Massachusetts Institute of Technology

Planning and Implementing STPA (and 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

Planning and Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Accelerating STPA

Implementing STPA

- **Getting buy-in**
- Learning the method
- Selecting suitable sys.
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Accelerating STPA

Need a motivation for doing STPA

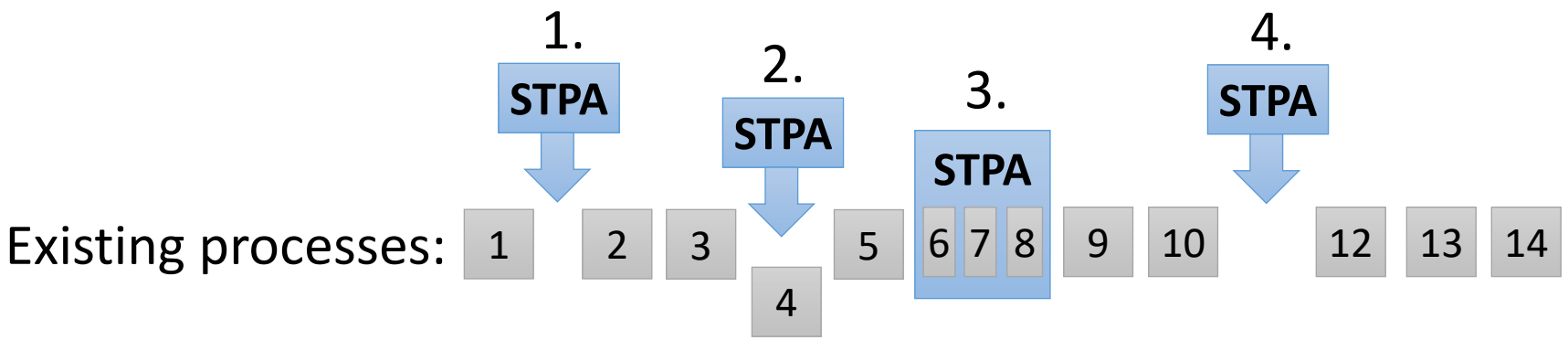
- Identify recent loss events, incidents
  - "teachable moments"
  - Would STPA have helped?
- Identify recalls, warranty issues, serviceability issues, etc.
  - Estimate cost to fix late vs. cost to perform STPA upfront and prevent
  - $X vs. $5M; $X vs. $5B
- If constrained, start small
  - Try STPA on a pilot application
  - Build evidence to warrant larger exploratory effort
  - Danger: Too small in scope, time, or team size to build a compelling motivation. Mitigation: Involve an STPA Facilitator in the planning to avoid pitfalls.
- Build cost-benefit / ROI argument
  - From public data
  - From in-house pilot projects

Implementing STPA (or CAST)

- **Getting buy-in**
- Learning the method
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Accelerating STPA

Integrating STPA (or CAST):

1. Add STPA as N+1 process
2. Replace process X with STPA
3. **Use STPA to streamline what we're doing now**
4. Use STPA to address a missing process



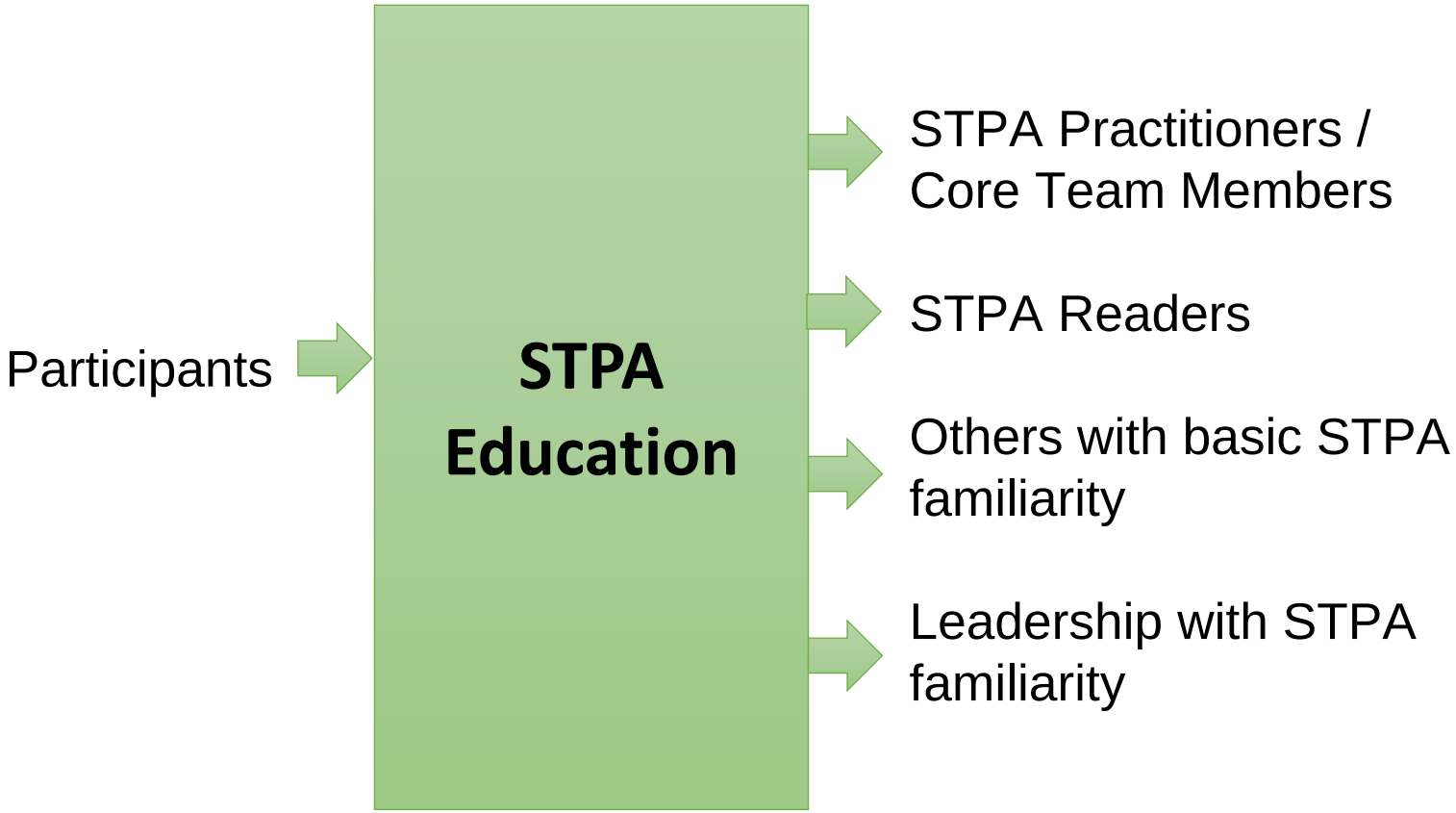
Implementing STPA (or CAST)

- Getting buy-in
- **Learning the method**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Accelerating STPA

