The Application of STPA in Commercial Product Development to Identify Causal Factors for Quality Losses

2013 STAMP Conference

Stephanie Goerges, Cummins

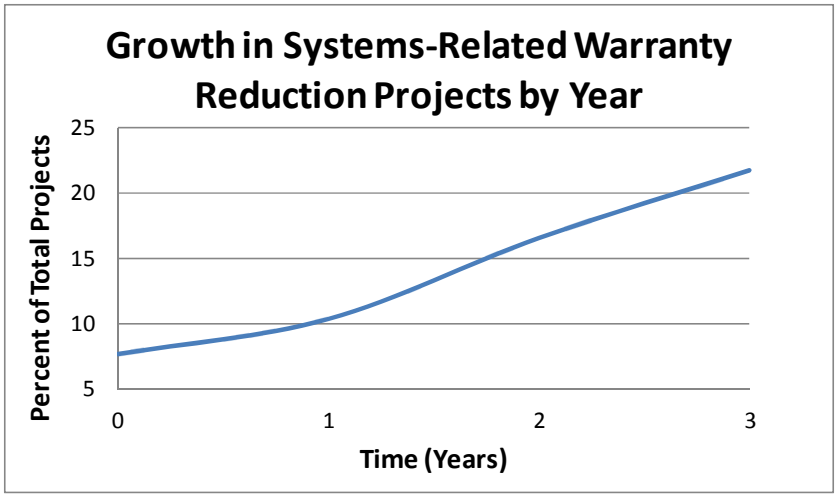
27 March 2013

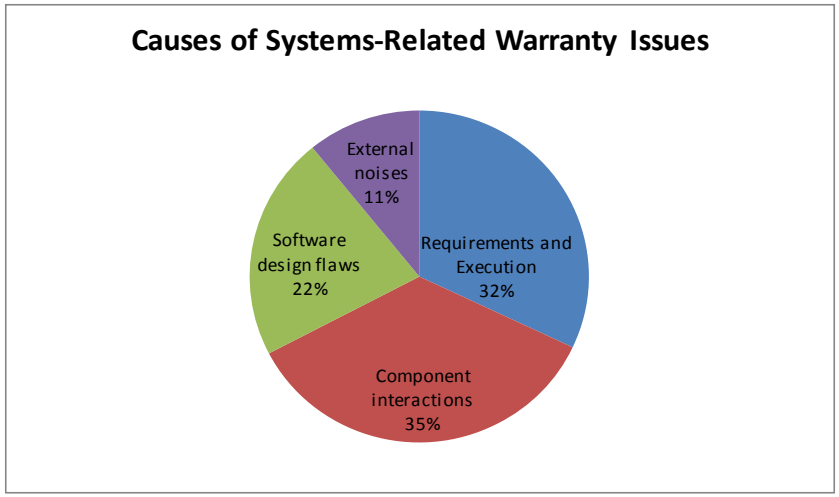
Motivation

- Identifying the factors that could lead to the loss of quality is difficult for large, complex systems
- Traditional design methods such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and Robust Design have been proven effective at the component level but are less effective for factors that involve interactions between components, software flaws and external noises

Motivation

- Recent growth of a class of warranty claims for which there was a customer complaint (low power, smoke) but no failed component, or a failed component was determined to be an effect rather than a cause
  - 60% of the issues were design related
  - Estimated 42% would have been predicted by FMEA

