SAND2016-7778C

Exceptional service in the national interest

Sandia National Laboratories



Timothy Stirrup

Principal Safety Basis Engineer

System Theoretic Process Analysis

Practical Application With Traditional HA Techniques

August 6 – 12, 2016

2016 EFCOG

Safety Analysis Working Group

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

STPA Background

Sandia National Laboratories

- Analysis Technique Evaluates Interfaces
  - Between System Components [Hardware], Controllers [Software], and People
  - Using Process Feedback Loops [Input/Output]
- Created as Computer/Controller Analysis Technique From Leveson/Thomas @ MIT Boston
- Use of Functional Control Diagram, System Requirements, Hazard Scenarios, Safety Constraints and Safety Requirements

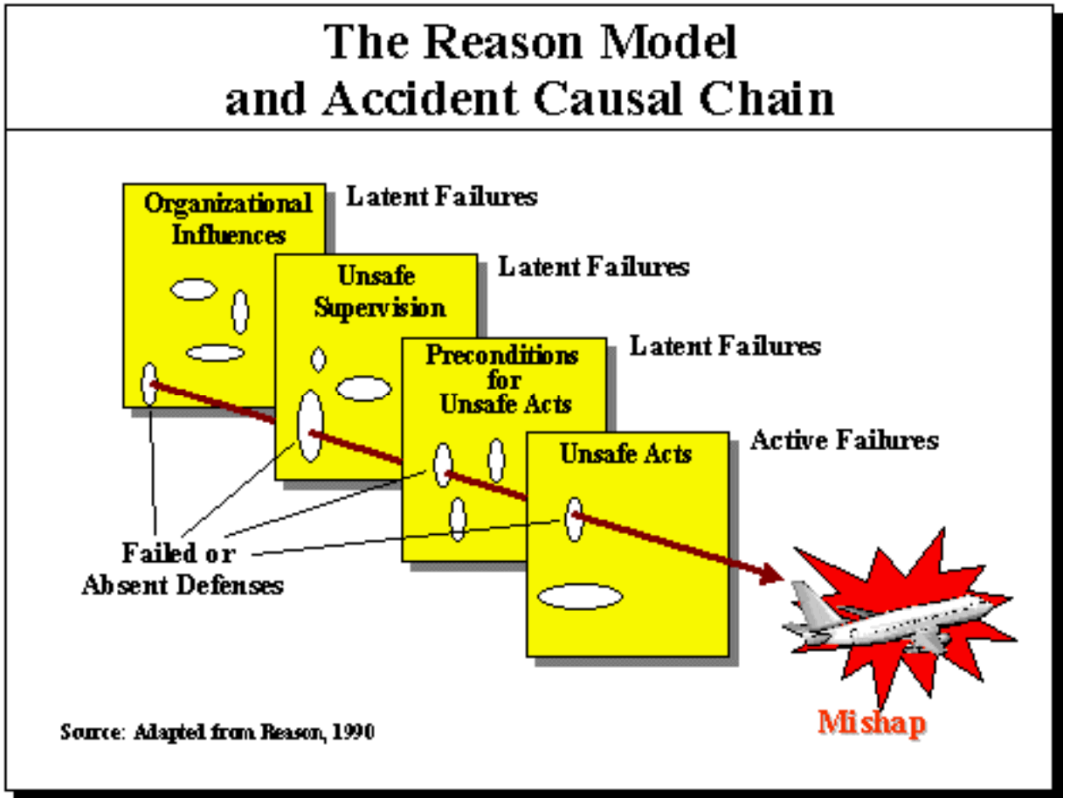
STPA Background

Sandia National Laboratories

- Leveson/Thomas Prescribe
  - Grew into Systems Theory to Address the Limitations of Traditional Safety Analysis Techniques (Leveson)
  - Top Down Hazards Evaluation Technique
    - Dysfunctional Interactions
    - Flawed Requirements
    - Design Errors
    - External Disturbances
    - Human Error
    - Human-Computer Interfaces
  - Any Stage of System Lifecycle

STPA Interfaces

- Traditional Looks at Controls
- STPA Looks In Between Controls



STPA Defining Terms

- Hazard (10 CFR 830)
  - A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to an operation or to the environment.
- Accident (DOE STD 3009)
  - An unplanned sequence of events that results in undesirable consequences.
- Hazard (Leveson)
  - A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)
- Accident (Leveson)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

