Industry Trials to Evaluate STPA's Effectiveness and Practicality for Digital Control Systems

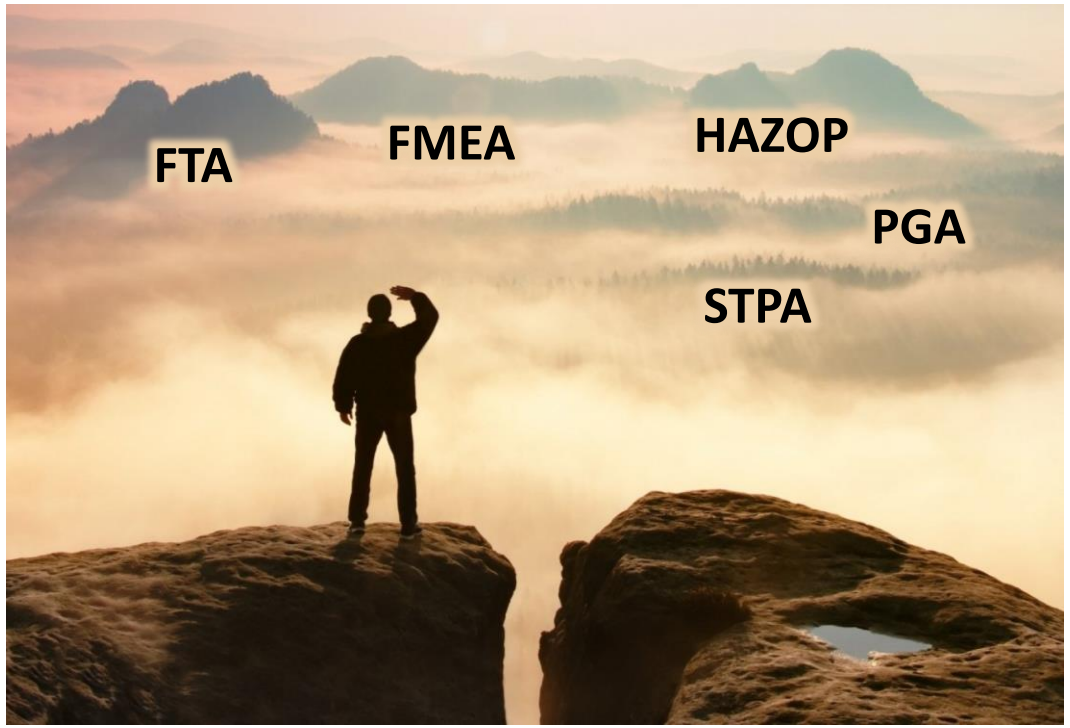
John Thomas (MIT)

Matt Gibson (EPRI)

EPRI 2011-2013: Begin exploring STPA

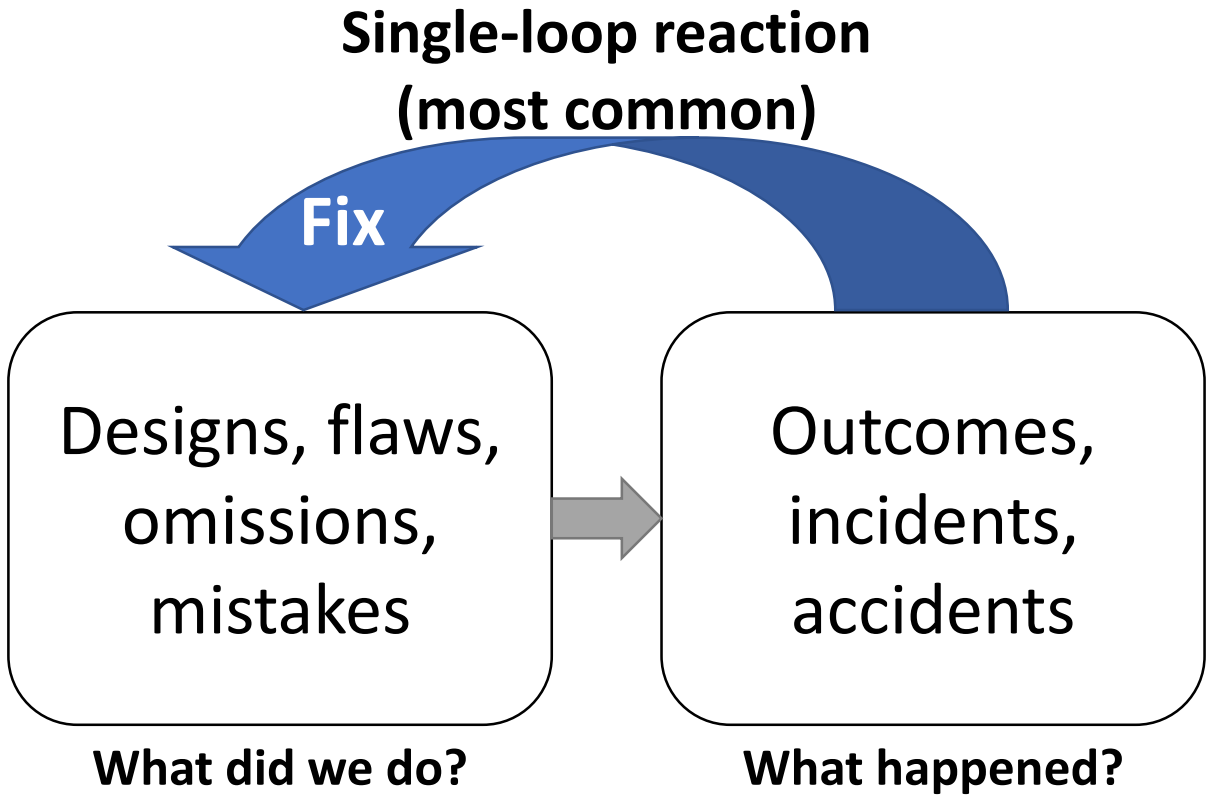
- What methods could help us do a better job preventing design flaws in digital I&C? (especially common-cause errors)
- Does STPA deserve consideration?
  - Same for FTA, HAZOP, FMEA, PGA

