LESSONS LEARNED FROM STPA APPLICATIONS

07 JUNE 2022

MIT STAMP WORKSHOP 2022

MEAGHAN O'NEIL

SYSTEM DESIGN AND STRATEGY LTD

BRISTOL, UNITED KINGDOM

WWW.SYSTEMDESIGNSTRATEGY.CO.UK

MEAGHAN O'NEIL, SYSTEMS PRACTITIONER
18+ YEARS DESIGN AND DELIVERY EXPERIENCE IN SAFETY CRITICAL SYSTEMS

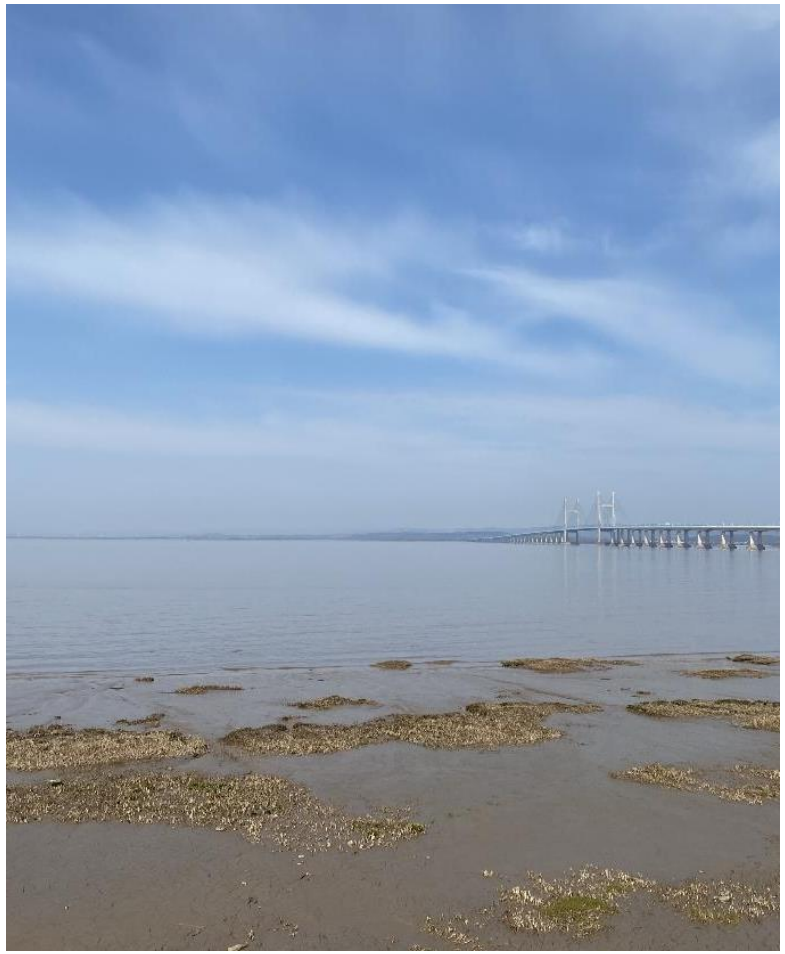
- **System Safety experiences with systems including products and services** Medical Device, Healthcare Services, Power Generation, Fire Fighting PPE and control systems, Infrastructure, Manual and Automated Manufacturing, Visual Inspection, Automotive, Aerospace
- **Provide extensive systems consulting 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 Treasure/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, Advanced Ground Instructor

