Massachusetts Institute of Technology

Introducing STPA to a Regulator: Lessons Learned from Providing STPA Training and Facilitation

John Thomas

Any questions? Email me! JThomas4@mit.edu

Before this project…

Industry STPA Comparison

	Safety-related Functional Requirements	Safety-related System Design Requirements	Safety-related Design Solutions
Number of STPA Safety Constraints (SC) that were already well-enforced by requirements/design (10 or more relationships)	8	75	236
STPA Safety Constraints (SC) that were minimally addressed by requirements/design (5 or fewer relationships)	208	75	34
STPA Safety Constraints (SC) that were not covered by any existing requirements or solutions	82	20	15

Covered
These STPA results were addressed before STPA was applied.

Not Covered
These STPA results had NO existing mitigations or corrective measures. These were accidents waiting to happen.

Table: *Use of STPA in the Development of a Reactor Protection System*, Paul Butchart (NuScale), 2020

Acceptance

- NuScale and the NRC engaged for several years in development of Hazards Analysis framework
- The NuScale Design Certification Application was the first implementation of an HA for a digital I&C system design.
  - Overall positive results from NRC safety reviews
- Electric Power Research Institute (EPRI) – very interested

- Overall the response and acceptance was very positive

Update:

- December 2016 - Rendered
- January 2017 - Submission completed
- July 2020 - Submitted Request for Standard Design Approval
- September 11, 2020 - Approved

This project…

NRC STAMP / CAST / STPA
Training

NRC STAMP / CAST / STPA

~~Training~~

Develop capability-building methods

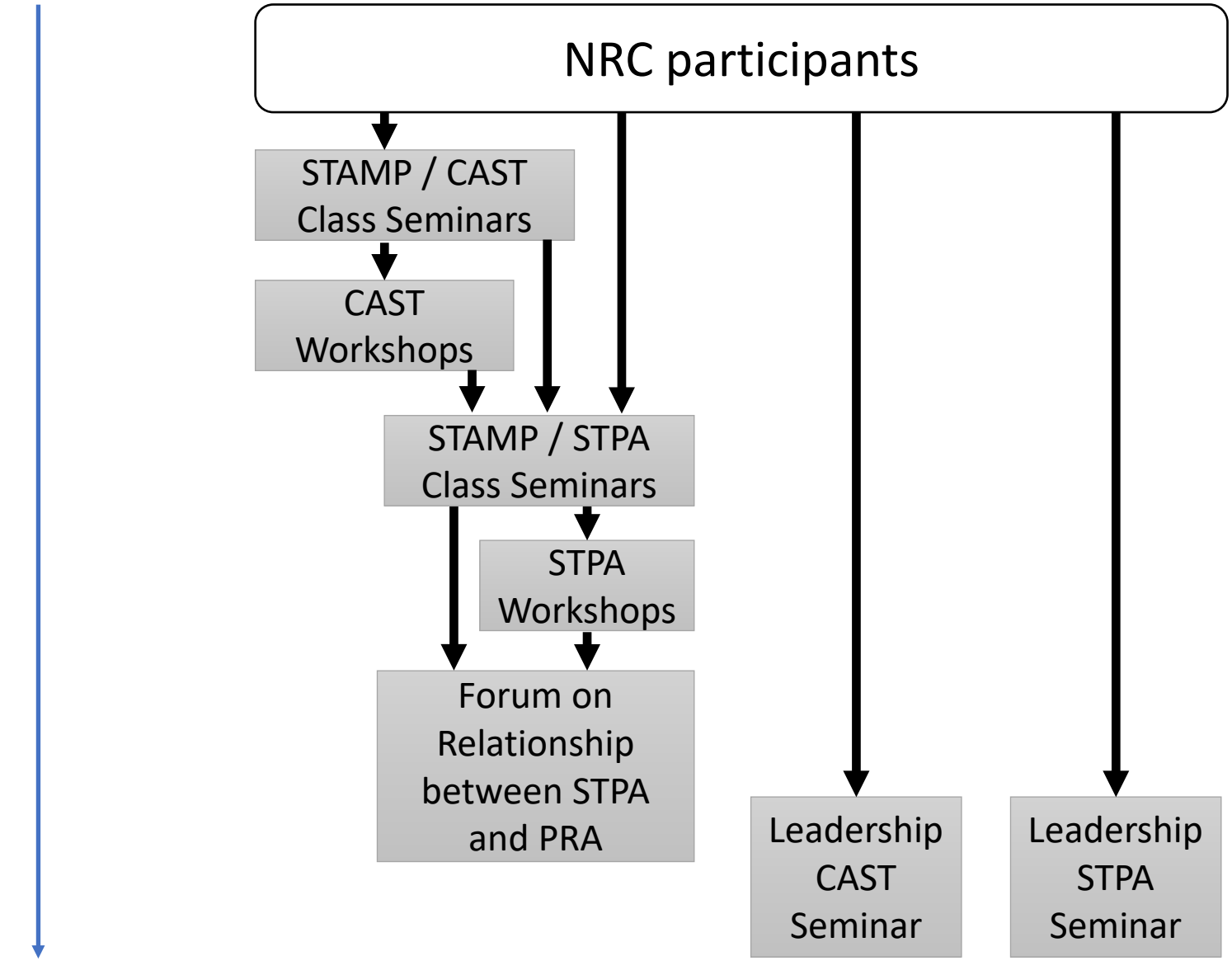
NRC STAMP / CAST / STPA

~~Training~~

~~Develop capability-building methods~~

Investigation of the Use of Systems-Theoretic Accident Model and Processes (STAMP)-based Methods for Digital Nuclear Safety System Evaluation

Overall Plan



Possible Skepticism

- “Doing STPA will require an MIT PhD”
- “STPA will take too long, less inefficient than what we do now”
- “STPA isn’t as effective as what we do now”
- “STPA won’t find any new insights”

Possible comments/assumptions against trying STPA.

Let’s turn these into questions to be investigated.

Questions to be Answered by NRC

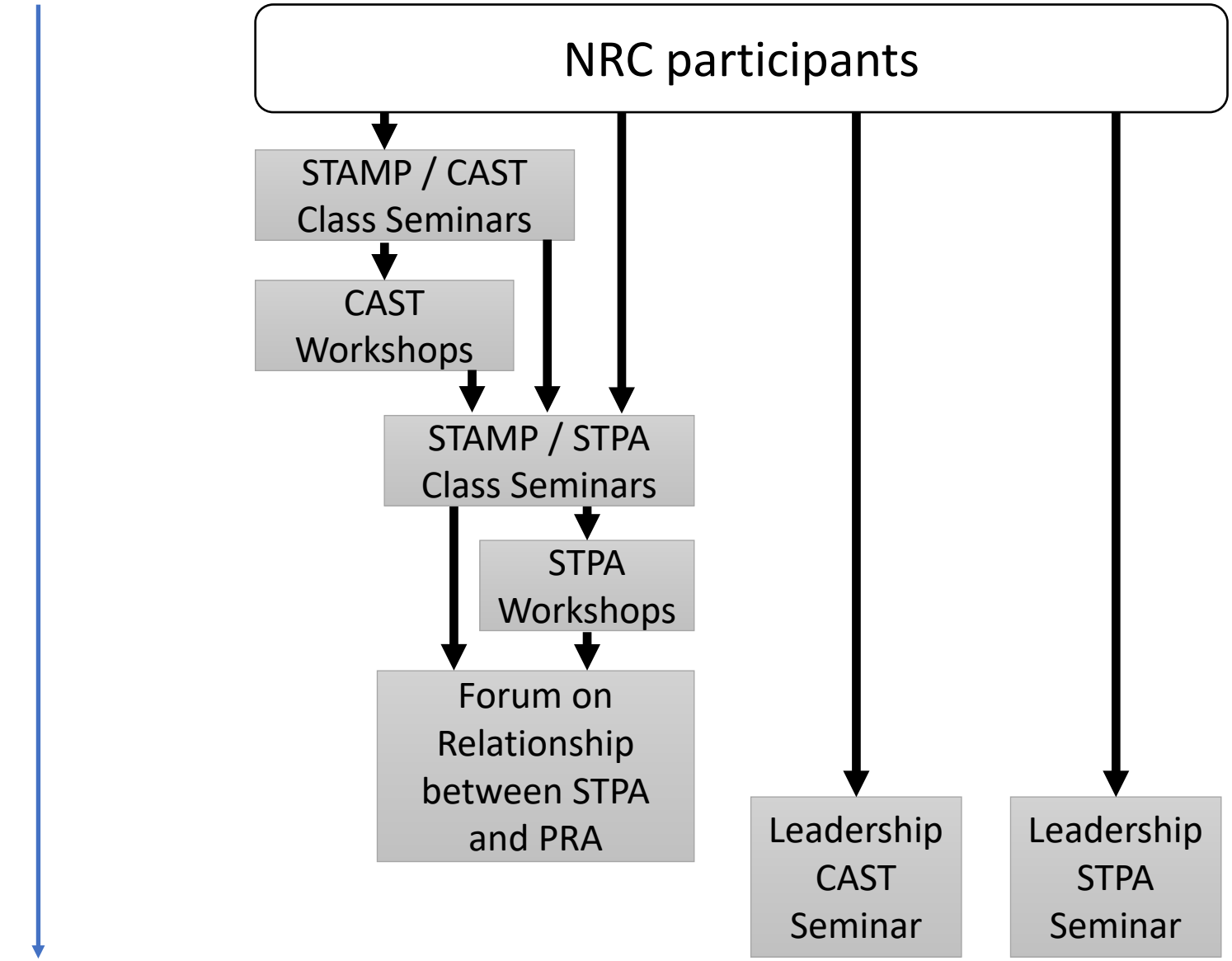
- Did you **understand** the topics covered in the STPA seminars / workshops?
- Is STPA an **effective** technique to help NRC achieve its objectives?
- Do you feel you could perform STPA successfully given sufficient guidance and access to a qualified STPA facilitator?
- Will applying STPA produce **new insights**, beyond what our current processes find?
- Would STPA help the NRC identify **practical ways** to increase safety?
- Would the NRC benefit from using STPA?
- Would the NRC benefit from industry use of STPA?
- Would the NRC be **willing to incorporate STPA** into NRC processes or NRC materials?

