Massachusetts
Institute of
Technology

Facilitating and Implementing STPA / CAST

Dr. John Thomas

Experiences across industries

(Aviation, Automotive, 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 / CAST

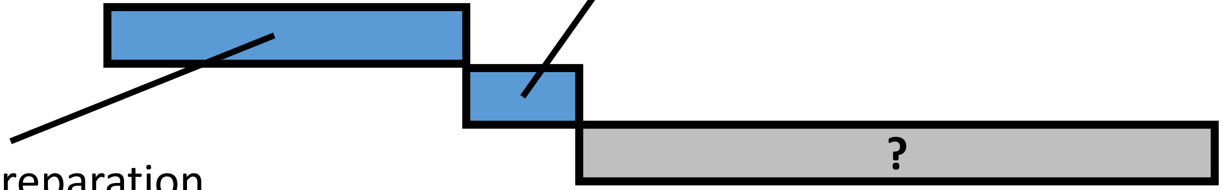
- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Data!

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 project	Low	Med	Low	Med
Attending training session	Med	Med	Med	High (but quality varies!)
Dedicated project-based workshop & education	High	Med	Low	Extremely High!

Implementing STPA / CAST

- **Training**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Data!



Training class
- Typically 3-4 days (STPA)
- Typically 1-2 days (CAST)

Planning, preparation
- Identify training goals, group size, backgrounds
- Create training plan

Implementing STPA / CAST

- **Training**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Data!

Training is flexible, tailorable

- Previous durations: 1-5 days
- Class size: 20-40 people typical
  - Previous sizes: 4-150 people
- May be followed by project-based workshop
  - Requires additional preparation, planning

Implementing STPA / CAST

- **Training**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

STPA / CAST Certificate?

Challenges

- Can test rote memorization, but not enough!
- STPA / CAST require thinking differently
- Knowledge vs. Skill
- Real, complex systems are different than small toy problems
- Discuss experiences with industry
- Discuss experiences with regulators
- Discuss experiences with consultants

Implementing STPA / CAST

- **Training**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

Producing facilitators

- Training not enough
- Need experience on real projects, complex problems
- After 1-2 real projects (months), may be ready
- Discuss successful apprenticeship strategy

We can certify that you've attended training, but more is needed to produce facilitators

Implementing STPA / CAST

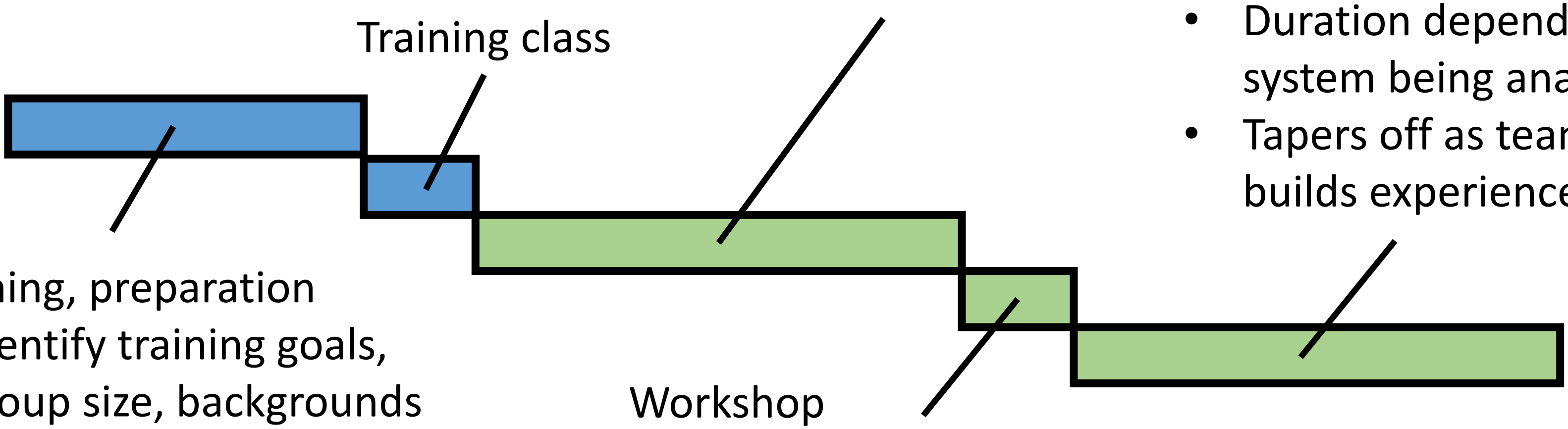
- **Training**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