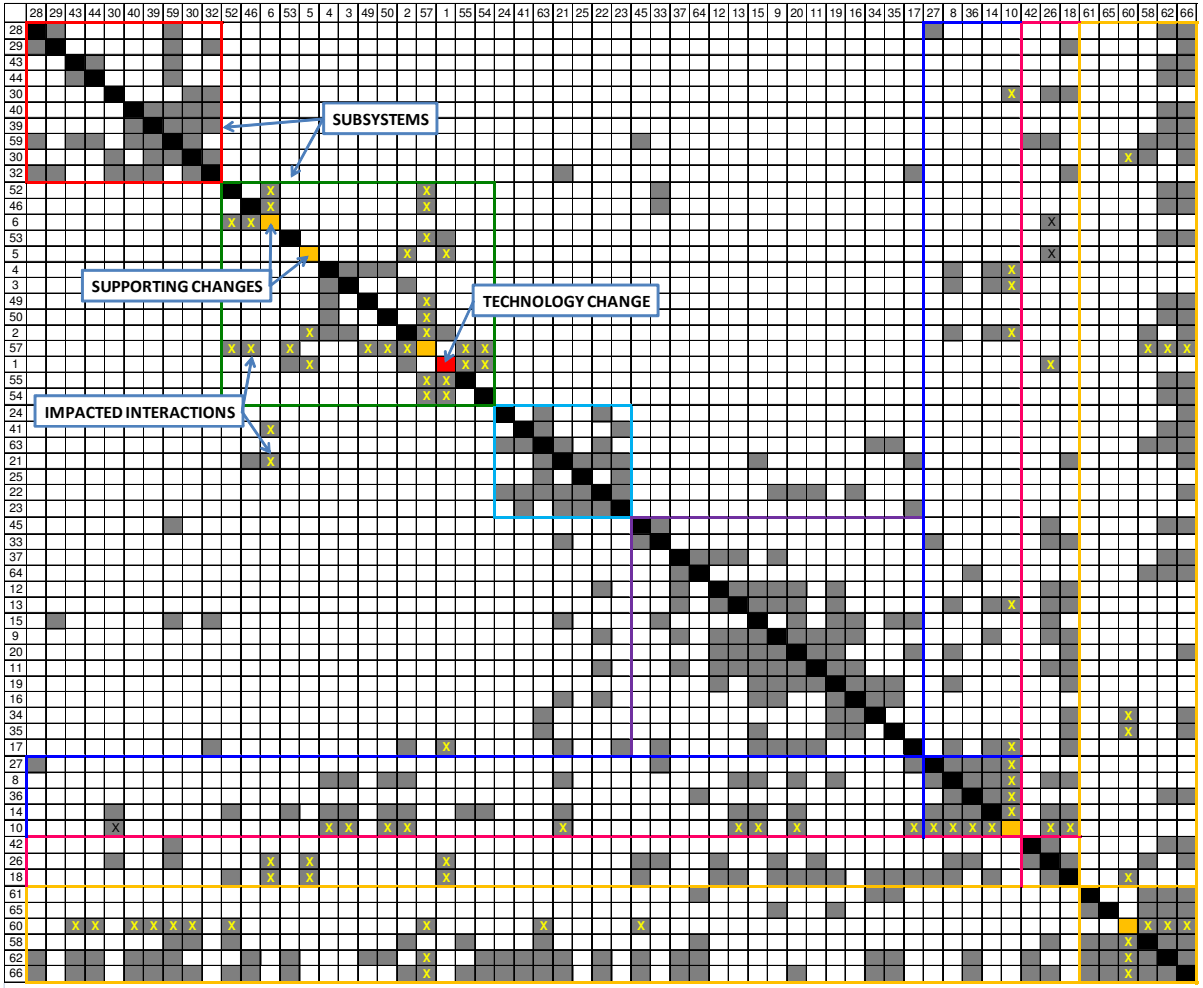




Adaptation of STPA for Quality Losses

STPA SAFETY TERM	DEFINITION	PROPOSED QUALITY LOSS TERM	DEFINITION
Accident	"An undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss (called a loss event)"	Loss or Loss Event	"Losses can be economic losses, losses of human lives, losses of function, losses of time, etc."
Hazard	"A state or set of conditions that, together with worst-case external conditions can lead to an accident."	Undesired system state	A state that can lead to a loss of the system's ability to deliver requirements
Safety	"The property of being free from accidents or unacceptable losses."	Quality (Any emergent property of interest, e.g. Manufacturability, could be substituted for Quality in this case.)	"Ability to deliver requirements at a "high" level, as perceived by people relative to other alternatives that deliver the same requirements."
Unsafe	Lacking the attribute of safety	Inadequate	Lacking the attribute of quality

Case Study – Technology Change to an Existing System



- Functions unchanged
- The behavior of the component of interest and the interactions with other components known for the current product system
- Are there any new or undesirable behaviors of the component or interactions as a result of the change?

