Massachusetts
Institute of
Technology

Implementing STPA successfully in industry

Dr. John Thomas

Experiences across industries

(Automotive, Aviation, Space Systems, Chemical, Oil & Gas, Nuclear Power, Defense, Healthcare, Medical Devices, Particle Accelerators, National Labs, Universities)

Any questions? Email me! JThomas4@mit.edu

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in from high-level management
- Data!

Learning enough to adopt STPA

	Cost	Effort needed	Scalability	Effectiveness
Reading existing papers, reports, books	Free	High	High	Low
Attending MIT STAMP workshop	Low	Low	Low	Med
Participating in existing STPA project	Low	Med	Low	Med
Attending STPA training session	Med	Med	Med	High (but quality varies!)
Dedicated project-based workshop & education	High	Med	Low	Extremely High!
Online education (planned by Leveson/Thomas)	Free	Low	High	<unknown>

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Complexity makes STPA shine!

- The more complex the problem, the more powerful STPA will be
- Choose systems where there is opportunity to be surprised
- Potential for unexpected behavior or unanticipated interactions

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Complexity makes STPA shine!

- Systems with many interactions, where systems are being made
- Different decision-makers trying to work together: computers, humans, organizations, etc.
- Especially incentives to optimize locally, but not necessarily globally

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Complexity makes STPA shine!

Maximize impact

- Identify areas of concern, start there
- Start with high-severity problems like risky phases of operation (e.g. docking HTV)
- Choose systems where people aren’t sure if you already addressed everything

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

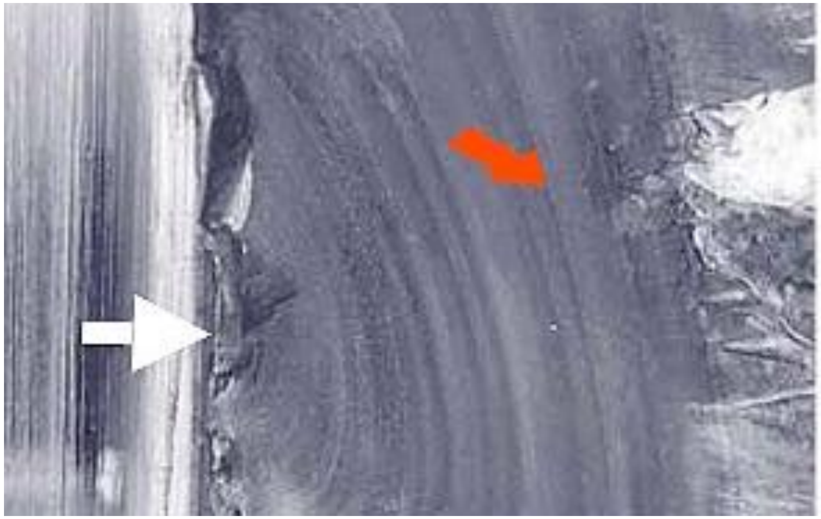
Complexity makes STPA shine!

Maximize impact

Functional analysis

- Focus on people or machines providing functions
- Not just purely physical phenomenon
  - Material flammability?
  - Physical metal fatigue?

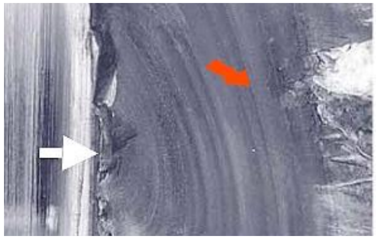
Implementing STPA successfully



Metal Fatigue

Material flammability

Not best choice for purely physical phenomena!



HOWEVER

STPA is a great choice as soon as you consider the bigger picture!

“Oakland Firefighters Say Their Department Is So Badly Managed, Ghost Ship Warehouse Wasn't Even In Its Inspection Database”

“FAA orders airlines to inspect 737s for cracks: three days earlier, undetected cracks widened into a five-foot hole in the roof of a Southwest 737, forcing an emergency landing”

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Interdisciplinary team

- Depends on the problem and control structure!

