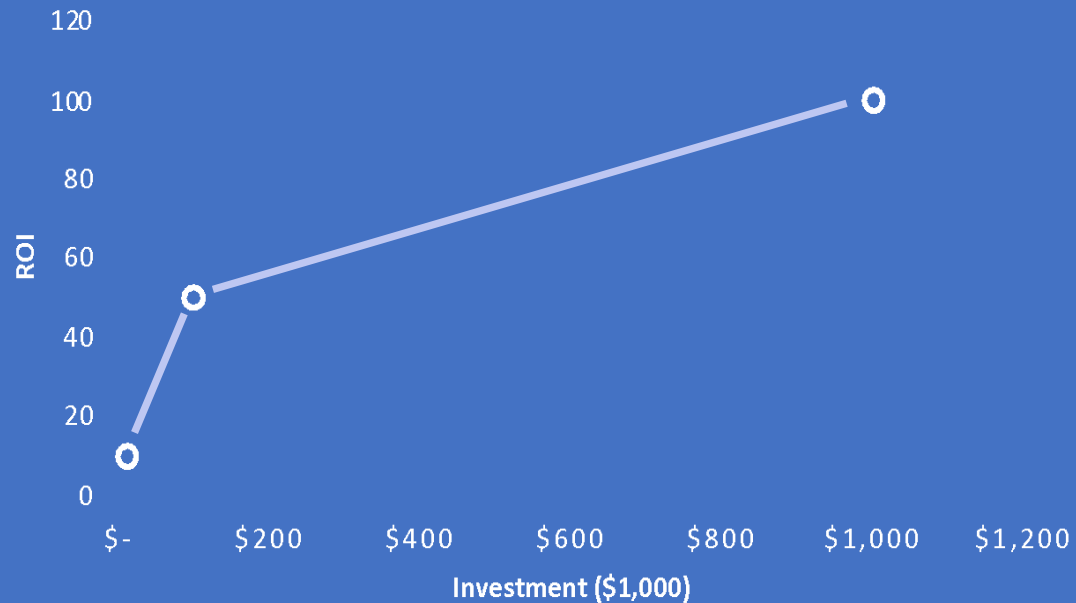


“FORESIGHT IS NOT ABOUT PREDICTING THE FUTURE;
... IT'S ABOUT MINIMIZING SURPRISE”