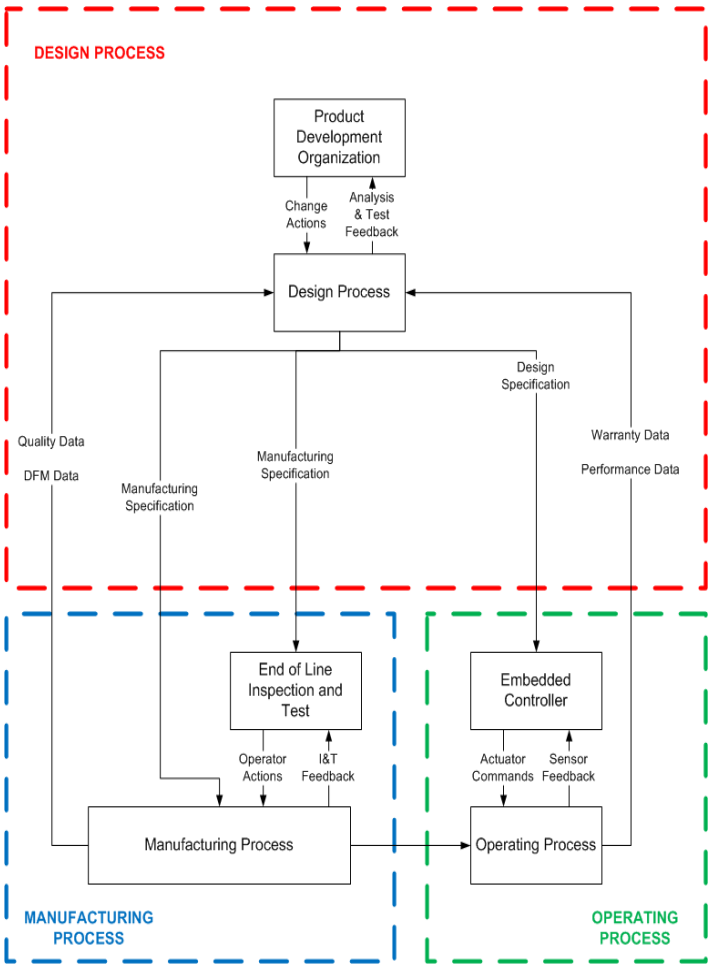
Preparatory Step 1: Identify the Losses and Undesired System States

- Losses: Failure to meet regulated emissions, System is over-designed (material cost), System is under-designed (warranty cost)

UNDESIRED SYSTEM STATE	LOSS	PROCESS	PRIORITY[1]
USS1	Cost – System over-designed	Design & Manufacturing	3
USS2	Failure to meet emissions	Design & Operating	1
USS3	Failure to meet emissions	Design & Manufacturing	1
USS4	Failure to meet emissions	Design & Operating	1
USS5	Failure to meet emissions	Design & Operating	1
USS6	Failure to meet emissions	Operating	1
USS7	Failure to meet emissions	Operating	1
USS8	Cost – System under-designed	Design	2
USS9	Cost – System under-designed	Design	2
USS10	Cost – System over-designed	Design	3
USS11	Cost – System under-designed	Design	2