Similar Questions Identified for CAST

Additional Questions for NRC Staff to Answer (proposed by NRC staff during STPA seminars)

- Would STPA provide a way to identify **unbounded or unanalyzed events** relevant to NRC objectives?
- Would STPA **inform existing likelihood** categorizations, such as likelihoods that may be incorrect or based on incorrect assumptions?
- Would STPA provide a **more efficient** analysis in terms of effort needed to review?
- Would STPA provide a **more effective** means of development assurance than what is currently done? (validation of design intent)

Overall Plan



What NRC Groups Participated?

59 NRC Staff from:

- Office of Nuclear Regulatory Research (RES)
  - Division of Engineering
  - Division of Risk Analysis
  - Division of Systems Analysis
- Office of Nuclear Reactor Regulation (NRR)
  - Division of Advanced Reactors and Non-Power Production and Utilization Facilities
  - Division of Engineering and External Hazards
  - Division of Reactor Oversight
  - Division of Risk Assessment
- Office of the Chief Information Officer
- Office of Nuclear Security and Incident Response
  - Division of Physical and Cyber Security Policy
- Region II—Division of Reactor Safety
- Region III—Division of Reactor Safety

I&C branches are included from the Office of Nuclear Reactor Regulation (NRR) and the Office of Nuclear Regulatory Research (RES).

What NRC Groups Participated?

- Participants included NRC technical reviewers, regional inspectors, researchers, and managers.
- The areas of expertise of the NRC participants included the following:
  - electrical engineering
  - mechanical engineering
  - nuclear engineering
  - PRA
  - operating experience
  - instrumentation and control
  - cybersecurity
  - information technology

Intermediate feedback collected

What was the “muddiest” part of today’s meeting? Are there any lingering points of confusion?

Early staff responses at the start of project:

- “None.”
- “What doesn’t STPA do well?”
- “The ad hoc discussion of FT, PRA "versus" STPA. It should not be "versus". As you said, PRA and STPA should be treated as complementary. STPA provides the "what can go wrong" from the perspective of systemic causes (hazardous interactions ... interdependencies). Thus, it could serve as improving the "input" to PRA models.”

These responses were continuously used to tailor the remaining STPA seminars / workshops.

Other thoughts or comments?

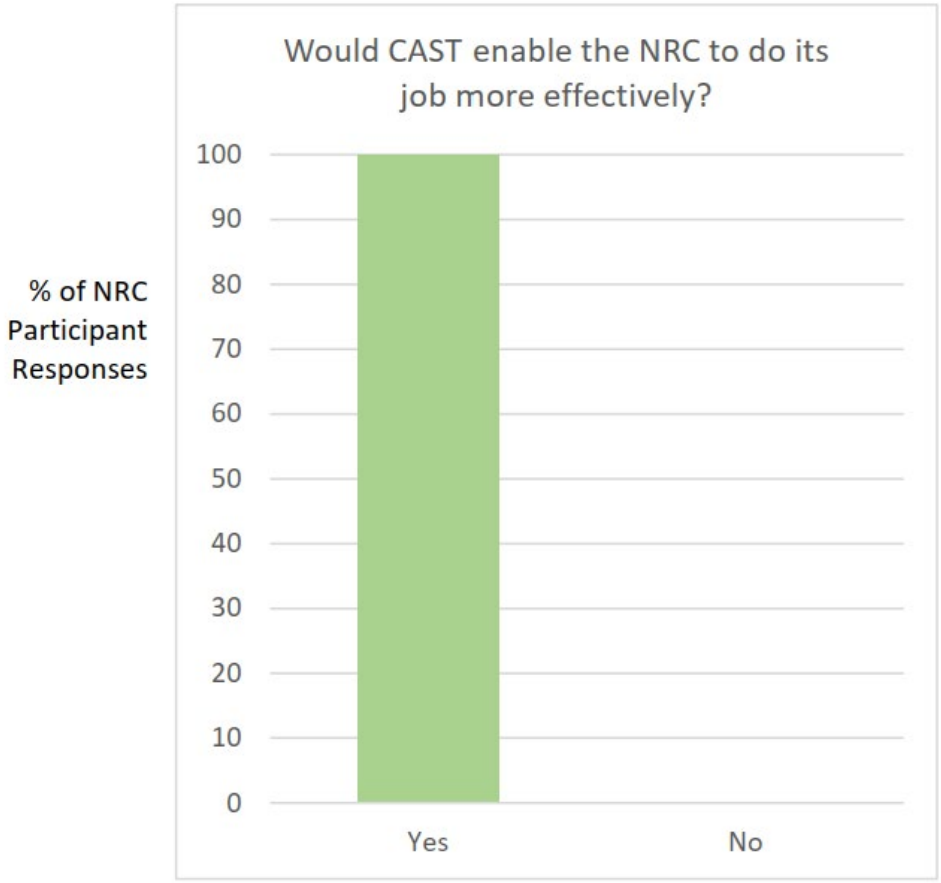
Examples of staff responses:

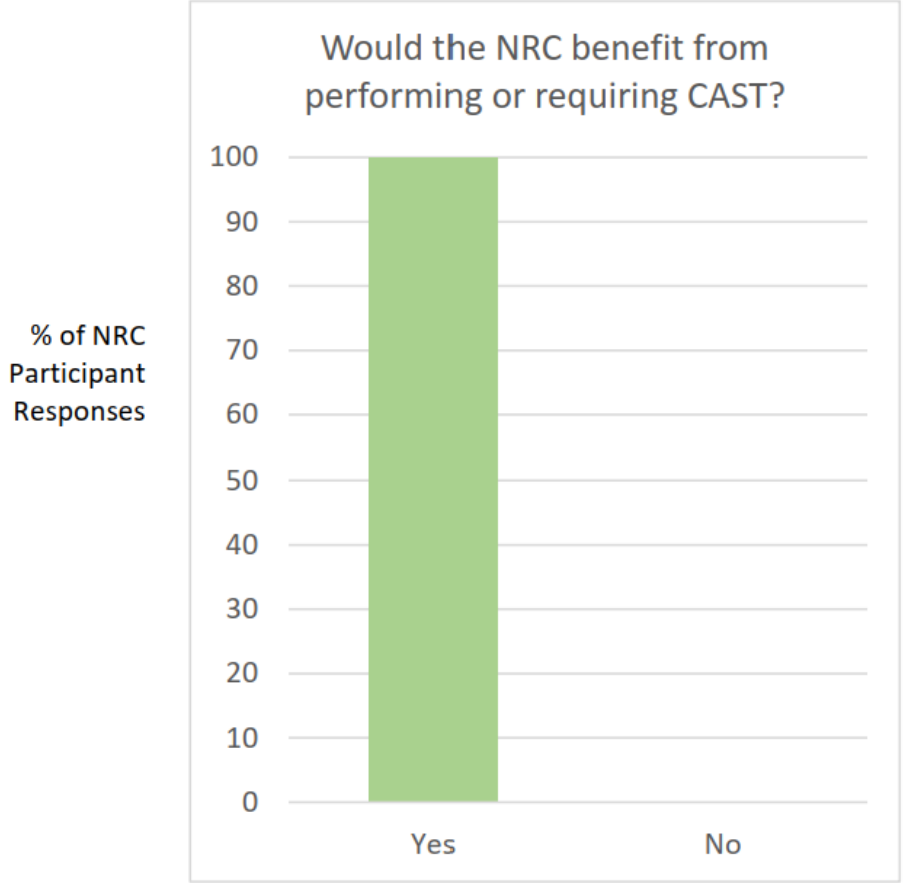
- “When you get to analyzing what & why human operators do things in complex systems that require substantial training, educations, etc., there's no replacement for operator interviews, observations, etc.”

These responses were continuously used to tailor the remaining STPA seminars / workshops.

NRC Staff Conclusions (at the end)

CAST
(Retrospective – Past Events)


Would CAST enable the NRC to do its job more effectively?
% of NRC Participant Responses
100
90
80
70
60
50
40
30
20
10
0
Yes
No


Would the NRC benefit from performing or requiring CAST?
% of NRC Participant Responses
100
90
80
70
60
50
40
30
20
10
0
Yes
No

Where might CAST be used at the NRC?
NRC Staff Answers:

Event Response

- **NRC Inspection teams** deployed to sites for significant events
- NRC staff that **review OE**, discuss initial **LERs**, review LERs, and review RCAs
  - "Really good way to truly understand what has happened and why versus just who is at fault."
- **CAST use by licensees** would allow for more directed/focused/appropriate recommendations than the scattershot approach that happened after TMI

NRC Internal Use

- NRC staff who **evaluate our own processes** and procedures (even when there is not obvious "failure.")
- NRC staff who **develop questions** (e.g., Requests for Additional Information) for licensing requests
- In **NRC policy** so that we can have NPPs adhere to it

What NRC groups would benefit from CAST?

NRC staff answers :

- Resident inspectors
- Human factors
- Management
- Licensing offices
- Probabilistic Risk Assessment (PRA) [Staff]
- Rulemaking groups
- Cybersecurity
- Licensees
- I would argue that at the NRC, most everyone would benefit. Even for people who are not practitioners in this area, they can learn a great way of looking at things. A very valuable “awakening of their perspective.”