STPA HIGHLIGHTS

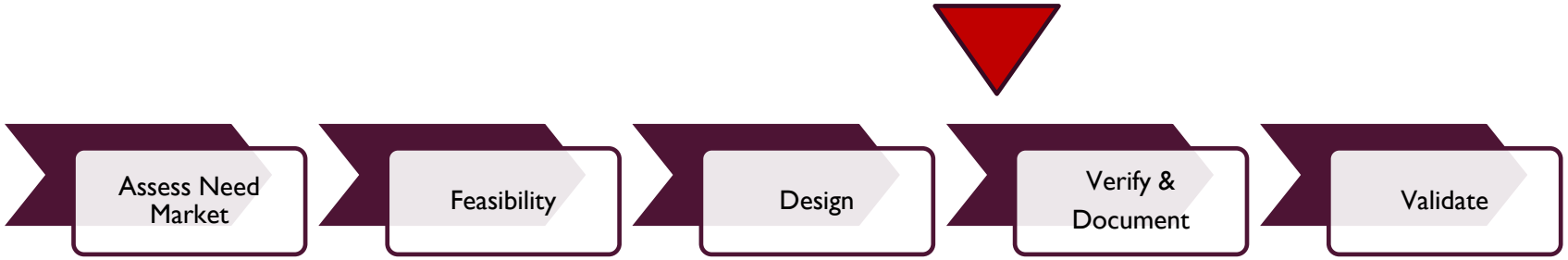
- Master thesis, MIT; Dr. Nancy Leveson
  - Application of CAST to Healthcare Adverse Events (2014)
- System responsibilities as director level leader and as consultant:
  - Director for System Engineering and responsible owner for Risk Management, Class I and II medical device which included STPA and 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 of Systems:
  - Medical Device (Class I and Class II), Biomedical Reactor Design, Healthcare Services, Power Generation and Storage, Fire Fighting PPE and control systems, Infrastructure, Manual and Automated Manufacturing,Visual Inspection, Automotive, Aerospace

LESSONS LEARNED HIGHLIGHTS FROM MY PRACTITIONER EXPERIENCE WITH APPLYING STPA OVER THE LAST TEN YEARS

- Apply STPA early iteratively throughout design process to maximize benefits
- Process aids developing a consistent mental model across the design team
- Successful approaches are a "team sport"
- Common design challenges uncovered: underdeveloped feedback loops and changes in control structure
- Manage expectations and value diversity



FIRST APPLICATIONS OF STPA OFTEN OCCUR LATE IN A PROGRAM SCHEDULE



Common reasons:

<u>External consultation:</u>

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

<u>Internal application:</u>

- STPA applied when design FMEA's sessions are scheduled

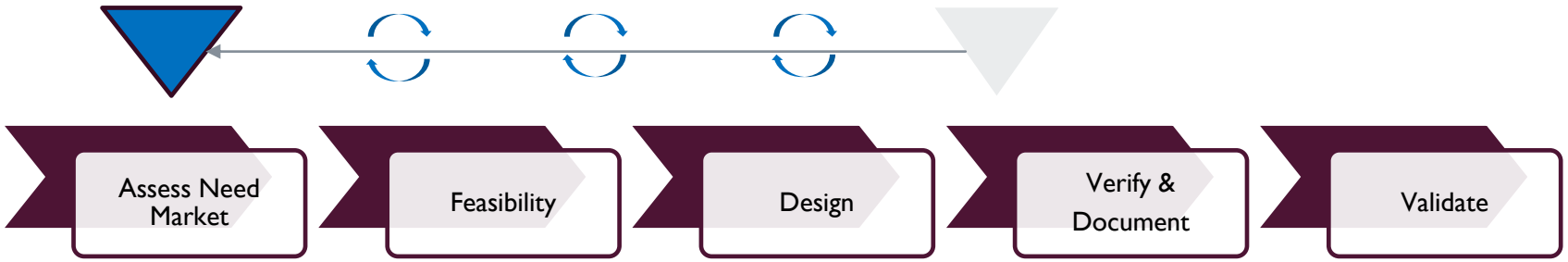
Common challenges that result

- 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

Phase when error is detected and fixed	Cost to Fix
Requirements	x1 (reference)
Design	x3 - x8
Build	x7 - x16
Test	x21 – x78
Operations	x29 – x1615

INCOSE UK Z3 Guide
Primary Reference: "Error Cost Escalation Through the Project Life Cycle", Haskins et al, Proceedings of INCOSE International Symposium 2004.

