Integrating STPA in Large Organizations
(Thoughts and Perspectives)

Mark Vernacchia
GM Technical Fellow
Principal System Safety Engineer – Propulsion Systems

MIT STAMP Workshop
March 25 - 28, 2019

Integrating STPA in Large Organizations

- Presentation summarizes observations made by the writer
  - Initial introduction activities
  - Finding an initial application for STPA
  - Demonstrating value of STPA and validating STPA usefulness
  - Comparison of STPA to other system safety analysis methodologies
  - STPA and Model-Base Safety Representation
  - STPA evaluation effort
  - Effort to educate system safety engineers
  - Expansion of STPA usage beyond initial niche
  - Use of “systems thinking” and “systems engineering” philosophies
  - Potential future areas of STPA usage

Integrating STPA in Large Organizations

Integrating STPA in Large Organizations

- Initial Introduction Activities
  - Bring back STPA information from conferences/symposiums to your organization
  - Attend MIT STPA Workshops or review presentations from MIT PSAS site
  - Be open minded
  - Perform internal review of your own safety process
  - Assess possible usefulness

Integrating STPA in Large Organizations

- Tips for success
  - First and foremost - Make sure there is a need STPA can fill (ie: HMI – socio technical benefits)
  - Don’t try to change the whole world . . .
    - The goal should be not to solve world hunger, but just to feed the family . . .[1]

[1] G. Ressler – GM Tech Fellow

  - Maintain your vision . . . but be ready to modify based on good feedback or input
  - Leverage idea of continuous improvement for existing processes by enhancing use of systems engineering and systems thinking . . .
  - Talk to other people inside and outside of your organization . . .

Integrating STPA in Large Organizations

- Finding an initial application for STPA
  - Learn STPA to a working level
  - Look for an area with the greatest need
  - Propose STPA as an alternative to struggling methodology
    - Used STPA as alternative to a DFMEA effort to deal with human factors
  - Operate below the “radar”
    - Be focused
    - Do not alienate people with grandiose statements
    - Be respectful of people’s concerns

Integrating STPA in Large Organizations

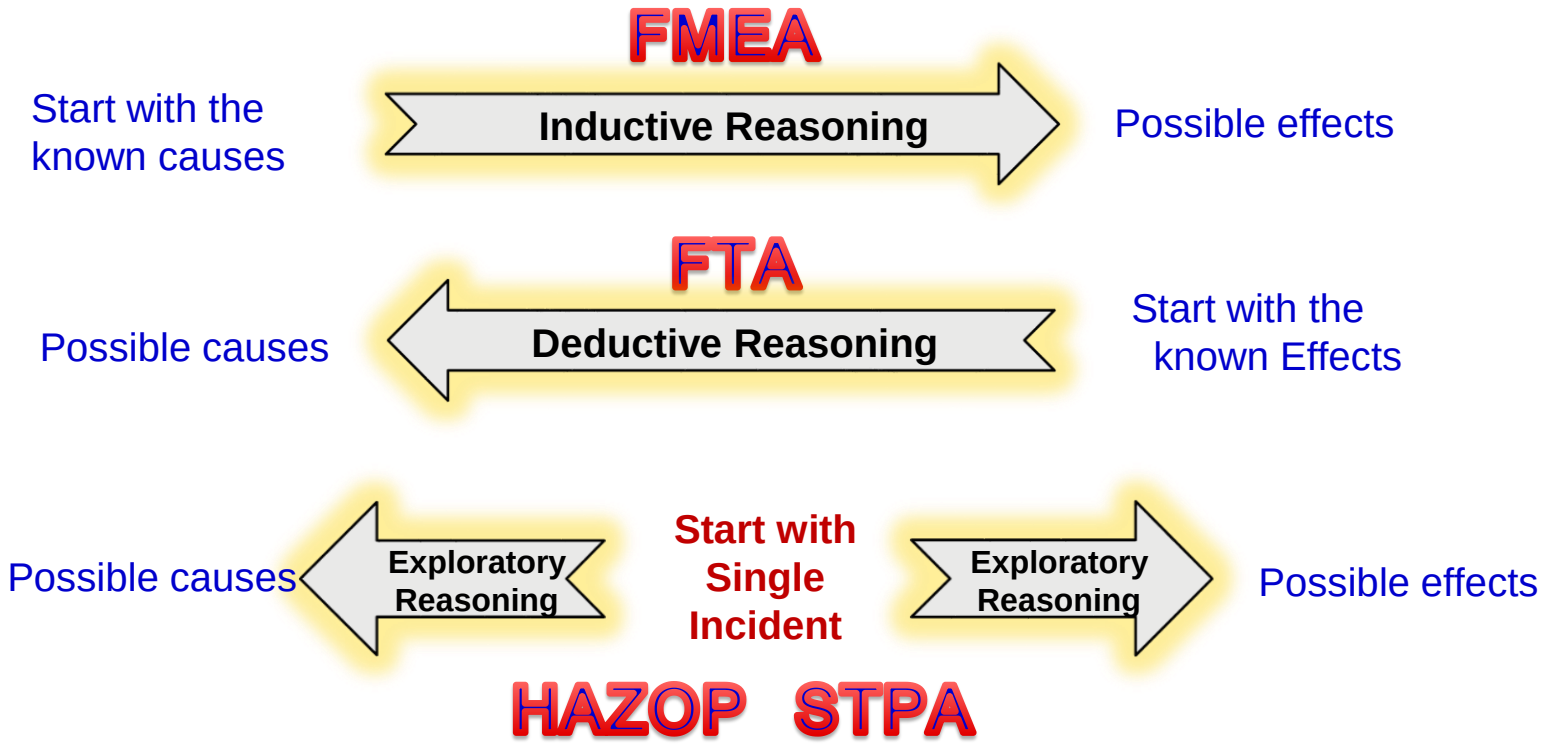
- Demonstrating value of STPA
  - Review results with program team
  - Demonstrate traceability logic
  - Emphasize STPA's use of causal scenarios
    - Do not need physical failures to have potential hazard
  - Test usefulness by assessing acceptance/rejection by program team
  - Test usefulness by evaluation how STPA supplements existing "standards" or processes
    - ISO 26262
    - HMI strength