STPA Process Overview

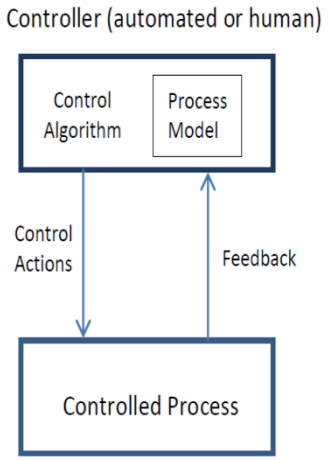
- Leveson Describes
  - Use of Functional Control Diagram
  - Define Safety Requirements for System/Component
  - Identify System Hazards
  - Identify Safety Constraints/Requirements for System/Component
- Leveson Defines 2 Steps
  - Step 1: Identify the Potential for Inadequate Control of the System Leading to Hazardous State
  - Step 2: Determine How Each Potentially Hazardous Control Action Could Occur

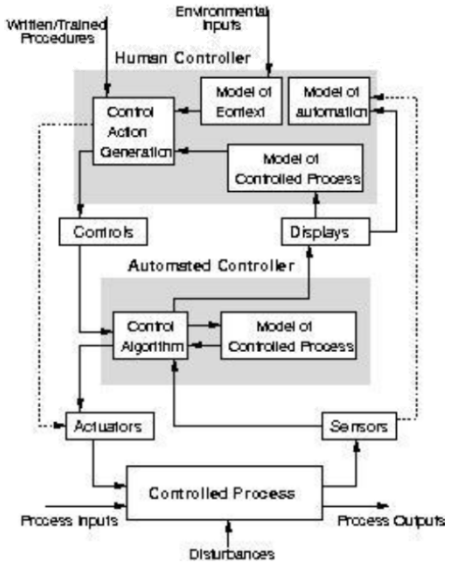
STPA Applied

- HAZOP Like: Use of “Prescribed” Terminology with Guidewords + Parameters + Context = Hazard [Scenario]
- Requires Skilled Facilitator with Scribe
- Requires Team Operations, Maintainance, & SMEs
- Supporting Information; Qualified Analyst; Representative Team; 9 – 100 Days Duration