APPLY STPA EARLY AND ITERATIVELY THROUGHOUT DESIGN PROCESS TO MAXIMIZE BENEFIT



Benefits:

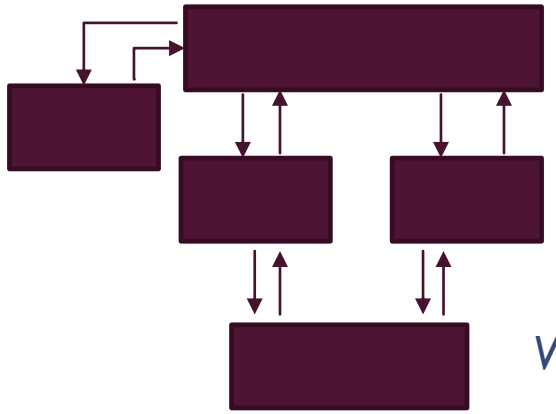
- Can allow a core team to become familiar and practiced with the method
- Hierarchical Control Diagrams can be less challenging to define at system level
- Design tool that enables safety driven design

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"

PROCESS AIDS DEVELOPING A CONSISTENT MENTAL MODEL ACROSS THE DESIGN TEAM … IF VIEWED AS A TEAM SPORT

- Develop and discuss hierarchical control structure
  - Develops the mental model within the team
  - Often prompts development of key system level documentation such as
    - Concept of Operations
    - Concept of Maintenance
    - Mode Transitions
    - Alternatives
    - Rationale for design decisions



Why would a user do that?

Why have you done it that way?

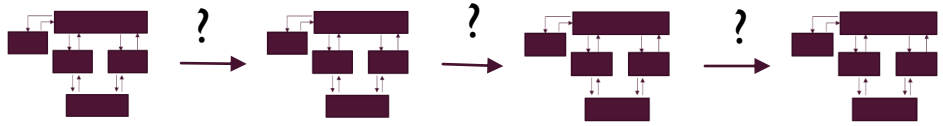
How often does that occur?

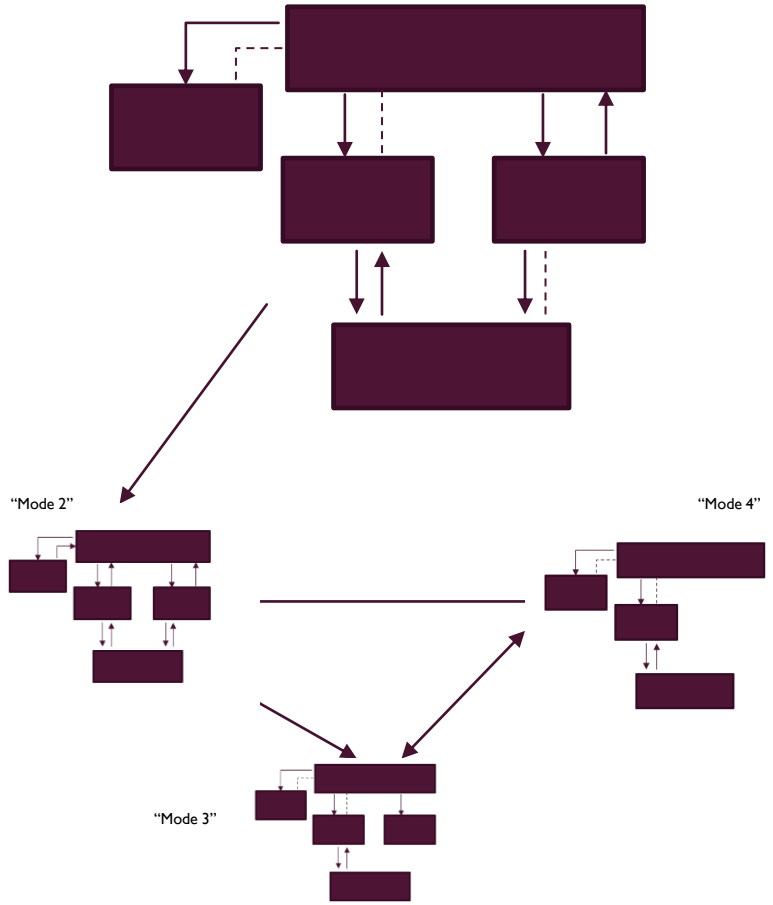
Would that always occur?