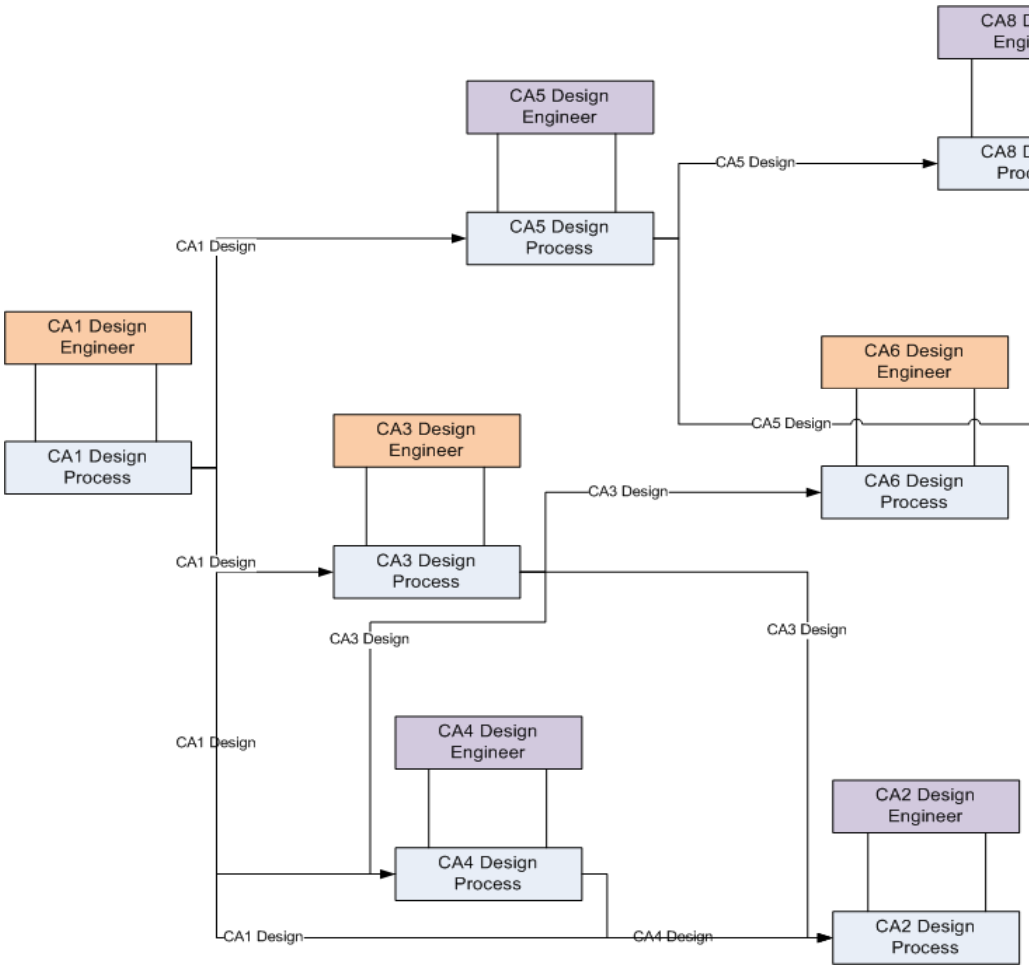
[1] Legend: 1-highest priority, 3-lowest priority

Preparatory Step 2: Construct the Hierarchical Control Structure



- Hierarchical control structure sub-divided into three areas:
  - Design process
  - Manufacturing process
  - Operating process
- Detailed control structures developed for each of the three areas