Learning enough to adopt STPA

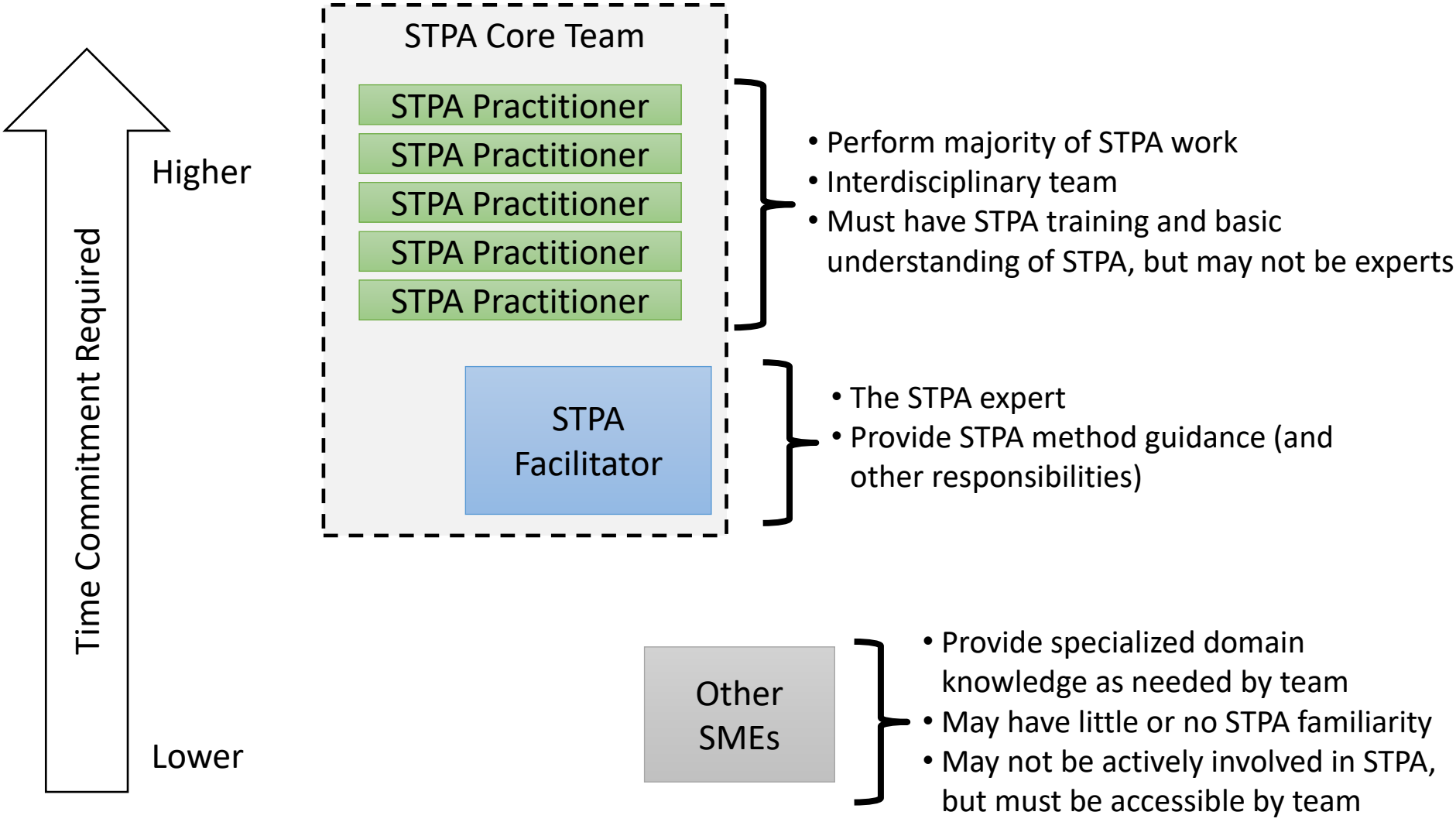
	Cost	Effort needed	Scalability	Effectiveness
Reading existing papers, reports, books	Free	High	High	Low
Attending MIT STAMP workshop	Free	Low	Low	Med
Participating in existing project	Low	Med	Low	Med
Attending training session	Med	Med	Med	High (but quality varies!)
Dedicated project-based workshop & education	High	Med	Low	Extremely High!

What does STPA Education (Class) produce?



STPA Education produces practitioners, but does not produce STPA experts.
Experience is needed to produce STPA facilitators.

STPA Project Participants



- Getting buy-in
- **Learning the method**
- […]

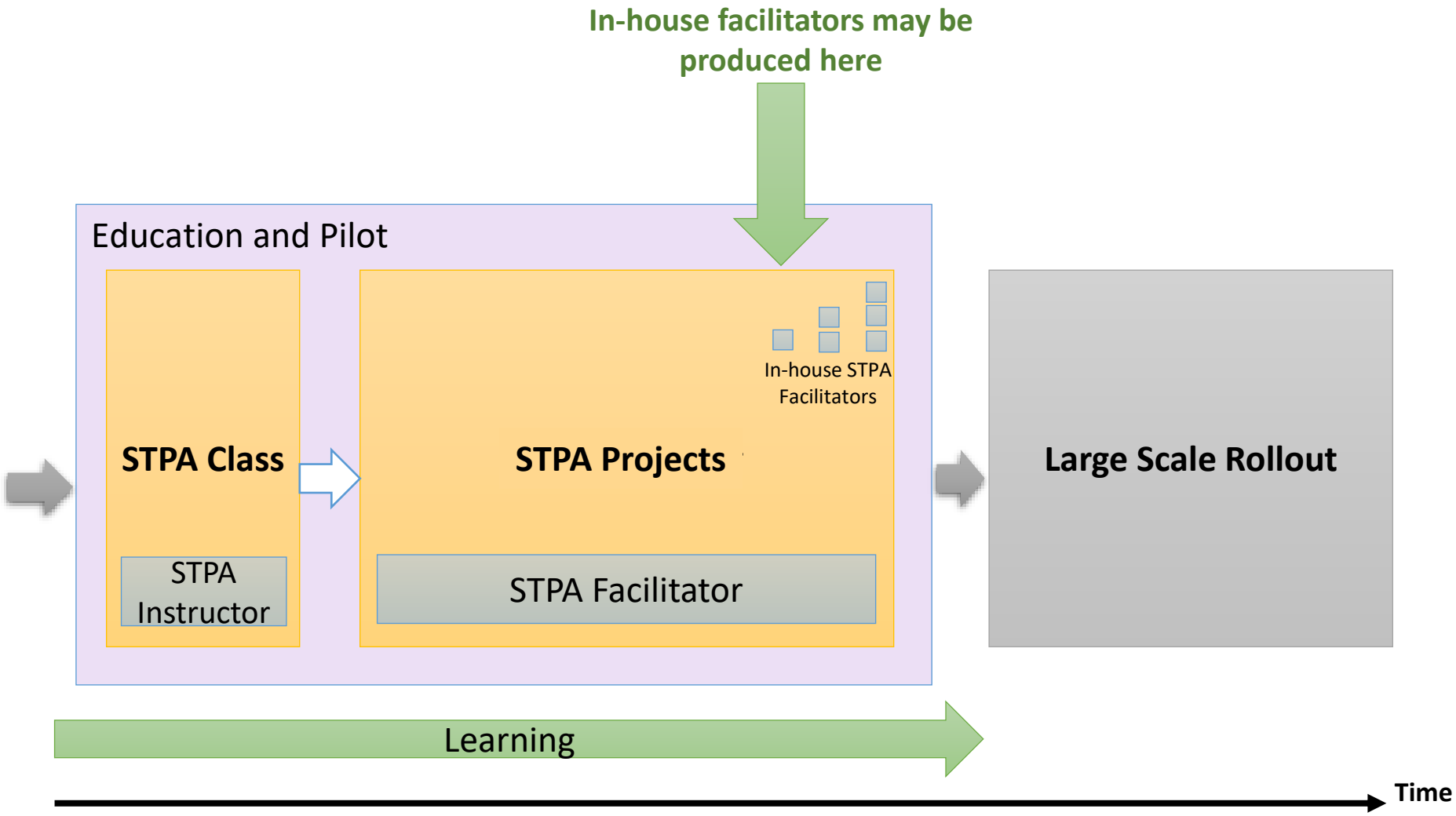
Lessons from HAZOP (chemical industry):

- Teams must include a HAZOP facilitator who is the method expert responsible for leading and managing the HAZOP team
- "only 1/3 of people who are otherwise qualified by education, experience, etc. actually make good HAZOP facilitators"
- "The expert facilitator role requires years of experience, not days/months."