May include:

- Maintenance expert
- Regulations expert
- Operators (e.g. Pilots)
- Software experts
- Testers
- Etc.

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Interdisciplinary team

STPA Facilitator

- Methodology guidance and expertise, help avoid common traps, help review results, etc.

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Interdisciplinary team

STPA Facilitator

Personalities Matter!

- Need open-minded people who want to try something new
- Need "systems thinkers" who recognize impact of indirect interactions

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Interdisciplinary team

STPA Facilitator

Personalities Matter!

- Designers: Most knowledge, but can get defensive
- Outsiders: Not defensive, but may have less knowledge
- Tradeoff!

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Interdisciplinary team

STPA Facilitator

Personalities Matter!

- Need people not afraid to dig deeper, suggest fundamental changes, question long-held assumptions, shed light on systemic problems
- Sometimes less experience helps!

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Develop a plan

- Guided by STPA Facilitator
- Start with project goals
  - Pilot demonstration, analyze whole system, just learn STPA, provide comparison data, produce facilitators, etc.?

Implementing STPA successfully

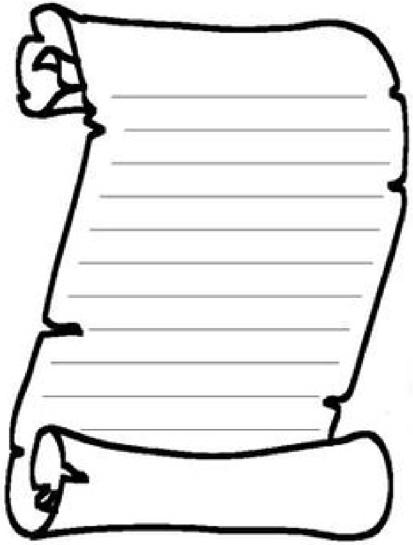
- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Develop a plan

- Guided by STPA Facilitator
- Consider constraints
    - Available resources
    - Budget
    - Schedule
    - Current projects
- Look at past experiences
    - What worked, didn’t work

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

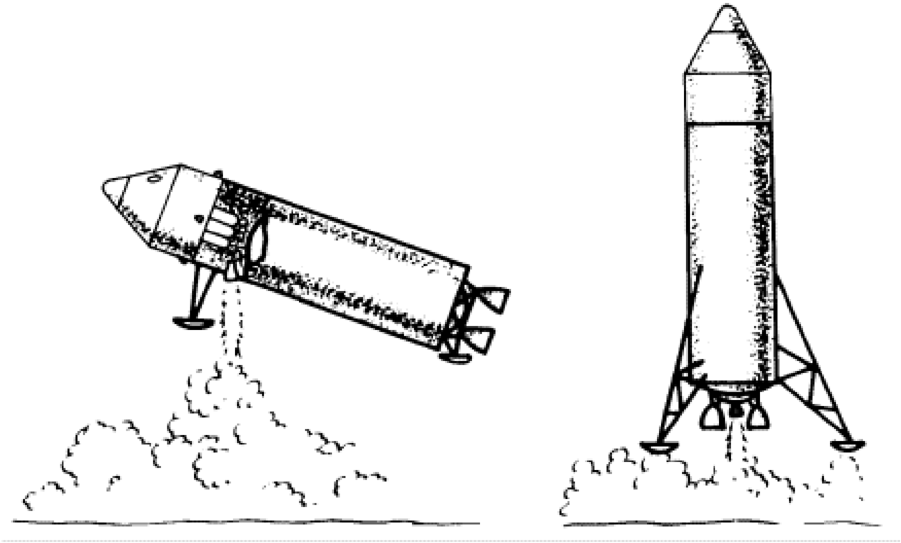


Generic plan may include

- Identify goals
- Select project
- Preparation
- Preliminary STPA work
- Workshop
- Follow-up activities
- Solutions development
- Consequences of solutions
- Summarize conclusions/key findings

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in



Ideal STPA project

- Still in early concept
- Not yet finished or implemented
- STPA is most powerful when used early!