Control Action Interactions



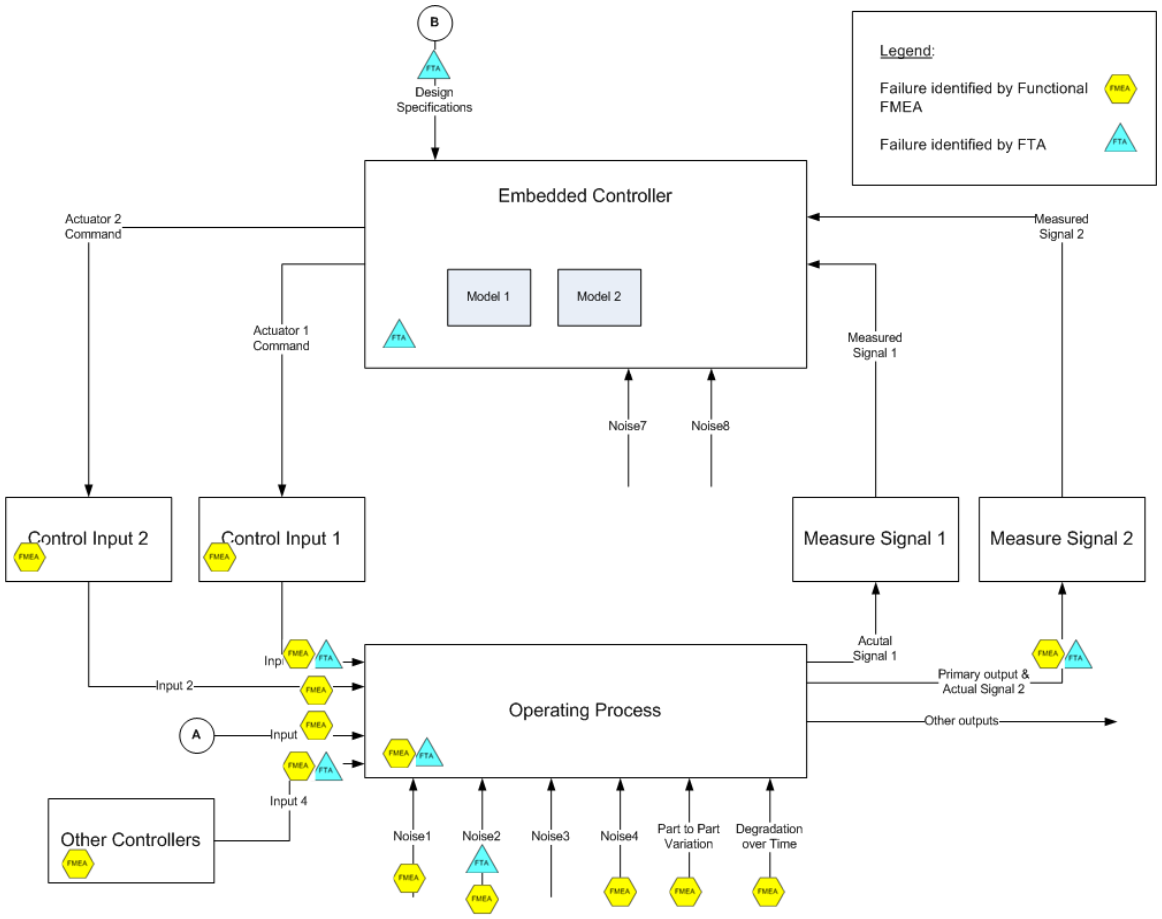
The design area was further sub-divided by the eight control actions

Analysis Step 1: Identify the Inadequate Control Actions

- Due to on-going product development, details of the inadequate control action analysis have been omitted
- Following Analysis Step 1, the inadequate control actions were mapped to the undesired system states