These lessons appear true for STPA also.

- Education is not enough to produce STPA experts and facilitators
- Invite top performers in class to become STPA core teammembers (future candidate facilitators)

2) Education and Pilot (typical)



Implementing STPA (and CAST)

- Getting buy-in
- **Learning the method**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

STPA / CAST Certificates

STAMP Accreditation and Certification Authority

- Standardized STPA & CAST certification and accreditation for practitioners and educators
- Three levels of certification
  - Practitioner
  - Facilitator
  - Instructor

Implementing STPA (and CAST)

- Getting buy-in
- **Learning the method**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

STPA / CAST Certification

- Practitioner level
  - Complete training course that meets requirements
  - Demonstrate knowledge—small project that meets all requirements is reviewed and approved
  - Level of effort: ~weeks
- Facilitator level
  - Satisfy practitioner level, plus…
  - Demonstrate skill—large project that meets all requirements is reviewed and approved
  - “Check ride” as candidate facilitator
  - Level of effort: ~months/years
- Instructor level
  - Satisfy facilitator level, plus…
  - Demonstrate skill—curriculum that meets requirements and “check ride” as candidate instructor
  - Level of effort: years

Implementing STPA

- Getting buy-in
- **Learning the method**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

How NOT to produce STPA facilitators

"We found the perfect facilitator"

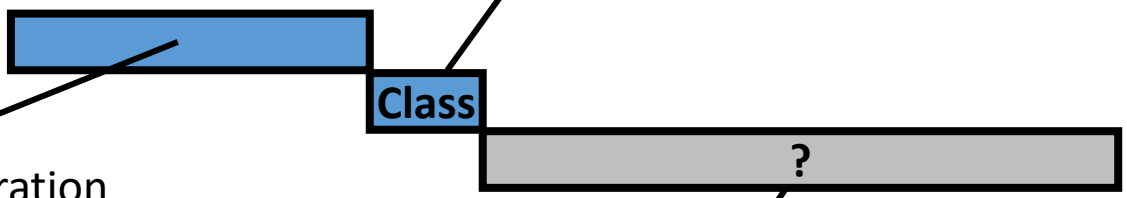
- No experience with STPA
- Decades of experience facilitating and performing fault tree analysis.
- Subject matter expert for our application
- Just give us a couple days to "bring him up to speed on the STPA methodology".

This org invested significant effort trying, but was not successful. Not an effective approach!

Implementing STPA (and CAST)

- Getting buy-in
- **Learning the method**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Accelerating STPA

Training class
- Typically 3-5 days (STPA)
- Typically ~2 days (CAST)



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

What happens next?
- Plan ahead. This knowledge will help inform the class planning, class participant selection, and class duration, intensity, and cost.

Implementing STPA (and CAST)

- Getting buy-in
- **Learning the method**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- Accelerating STPA

Training is flexible, tailorable

- Possible durations: 1-5 days
- Class size: 20-40 people typical
  - Possible sizes: 10-150 people
- May be followed by project-based workshop
  - Requires additional preparation, planning

Project-based workshop

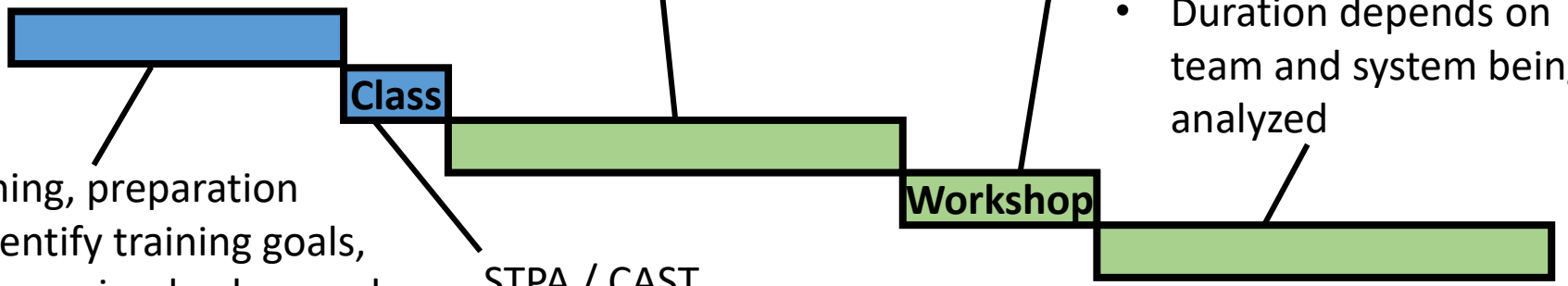
Implementing STPA

- Getting buy-in
- **Learning the method**
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

Project workshop (facilitated)
- Could be ~5-10 full days
- Could be periodic reviews over ~12 weeks

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

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



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

STPA / CAST Training class

Massachusetts Institute of Technology

Implementing STPA

- Getting buy-in
- Learning the method
- **Selecting suitable system**
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

USAF: 10 STPA pilots across 4 wings

- 9/10: Outstanding Success!
- 1/10: “It didn’t work”
  - Basis: STPA produced “similar results” to traditional test/safety process
  - Application: “simple familiar upgrade”; “has been done many times before”
  - Additional conclusions:
    - “STPA also found system design mitigations” that existing test/safety process didn’t
    - STPA provided an “easily understood model”
    - STPA “Expected to be useful for New Capabilities and Complex Systems”
    - STPA “Aids in planning ‘never before done’ tests”

Massachusetts Institute of Technology

Implementing STPA

- Getting buy-in
- Learning the method
- **Selecting suitable system**
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

USAF: 10 STPA pilots across 4 wings

- 9/10: Outstanding Success!
  - Why so successful?
  - Discuss key factors
    - Training
    - Team selection
    - Team mindset
    - Application selection
    - Planning
    - Vector checks
    - Aha! moments documented
    - Etc.

Implementing STPA

- Getting buy-in
- Learning the method
- **Selecting suitable system**
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

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

*for a qualified team!

Implementing STPA

- Getting buy-in
- Learning the method
- **Selecting suitable system**
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

I have many projects! Where do I start?

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

- Getting buy-in
- Learning the method
- **Selecting suitable system**
- Assembling a team
- Planning a project
- Guiding the analysis
- Management

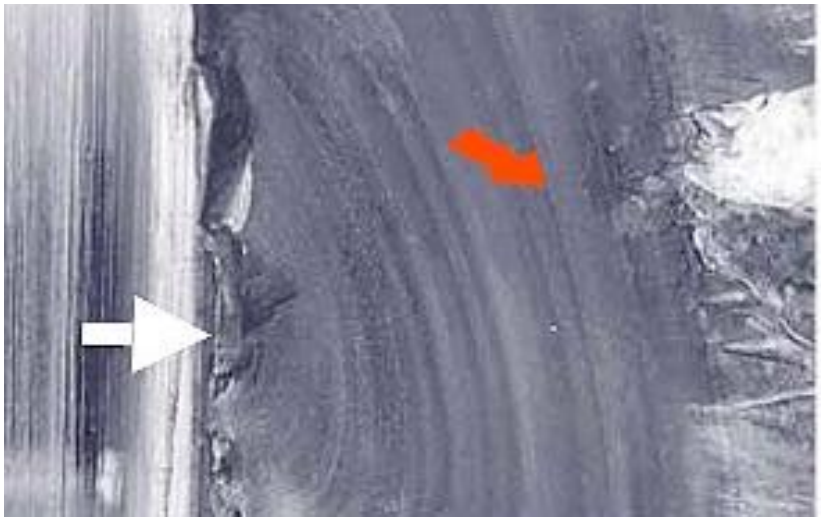
(For STPA)

Maximize impact

STPA is for functional analysis

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

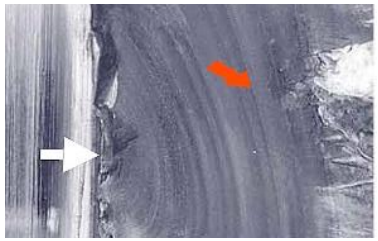
Selecting suitable system (STPA)



Metal Fatigue

Material flammability

STPA is not best choice to study purely physical phenomena!