How would they know that occurred?

COMMON DESIGN CHALLENGES UNCOVERED: UNDERDEVELOPED FEEDBACK LOOPS AND CHANGES IN CONTROL STRUCTURE

- Feedback loops often underdeveloped
- Mode Transitions are often challenging
  - Inconsistent mental models across team
  - Incorrect assumptions
  - Missing Feedback
- Hierarchical control changes
  - Between design, test, deployment
  - Related to alternative or past operator experience
  - Over time





MANAGE EXPECTATIONS AND VALUE DIVERSITY

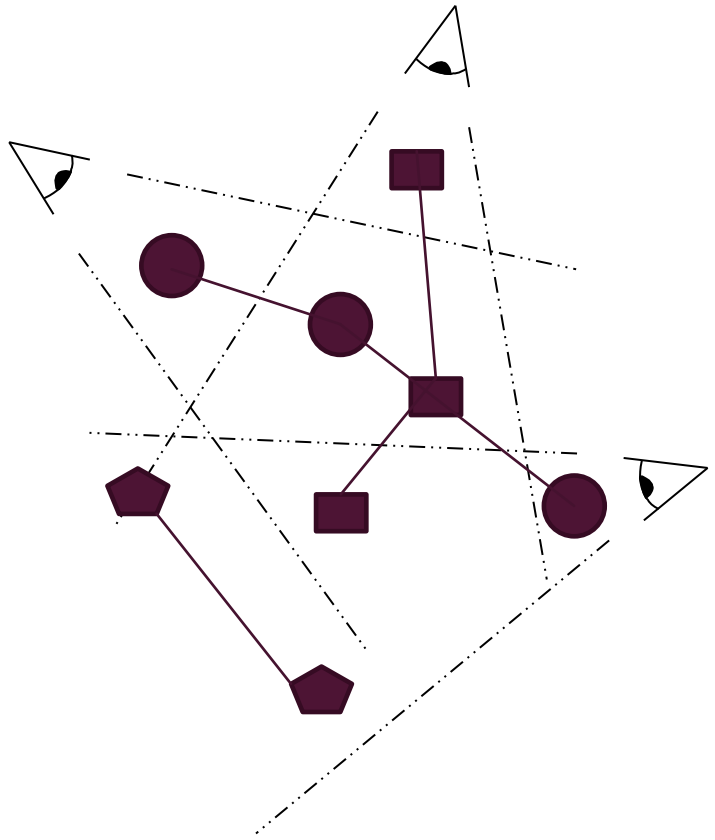
- Systems thinking 101
  - Diverse team, different perspectives
- Diversity in many forms e.g.
  - People
  - Approaches

Technical Disciplines | Non Technical

Novice | Expert

Internal | External

Application Experience



- Diversity can require effort
- Manage unrealistic expectations
  - "Silver bullet"
  - *"Single approach expected to be better, faster, and cheaper"*
  - Conducted by "expert" as a solo activity
- Uncovering issues late can be uncomfortable
- Early discoveries can be forgotten (document as you go)

LESSONS LEARNED HIGHLIGHTS FROM MY PRACTITIONER EXPERIENCE WITH APPLYING STPA OVER THE LAST TEN YEARS

SYSTEM DESIGN AND STRATEGY LTD

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

Meaghan O'Neil

moneil@systemdesignstrategy.co.uk

www.systemdesignandstrategy.co.uk

Bristol, UK