FUTURIST KARL SCHROEDER

ROI FINDINGS

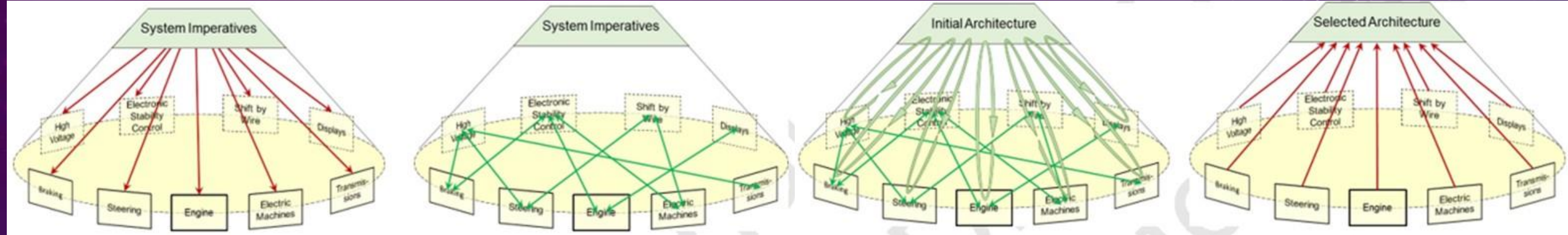
RETURN ON INVESTMENT



RECOMMENDATIONS

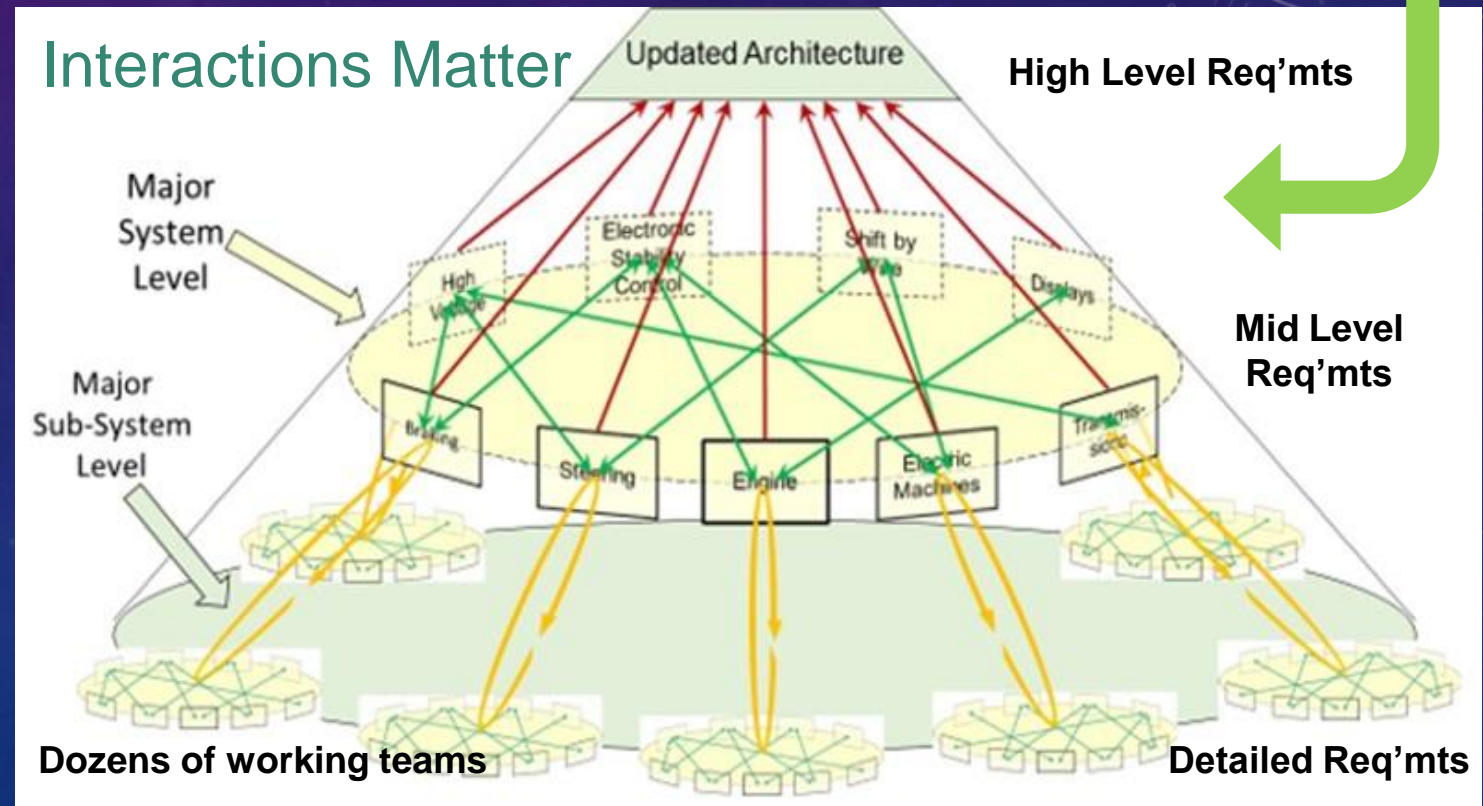
- START EARLY AND ITERATE
- LEVERAGE STPA “JEDI KNIGHTS”
- INCLUDE ENGINEERING, CYBER, FINANCE, MANUFACTURING AND SUPPLY CHAIN
- COMMIT TO RECTIFYING IDENTIFIED LOSSES
- EXPECT SIGNIFICANT OPPORTUNITIES IN CYBER AND SUPPLY CHAIN