What NRC groups would benefit from CAST?

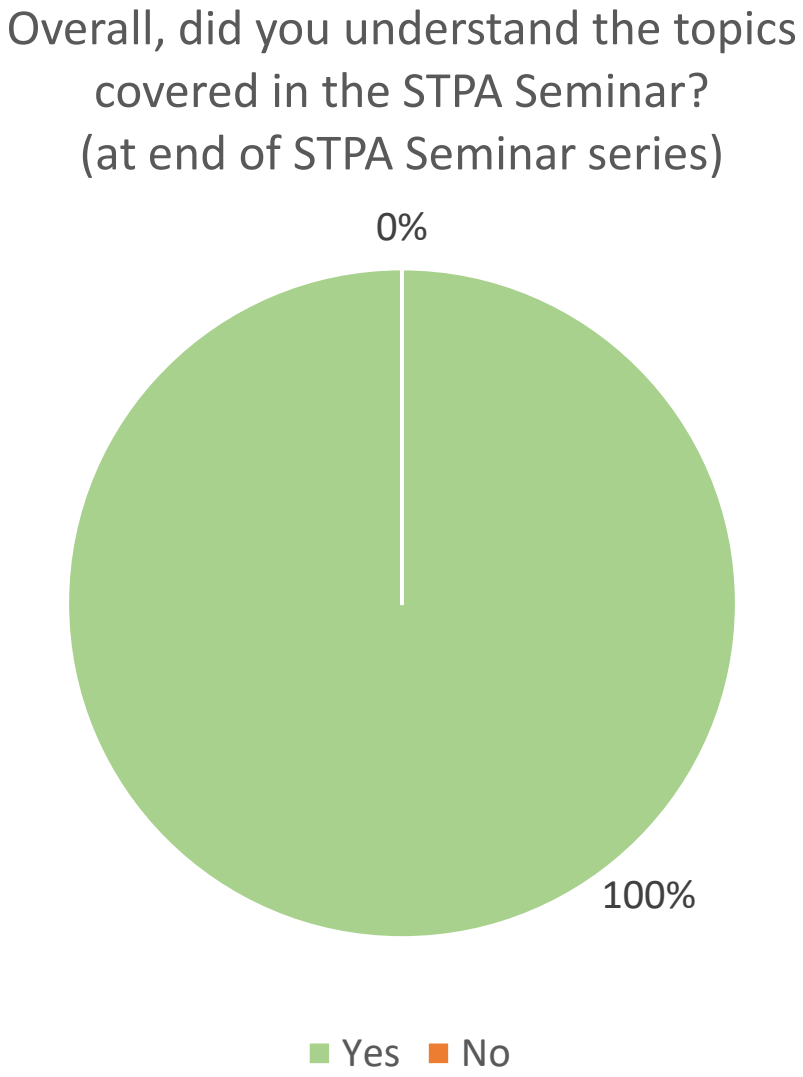
NRC staff verbatim answers :

- Resident inspectors are much closer to events and may be able to apply or encourage application of these concepts.
- Staff in human factors engineering
- Resident and regional inspectors
- Staff conducting operating experience review
- Management
- More people from the licensing offices
- I think that there should be staff in the Nuclear Materials Safety and Safeguards office—both for fuel processing and nuclear medicine/byproduct materials—who could benefit.
- Division of Systems Analysis (DSS) and Division of Risk Analysis (DRA) personnel
- Much higher-level management (Office of the Executive Director for Operations (EDO) and Commissioner Technical Assistants (TAs))
- Inspectors
- Probabilistic Risk Assessment (PRA) [Staff]
- I think exposure to CAST would be useful to all of NRC. Reviewing or applying an event using CAST would require assessment and interaction among multiple groups.
- Senior level management and rulemaking groups, who ultimately may need to be involved with and buy into the conclusion that the safety increase of applying CAST is cost-justified compared to existing licensee practice.
- Whichever NRC staff might initiate guidance to industry on acceptable methods to perform and document accident contributors as part of continuous learning.
- Top candidates: Inspectors; staff in the Operating Experience Branch.
- Staff in the Office of Nuclear Regulatory Research (RES) Division of Risk Analysis (RES/DRA) responsible for human factors engineering and operating experience research and Division of Engineering (RES/DE) responsible for Research and Development (R&D) in Digital Instrumentation and Controls (DI&C) and Electrical Engineering (EE).
- TTC runs the inspector training including root cause evaluation. Safety culture/human factors groups would also benefit (RES, Operating Experience (OE), and Office of Nuclear Reactor Regulation (NRR)).
- I would argue that at the NRC, most everyone would benefit. Even for people who are not practitioners in this area, they can learn a great way of looking at things. A very valuable “awakening of their perspective.”
- I think NRC management should be engaged. It seems we are more reliant on licensee’s programmatic and PRA approach to discuss plant safety rather [than] weaknesses in plant designs—the DC loss of engine mentality is parallel to NPP culture.
- Office of nuclear Material Safety and Safeguards (NMSS)—fuel processing facilities, industrial radiographers, etc. and radiation therapy (i.e., nuclear medicine)
- Inspectors, technical reviewers, management
- Cybersecurity
- Inspectors. The technique is flexible and it seems like it could be applied to almost any problem.
- Operating Experience (OpE). The current practice of the NRC with respect to operational experience is that the NRC helps/facilitates industry learning from each other’s mishaps. The NRC could look at certain types of OpE (e.g., no random hardware failures) to see if there are any systematic contributors, CAST would be one way of doing that. Basically, nothing is perfect, and everything could be improved. Why not look to see if we can do better?
- Operating Experience review staff
- Researchers
- New/Advanced and operating reactor licensing staff who may support special inspections
- Regional Inspectors
- Those in the Regions/Headquarters (HQ) who establish policies and procedures for regional inspectors to follow
- Vendor Inspectors
- Those in the Regions/HQ who establish policies and procedures for vendor inspectors to follow
- Staff that support the Allegations process
- Those in the Regions/HQ who establish policies and procedures to investigate allegations
- Staff in the Operating Experience section in NRR
- Resident inspectors
- Licensees
- People that work directly with the licensees
- Processes for which improvement potential is recognized (either by the stakeholders or by the staff or by the leadership)

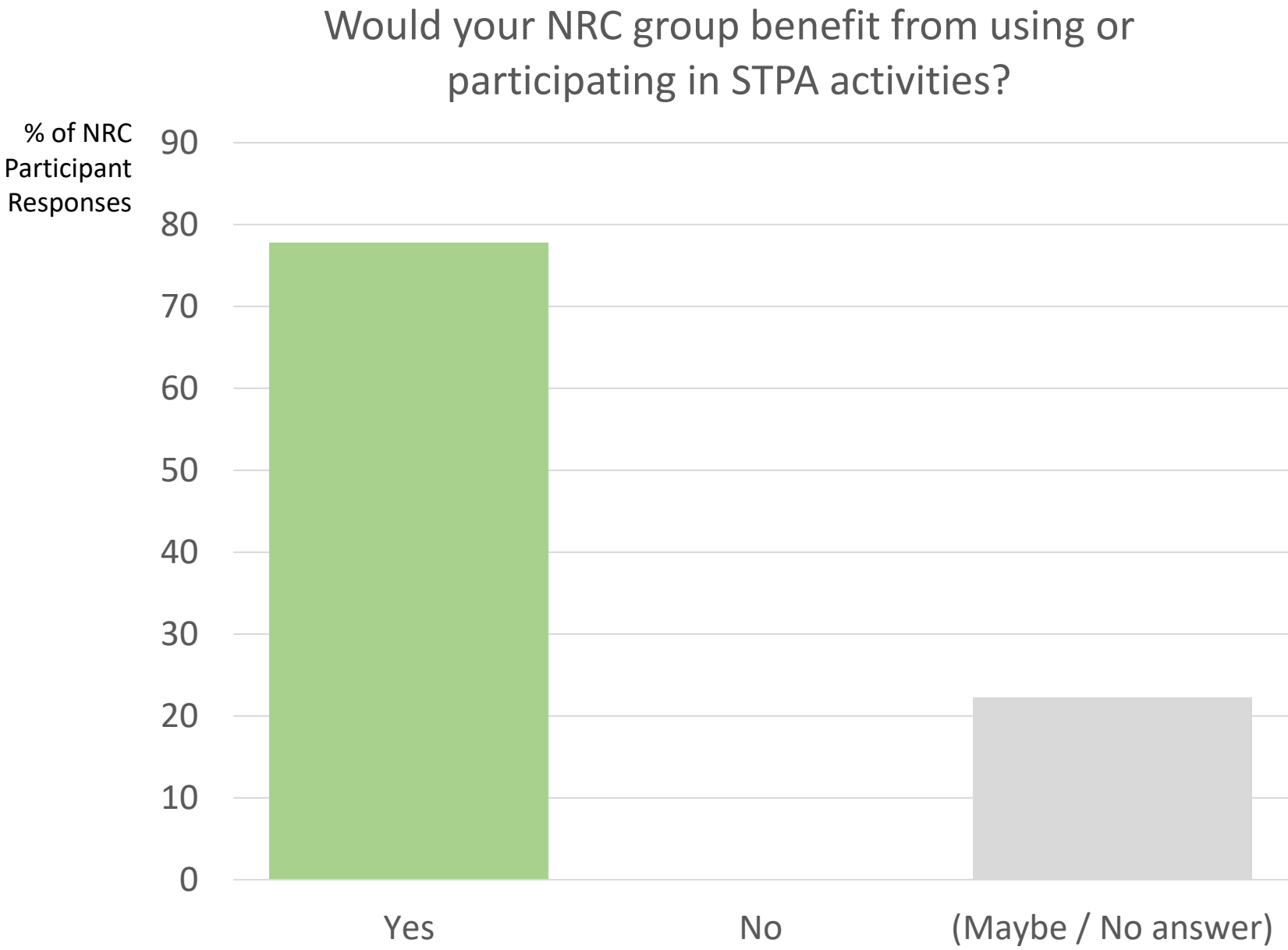
STPA
(Prospective)