- Research Approach
  - Conduct blind test of STPA
  - Select a real incident (Operating Experience) caused by digital I&C
  - Select two students familiar with STPA and blind to the selected OE
  - Provide students a general description of the system as it existed before the incident
  - Compare STPA results to the actual flaws that led to OE

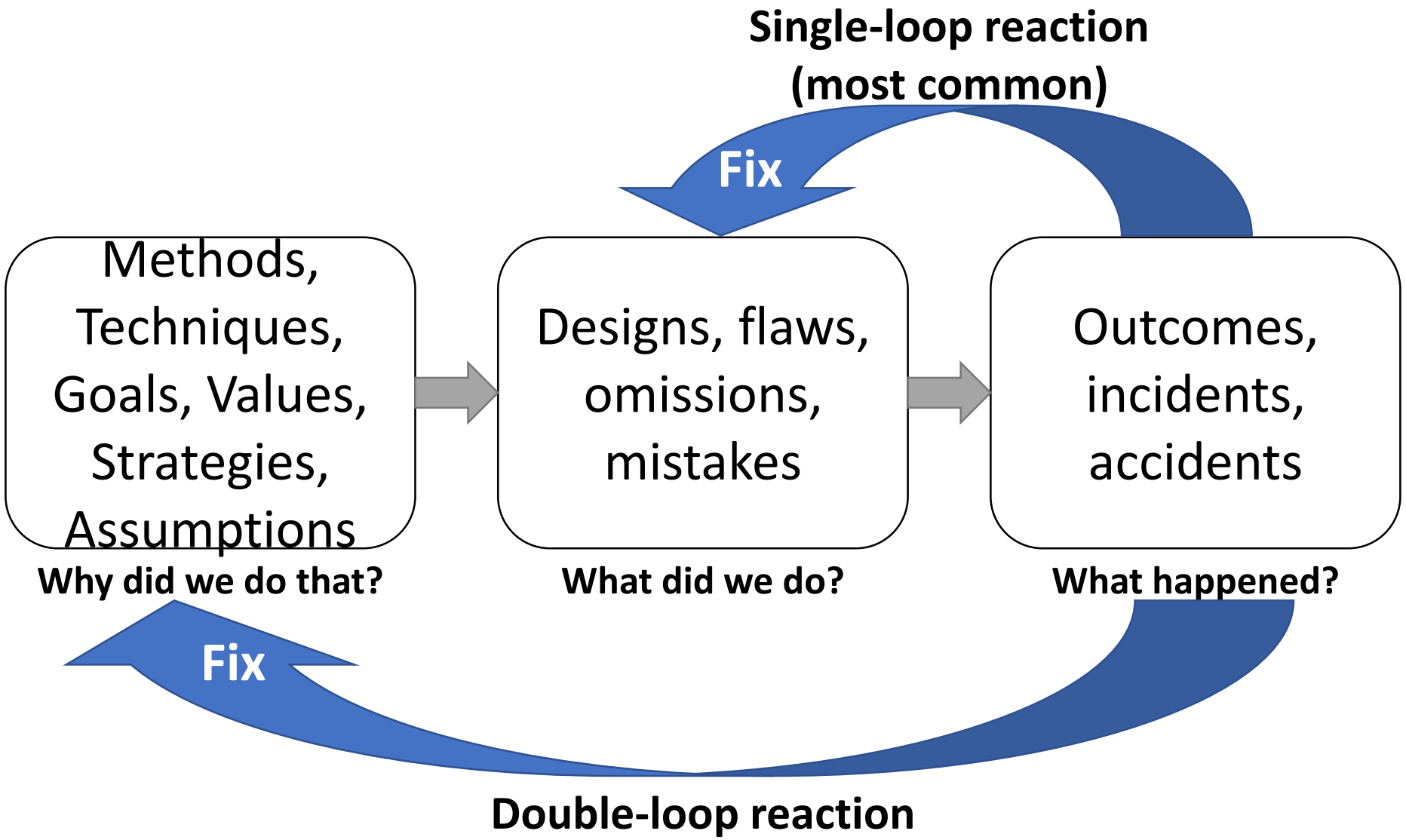


OE: Operating Experience
Digital I&C: Digital Instrumentation & Control

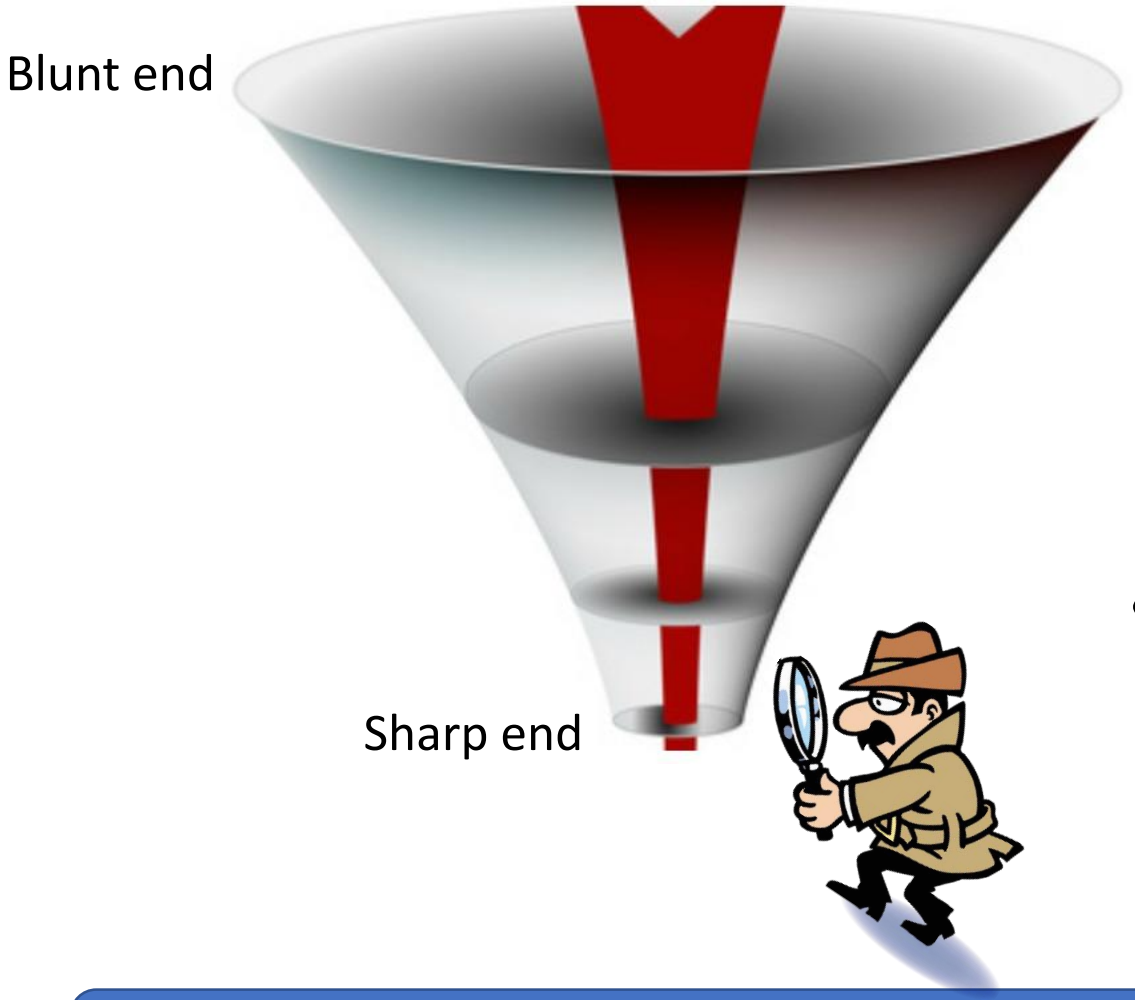
Single- vs. Double-Loop Reactions to Accidents



Single- vs. Double-Loop Reactions to Accidents



Beware of tunnel vision!