Examples – STPA System Engineering Leverage Perspective

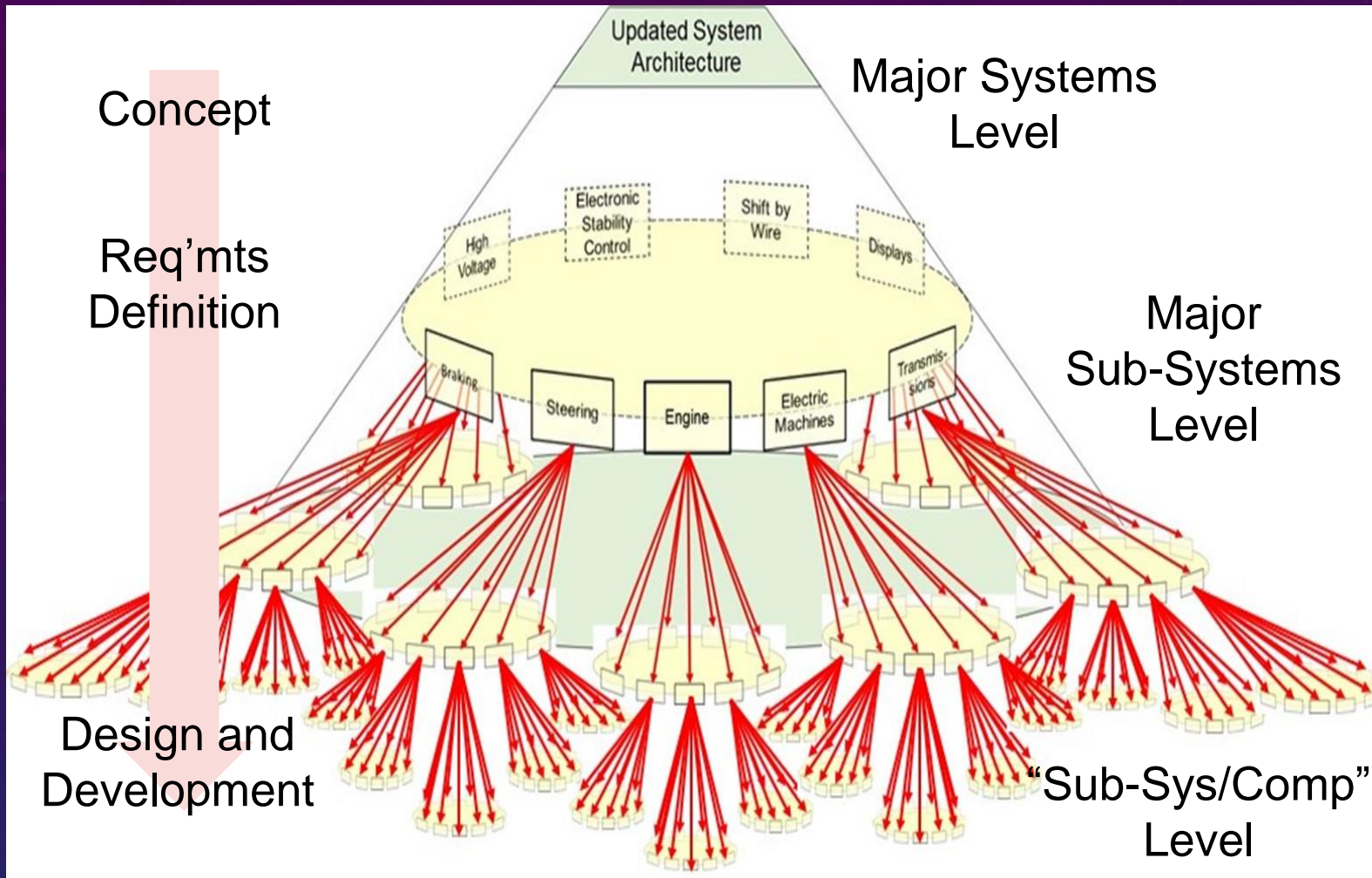


Top-down system design allows the:

- Right Requirements, at the
- Right Time, at the
- Right Level of Detail to be defined and delivered to system-level, HW, and SW engineers



Examples – Cascading Change Avoidance – For just one project



Major Level:

Teams: 5 – 11

Req'mt Changes Avoided: 10

Hours to Execute: $5 * 50 = 250$

Major Sub-Systems Level:

Teams: 25 - 75

Req'mt Changes Avoided: 100

Hours to Execute: $15 * 100 = 1,500$

Sub-System/Comp Level:

Teams: > 200

Req'mt Changes Avoided: 1000

Hours to Execute: $40 * 1,000 = 40,000$

- With this cascading effect, what is the cost of wrong requirements at the start of the project?
- What about impact of finding missing requirements as project design and development continues?
- What about the cost of never finding requirements that lead to field incidents?