STPA: NRC Staff Conclusions

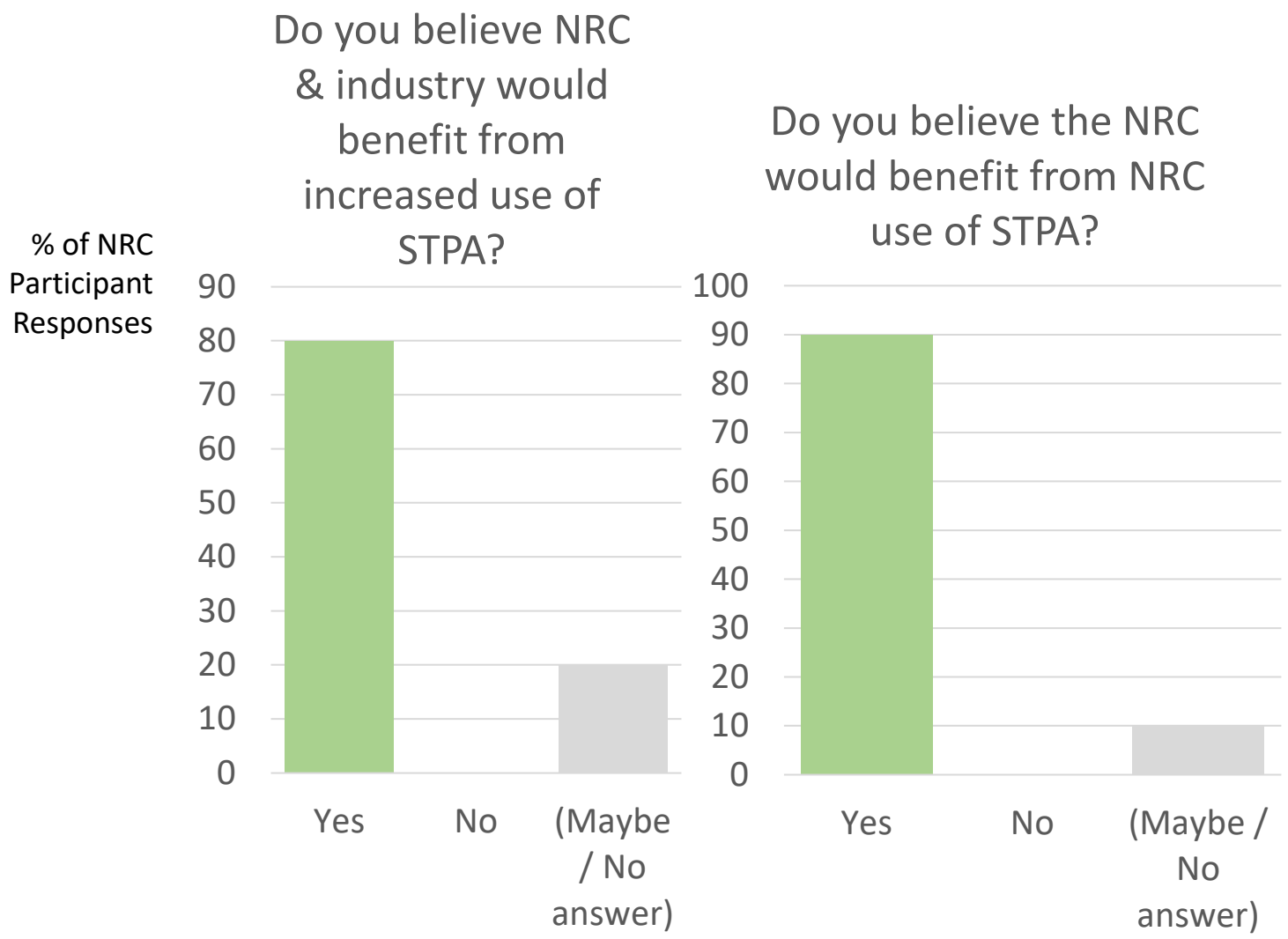
- STPA helps to address the "**unknown unknown**" space, which is increasing with the use of more digital automation.
- PRA usually represents a "typical" or "average" state of a plant and its response to an initiating event (which may be a rare event). However, **STPA can address additional unexpected** or extreme abnormal conditions that may not be within the scope of a PRA, including plant states that PRA does not define as "failures."
- To date and for U.S. commercial nuclear power plants, PRA has had limited application to modeling control systems and has not needed to model software except very simplistically. STPA models well the potential for hazardous behavior in **control systems and software**.
- STPA would be very helpful for new systems, as well as for upgrades.
- STPA has different strengths than PRA. The two approaches are complementary.
- It is obvious that STPA is different from PRA and produces different results (some people characterize STPA as qualitative and PRA as quantitative).
- PRA has identified design issues in the past, so it would be incorrect to say that PRA cannot identify design issues. However, **STPA seems to be better suited** for identifying design issues.
- STPA analysis results may be useful to better inform PRA models about the effects of **common causes**.



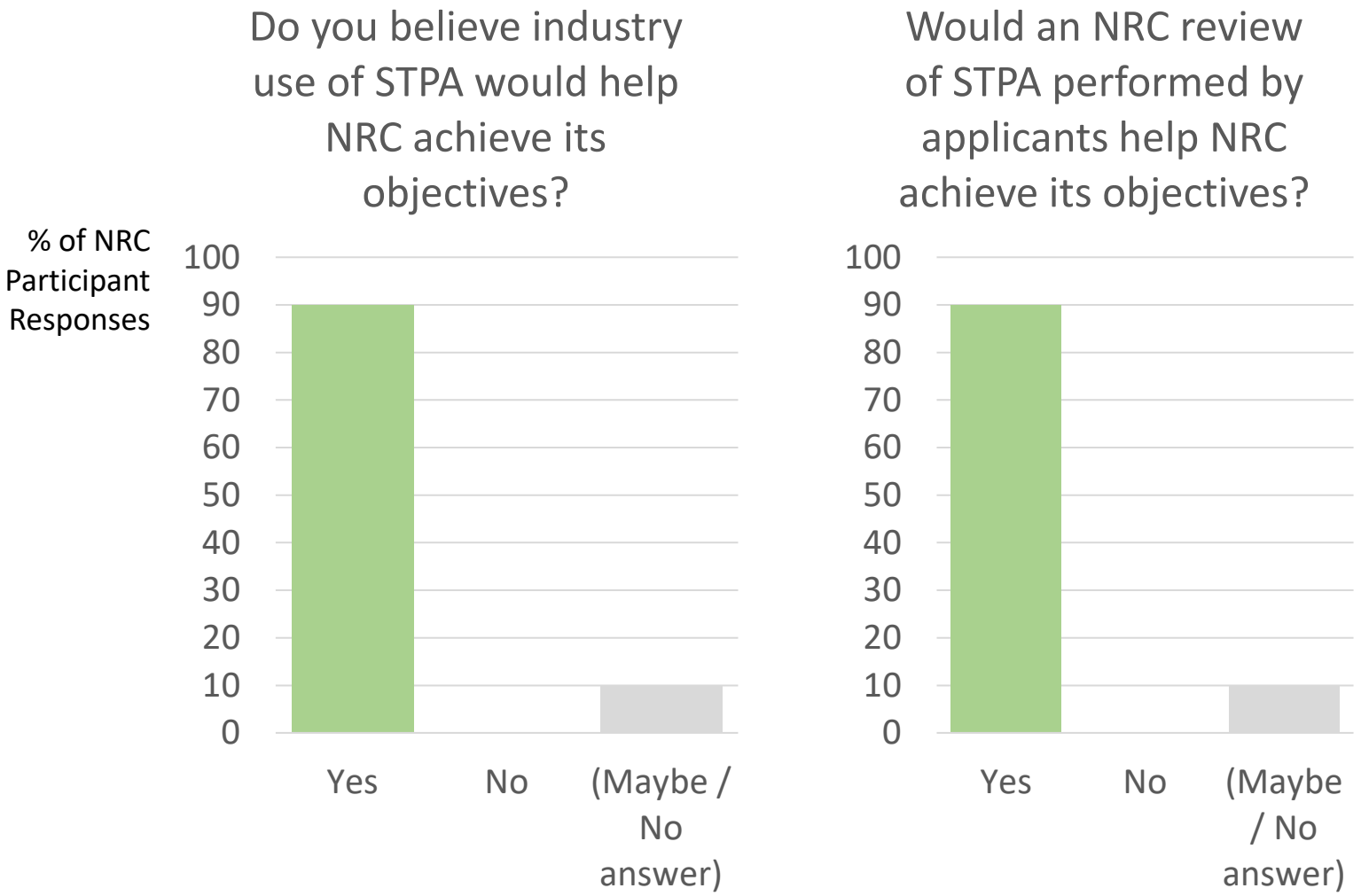
NRC participants reported that STPA was understandable and learnable