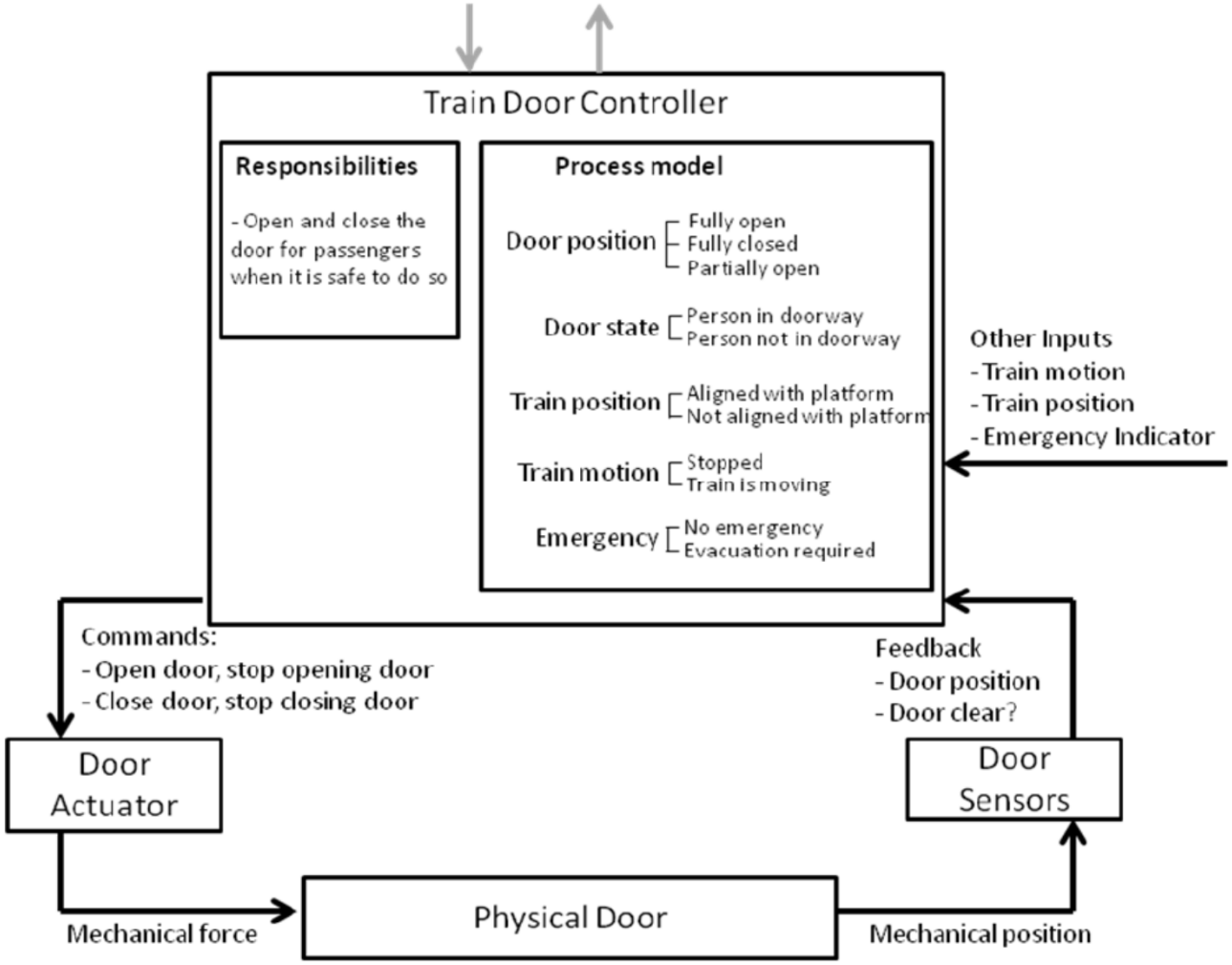
STPA Applied

- Create Process Model Diagrams
- Identify Feedback Loops
  - Human Interfaces
  - Controller Interfaces
  - Hardware Interfaces
- Start Small Depending on Lifecycle Stage of System
  - Evaluate Interfaces Within Each Interface
  - Evaluate Interfaces Between Each Interface
- Increase PMD Detail as Necessary





STPA Applied



STPA Applied

- Identify System Accidents
  - Simple vs Complex

Number	System Accident Description
A-1	Passenger Falls Out of Train
A-2	Passenger Hit By Door

- Identify System Hazard
  - Following Leveson Definition

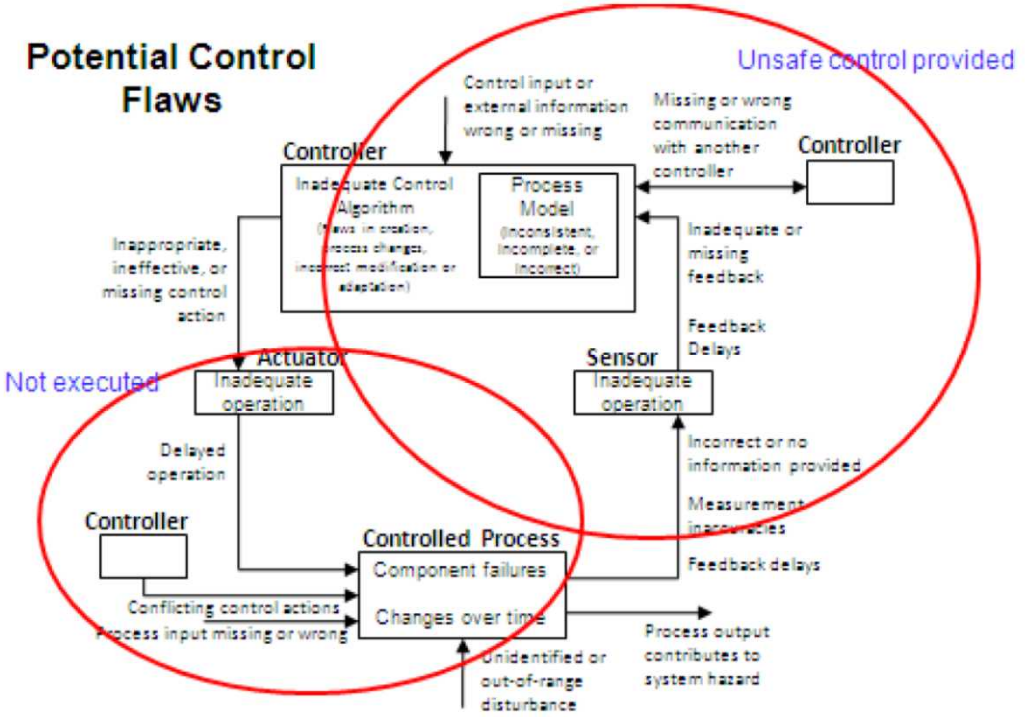
Number	System Hazard Description
H-1	Door is open when train starts
H-2	Door is open while train is moving
H-3	Door cannot be opened during an emergency