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Select project

Team Preparation

- Identify core STPA team
- Gather info about the system

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Select project

Team Preparation

STPA Preparation (quick)

- High-level control structures
- Initial UCAs, some scenarios
- Anticipate major questions and identify any roadblocks
- Identify any additional experts needed

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Workshop!

- Bring together interdisciplinary team, perhaps 5-12 people
- STPA overview and training (if new to STPA)
- Review prepared control structures
- Perform STPA, iterate and add details as appropriate
- Generate new questions, identify follow-up activities and outstanding areas
- Tends to produce lots of critical results very quickly!
  - 70% of final results may be generated here
  - Usually within 3-5 days
  - Disseminate big issues immediately!

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Select project

Team Preparation

STPA Preparation (quick)

Workshop

Finish STPA for identified areas

- Iterate on outstanding areas
- Follow-up activities, check assumptions made
- Incorporate new changes, new details if needed
- Review results

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Solutions Workshop

- Identify solutions for unsolved or stubborn issues
- Phase 1: Generation
  - Encourage creativity, cross-pollination of ideas
  - Wild suggestions encouraged (they trigger other ideas)
- Phase 2: Building practical solutions
  - Select, adapt, and combine solutions to ensure feasibility
- Consequences of solutions

Implementing STPA successfully

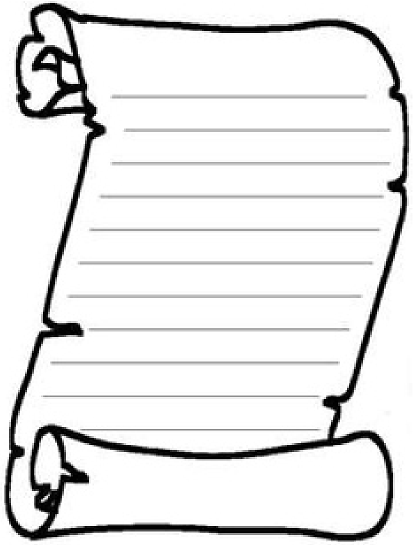
- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

Summarize conclusions/key findings

- Ideally, detailed findings already given to engineering team
- Need high-level message for managers and decision-makers
- Find the powerful results, the "aha moments"
- Identify other teams, groups, departments that would benefit
- Spread the word!

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in



Generic plan may include

- Identify goals
- Select project
- Preparation
- Preliminary STPA work
- Workshop
- Follow-up activities
- Solutions development
- Consequences of solutions
- Summarize conclusions/key findings

Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

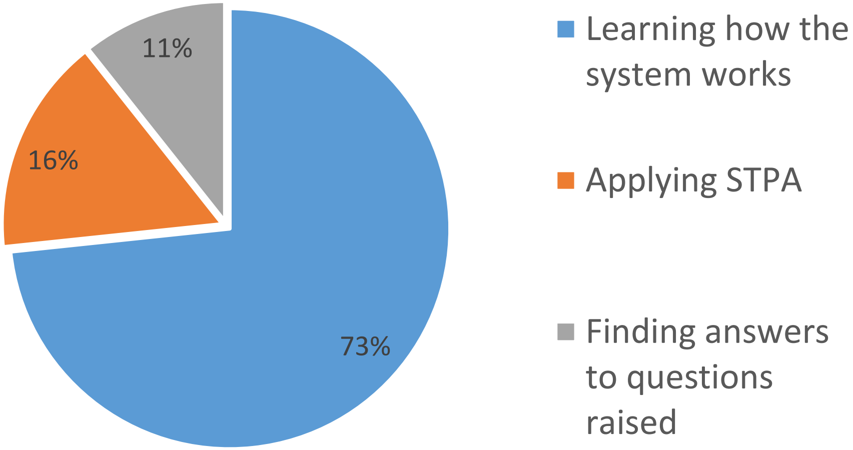
- STPA encourages high-impact long-term solutions that may involve fundamental changes, not just minor low-level patches
- Helps to know managers want these proposals, not just temporary or superficial recommendations!