Project-based workshop

Preparation
- Select suitable system
- Identify appropriate team
- Schedule
- Initial analysis

Support
- Duration depends on system being analyzed
- Tapers off as team builds experience

Training class



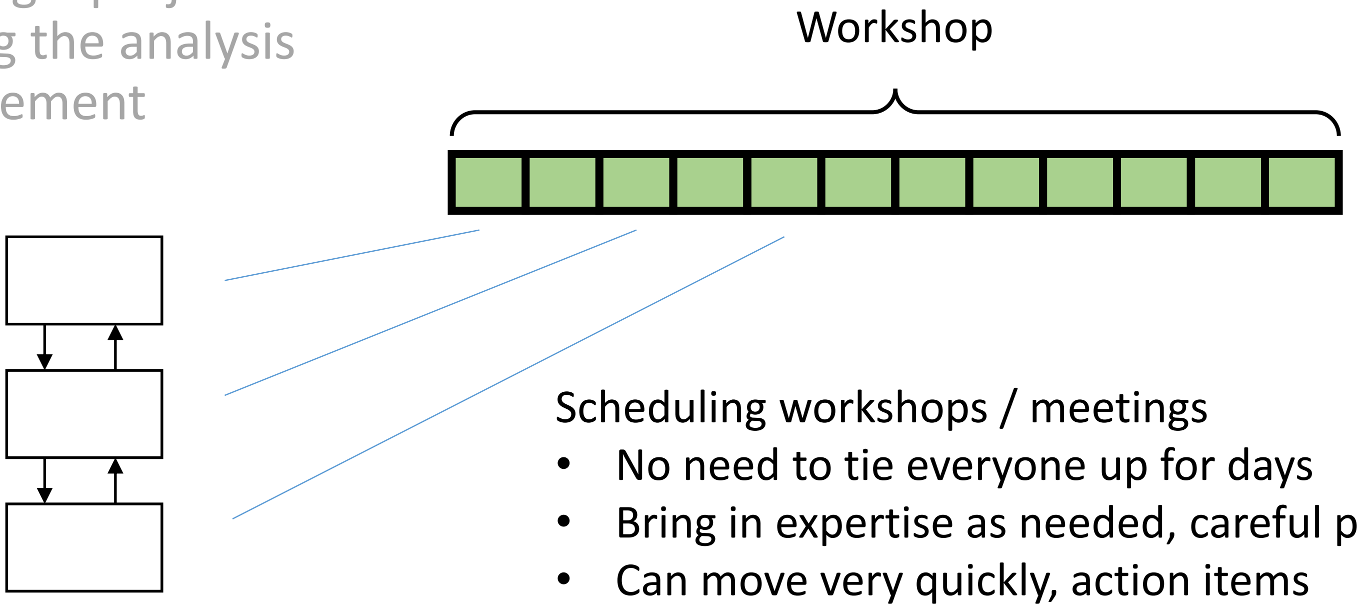
Planning, preparation
- Identify training goals, group size, backgrounds
- Create training plan

Workshop
- Could be 3-4 days

Implementing STPA / CAST

- **Training**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

Project-based workshop



Scheduling workshops / meetings

- No need to tie everyone up for days
- Bring in expertise as needed, careful planning
- Can move very quickly, action items
- Can be spread out over longer period

Implementing STPA / CAST

- Training
- **Selecting a suitable system**
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