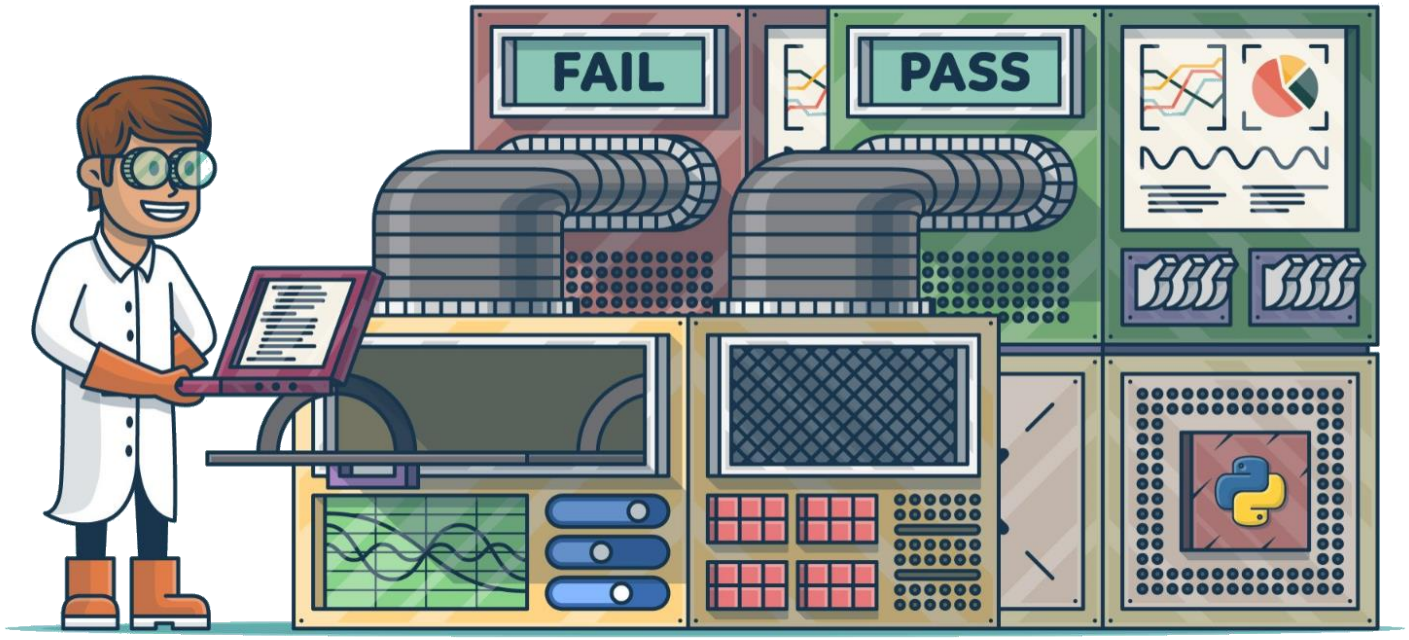


- Easy to focus on sharp-end failure

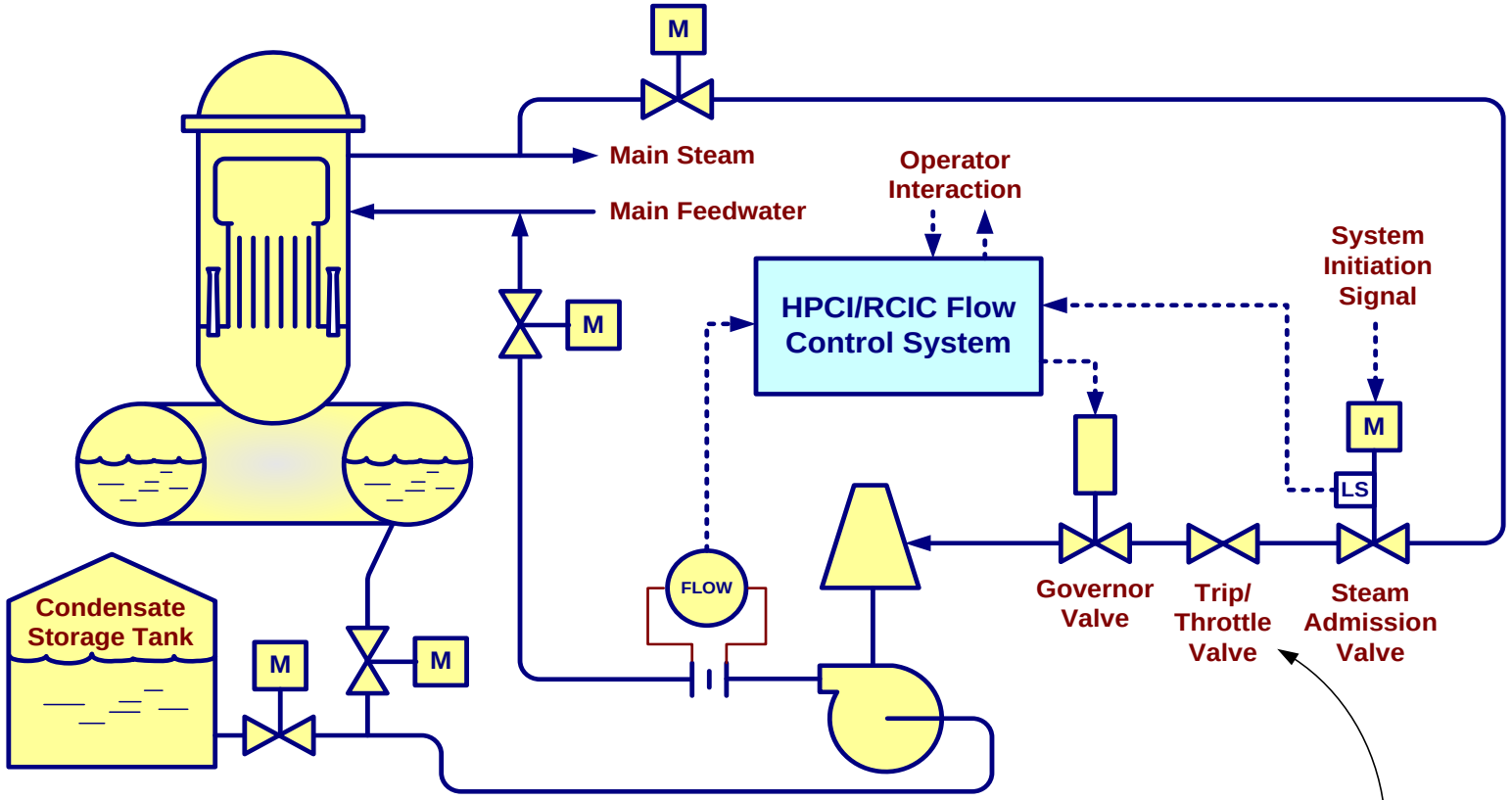
There are always deeper systemic factors!

A problem with standards

- Where is the testing and validation!
- Where is the empirical evidence that it achieves the objectives?
- Many never scientifically tested or proven!
- Don’t confuse consensus with evidence!



Nuclear HPCI Example



System Initiation Signals
(Open Steam Admission Valve & Process Valves)
1. Low Reactor Level (-48")
2. High Drywell Pressure (HPCI only; +2 psig)

System Isolation Signals
(Trip Turbine & Close Process Valves)
1. High Steam Line Flow
2. High Area Temperature
3. Low Steam Line Pressure (HPCI only)
4. Low Reactor Pressure (RCIC only)
5. Manual

Turbine Trip Signals
(Close Trip/Throttle Valve)