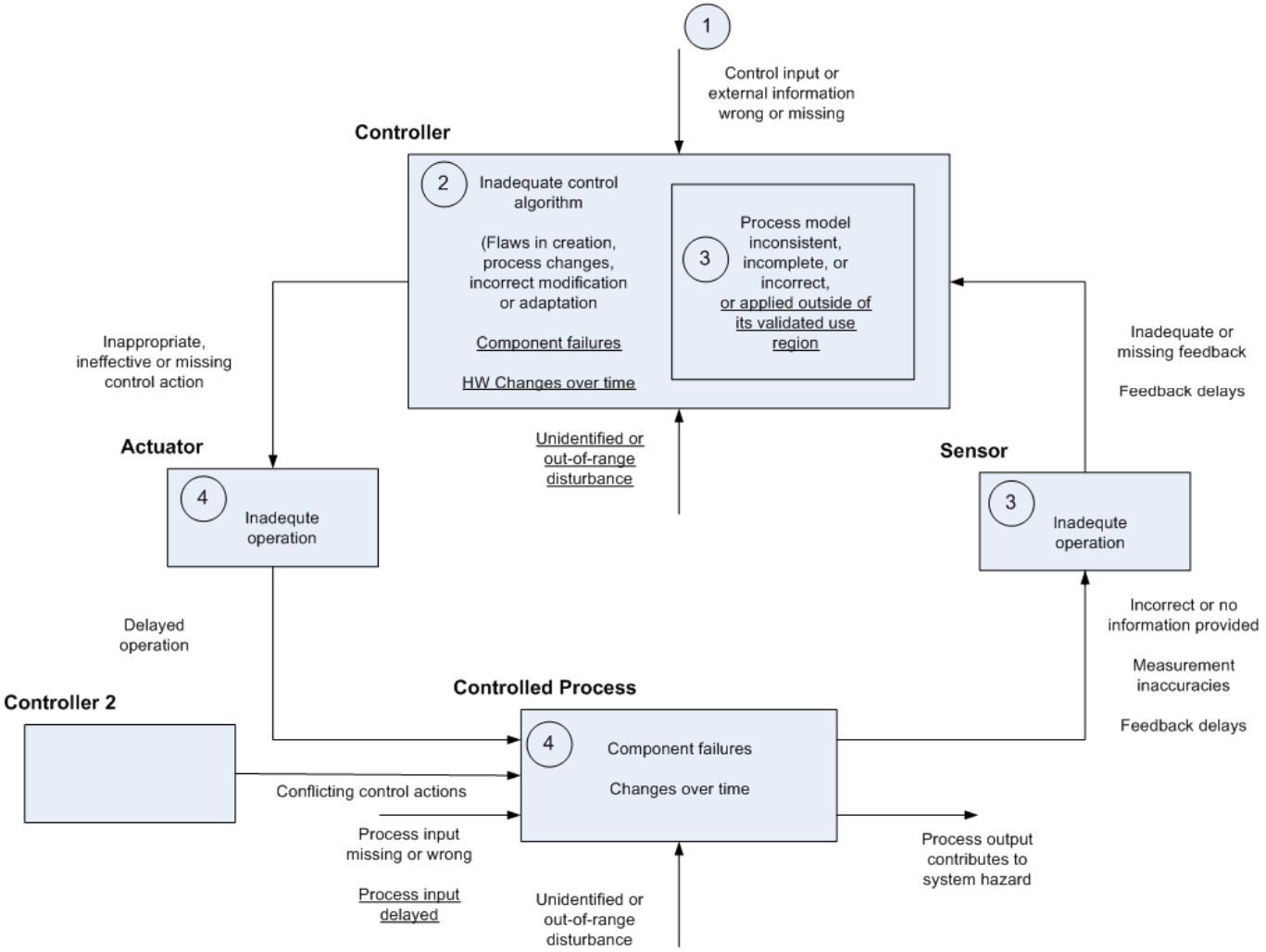
	USS1	USS2	USS3	USS4	USS5	USS6	USS7	USS8	USS9	USS10	USS11
CA1	X	X									
CA2			X				X				
CA3	X	X									
CA4	X	X									
CA5				X	X			X	X		
CA6		X								X	X
CA7						X			X		
CA8						X		X			

Analysis Step 2: Identify Causes of Inadequate Control Actions



- Causal factors were identified for all elements of the control structure using STPA
- Comparison to FMEA and FTA indicated

Additional Guidewords Used in the Case Study



- Unidentified or out of range disturbances on the controller
- Component failures of the controller
- HW changes over time of the controller
- Controlled process input delayed
- Process model applied outside of its validated use region

Conclusions from Case Study

- Use of STPA allowed the design teams to identify more causal factors for quality losses than FMEA or FTA, including component interactions, software flaws, and omissions and external noises
- STPA was also found to be complementary to Robust Design Methods
- Use of STPA was effective for analyzing the complete hierarchical structure of the system for solutions to potential causes of quality losses

Acknowledgements

- I offer my sincerest thanks to Cummins, Inc. for sponsoring my research
- I also wish to thank the following individuals:
  - *Elizabeth Carey (Cummins)*, for mentoring and motivating me throughout my career as a Systems Engineer and Change Agent
  - *Karen DeSanto (Cummins)*, for sharing my vision of what is possible and giving me the opportunity to make it real
  - *Nancy Leveson (MIT)*, for inspiring me to think about failure in a new way by bringing me back to my control theory roots
  - *Qi van Eikema Hommes (MIT)*, for sharing your wisdom and experiences and for patiently guiding me through this process

References

- Leveson, Nancy (2011) Engineering a Safer World, MIT Press, Cambridge, MA.
- deWeck, O., Ross, A., Rhodes, D., "Investigating Relationships and Semantic Sets amongst System Lifecycle Properties (Ilities)," Third international Engineering Systems Symposium, CESUN 2012, Delft University of Technology, 18-20 June 2012.