Maximize impact

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

Implementing STPA / CAST

- Training
- **Selecting a suitable system**
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

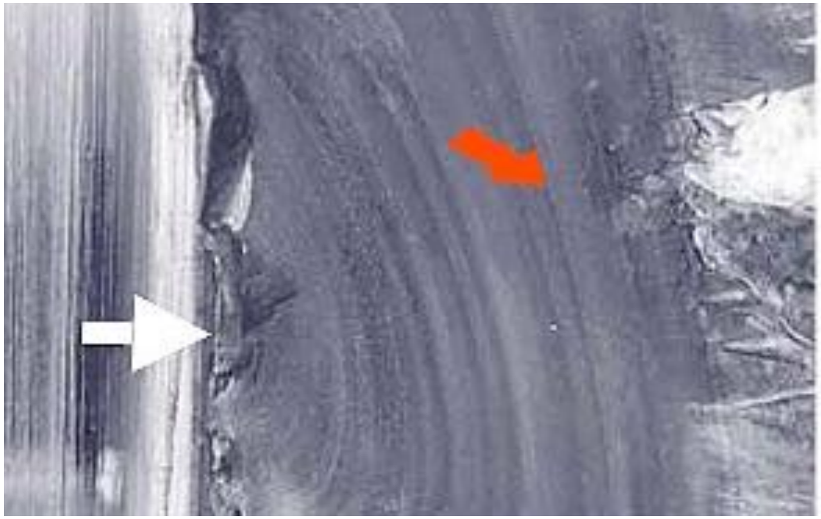
(For STPA)

Maximize impact

STPA is for functional analysis

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

Selecting suitable system (STPA)



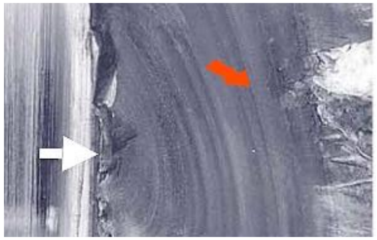
Metal Fatigue

Material flammability

Not best choice to study 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 / CAST

- Training
- Selecting a suitable system
- **Assembling a team**
- Planning a project
- Guiding the analysis
- Management

Interdisciplinary team

- Depends on the problem and control structure!

May include:

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

Must include:

- STPA / CAST Facilitator (expert)

Implementing STPA / CAST

- Training
- Selecting a suitable system
- **Assembling a team**
- Planning a project
- Guiding the analysis
- Management

Interdisciplinary team

STPA / CAST Facilitator

- Support project planning, methodology guidance and expertise, help avoid common traps, allocate analysis steps among team members, aggregate results, help review analysis, etc.

Implementing STPA / CAST

- Training
- Selecting a suitable system
- **Assembling a team**
- Planning a project
- Guiding the analysis
- Management

Who should be on the team?

Personalities Matter!

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

Implementing STPA / CAST

- Training
- Selecting a suitable system
- **Assembling a team**
- Planning a project
- Guiding the analysis
- Management

Who should be on the team?

Personalities Matter!

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

Implementing STPA / CAST

- Training
- Selecting a suitable system
- **Assembling a team**
- Planning a project
- Guiding the analysis
- Management

Who should be on the team?

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 / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

- Facilitators have experience--use it!
- Facilitators help develop the plan based on previous successes, lessons learned, etc.
- Look at past experiences: what worked, didn't work

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Start with project goals

- Pilot demonstration, analyze whole system, just learn STPA / CAST, provide comparison data, produce facilitators, etc.?