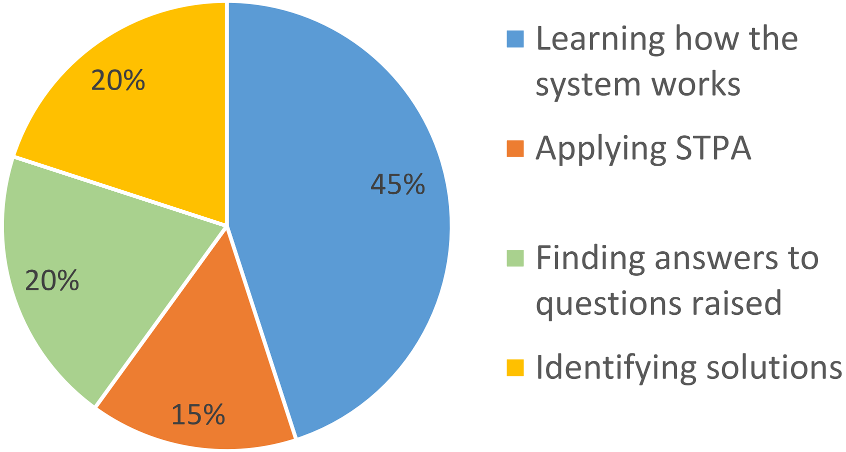
Implementing STPA successfully

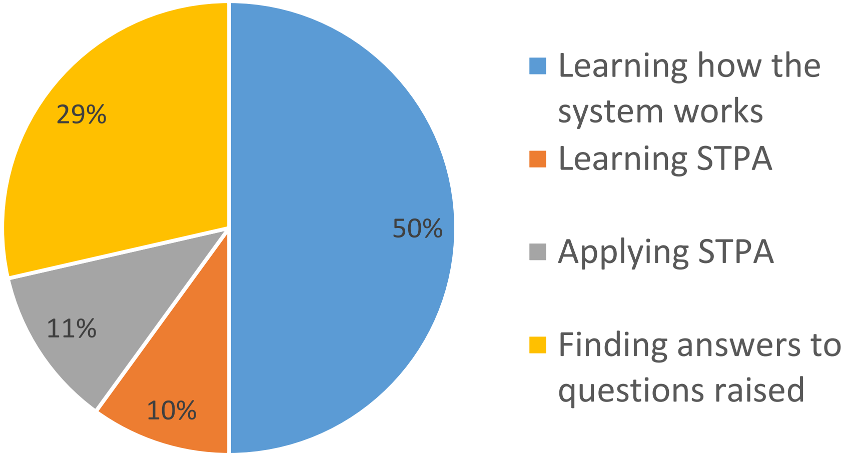
- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in

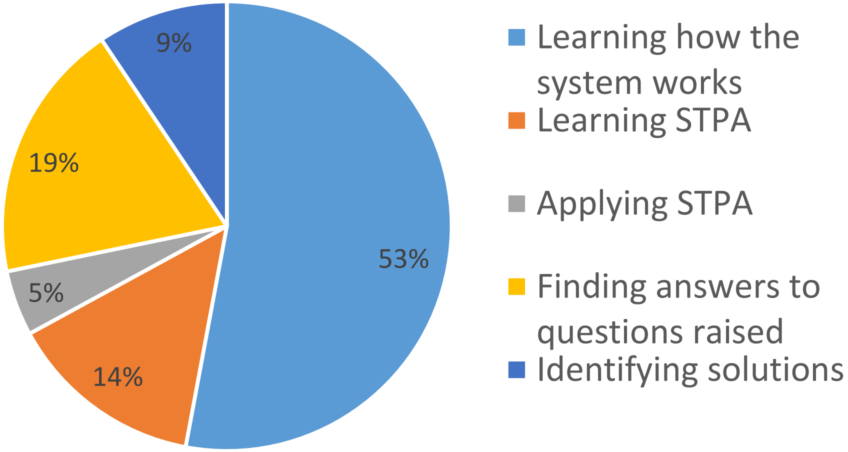
- Sometimes seen as a competitive advantage
  - Secrecy
- “We want to be recognized as a leader in our industry”
  - We want everyone to know we were first!