1. Any system isolation signal
2. High Steam Exhaust Pressure (150 psi)
3. High Reactor Level (+46")
4. Low pump suction pressure (15" Hg)
5. Turbine overspeed
6. Manual (local or remote)

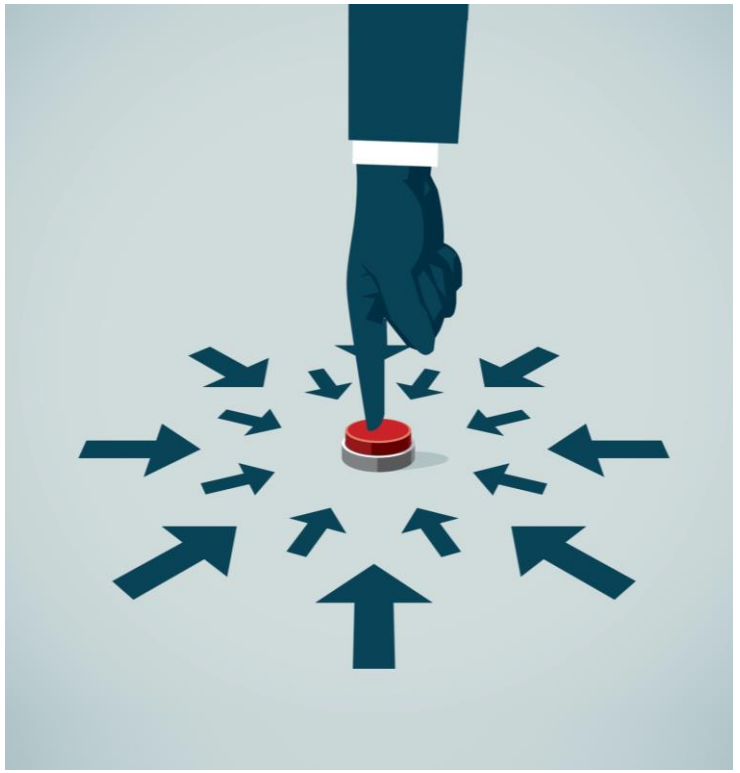
EPRI 2011-2013: Begin exploring STPA

- STPA anticipated the exact scenario and the exact flaw in a matter of days (after learning how the system worked)

- STPA also identified ~9 other important scenarios beyond the subject of the trial

2019: Industry trials

- New questions:
  - Is STPA practical?
  - Can professionals apply STPA effectively?
  - Can teams of utility engineers learn STPA and use it identify real flaws that have been overlooked with existing approaches?
  - Can STPA be applied early and quickly with limited design information?