HOWEVER

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

Massachusetts Institute of Technology

"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

- Getting buy-in
- Learning the method
- 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)
- Automation experts
- Testers
- Etc.

Must include:

- STPA Facilitator (expert)

Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- **Assembling a team**
- Planning a project
- Guiding the analysis
- Management

Interdisciplinary team

STPA Facilitator

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

Massachusetts Institute of Technology

Example STPA Facilitator Duties

Responsible for Overall STPA Compliance

- Develop STPA Project Plan
- Define connections to upstream and downstream processes
- Ensure suitable STPA application and scope
- Assemble appropriate interdisciplinary STPA Team (initial & ongoing)
- Ensure STPA Team receives appropriate education
- Engage external stakeholders and SMEs
- Allocate STPA activities among team
  - Initial performance of each step
  - Reviews of each step with appropriate attendance
- Supervise STPA performance
- Ensure new mitigations/requirements are incorporated in STPA
- Provide STPA clarification, guidance, corrections
- Plan STPA vector checks
- Manage, monitor, and control biases (e.g. confirmation bias, anchoring bias, etc.)
- Make course corrections based on vector checks
- Plan briefings with stakeholders, leadership, downstream users
- Manage handoff to downstream processes
- Review STPA work for process compliance

Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- **Assembling a team**
- Planning a project
- Guiding the analysis
- Management

Who should be on the team?

Personalities Matter!

- Designers: High knowledge, but can get defensive
- Outsiders: Not defensive, but may have less knowledge
- Tradeoff! Mitigations: Apply early, Team diversity (in knowledge, biases, etc.)

Implementing STPA (and CAST)

- Getting buy-in
- Learning the method
- 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 the impact of broader factors

Implementing STPA

- Getting buy-in
- Learning the method
- 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
- Tradeoff: sometimes less experience helps!

Implementing STPA

- Getting buy-in
- Learning the method
- 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
- Plan vector checks
- Perform STPA
- Follow-up activities
- Solutions / recommendations development
- Consequences of solutions
- Summarize conclusions/key findings

Let's discuss each of these…

Implementing STPA

- Getting buy-in
- Learning the method
- 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, provide comparison data, produce facilitators, etc.?

Implementing STPA

- Getting buy-in
- Learning the method
- 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
- Ensure the team size is appropriate for the system & scope
  - STPA facilitator will evaluate
  - STPA teams have ranged from 3-100+ depending on system/scope
- Ensure team skillset is appropriate
- Classes/training (for new teams)

Implementing STPA

- Getting buy-in
- Learning the method
- 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

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Perform STPA

- This step is the main focus of the handbook and classes/training
- 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!
  - The 80/20 rule of thumb usually applies
  - Disseminate big issues immediately!

Implementing STPA

- Getting buy-in
- Learning the method
- 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

Follow-up

- Iterate on outstanding areas
- Follow-up activities, check assumptions made
- Incorporate new changes, new details as development continues (for STPA)
- Reviews with SMEs and incorporate guidance from STPA expert facilitator

Massachusetts Institute of Technology

Implementing STPA

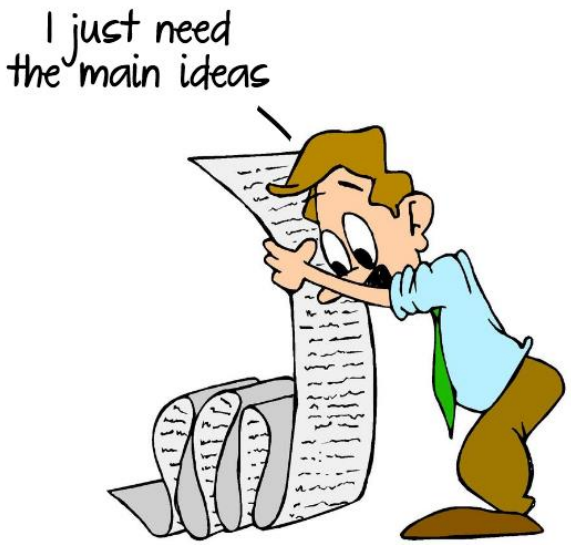
- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

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
- Roll the solutions into STPA, evaluate consequences of solutions

Implementing STPA

- Getting buy-in
- Learning the method
- 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!

Massachusetts Institute of Technology

Summarize conclusions/key findings

Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

Record Aha! Moments

- Most important STPA output may not be the detailed scenarios, requirements, and solutions
- Record the Aha! moments as they happen. Record team insights and impact as they happen.
- Take snapshots of the control structure to show its evolution
  - Initial sketch: reflects team's initial mental model of system on day 1
  - Intermediate snapshots: reflects additions & changes based on team insights along the way
  - Final: Highlights the full scope of insights & impact
- Use Aha! moments and control structure snapshots at the end of project to summarize and highlight the key findings.

Difficult or impossible to reconstruct these at the end!

Massachusetts Institute of Technology

STPA Vector checks

Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- **Planning a project**
- Guiding the analysis
- Management

If Aha moments, insights, and impact are not being generated during STPA, something is wrong. Monitor throughout the STPA effort and correct—don't wait until the end!

- Evaluate all criteria in this presentation
- Is STPA being done correctly?
- Are reviews being conducted with SMEs?
- Are reviews being conducted with STPA expert facilitators?
- Appropriate application selected?
- Appropriate scope defined?
- Wrong team selection?
- Wrong directive?
- Wrong mindset?
- Too late to have impact?
- Low SME engagement?
- Low STPA facilitator/team engagement?
- No STPA facilitator?
- STPA facilitator not qualified/certified?
- Team not trained & certified in STPA?

Implementing STPA

- Getting buy-in
- Learning the method
- 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
- ✓ Plan vector checks
- ✓ Perform STPA
- ✓ Follow-up activities
- ✓ Solutions / recommendations development
- ✓ Consequences of solutions
- ✓ Summarize conclusions/key findings

Implementing STPA

- Getting buy-in
- Learning the method
- 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

- Getting buy-in
- Learning the method
- 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!
- How is this different than XXX?
- Should we assume A or B?
- Do we write this down?

Massachusetts Institute of Technology

Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- Planning a project
- **Guiding the analysis**
- Management

Common question:

How do you prioritize the results?

- Many results may not require prioritization: “no-brainer”
  - Often these are the most powerful results!
- Severity (almost always used)
- Effectiveness/strength of controls
- Frequency of a causal factor across scenarios
- How many UCAs/scenarios does this requirement prevent or mitigate?
- Controllability
  - One example: MIL-STD-882 Appendix A
- Capacity to detect & recover
- “Immediately hazardous”: How quickly is intervention needed to prevent loss?
- Pareto chart

Massachusetts Institute of Technology

MIL-STD-882E: Risk matrix for software

TABLE A-VI. EXAMPLE SOFTWARE RISK INDEX MATRIX.