EXAMPLE - Effort Savings and Potential Tooling Cost Avoidance

Major Level:

Savings Estimate: $\$100/\text{hr} * 250 = \$25,000$

Major Sub-Systems Level:

Savings Estimate : $\$100/\text{hr} * 1,500 = \$150,000$

Sub-System/Component Level:

Savings Estimate : $\$100/\text{hr} * 40,000 = \$4,000,000$

Major Level:

Hardware Change Impact Factor: 1

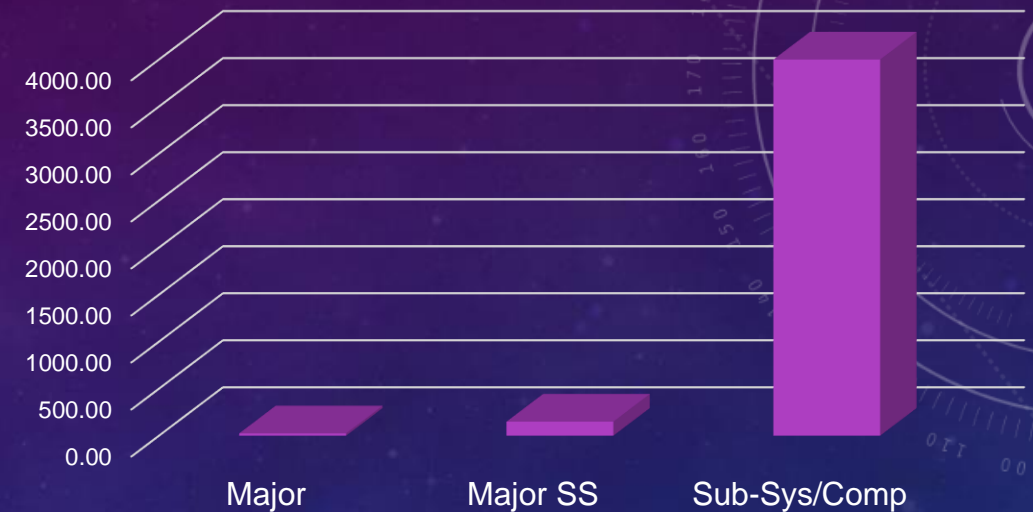
Major Sub-Systems Level:

Hardware Change Impact Factor: 10

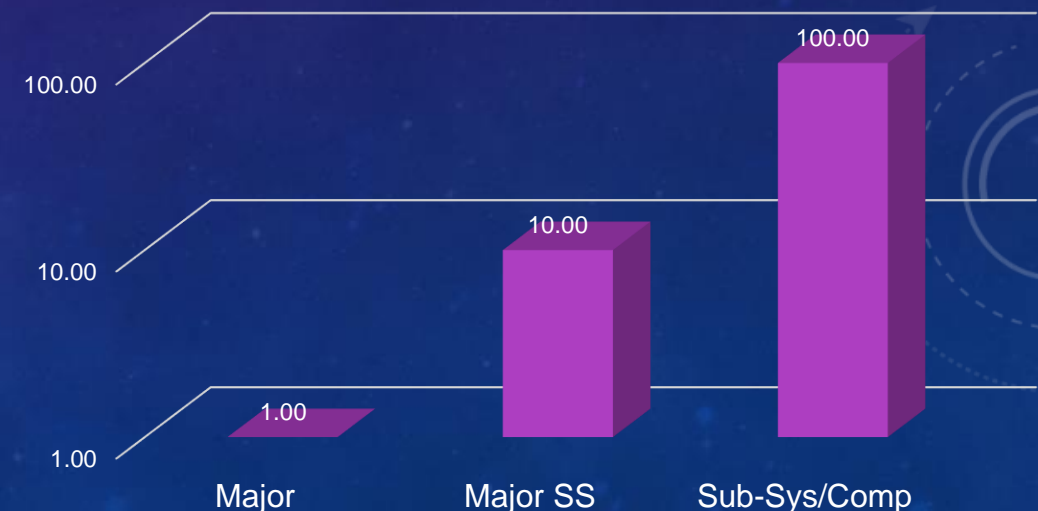
Sub-System/Component Level:

Hardware Change Impact Factor: 100

Example Savings (000s)