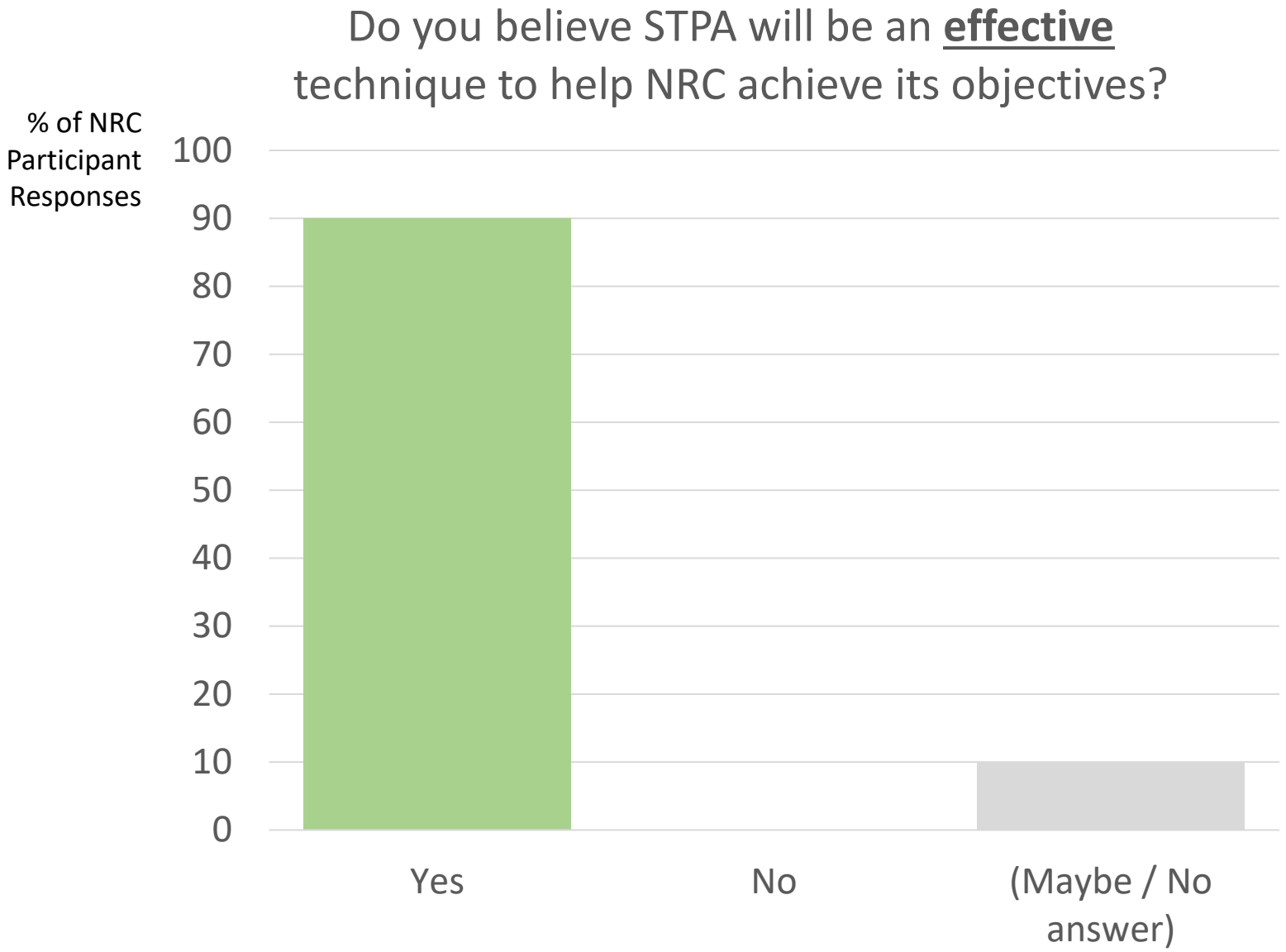


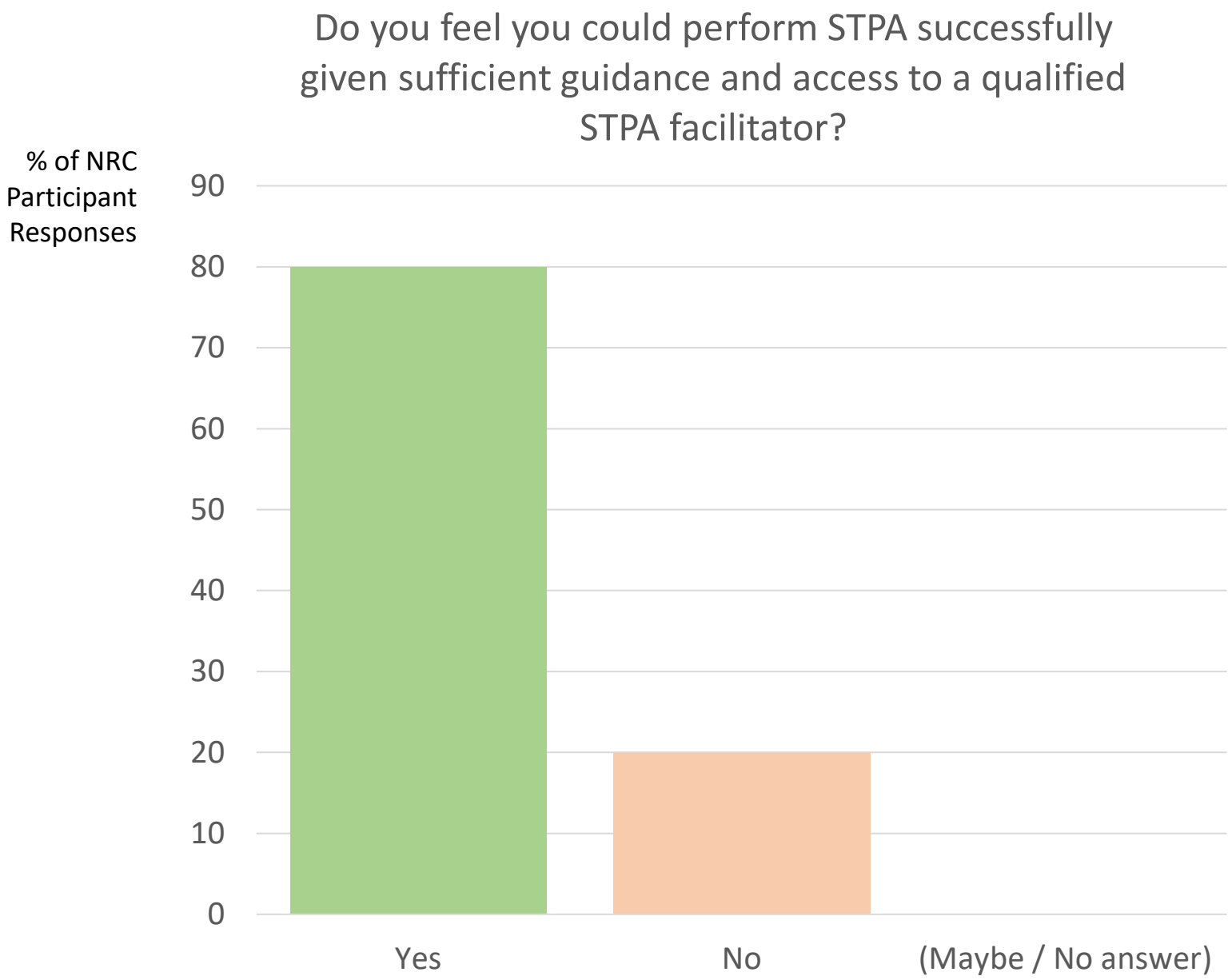
Should NRC use STPA?



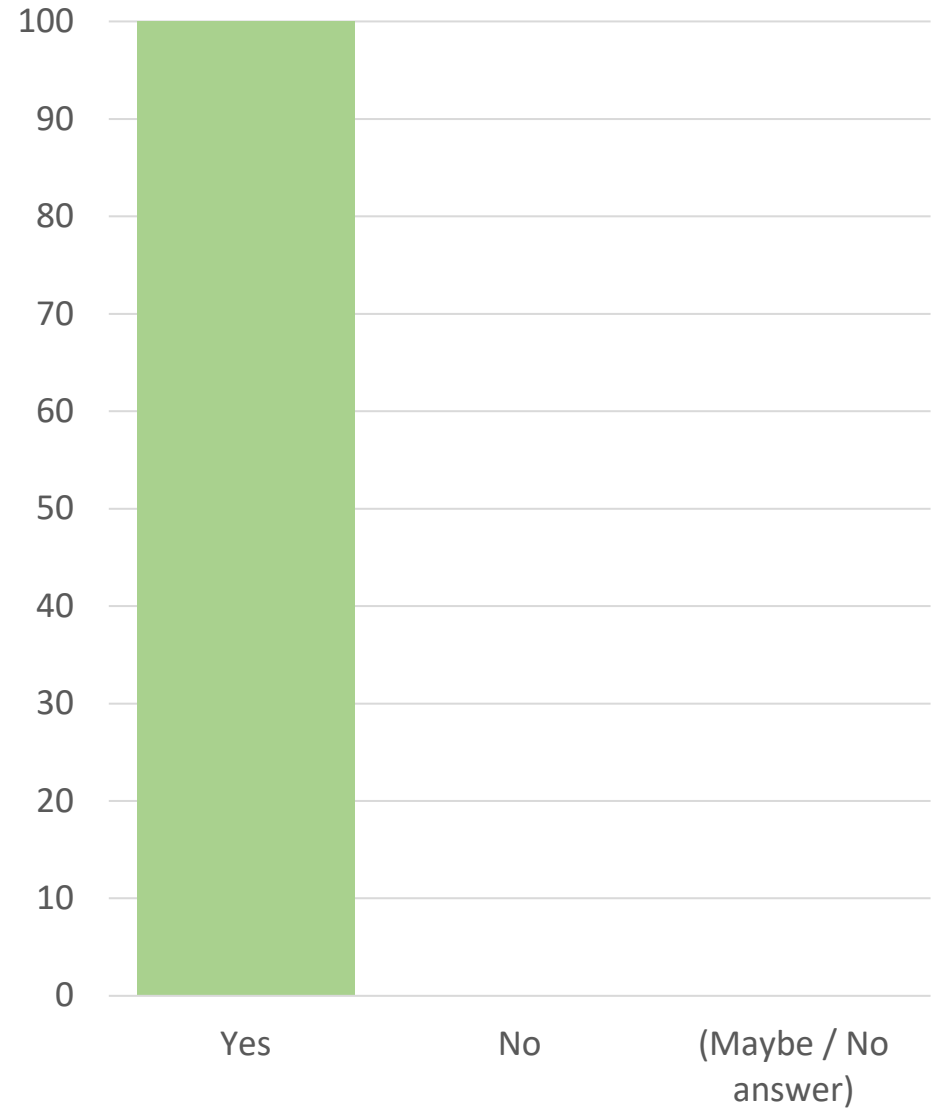
Should Industry Use STPA?