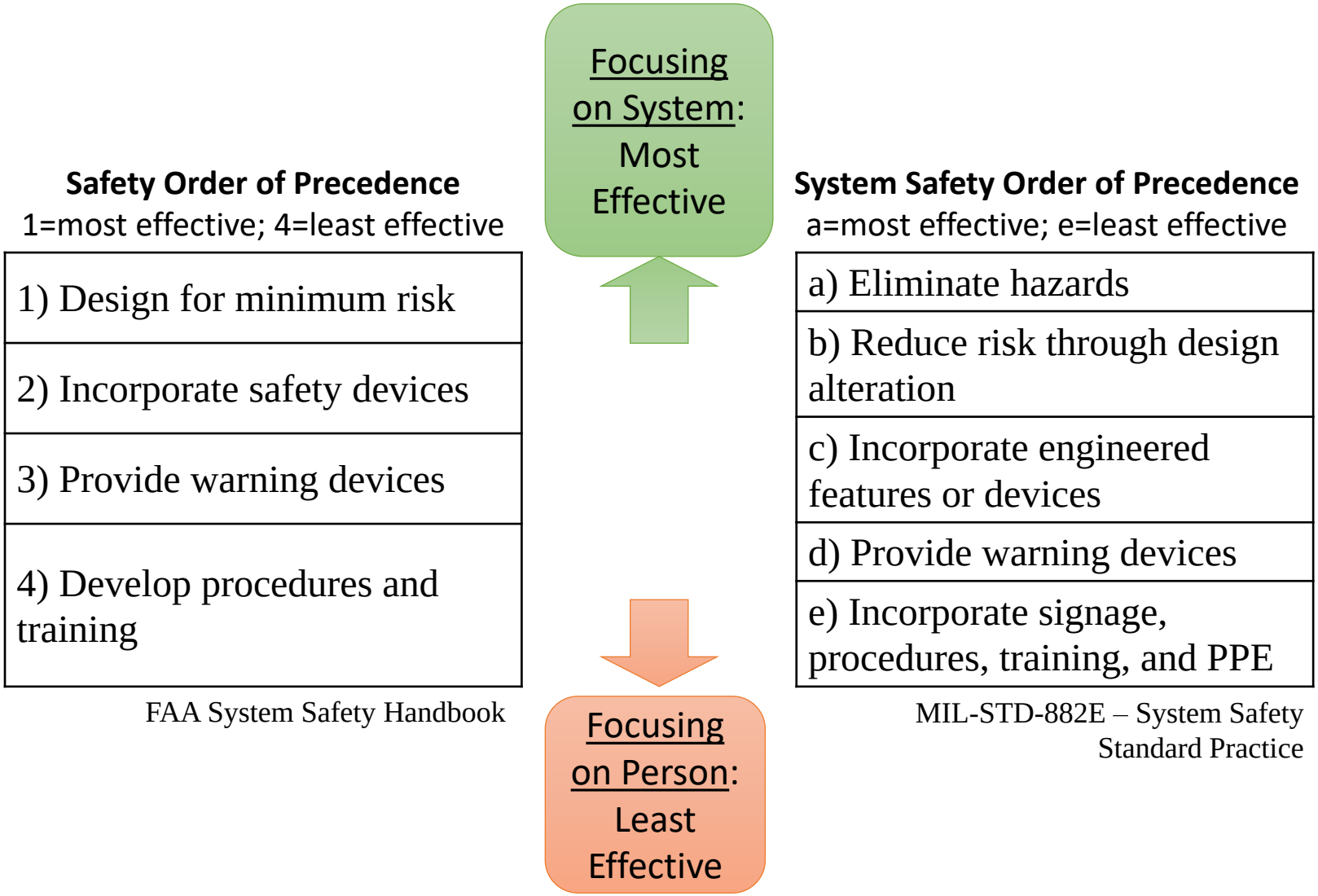
SEVERITY / CONTROL	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
I	1	1	3	5
IIa/b	1	2	4	5
IIIa/b	2	3	5	5
IV	3	4	5	5

Software Control Categories

- I Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazard's occurrence.
- IIa Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.
- IIb Software item displays information requiring immediate operator action to mitigate a hazard. Software failures will allow or fail to prevent the hazard's occurrence.
- IIIa Software item issues commands over potentially hazardous hardware systems, subsystems or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.
- IIIb Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.
- IV Software does not control safety critical hardware systems, subsystems or components and does not provide safety critical information.

MIL-STD-882E Appendix A

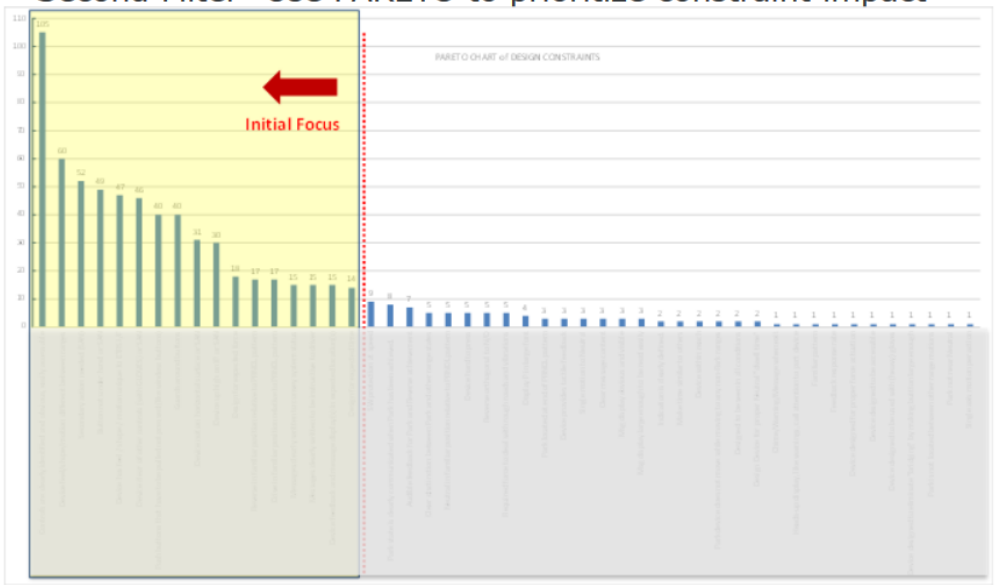
System Safety Order of Precedence



Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- Planning a project
- **Guiding the analysis**
- Management

"Second Filter" Use PARETO to prioritize constraint impact



Mark A. Vernacchia and Bill Arnold (GM)
"**Human Interaction and Potential Error Evaluation Associated with Shift By Wire Devices**"
2016 MIT STAMP Workshop

STPA-Informed Risk Matrix

Least [A]	0				
Somewhat [B]	1		4.4.1		
Moderate [C]	2-3			2.0.2, 2.0.5, 2.3.1, 2.4.2, 2.5.1, 4.0.2, 6.2.2, 6.3.1	2.1.1, 3.2.1, 4.0.3, 4.6.2, 5.3.1
Very [D]	4-5	4.1.2, 7.0.1	2.[illegible].1, .2	2.0.3, 2.0.4, 2.2.1, 2.7.3, 2.8.4, 3.0.1, 5.1.1, 7.1.1, 7.1.3	4.0.4, 4.6.1
Most [E]	6			2.6.1, 2.7.1, 2.7.2, 2.7.4, 2.8.1, 2.8.2, 2.8.3, 2.9.1, 2.9.2, 2.9.3, 4.3.1	2.5.2, 2.5.3
Eliminated [F]	N/A	2.0.1, 3.0.2, 3.1.1, 6.0.1	[illegible], 3.4.1, 4.0.1, 4.1.1, 4.5.1, 5.0.1, 5.2.1, 5.4 [illegible].1, 6.2.1, 6.5.1, 7.0.2, 7.1.2, 7.1.4, 7.1.5, 7		[illegible].1, 5.6.1,
CMES		1	2	3	4
		Catastrophic	Critical	Marginal	Negligible

Combined Mitigation Effectiveness Score (CMES)