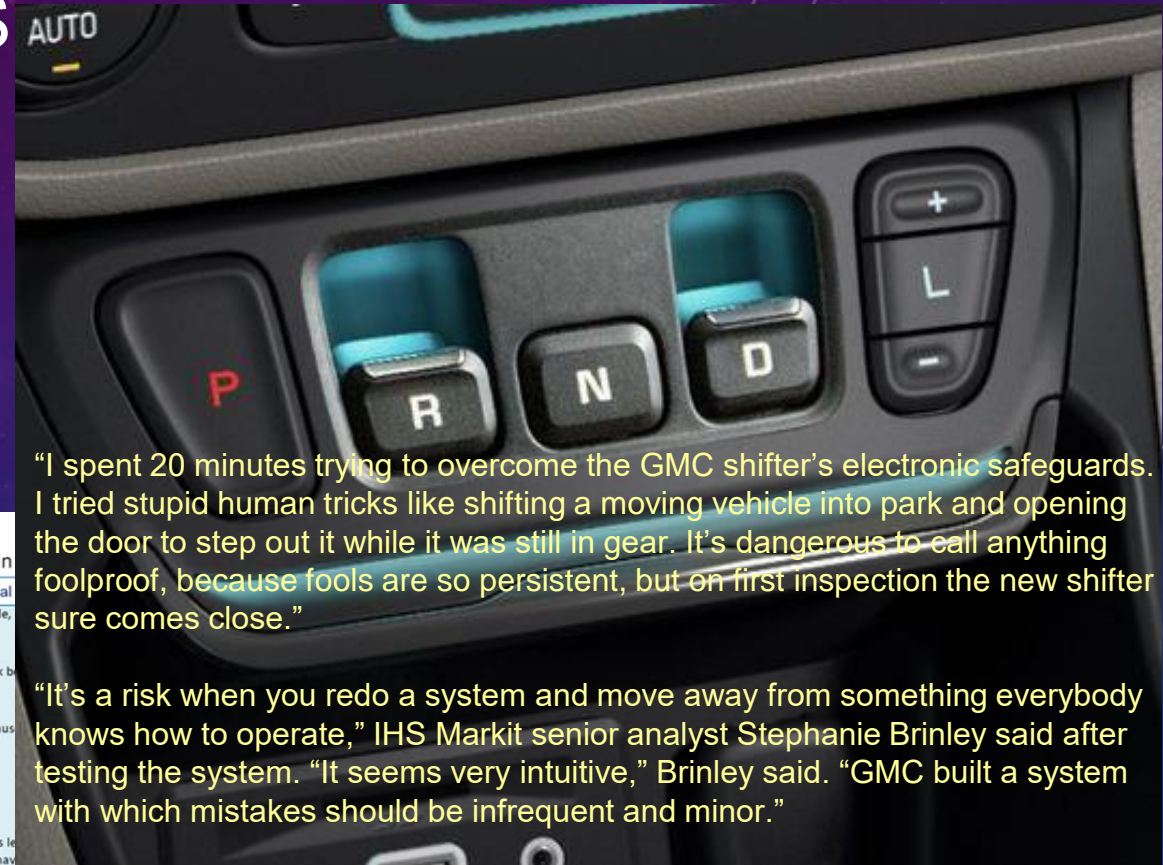
HW/Tooling Impact Factor



Examples – General Motors Company

SHIFT-BY-WIRE – HMI INTERACTIONS

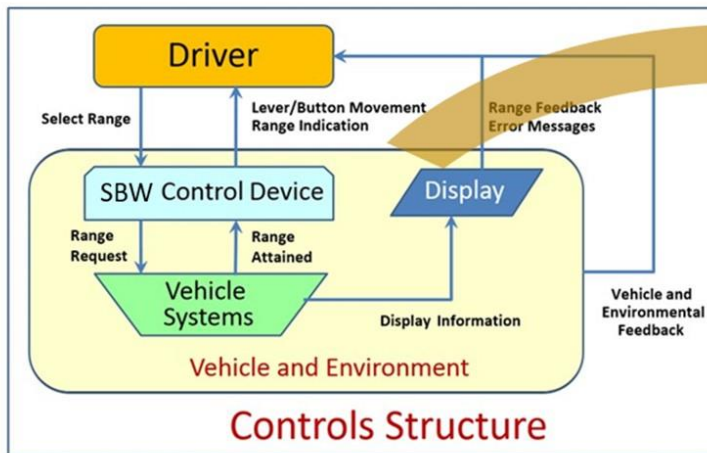
- Early use of STPA enabled tradeoff studies and alternative concepts
- Control issues discovered and corrected before HW/SW requirements dates



“I spent 20 minutes trying to overcome the GMC shifter’s electronic safeguards. I tried stupid human tricks like shifting a moving vehicle into park and opening the door to step out it while it was still in gear. It’s dangerous to call anything foolproof, because fools are so persistent, but on first inspection the new shifter sure comes close.”