"If you have to get a PhD to do this, it won't work!"

2019: Industry trials

- Test sites: 4 major utilities
  - Utility A
  - Utility B
  - Utility C
  - Utility D
  - [some suppliers, system integrators also invited to attend]
- Attendee backgrounds:
  - Digital I&C designers (blind)
  - PRA experts (blind)
  - Operators/supervisors (blind)
  - Observers (not blind)
- Selected 7 incidents based on OE
  - Related to digital I&C flaws that had been overlooked during design, analysis, and testing

PRA: Probabilistic Risk Assessment
Digital I&C: Digital Instrumentation & Control

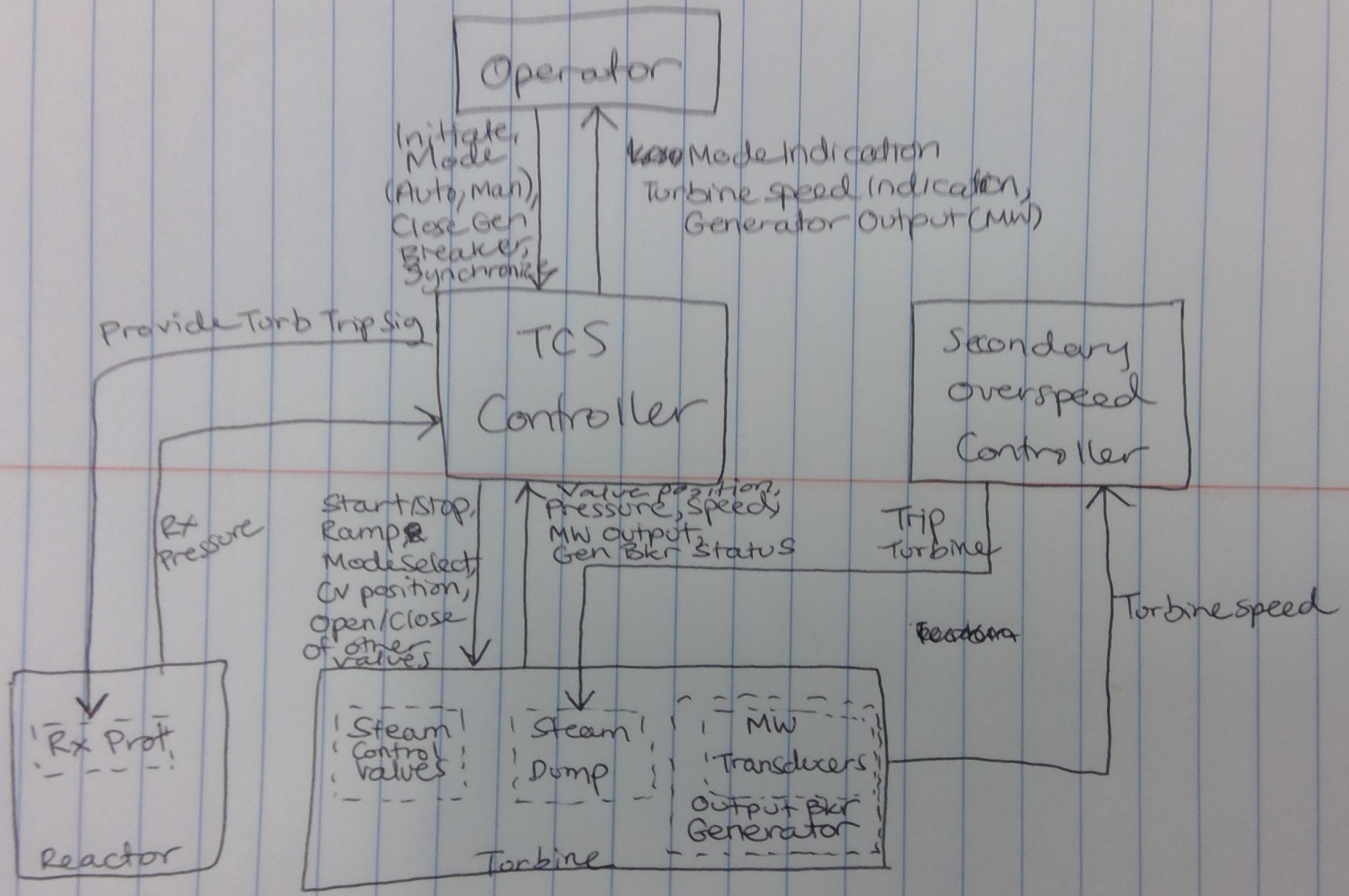
Some applications selected from real OE as test cases (flaws unknown to attendees)