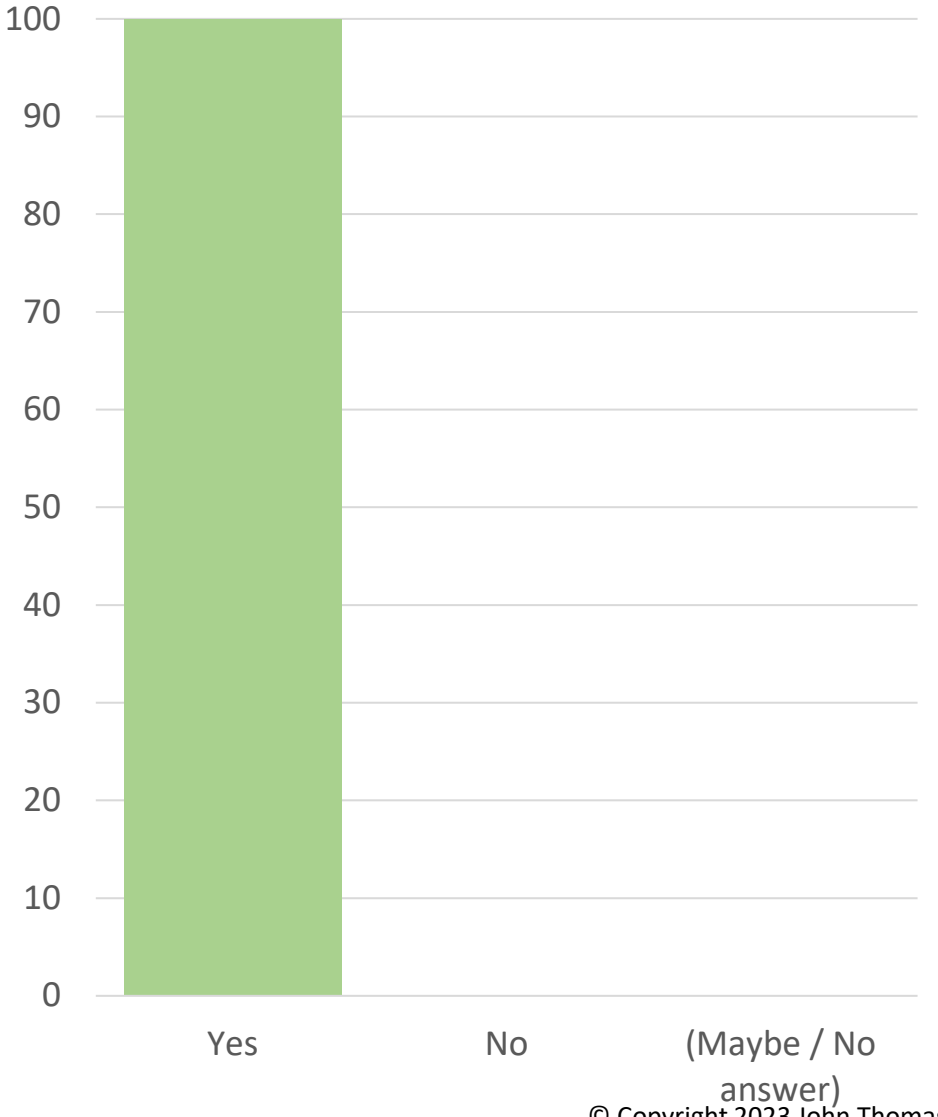


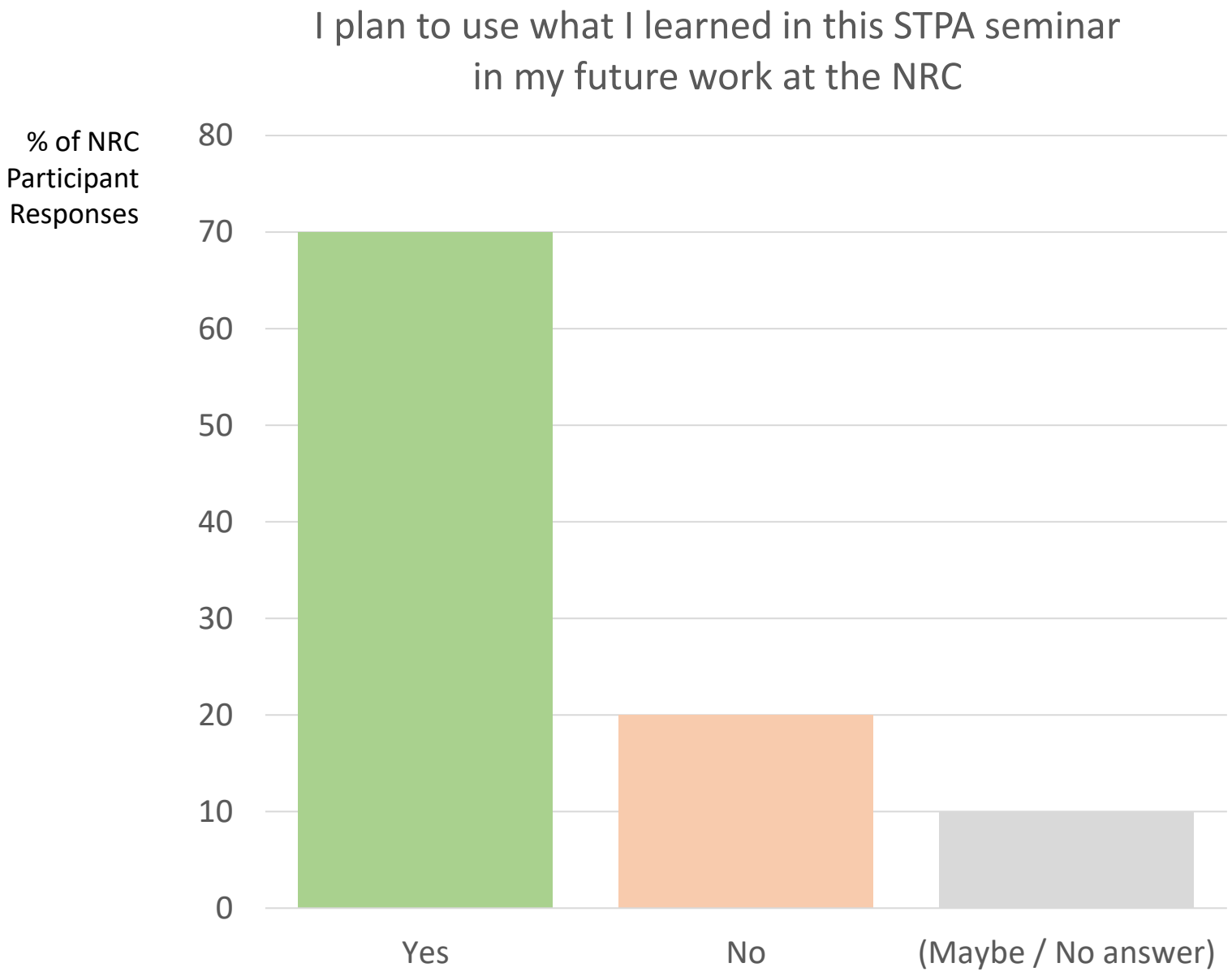


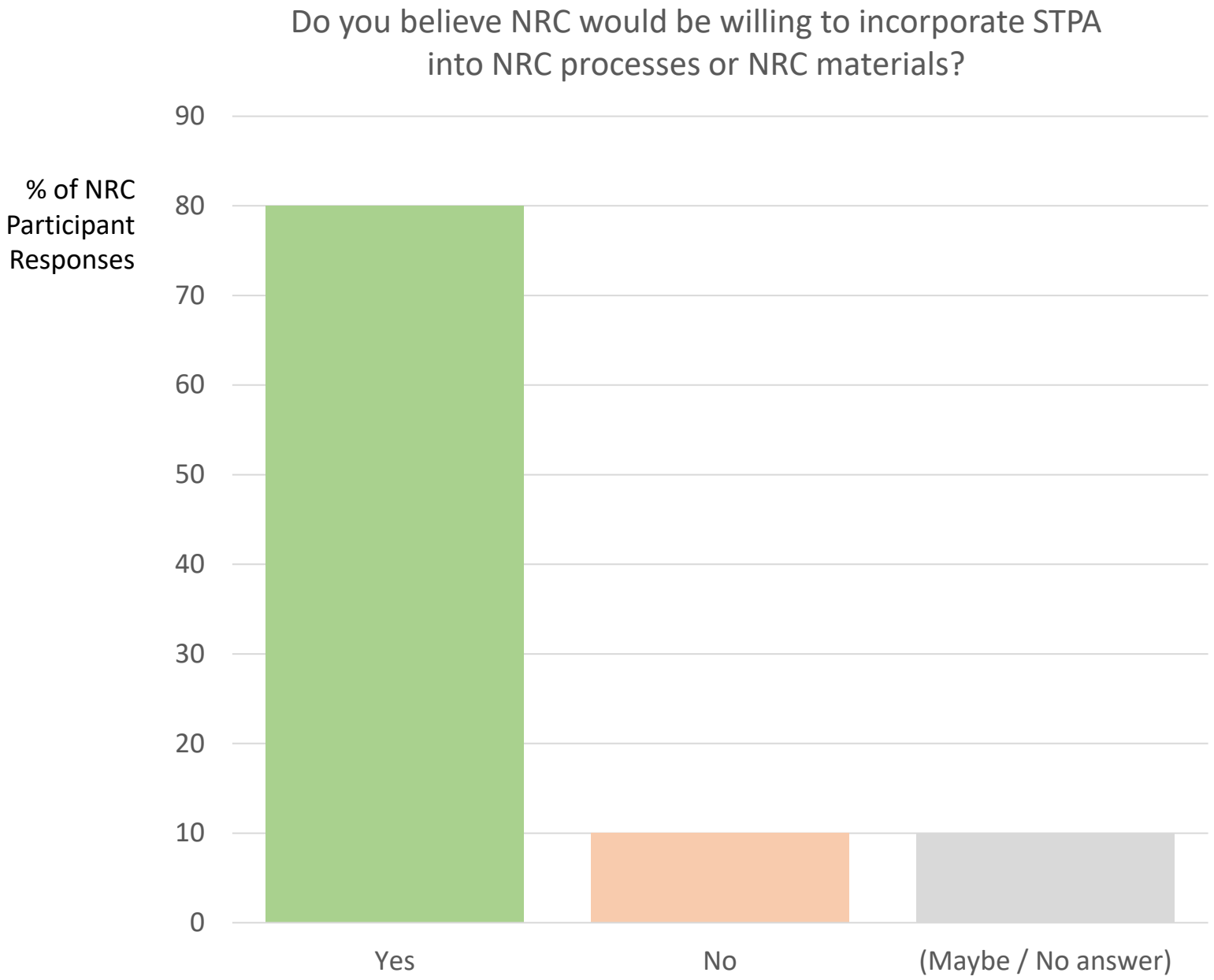
Based on what you have learned so far, do you believe that applying STPA to nuclear systems will produce **new insights** (beyond what our current processes find)?



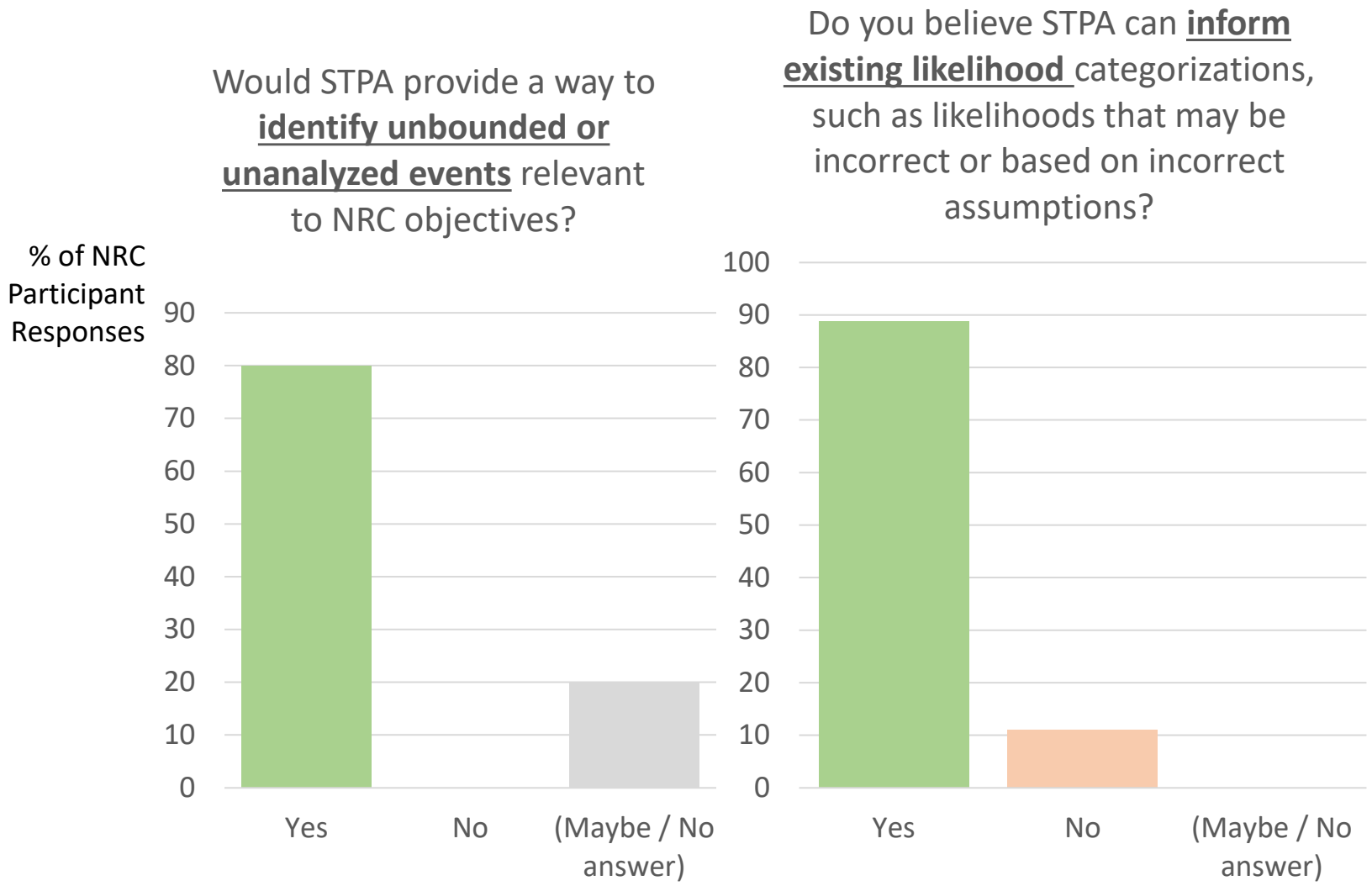