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Start with project goals

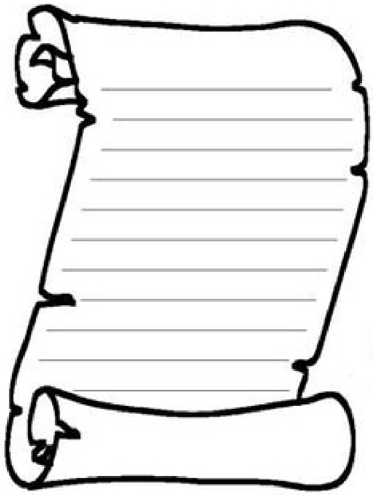
Identify constraints

- Available resources
- Budget
- Schedule
- Current projects

Develop a plan to achieve goals

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management



Generic plan may include

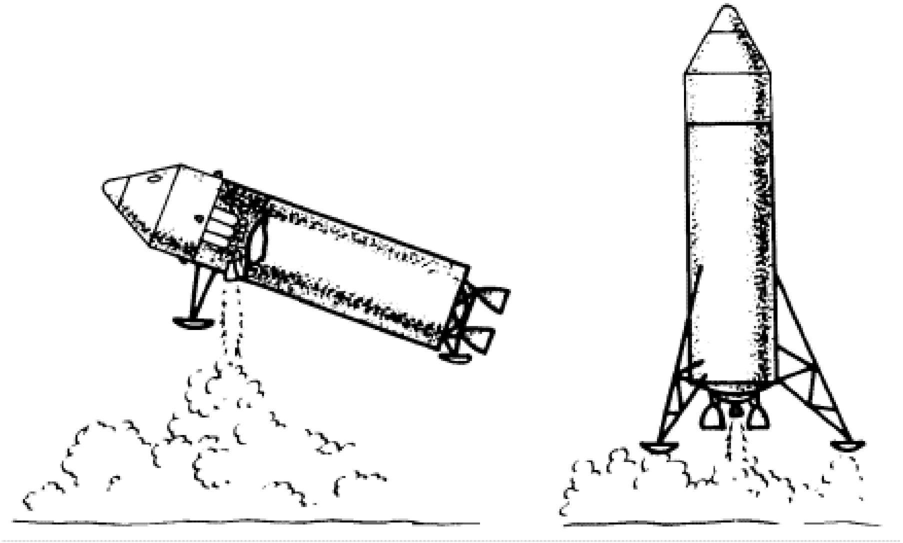
- Identify goals, constraints
- Select project
- Team preparation
- Preliminary work
- Perform STPA / CAST
- Follow-up activities
- Solutions development
- Consequences of solutions
- Summarize conclusions/key findings

Let’s discuss each of these…

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

(For STPA)



Ideal project selection

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

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Start with goals, constraints

Select project

Team Preparation

- Identify core team
- Gather info about the system
- Method overview, introduction, or training (for new teams)

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Start with goals, constraints

Select project

Team Preparation

Preliminary work (quick)

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

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Perform STPA / CAST

- Review prepared control structures
- Perform STPA / CAST, 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!
  - For STPA, 70% of final results may be generated in 2-5 days (but depends on many factors)
  - For CAST, begin with physical equipment but keep going towards systemic factors
  - Disseminate big issues immediately!

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Start with goals, constraints

Select project

Team Preparation

Preliminary work (quick)

Perform STPA / CAST

Follow-up

- Iterate on outstanding areas
- Follow-up activities, check assumptions made
- Incorporate new changes, new details as development continues (for STPA)
- Review results

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Solutions / Recommendations

- 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 / CAST

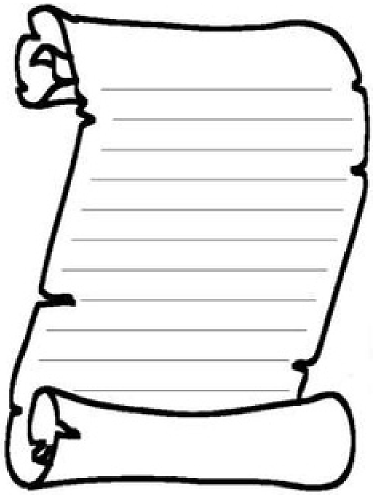
- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

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 / CAST

- Training
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management



Generic plan may include

- Identify goals, constraints
- Select project
- Team preparation
- Preliminary work
- Perform STPA / CAST
- Follow-up activities
- Solutions / recommendations development
- Consequences of solutions
- Summarize conclusions/key findings