Severity

STPA-identified Scenario
High Risk: High severity, not effectively mitigated

STPA-identified Scenario.
Low Risk: Low severity, effectively mitigated

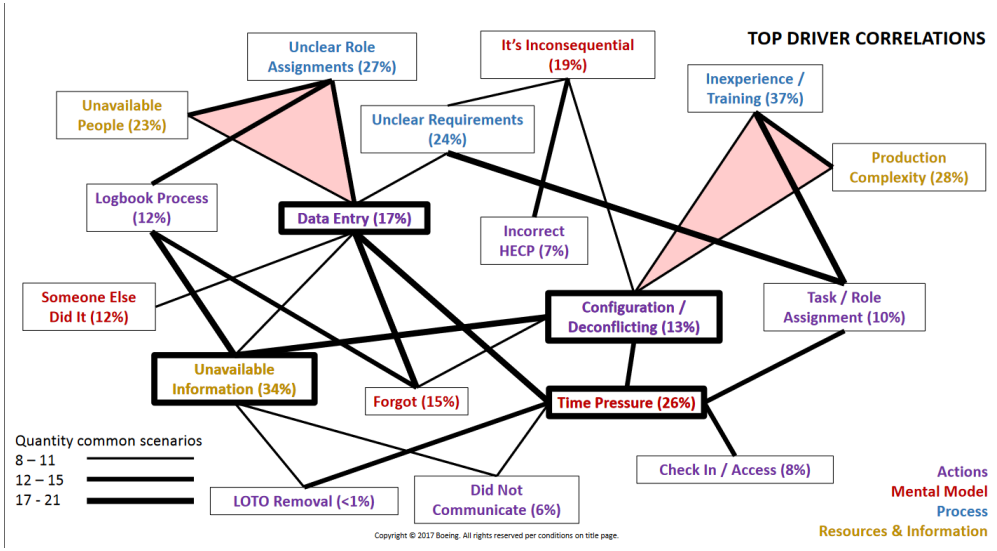
- Use **Mitigation Effectiveness** in place of likelihood
- Captures additional causes **beyond random failures.** Includes failures, non-failures, interactions, flawed requirements, and future threats.
- Enables **risk-informed** decision making
- Provides risk planner with an **improved risk decision tool**

Definitions:
Risk: A combination of the severity of the hazard and the *mitigation effectiveness* in controlling the hazard. Hazards may include reliability, safety, security, and production-related losses.
Combined Mitigation Effectiveness Score (CMES): The combined impact of mitigation methods

Sam Yoo and Dro Gregorian, 2021

Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- Planning a project
- **Guiding the analysis**
- Management



Katherine Belvin (Boeing)
"Using STPA Trend Analysis to Determine Key System Drivers"
2017 MIT STAMP Workshop

Implementing STPA

- Getting buy-in
- Learning the method
- 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

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- **Management**

Sharing results

- STPA sometimes seen as a competitive advantage
  - Leads to secrecy

VS.

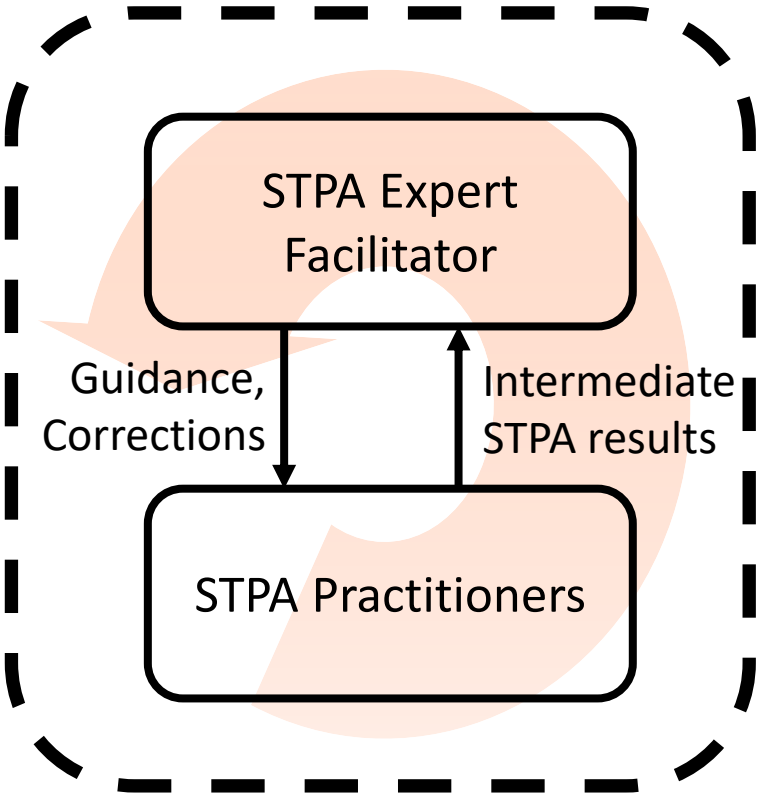
- "We want to be recognized as a leader in our industry"
  - We want everyone to know we were first!

Implementing STPA

- Getting buy-in
- Learning the method
- Selecting a suitable system
- Assembling a team
- Planning a project
- Guiding the analysis
- Management
- **Accelerating STPA**

Massachusetts Institute of Technology

Exploiting the learning curve



Accelerated Learning

Two types of dynamics
- Reinforcing Loops (exponential behavior)
- Balancing Loops (asymptotic – "diminishing returns")

Shape the learning curve by planning a tightly-coupled Reinforcing Loop

Acceleration means strengthening this loop!

We can quantify the accelerated learning from this strategy!

Massachusetts Institute of Technology

Strategies for Accelerating STPA

Assign more people

- But, this requires skilled coordination by STPA facilitator
- Common mistake: Not assigning enough people/time to support the analysis scope
- DANGER: Just throwing more people on the problem without careful planning/coordination can bog down the project

Select people with the right backgrounds

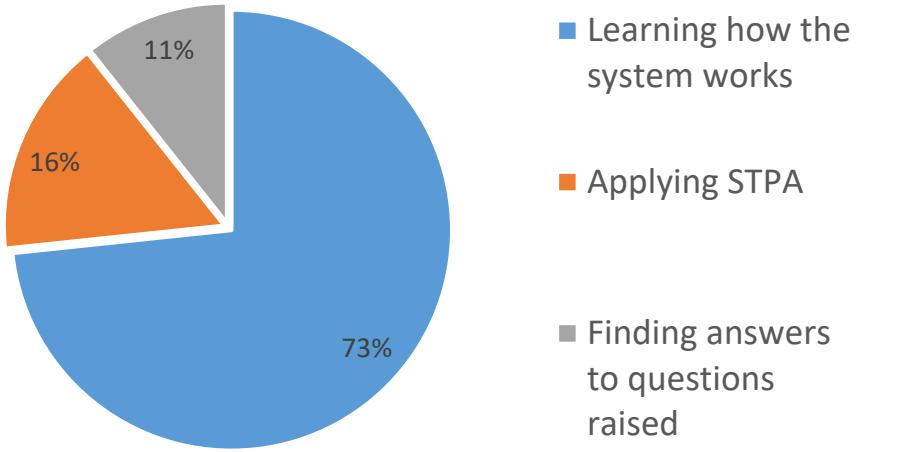
- Like most techniques, need to match the right job to the right skillset
- STPA excellence requires the right skillset
- Jumpstart skill development by leveraging existing skillsets:
  Recruit System thinkers & controls thinkers & "Ok, but I can break that" thinkers
- E.g. testers, instructors, systems/requirements developers, controls engineers, ops supervisors/trainers, etc.
- Allow folks to self-select for STPA work. Skilled STPA practitioners tend to want more.