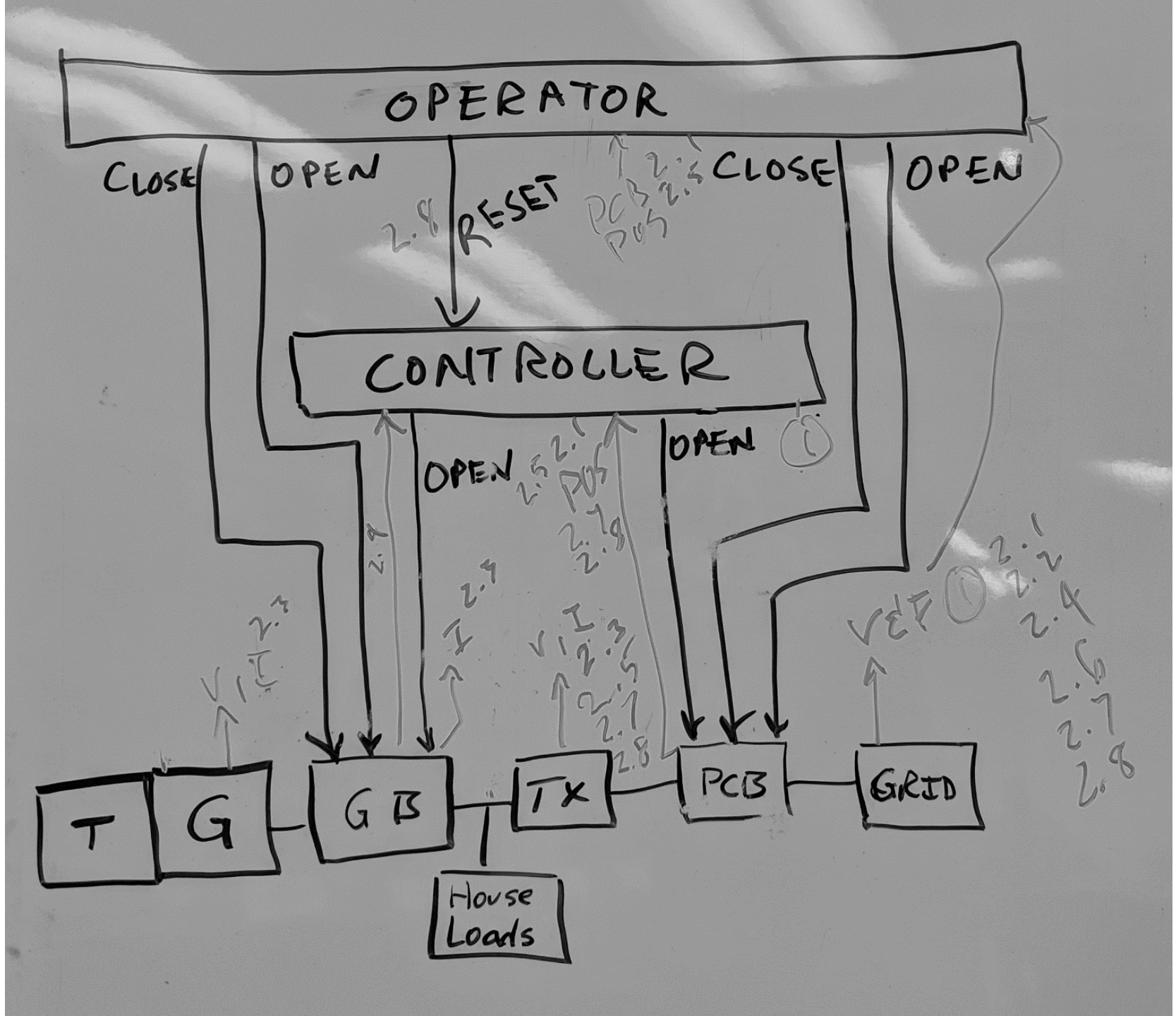
- Turbine control system
  - E.g. inadvertent turbine/reactor trip due to certain assumptions embedded in the logic
- Pressurizer control system
  - E.g. reactor trip due to combined digital I&C and operator actions
- Turbine protection system
  - E.g. inadvertent turbine/reactor trip due to new features in a digital upgrade
- Main power system & protective relays
  - E.g. unintended loss of offsite and generated power due to digital I&C actions in an unanticipated scenario
- High Pressure Coolant Injection
  - E.g., inadvertent loss of HPCI due to design of protective logic
- Rod control system
- Simple time-delay relay

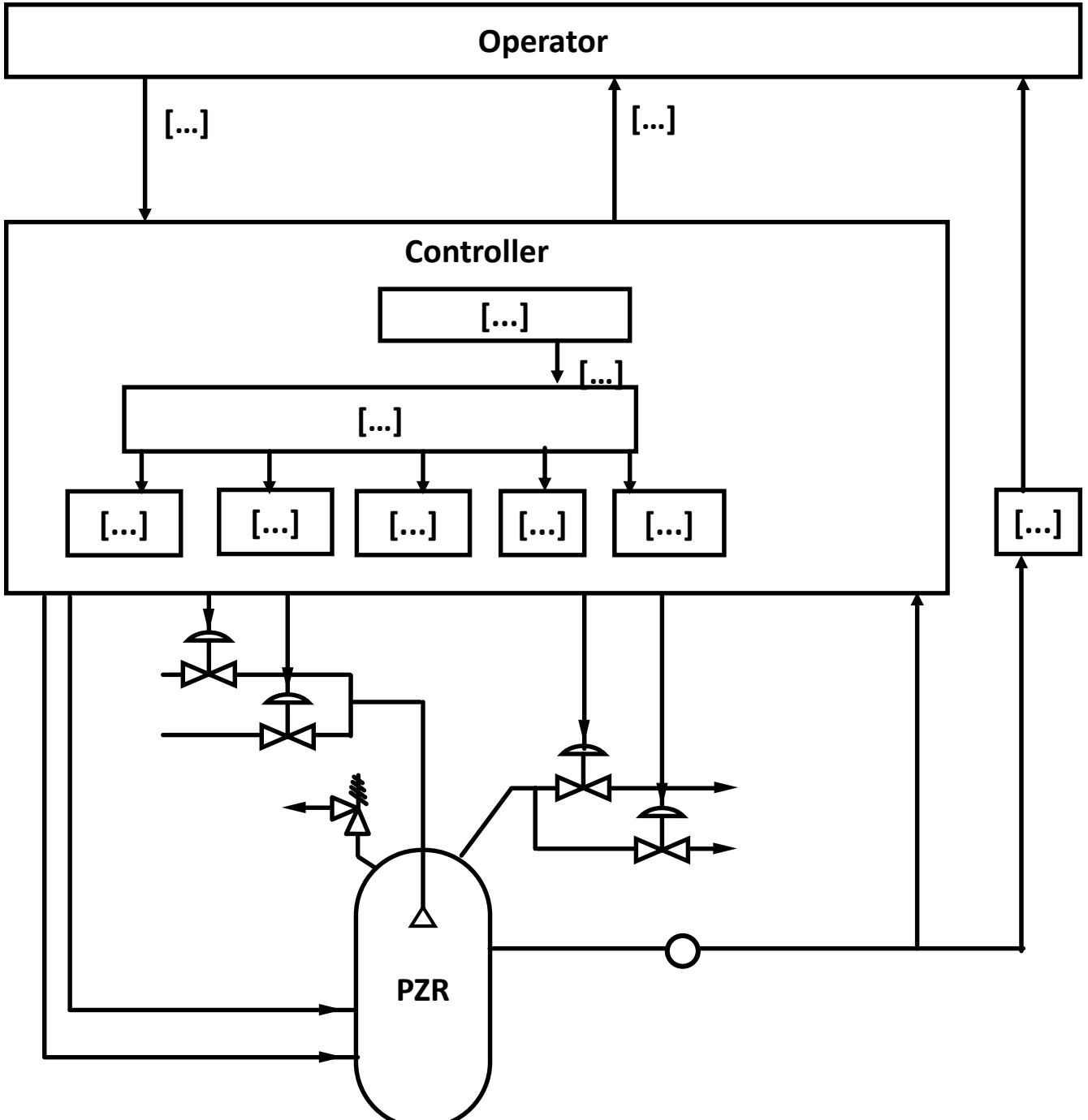
Practically all of these include common-cause issues
Practically all were introduced during a digital mod/upgrade