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- **Guiding the analysis**
- Management

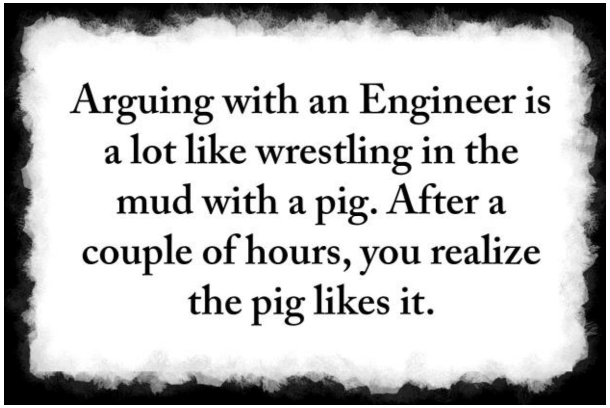
<discuss experiences>

- Past examples of team resistance
  - UCAs
  - Scenarios
- Misunderstandings
- Comments that facilitators must be prepared to respond to

	Not Provided Causes Hazard	Providing Causes Hazard	Too early, Too late, Out of order	Stopped too soon, Applied too long
Brake Cmd				
Accelerate Cmd				
Steering Cmd				

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- **Guiding the analysis**
- Management



Arguing with an Engineer is a lot like wrestling in the mud with a pig. After a couple of hours, you realize the pig likes it.

	Not Provided Causes Hazard	Providing Causes Hazard	Too early, Too late, Out of order	Stopped too soon, Applied too long
Brake Cmd				
Accelerate Cmd				
Steering Cmd				

"There are no UCAs because my design is safe/secure!"

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- **Guiding the analysis**
- Management

Example team comments facilitators must respond to

- Historically, this has never happened before
- We already have a mitigation in place
- Can this really happen? We assumed it can't.
- We already know about UCA X. Let's skip scenarios for this.
- That will never happen!

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- **Guiding the analysis**
- Management

Example team comments facilitators must respond to

- What about failures? You’re overlooking the most important part!
- Should we assume X or Y?
- Do we write this down?

Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- **Management**

- 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 / CAST

- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- **Management**

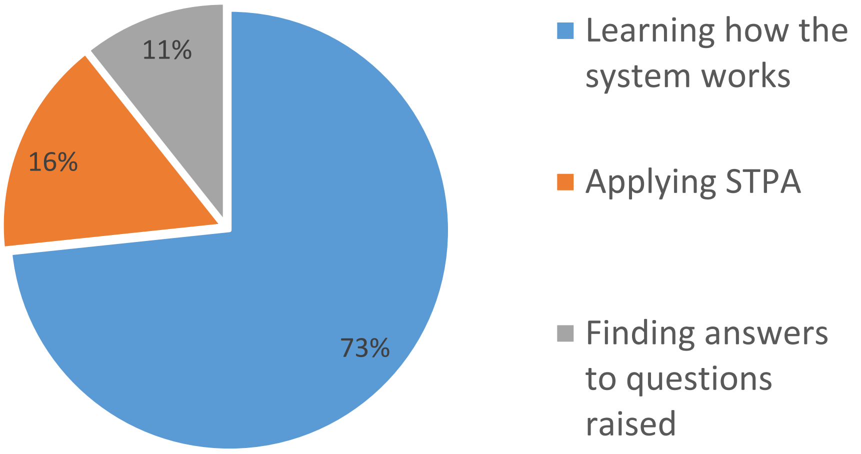
- Sometimes seen as a competitive advantage
  - Secrecy
- “We want to be recognized as a leader in our industry”
  - We want everyone to know we were first!