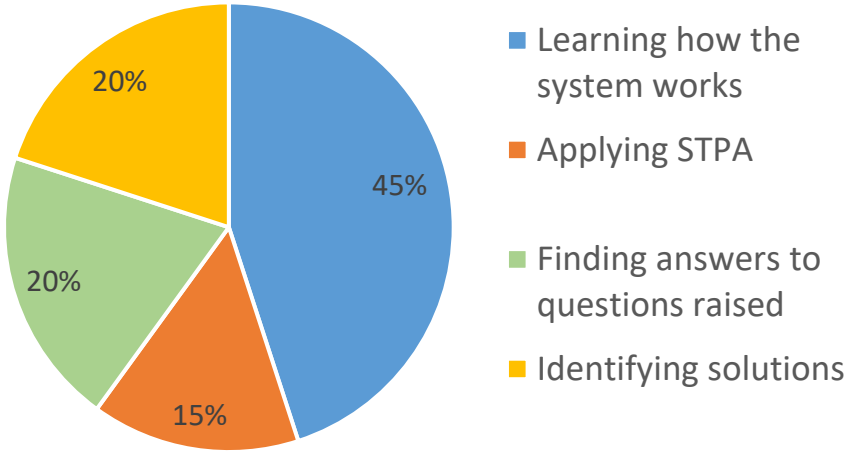
Exploit the learning curve

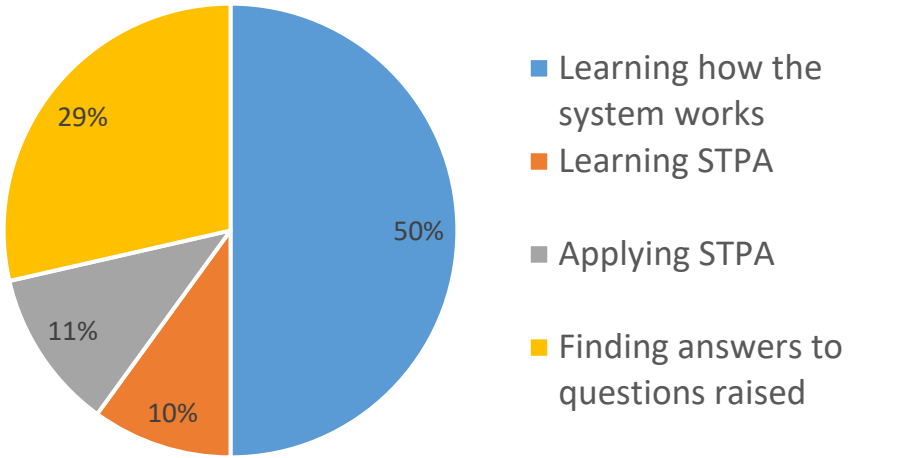
- Facilitated repetitions on real projects significantly accelerates skill development!
- DANGER: Requires a solid plan to prevent learning bad habits
- Common mistake: Applying STPA incorrectly, not realizing it, and getting proficient at applying it incorrectly! Unlearning is hard!