“It’s a risk when you redo a system and move away from something everybody knows how to operate,” IHS Markit senior analyst Stephanie Brinley said after testing the system. “It seems very intuitive,” Brinley said. “GMC built a system with which mistakes should be infrequent and minor.”

Define system content (control structure) and the interactions between the driver and the system



STPA ACTIVITIES

Determine possible causal scenarios that could result in

UCA	37 UCAs Defined	Potential C	100 Potential Causal
UCA1: Driver does not put car in Park on hill		Driver is distracted, or in a panic mode, decide to get into park	
UCA1: Driver does not put car in Park on hill		Driver already thinks the car is in Park b action	
UCA1: Driver does not put car in Park on hill		Driver thinks it is already in Park because will do it automatically	
UCA1: Driver does not put car in Park on hill		Driver cannot find Park	
UCA1: Driver does not put car in Park on hill		Driver performs prior habitual actions le Park in this vehicle (Prior Learned Behav	
UCA1: Driver does not put car in Park on hill		System feedback is confusing to driver	

STPA ACTIVITIES

Condense functional and design constraints into requirements

Meets FMVSS Requirements 101, 102, and 114
Buttons, Knobs, Levers Must Be "Mono-Stable" (momentary activation)
Brake, plus two motions, necessary to exit Park; P => N (Safe)
One motion from D => N (Easy)
Two Motions to get to Reverse from any "Drive" gear (D,L,M)
Controls are clearly identified and obvious, easily accessible
Park button easy to find

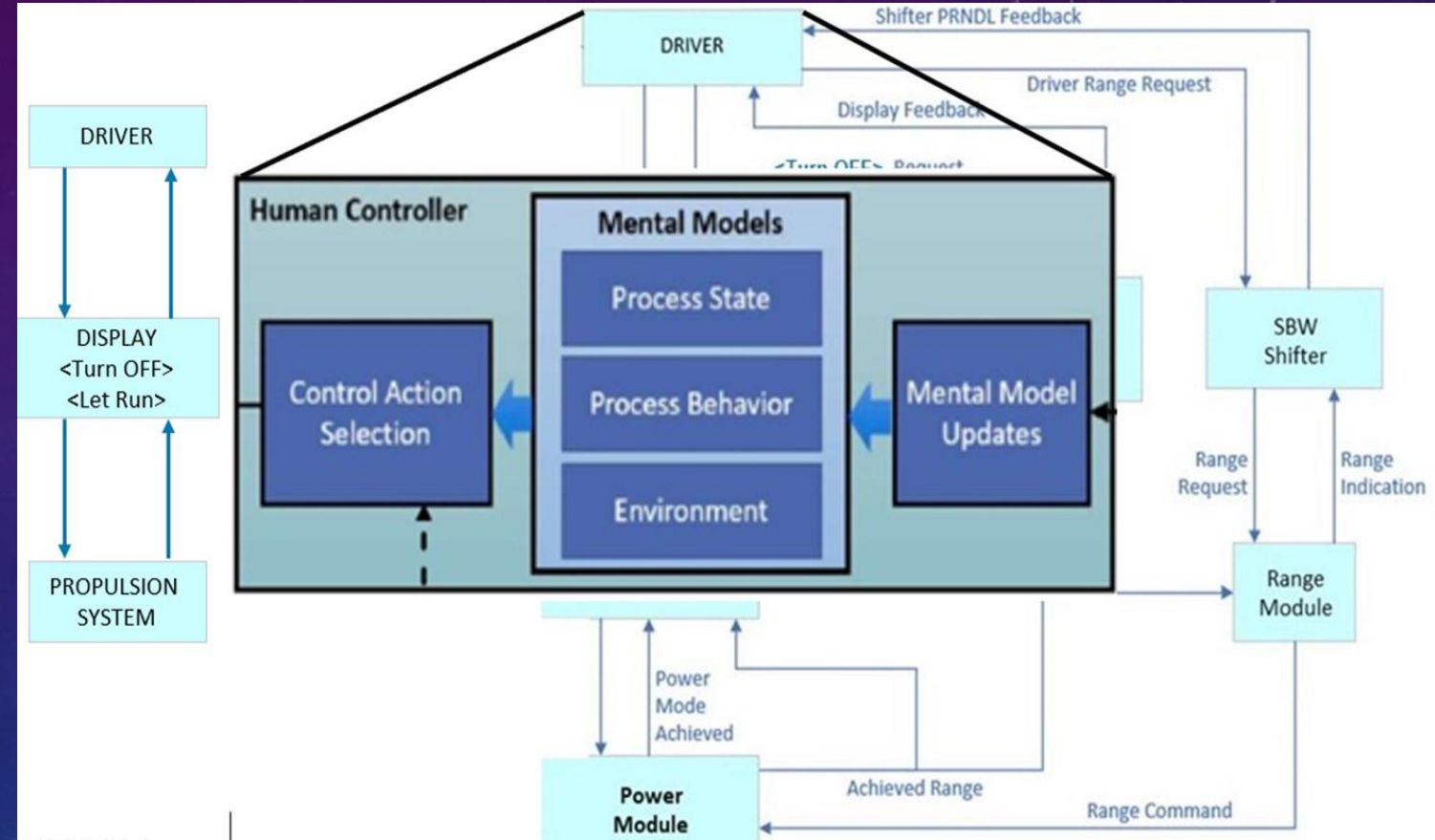
Incorporation of STPA Requirements into Appropriate Sub-System and Component Specification Documents And into Design Center "Best Practices"