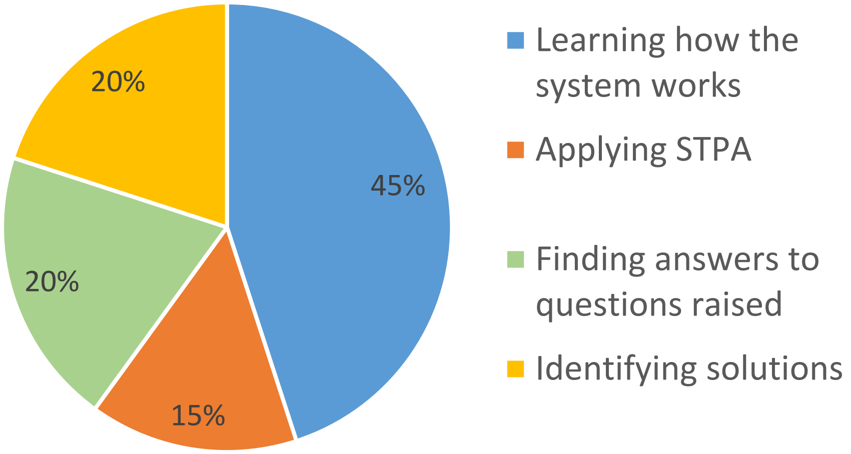
Implementing STPA / CAST

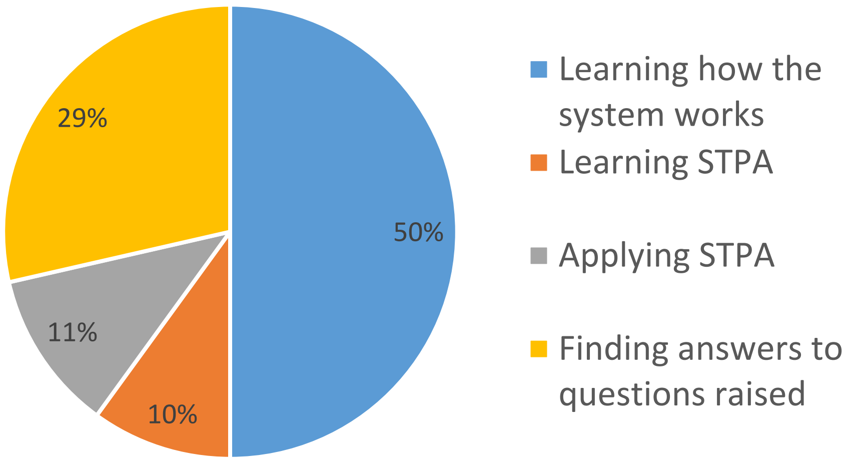
- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- **Data!**