Integrating STPA in Large Organizations

- Comparison of STPA to other safety analysis methodologies
  - Need to choose your “spectrum” philosophy

  - Consider how much effort needed to get rid of other methodologies and if organization would even entertain that idea
  - STPA is an “exploratory” to complement “inductive” (FMEA) and deductive (FTA) evaluation methodologies
  - Consider how STPA would/could feed or flow into other methods
  - Emphasize STPA can be very effective in finding missing requirements especially early in concept phase on systems that have significant HMI considerations

Integrating STPA in Large Organizations



Integrating STPA in Large Organizations

		Causes: Unknown	Causes: Known
Effects	Unknown	*Exploratory Analysis*	*Inductive Analysis*
Effects	Known	*Deductive Analysis*	*Descriptive Analysis*

- Deductive Analysis (e.g., FTA)
- Inductive Analysis (e.g., FMEA, Interface Analysis, Sneak Circuit Analysis)
- Exploratory Analysis (e.g., HAZOP, what-if, STPA)
- Descriptive Analysis (relatively straight forward observations)

Integrating STPA in Large Organizations

- STPA and Model-Base Safety Representation
  - Representation Examples
    - UCA constraints equivalent to “safety goals”
    - UCA themselves equivalent to “malfunctions”
    - Causal scenarios/factors equivalent to “malfunction causes”
    - Requirements linked to “safety goals”
  - OMG (Object Management Group) standard
    - Influence on methodology
    - Tool supplier review and response

Integrating STPA in Large Organizations

- STPA evaluation effort
  - Emphasize STPA provides straightforward methodology to assess designs and define requirements necessary to prevent or manage hazard
  - STPA can be used instead of other evaluation methods
    - HMI – STPA worked better than FMEA approach to deal with causal scenarios
    - Electric Power Steering – STPA provided requirements at multiple levels more efficiently than a system element fault analysis did (use of abstraction)
  - STPA can save effort by substituting or supplementing for current evaluations methods or by filling a role for a missing evaluation.
  - Take time to work 1-on-1 with groups to educate them on STPA opportunities

Integrating STPA in Large Organizations

- Effort to educate system safety engineers
  - Having STPA as a recognized part of internal system safety process
  - Develop educational collateral to be used by SSE
    - Training sessions
    - Documents explaining and providing examples, examples, examples (did I say “examples”?)
    - Hands on sessions
  - Find willing practitioners
  - Leverage system engineering and system thinking perspective

Integrating STPA in Large Organizations

- Expansion of STPA usage beyond initial application
  - Integrate STPA as part of expected process(es)
  - Apply STPA to applications of HMI and complex programs
  - Relentless, respectful, enthusiastic support without alienating people
  - Find a different respected person/people to be STPA proponents
  - Incorporate STPA generated requirements into corporate requirement documents and specifications
  - Seek out like-minded STPA practitioners in your industry or across industries to find common interests and needs
    - SAE STPA Recommended Practices Task Force

Integrating STPA in Large Organizations

- Expansion of STPA usage beyond initial application
  - Demonstrate value of STPA requirements addressing safety concerns
  - Associate STPA with corporate initiatives when it helps those initiatives
  - Leverage systems engineering and system thinking
  - Use on programs with new functions and features that have not been implemented yet or implemented together yet
  - Gather objective data showing results
    - Requirements generated
    - Design updates and changes driven by STPA evaluations
    - Short time to get results

Integrating STPA in Large Organizations

- Use of “systems thinking” philosophies (INCOSE ref.)
  - Systems thinking is a holistic approach to analysis that focuses on the way that a system's constituent parts interrelate and how systems work over time and within the context of larger systems.
  - The approach of systems thinking is fundamentally different from that of traditional forms of analysis. Traditional analysis focuses on the separating the individual pieces of what is being studied; in fact, the word "analysis" actually comes from the root meaning "to break into constituent parts."
  - Systems thinking, in contrast, focuses on how the thing being studied interacts with the other constituents of the system - a set of elements that interact to produce behavior - of which it is a part.

Integrating STPA in Large Organizations

- Use “systems engineering” philosophies –
  - Systems Engineering is an engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and stakeholder's needs are satisfied in a high quality, trustworthy, cost efficient and schedule compliant manner throughout a system's entire life cycle. (INCOSE)
- Apply Father Flanagan’s belief that “there is no such thing as a bad boy” to engineers . . .
  - Engineers want to do good engineering
- Realize that not all engineers can do systems engineering well

Integrating STPA in Large Organizations

- Potential future areas of STPA usage
  - More HMI evaluations
  - Complex systems evaluations
  - SOTIF evaluations
- *Questions??*