[STPA-Integrated-into-GM-Safety-Process-20feb18-Approved-Rev1.pdf \(mit.edu\)](#)

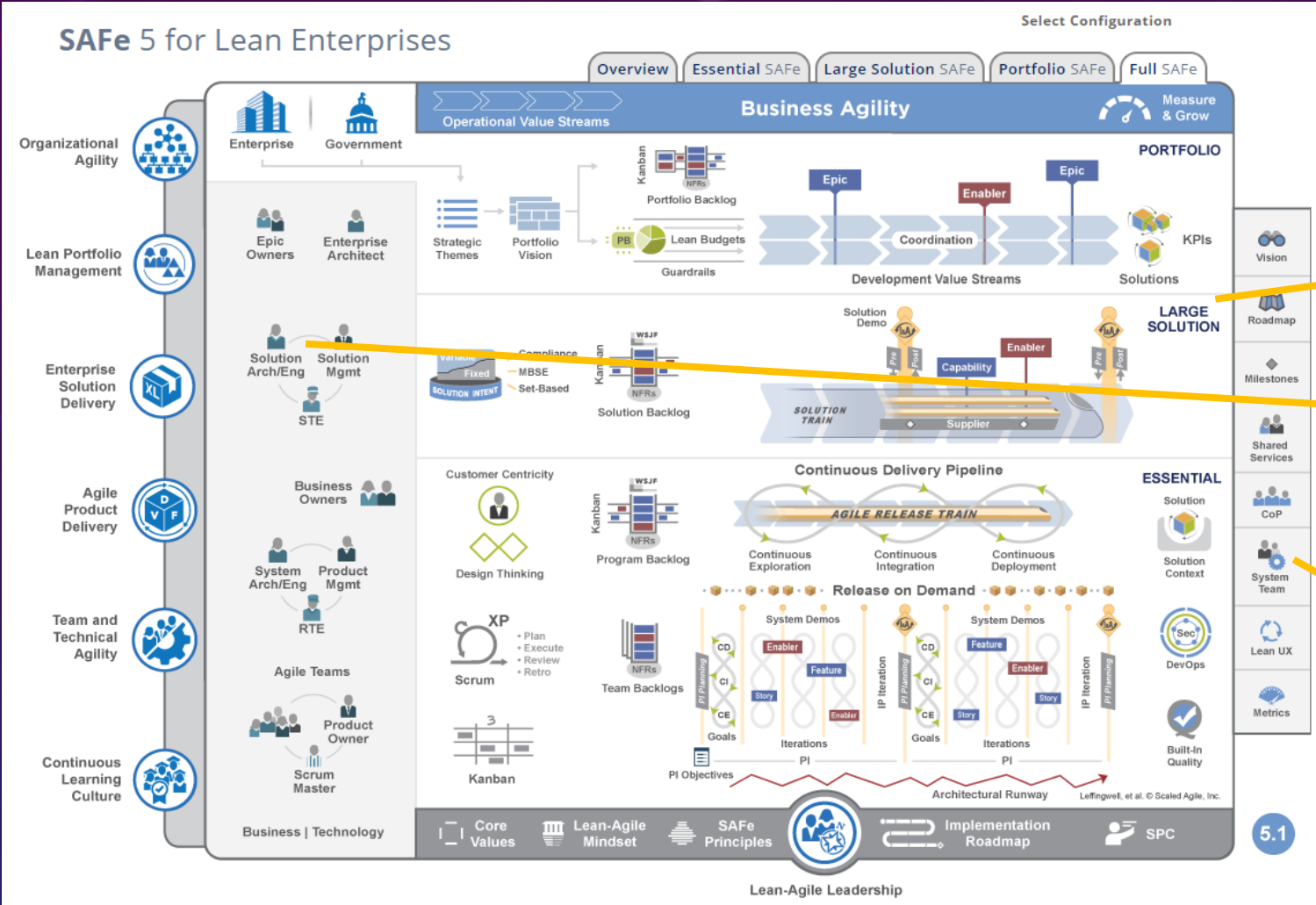
Examples – General Motors company

“HUMAN CONTROLLER MODEL” POWER MODE INTERACTION

- Early use of STPA drove various design changes that addressed uncovered potential hazards
- Conflicting commands between intelligent control structure elements were identified and precedence established prior to Req'mts being sent to numerous development teams



STPA and SAFe – Initial Thoughts

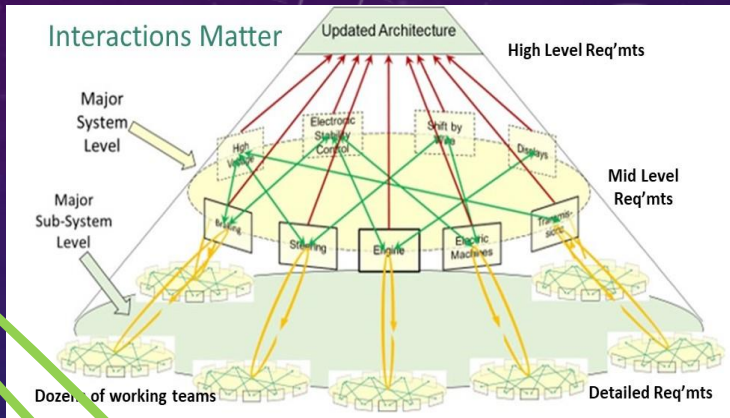
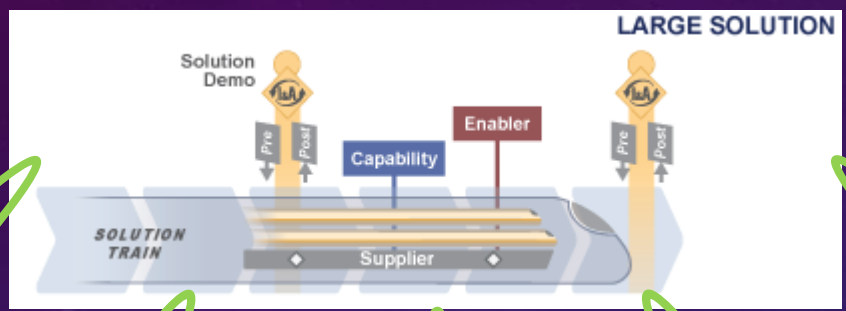


- Propose that STPA useful at “Large Solution” Level
- Right Requirements, Right Time, Right Level of Detail
- Risk is that numerous SAFe teams at ESSENTIAL level are quickly working on wrong requirements, or they are missing requirements

STPA and SAFe – Initial Thoughts

SAFe deals with hierarchal approach and same principles would apply

STPA in Top-Down System Design Role



SUMMARY

- STPA CAN PROVIDE POSITIVE AND SIGNIFICANT RETURN ON INVESTMENT (ROI) FOR LARGE AND SMALL PROJECTS
- THE EARLIER ONE STARTS STPA IN SYSTEMS CONCEPT DEVELOPMENT, THE MORE OPPORTUNITIES CAN BE REALIZED
- STARTING STPA PRE-ARCHITECTURE PROVIDES MOST BENEFIT
- STPA MAY APPEAR AS EXTRA WORK BUT IT MAY BE CONSIDERED AS THE EXPECTED ENGINEERING THAT SHOULD HAVE BEEN DONE ANYWAY AS PART OF A ROBUST ENGINEERING PROCESS
- FINDING SYSTEM LOSSES IS NOT THE SAME AS FIXING LOSSES

QUESTIONS?