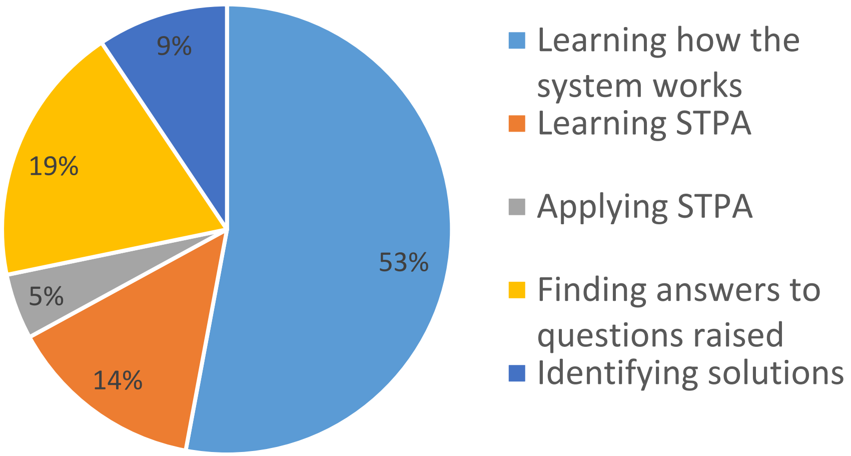
Massachusetts Institute of Technology

Data from 4 projects



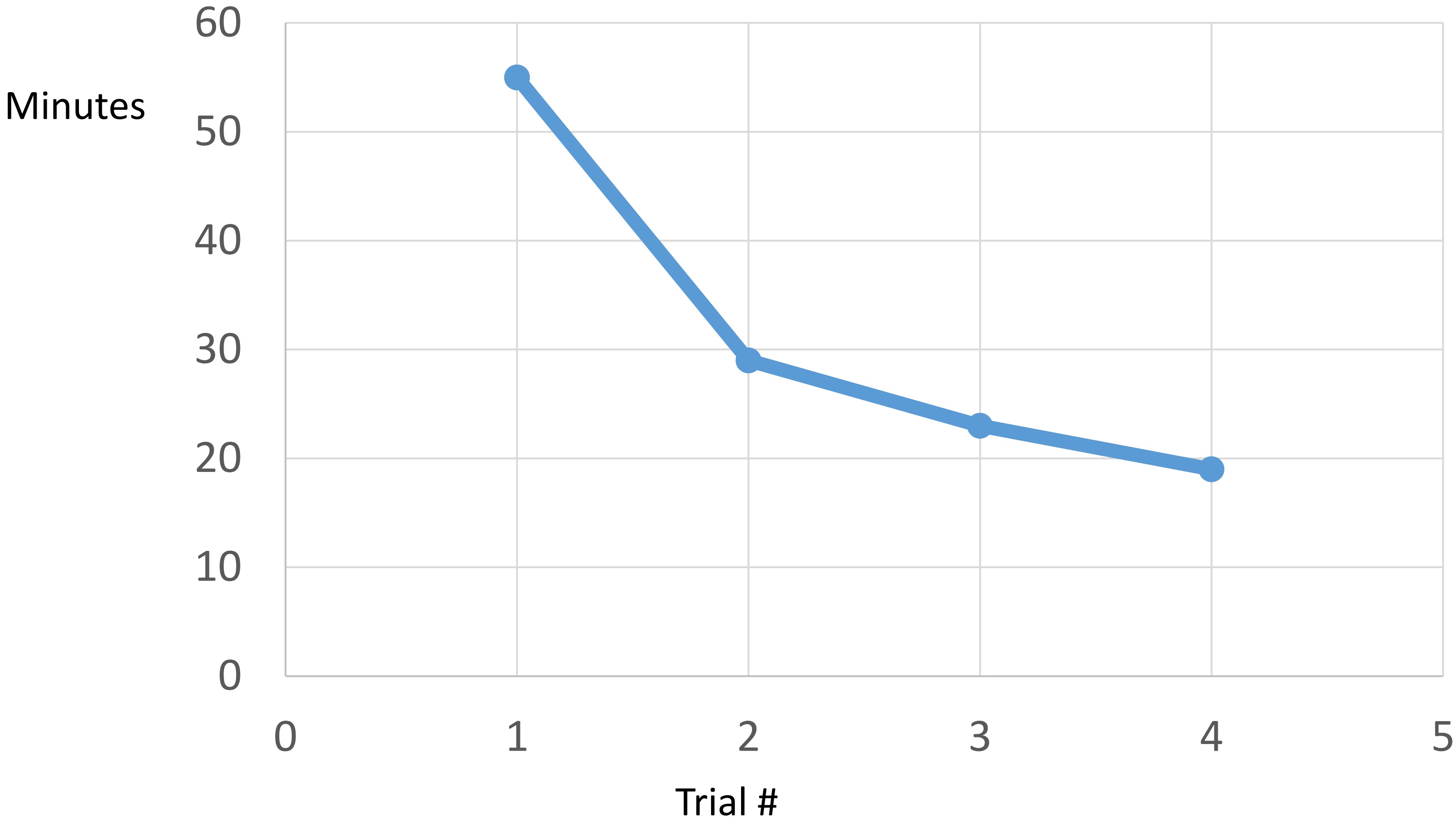






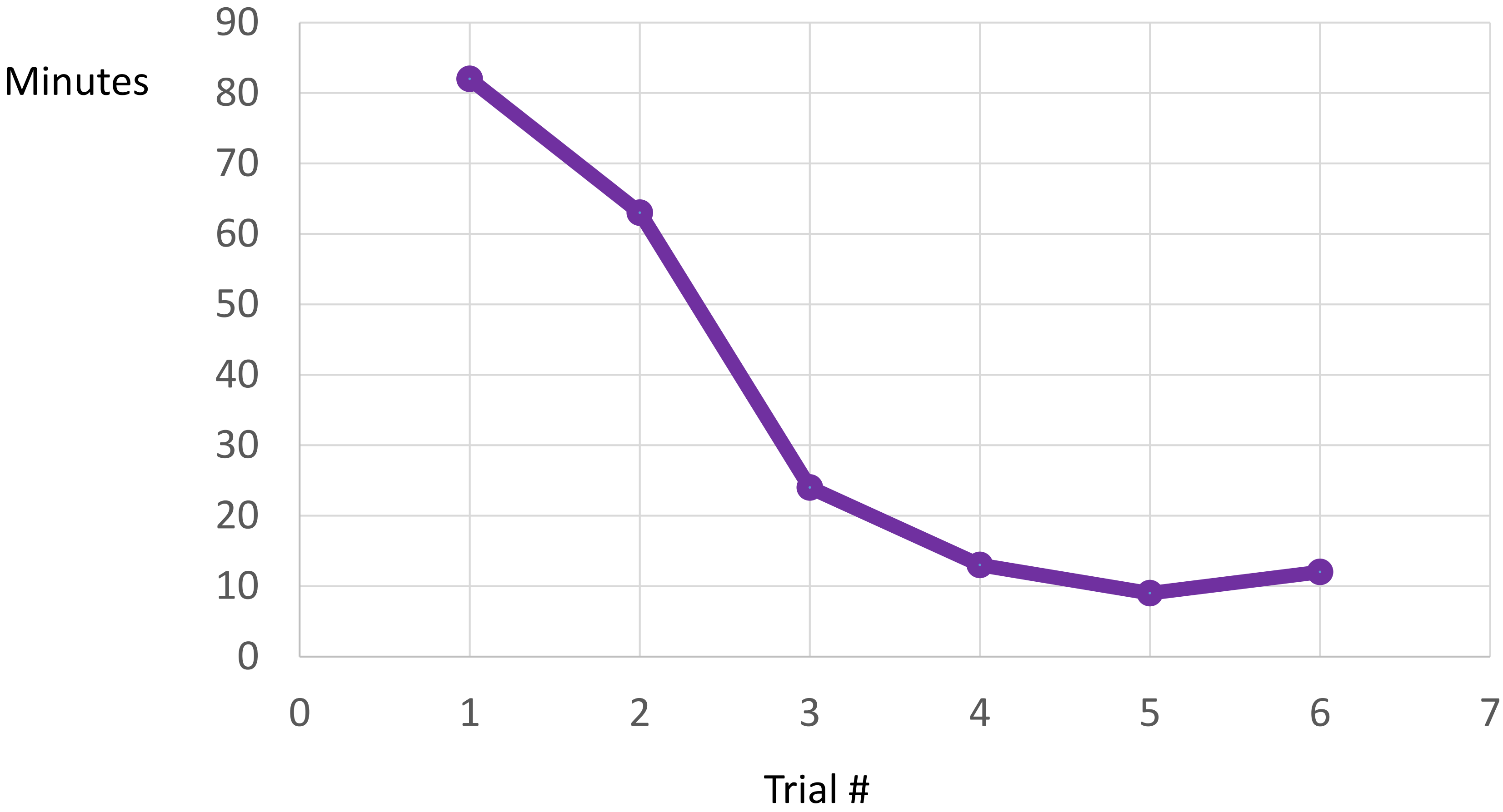
Data: Learning curve

Time spent developing Step 1 UCA table



Data: Learning curve

Time spent developing Step 2 scenarios



Implementing STPA / CAST

- Training
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Data!

Any questions? Email me! JThomas4@mit.edu

Thank you!