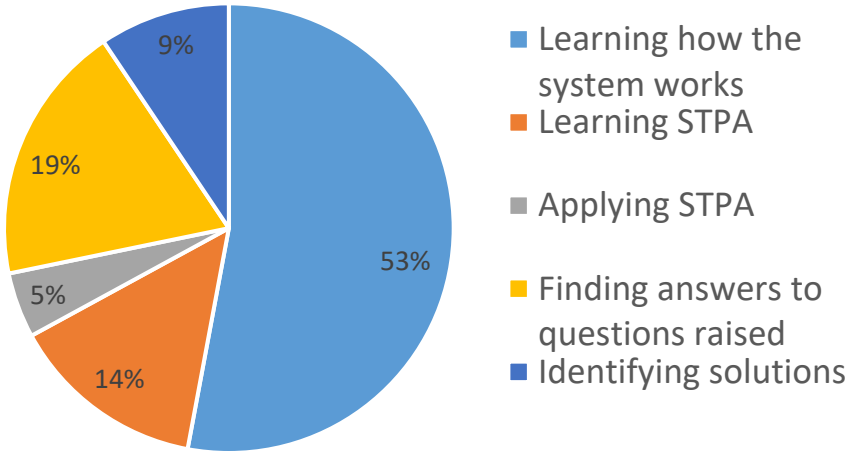
Massachusetts Institute of Technology

Data from 4 projects





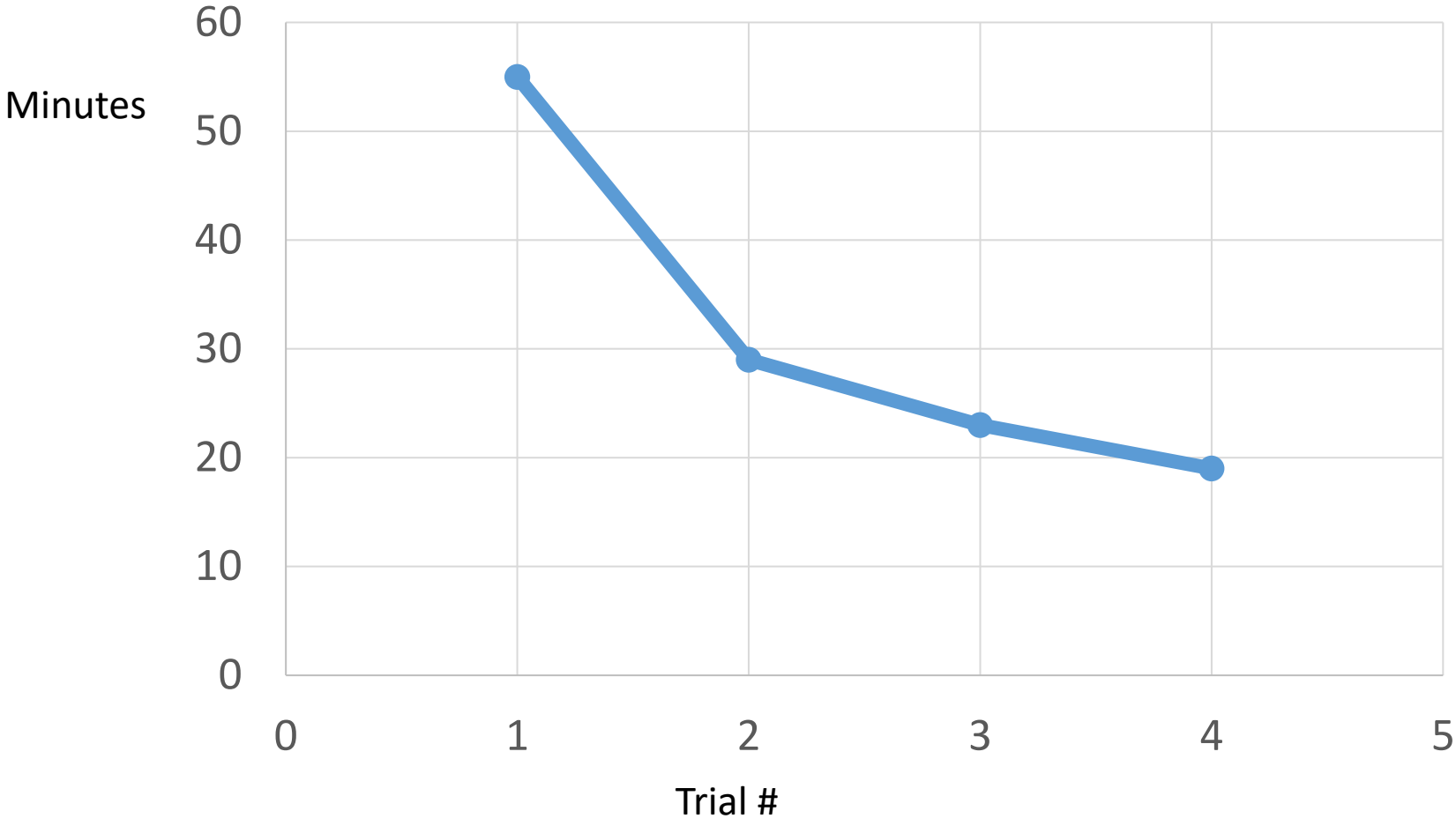




Massachusetts Institute of Technology

Data: Learning curve

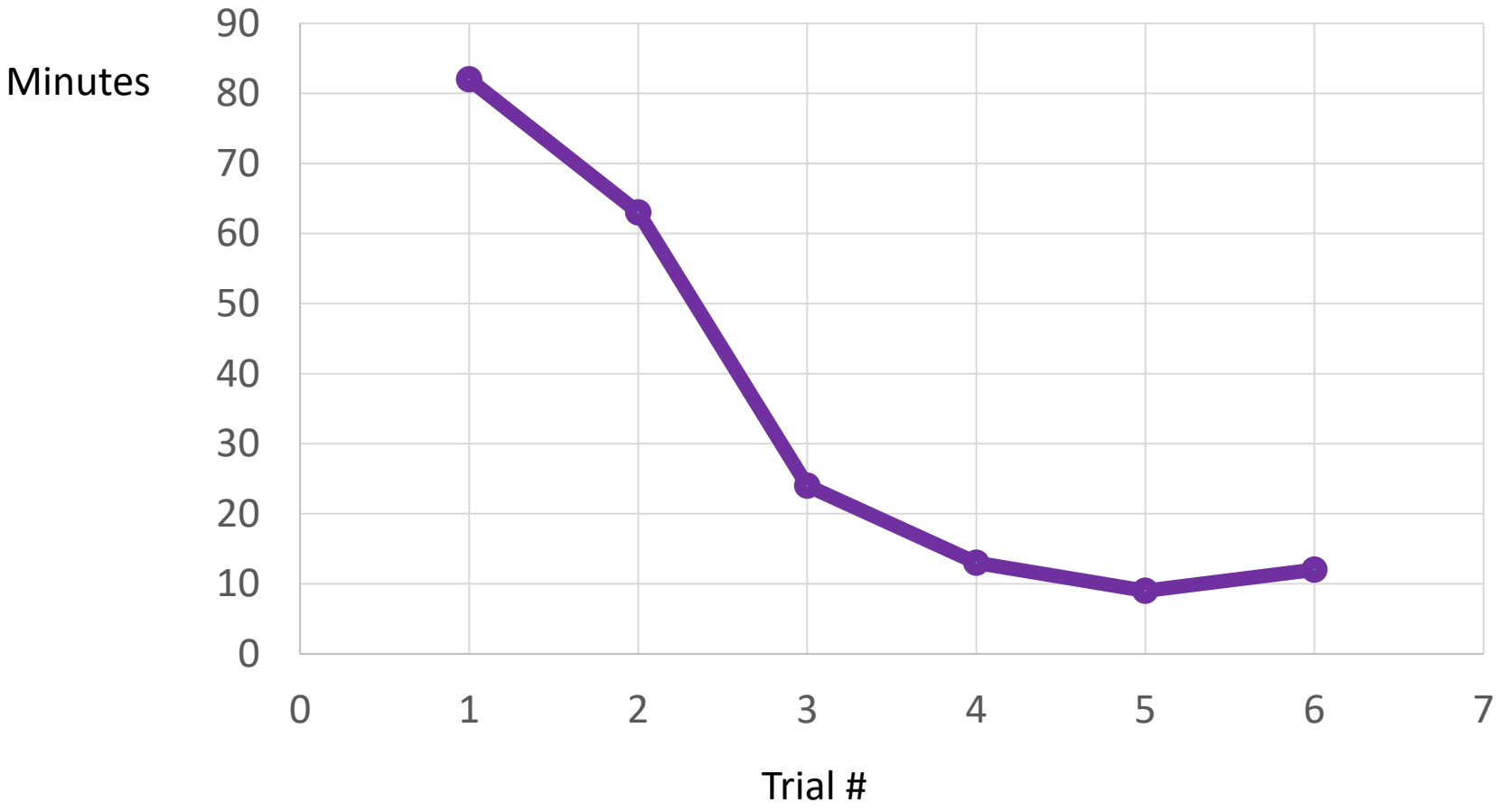
Time spent developing Step 3 UCA table



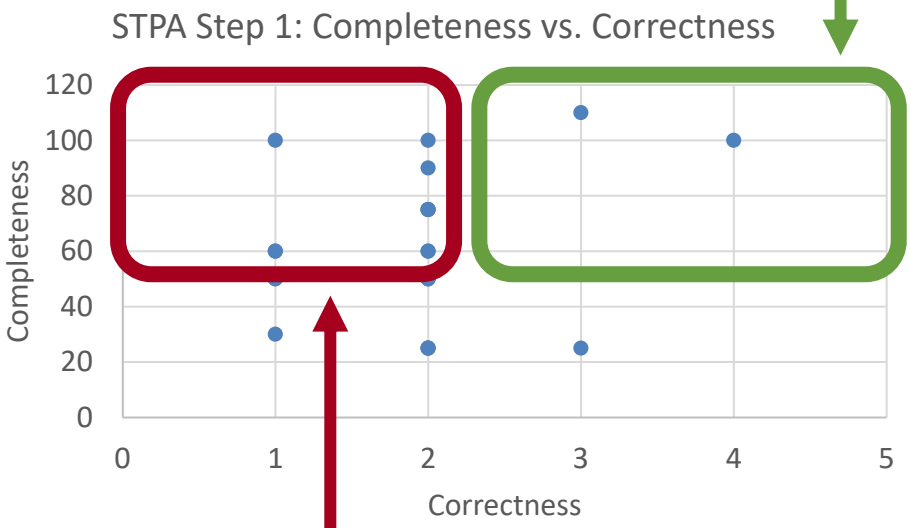
Massachusetts Institute of Technology

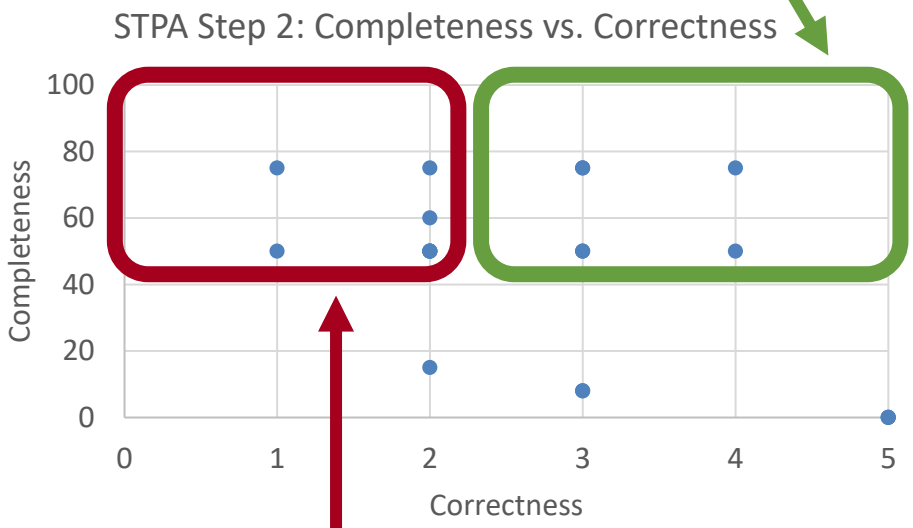
Data: Learning curve

Time spent developing Step 4 scenarios



Complete & Correct STPA Work
Ideal candidates to lead STPA efforts!





Complete, but Incorrect STPA Work
DANGER: Not yet ideal candidates to lead STPA efforts—more practice/experience needed.

Participants' work graded after given a fixed amount of time to perform STPA

Massachusetts Institute of Technology

Implementing STPA

- ✓ Getting buy-in
- ✓ Learning the method
- ✓ Selecting a suitable system
- ✓ Assembling a team
- ✓ Planning a project
- ✓ Guiding the analysis
- ✓ Management
- ✓ Accelerating STPA

Any questions? Email me! JThomas4@mit.edu

Thank you!