Do you believe that STPA would help the NRC identify **practical ways** to increase safety?







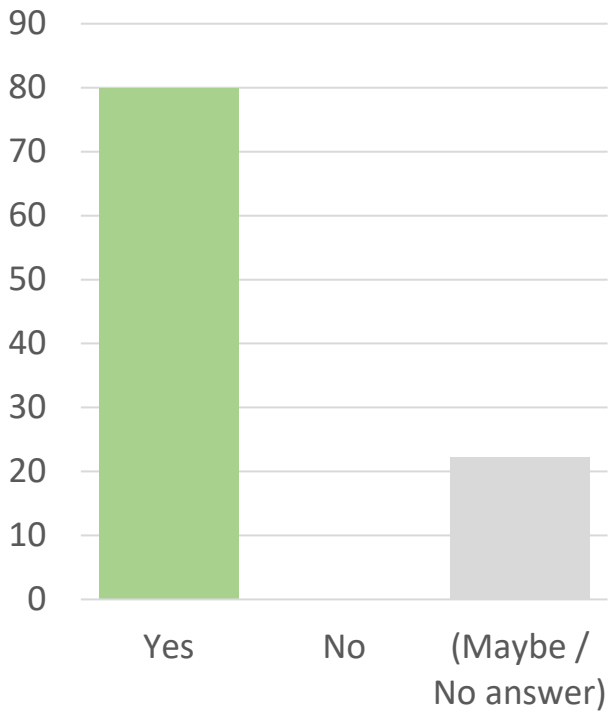
Exactly how would STPA help achieve NRC safety objectives?



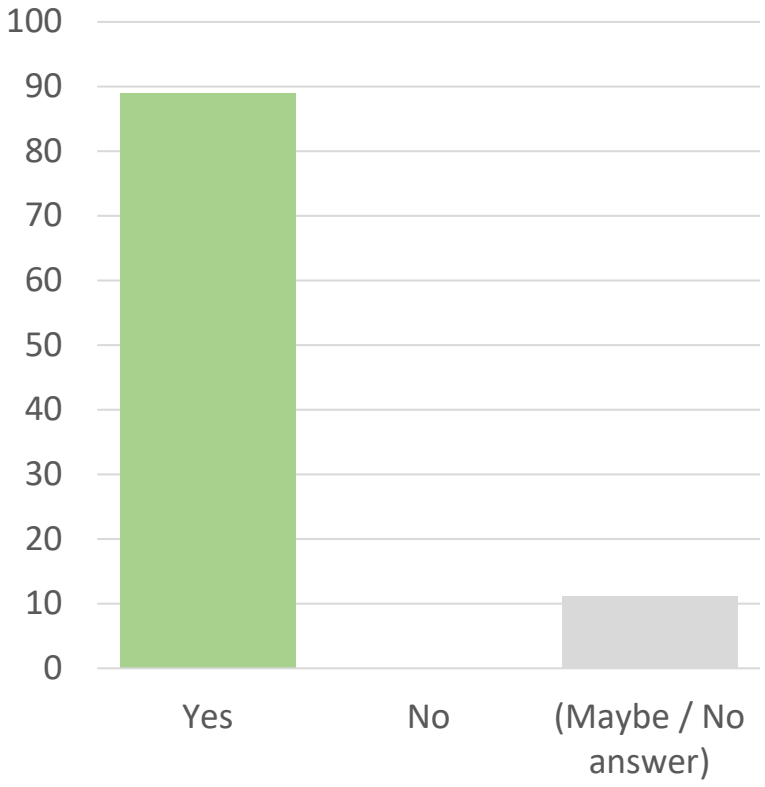
Exactly how would STPA help achieve NRC safety objectives?

