STPA Industrialization / Adoption in Industry
(Thoughts and Perspectives - 2020)

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

MIT STAMP Workshop
July 29, 2020
STPA Industrialization and Adoption in Industry

• Presentation summarizes observations made by the writer
  • Initial introduction activities
  • Finding an initial application for STPA
  • Demonstrating value of STPA and validating STPA usefulness
  • STPA and other system safety analysis methodologies
  • STPA evaluation effort
  • Effort to educate system safety engineers
  • Expansion of STPA usage beyond initial niche
  • Potential future areas of STPA usage
STPA Industrialization and Adoption in Industry

- Inductive Reasoning: Start with the known causes, Possible effects
- Deductive Reasoning: Start with the known effects, Possible causes
- Exploratory Reasoning: Start with Single Incident, Possible causes
- FMEA
- FTA
- HAZOP
- STPA

Mark Vernacchia - GM Technical Fellow - Principal System Safety Engineer – Propulsion Systems
## STPA Industrialization and Adoption in Industry

<table>
<thead>
<tr>
<th>Causes</th>
<th>Unknown</th>
<th>Known</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effects</td>
<td><strong>Unknown</strong></td>
<td><strong>Inductive Analysis</strong></td>
</tr>
<tr>
<td>Unknown</td>
<td><strong>Exploratory Analysis</strong></td>
<td><strong>Descriptive Analysis</strong></td>
</tr>
<tr>
<td>Known</td>
<td><strong>Deductive Analysis</strong></td>
<td></td>
</tr>
</tbody>
</table>

- Deductive Analysis (e.g., FTA)
- Inductive Analysis (e.g., FMEA, Interface Analysis)
- Exploratory Analysis (e.g., HAZOP, what-if, STPA)
- Descriptive Analysis (e.g., straight forward observations)
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
Incorporation of STPA Requirements into Appropriate Sub-System and Component Specification Documents And into Design Center “Best Practices”
Integration of STPA into GM Safety Process – Shift by Wire Example

• Understanding requirements linkage to potential hazardous states allowed “Design Center” teams to accommodate safety requirements (data driven)

• STPA derived requirements GMC Terrain Push-Button design:
  • Different motions to obtain Drive or Reverse versus Neutral or Park
  • Pull buttons for any propulsion range selection (Reverse and Drive)
  • One motion (push to get easily to Park or to Neutral)
  • Buttons laid out in familiar, expected pattern (PRNDL)
  • Buttons do not latch, instead are mono-stable
  • Software content to manage inappropriate shift requests while at speed
  • Auto-park capability if vehicle not placed in Park when required
Backup
STPA Industrialization and Adoption in Industry

• 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
STPA Industrialization and Adoption in Industry

• Tips for success
  • First and foremost - Make sure there is a need STPA can fill (i.e., 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\(^1\)
  • 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 . . .

\(^1\) G. Ressler – GM Tech Fellow
STPA Industrialization and Adoption in Industry

• 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
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
  - ISO PAS 21444 (SOTIF)
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 to deal with causal scenarios
  - Electric Power Steering – STPA provided requirements at multiple levels more efficiently than system element fault analysis did (use 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
STPA Industrialization and Adoption in Industry

• Effort to educate system safety engineers
  • 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
STPA Industrialization and Adoption in Industry

• 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 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

Mark Vernacchia - GM Technical Fellow - Principal System Safety Engineer – Propulsion Systems
• Expansion of STPA usage beyond initial application
  • Demonstrate value of STPA requirements for safety concerns
  • Associate STPA with corporate initiatives when it helps
  • 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
Integration of STPA into GM System Safety Process

• **Why Do This?**

  • *ISO26262 does not sufficiently address the evaluation of human behavior as part of its process as thoroughly as GM desires for HMI*

  • *This is an instance of the GM strategy to incorporate the “best of the best” from system safety sources outside of GM*
Integration of STPA into GM Safety Process – Shift by Wire Example
Integrating STPA in Large Organizations

• Potential future areas of STPA usage
  • More HMI evaluations
  • Complex systems evaluations
  • SOTIF evaluations

Questions??