STPA DRIVEN DESIGN
INFORMING DIGITAL TWIN DEVELOPMENT & LESSONS LEARNED FOR FACILITATORS

07 JUNE 2023

MIT STAMP WORKSHOP 2023

LEAD AUTHOR

MEAGHAN O'NEIL
SYSTEM DESIGN AND STRATEGY LTD
BRISTOL, UNITED KINGDOM
WWW.SYSTEMDESIGNSTRATEGY.CO.UK
INCOSE SYSTEM SAFETY WORKING GROUP CO-CHAIR

CO-AUTHOR

RICHARD BYE
HEAD OF ERGONOMICS
NETWORK RAIL
UNITED KINGDOM
MEAGHAN O’NEIL, SYSTEMS PRACTITIONER
19+ YEARS DESIGN AND DELIVERY EXPERIENCE IN SAFETY CRITICAL SYSTEMS

- **System Safety experiences with systems including products and services**
  Medical Device, Healthcare Services, Power Generation, Fire Fighting PPE and control systems, Infrastructure, Manual and Automated Manufacturing, Visual Inspection, Automotive, Aerospace, Rail

- **Provide extensive systems consulting experience.** Founder of System Design and Strategy Ltd, previous experience at Accenture and Cambridge Consultants. Experience providing systems consulting and training to a wide range of industry sectors worldwide.

- **Contribute internationally to progress the state of the practice of system safety and system engineering practices.** Leader (10+ years) International Council on Systems Engineering (INCOSE), Co-chair International Systems Safety Working Group, Elected International Treasurer/Officer INCOSE Board, Co-chaired International Biomedical Working Group.

- **Education and research background.** Chemical Engineering Bachelors (Cornell University), System Design and Management Masters (Massachusetts Institute of Technology), dissertation on System Safety Approaches Applied to Healthcare Adverse Events. Experience in Genetics, Healthcare and Systems Research.

- **General Aviation Pilot:** FAA Commercial Single Engine License, Instrument Rated
STPA HIGHLIGHTS

- Master thesis, MIT; Dr. Nancy Leveson
  - Application of CAST to Healthcare Adverse Events (2014)
- System responsibilities as director level leader and as consultant:
  - Director for System Engineering and responsible owner for Risk Management, Class I and II medical device which included STPA and other methods
  - STPA trainer, facilitator
  - External reviewer of system safety approaches and safety critical system designs
  - Applied STPA to identify business development opportunities
- Application in a wide range of systems:
RECAP ON PREVIOUS FOCUS: COMPARING STPA APPLICATIONS BASED ON WHEN IT IS APPLIED

STPA Applied After Design

Assess Need
Market

Feasibility

Design

Verify & Document

Validate

“Versus”

STPA Applied Early and Iteratively

Assess Need
Market

Feasibility

Design

Verify & Document

Validate
FIRST APPLICATIONS OF STPA OFTEN OCCUR LATE IN A PROGRAM SCHEDULE

External consultation:
- Unresolved concern(s) at entry to formal testing
- First time applying STPA internally falters

Internal application:
- STPA applied when design FMEA’s sessions are scheduled

Common challenges that result
- Design “freeze” leads to high resistance to change (launch date inertia)
- Viewed as documentation exercise for a regulatory filing, not part of design
- Time with designers may be limited
- “Blame culture” common when late changes realised

Common reasons:

<table>
<thead>
<tr>
<th>Phase when error is detected and fixed</th>
<th>Cost to Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>x1 (reference)</td>
</tr>
<tr>
<td>Design</td>
<td>x3 - x8</td>
</tr>
<tr>
<td>Build</td>
<td>x7 - x16</td>
</tr>
<tr>
<td>Test</td>
<td>x21 – x78</td>
</tr>
<tr>
<td>Operations</td>
<td>x29 – x1615</td>
</tr>
</tbody>
</table>

INCOSE UK Z3 Guide
APPLY STPA EARLY AND ITERATIVELY THROUGHOUT DESIGN PROCESS TO MAXIMIZE BENEFIT

Benefits:

- Can allow a core team to become familiar and practiced with the method
- Hierarchical Control Diagrams can be less challenging to define at system level
- Design tool that enables safety driven design

Common pitfalls to avoid:

- Viewed as a preliminary hazard analysis and not maintained as design changes
- Schedule does not account for time needed
- Discussions but not documented
- Viewed as time based activity; has been “completed” therefore “sufficient”
- Focus on time / cost savings leads to false expectations as “silver bullet”
THE FOCUS OF THIS PRESENTATION IS THE APPLICATION OF STPA EARLY IN THE DESIGN PROCESS

STPA Applied
After Design

Assess Need Market
Feasibility
Design
Verify & Document
Validate

STPA Applied
Early and Iteratively

Assess Need Market
Feasibility
Design
Verify & Document
Validate
Focus of this presentation is on the application of STPA early in the design process
FACILITATION: RECOMMENDATIONS FOR FACILITATION OF STPA IN PRACTICE IN EARLY-STAGE DESIGN

1) Consider Context and Tailor
2) Value Diversity and Plan for It
3) Partnership and the power of 2
4) Commonly Overlooked Opportunities
1. CONSIDER THE CONTEXT OF YOUR STPA ANALYSIS AND TAILOR YOUR FACILITATION APPROACH ACCORDINGLY

- Level of STPA experience
- Programmatic Schedule Pressure
- Approach to analysis
- Documentation approach
2. VALUE DIVERSITY AND SEEK IT OUT; DON’T FORGET TO CONSIDER HOW TO ADJUST YOUR APPROACH

- System Perspectives
- Group versus interviews
- Objection handling and common areas of confusion
3. THE POWER OF 2: PARTNERING IN STPA FACILITATION CAN BE HIGHLY EFFECTIVE

- No position is perfect; there are different advantages to being internal versus external
- Cross disciplinary pairing can be highly effective
- Knowledge pairing: Method, Domain, Enterprise, Culture, Design Process
4. COMMONLY OVERLOOKED AREAS OF STPA

- STPA Step 1: Assumptions
- Operational Reality
- Current and New
- Dynamics of Control Structure
- Purpose (confusing ends, ways, means)
EXPLORATION: EVALUATE THE DESIGN SPACE EFFICIENTLY AND EFFECTIVELY

1) Opportunity
2) Approach: Model and Simulation
3) STPA Driven Design for Synthetic Environments, Digital Twin
FOCUS: GAINING INSIGHT AND AIDING DECISION MAKING

1) Areas of concern, opportunity
2) Communication to stakeholders
3) Managing expectations
LESSONS LEARNED FROM A PRACTITIONERS PERSPECTIVE ON STPA APPLIED IN EARLY-STAGE DESIGN

SYSTEM DESIGN AND STRATEGY LTD

Supporting design, improvement, and strategic decision making at the intersection of people and technology

Meaghan O'Neil
monell@systemdesignstrategy.co.uk
www.systemdesignandstrategy.co.uk
Bristol, UK