Selecting applications for each test site

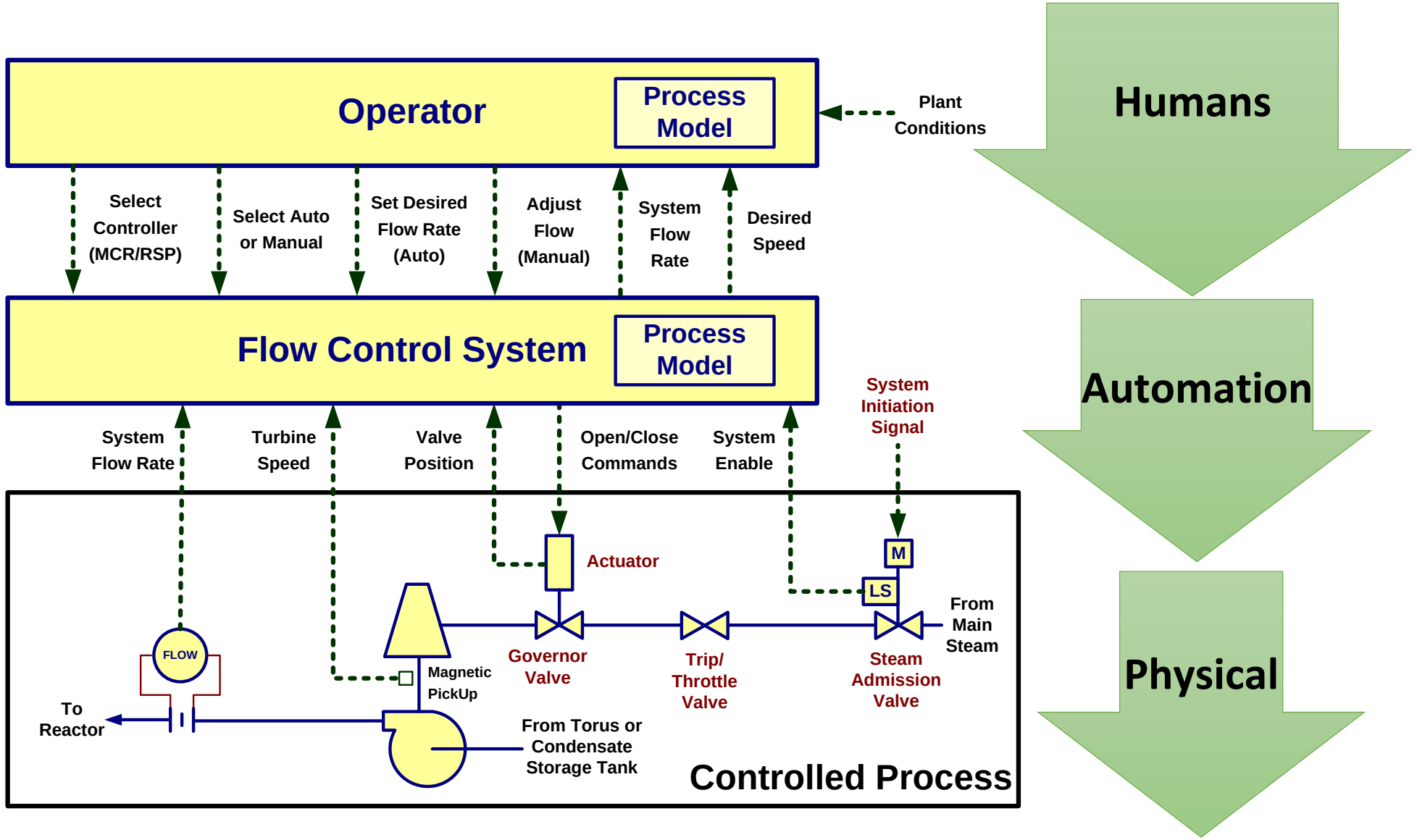
- Each company asked to analyze ~2-4 applications
- Choice: Use a specific design from their own company or a similar design from another company?
  - Answer: Do both!
- Attendees pre-screened for any knowledge of the selected incident or flaw
  - Participants must not have pre-existing knowledge of the incident/flaws
  - Observers allowed to have pre-existing knowledge, but cannot participate