- Develop System Requirements/Constraints

Hazard	Safety Constraint
Door is open while train is moving	Train must never open while train is moving

STPA Applied

- Identify Potential Inadequate Control Action of the System
  - Identify Missing Interfaces
  - Where is Feedback Necessary
  - Identify Missing Elements of PMD
    - Could Identify Additional Controls



STPA Applied

Sandia National Laboratories

- Determine How Potential Inadequate Control Actions Occur
  - Causal Analysis
  - Context of Action

Control Action	Train Motion	Emergency	Train Position	Hazardous control action?		
				If provided any time in this context	If provided too early in this context	If provided too late in this context
Door open command provided	Train is moving	No emergency	(doesn't matter)	Yes (H-2)	Yes (H-2)	Yes (H-2)
Door open command provided	Train is moving	Emergency exists	(doesn't matter)	Yes[6](H-2)	Yes (H-2)	Yes (H-2)
Door open command provided	Train is stopped	Emergency exists	(doesn't matter)	No	No	Yes (H-3)
Door open command provided	Train is stopped	No emergency	Not aligned with platform	Yes (H-2)	Yes (H-2)	Yes (H-2)
Door open command provided	Train is stopped	No emergency	Aligned with platform	No	No	No

STPA Applied

- Table Format Identifying Unsafe Control Actions
  - Safe Control Action is Not Provided
  - Unsafe Control Action is Provided
  - Safe Control Action is Provided Too Late or Too Early
  - Safe Control Action is Stopped Too Soon or Applied Too Long
- Bin Hazardous Control Actions
- Resolve Hazardous Control Actions

Control Action	Hazardous Control Actions			
	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
Open train doors	Door open command not provided when train is stopped at platform and person in doorway (H-1) Door open command not provided when train is stopped and emergency exists (H-3)	Door open command provided when train is moving and there is no emergency (H-2) Door open command provided when train is moving and there is an emergency[9] (H-2) Door open command provided when train is stopped unaligned with platform and there is no emergency (H-2)	Door open command is provided more than X seconds after train stops during an emergency (H-3)	N/A

STPA Results

Sandia National Laboratories

- Qualitative Report
  - Completed “Hazardous Control Action” Table
  - List of Causal Scenarios
- Potential for Inherent Safety Review ~ Resolve Hazardous or Unsafe Control Actions
- Does
  - Result in Identification of Interface Issues
  - Result in a List of Control Actions That Provide System Control Requirements
- Does Not
  - Result in a Traditional List of Hazards & Controls
  - Readily Produce Results Conducive to Risk Evaluation

STPA Reality

- Disadvantages
  - Selling of STPA as Superior to All Other Techniques
    - Comparative Results Number Driven for Causal Identification
    - Primary Comparison to FTA/ETA not What-If/Checklist or HAZOP
  - Not Conducive to Overlay of Qualitative/Quantitative Risk Analyses
  - Does not Identify Traditional Controls/Safetguards
  - Computer/Controller Based Solutions
- Advantages
  - Preferred Use After Traditional Analyses That Define Controls & Risk
  - Key Analysis Technique
    - Iterative Process to Define Process Diagram
  - Excellent Technique for Interfaces
  - Use for System Design & Requirements Definition
  - Potential for Automated Analysis Using Spreadsheets/Binning

STPA References

- *Safeware: System Safety and Computers*; Leveson (1995) – Addison Wesley
- *Engineering A Safer World, Systems Thinking Applied to Safety*; Leveson (2011) – MIT Press
- *An Integrated Approach to Requirements Development and Hazard Analysis*, Thomas, John et al (2015) – SAE International