Data from 4 projects



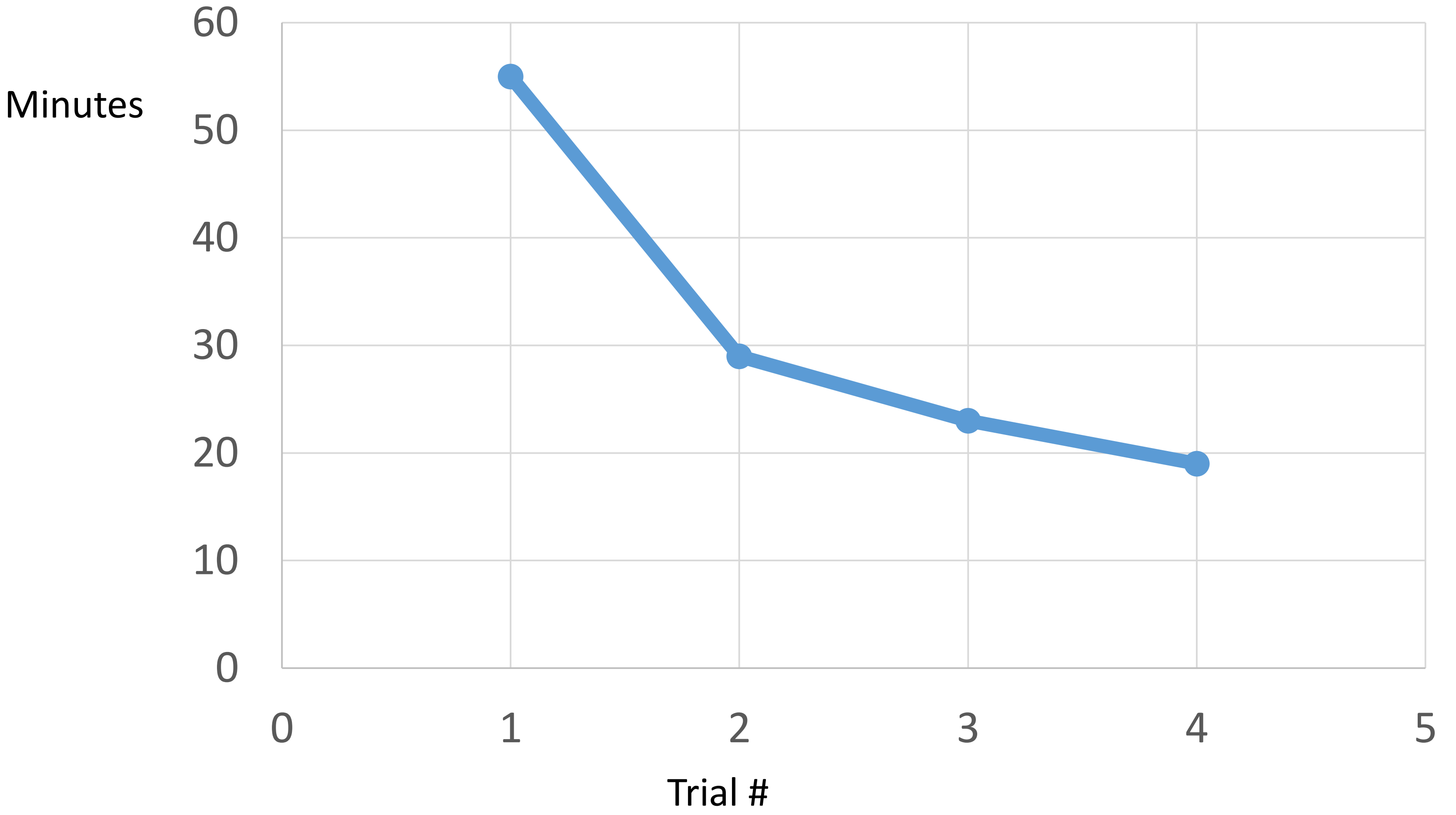






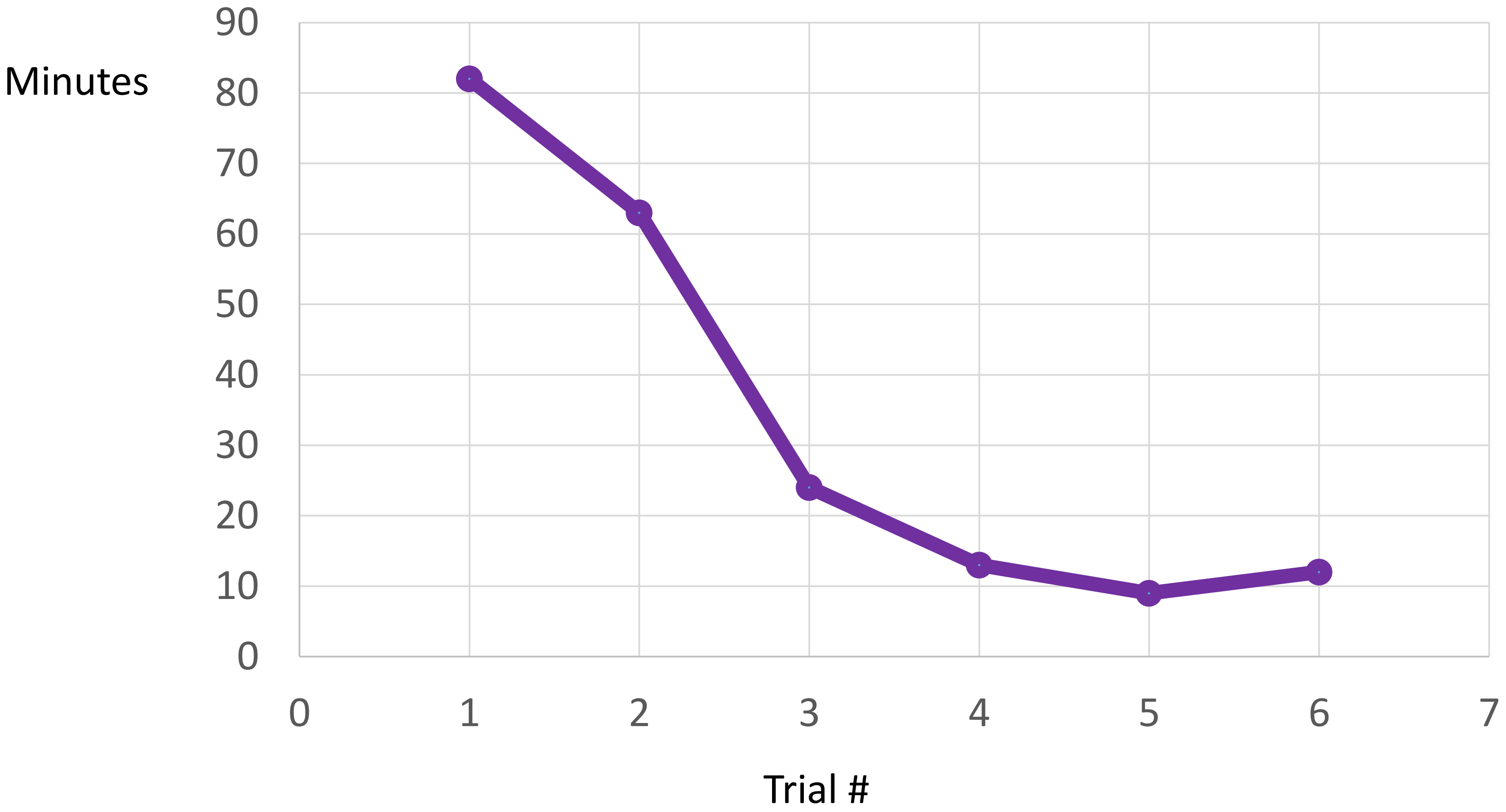
Data!

Time spent developing Step 1 UCA table



Data!

Time spent developing Step 2 scenarios



Implementing STPA successfully

- Learning STPA
- Selecting a suitable system
- Assembling a team
- Planning an STPA project
- Support and buy-in from high-level management
- Data!

Any questions? Email me! JThomas4@mit.edu

Thank you!