% of NRC Participant Responses

Do you believe STPA could provide a **more efficient** analysis in terms of effort needed to review?



Can STPA provide a **more effective means** of development assurance than what is currently done? (validation of design intent)



What groups at NRC would benefit from STPA?

NRC Staff Responses:

- Cyber security
- Software
- Any offices that consider risk and design
- Licensing Folks
- NSIR CSB
- I&C
- Folks doing research on design
- Human factors engineering
- Division of Risk Analysis (DRA) in Research (RES)
- Inspectors
- Licensing Reviewers
- Management
- Licensing
- Any risk or management group. Especially those who inform regulation.
- NRC regional inspectors, cyber inspectors
- Any organization that has responsibility for a system or facility that plans to incorporate a significant amount of automation or remote control.
- All areas that review
- NSIR
- NRR
- RES
- NMSS
- Just about any process can use this concept to identify situations where the planned thing occurs, but it is not the right thing. The fact that this catches incorrect/invalid/incomplete requirements is very valuable.

What NRC activities could STPA help to support?

NRC staff responses:

- Licensing reviews
- Generic issue reviews
- Inspections
- Design review
- Data analysis of system safety and integrity
- Informing licensing requirements for upgrades with automation
- Informing licensing requirements for new reactor designs that cannot borrow from existing designs

Other NRC staff responses:

- “I think that STPA could be an important & useful complement to PRA. Also, I think that **STPA is the only tool that could identify [certain] automation/operation control problems**.”
- “Because STPA embeds traceability to losses of concern, it seems to provide appropriate regulatory review focus. Unstructured descriptions of design details, **especially when presented as components or subsystems**, don't necessarily reveal the context necessary for safety conclusions.”
- “I believe there to be regulatory utility from accessing a licensees STPA. With EPRI's DEG, HAZCADs, and DRAM being adopted, and NuScale's experience, I expect STPA will be performed in our domain. The question then is how would we credit those, what is required to audit their STPA, and what degree of qualification do we need as regulators to competently review an STPA if it is being relied upon to come to a safety determination.”

What will be needed after this seminar in order to be successful with STPA at NRC?

NRC staff responses:

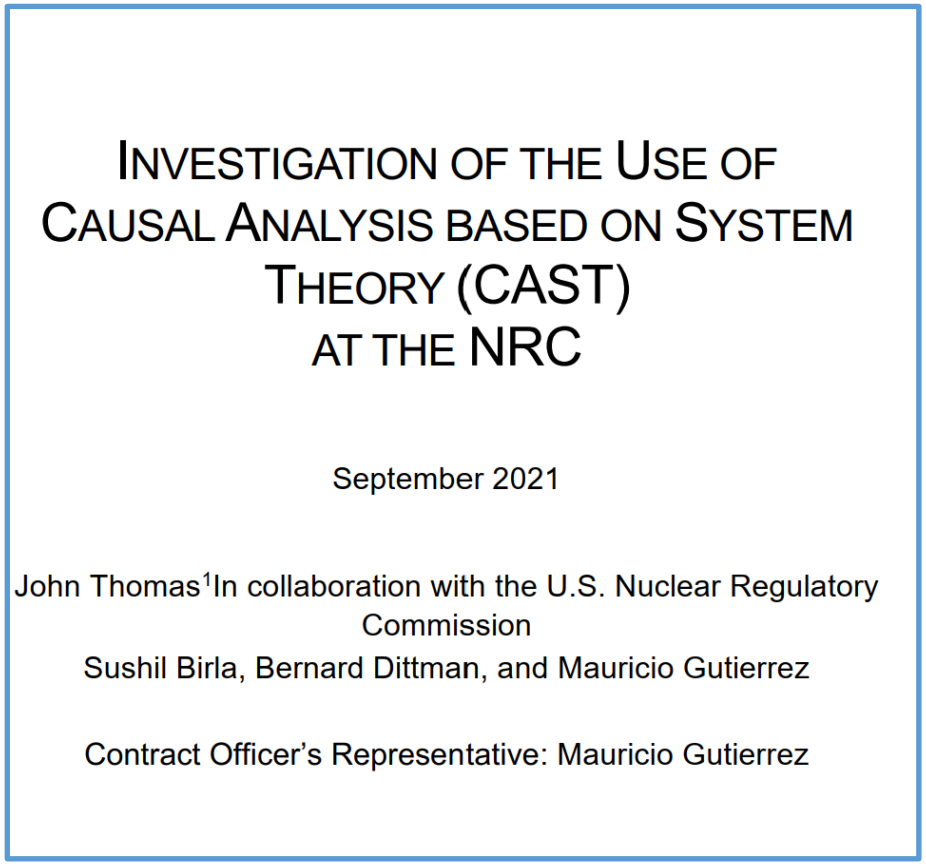
- “Need more presentations to further socialize the concept. Perhaps some shorter, higher level condensed ones for upper management as they could be one of the biggest roadblocks (if they are at all).”
- “More exposure of STPA to NRC staff and management. Need to build support to get it implemented as a method that can be used throughout the agency.”
- “A practical application of STPA on a business process to show efficacy to management.”
- “One needs practice to instill the concepts.”
- “Need a specific activity or project for application as a test case; perhaps a joint project between PRA and I&C groups on an upgrade involving new automation features.”
- “NRC [STPA] Guidance”

NRC Leadership Seminars

- RES Division of Risk Analysis
  - Division Director
  - Senior Technical Advisor
  - Senior Reliability & Risk Engineer
  - Branch Chiefs from:
    - Performance and Reliability Branch
    - Probabilistic Risk Assessment Branch
    - Human Factors and Reliability Branch
- RES Division of System Analysis Accident Analysis Branch Chief
- RES Division of Engineering Deputy Director
- NRR Division of Engineering & External Hazards Director

NRC actions after this work concluded

- NRC STPA Pilot Project
- The Commission approved (all five commissioners approved) the staff's recommendation to expand the existing policy for digital instrumentation and control (I&C) common-cause failures to allow for the use of **risk-informed** approaches to demonstrate the appropriate level of defense-in-depth.



INVESTIGATION OF THE USE OF CAUSAL ANALYSIS BASED ON SYSTEM THEORY (CAST) AT THE NRC

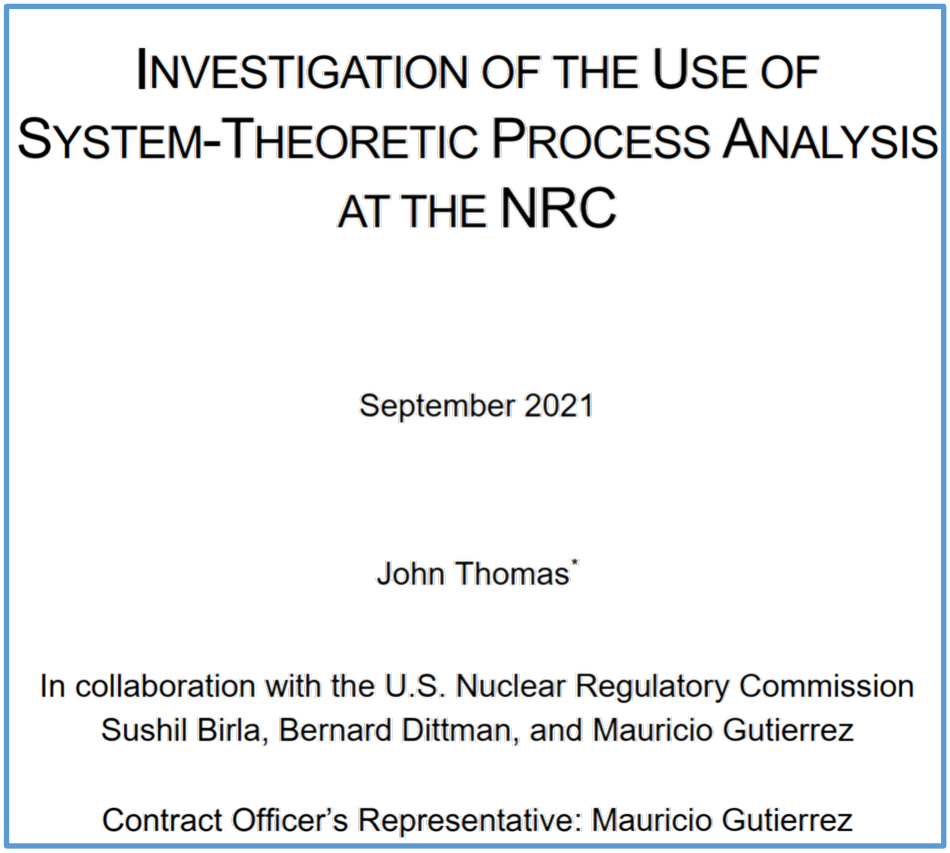
September 2021

John Thomas[1]In collaboration with the U.S. Nuclear Regulatory Commission
Sushil Birla, Bernard Dittman, and Mauricio Gutierrez

Contract Officer's Representative: Mauricio Gutierrez

CAST Report on NRC Website

https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML22277A013



INVESTIGATION OF THE USE OF SYSTEM-THEORETIC PROCESS ANALYSIS AT THE NRC

September 2021

John Thomas*

In collaboration with the U.S. Nuclear Regulatory Commission
Sushil Birla, Bernard Dittman, and Mauricio Gutierrez

Contract Officer's Representative: Mauricio Gutierrez

STPA Report on NRC Website

https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML22272A315