Operator
Initiate, Mode (Auto, Man), Close Gen Breaker, Synchronize
Mode Indication
Turbine speed indication,
Generator Output (MW)
Provide Turb Trip Sig
TCS Controller
Secondary Overspeed Controller
Rx Pressure
Start/Stop, Ramp, Mode Select, CV position, Open/Close of other valves
Valve position, Pressure, Speed, MW output, Gen Bkr Status
Trip Turbine
Turbine speed
Rx Prot
Reactor
Steam Control Valves
Steam Dump
MW Transducers
Output Bkr Generator
Turbine


OPERATOR
CLOSE
OPEN
RESET
CLOSE
OPEN
CONTROLLER
OPEN
OPEN
T
G
GB
TX
PCB
GRID
House Loads

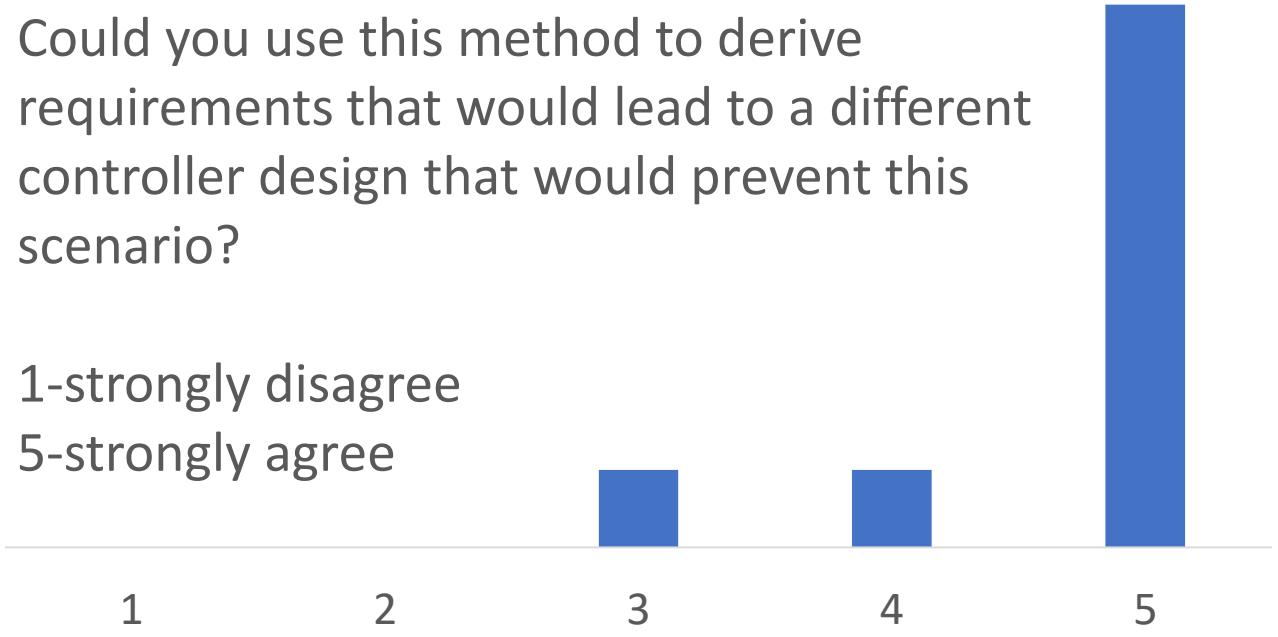

Operator
[...]
[...]
Controller
[...]
[...]
[...]
[...]
[...]
[...]
[...]
[...]
[...]
PZR

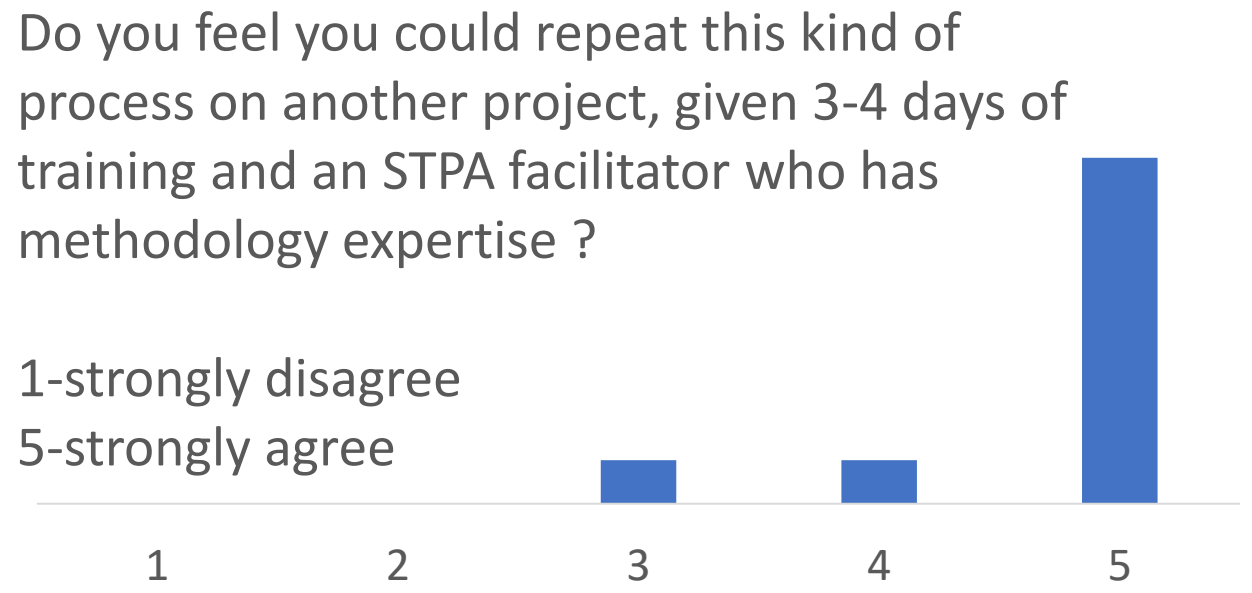
STPA Control Structure (simplified)



Feedback and Surveys

- “The STPA control structure UCAs, requirements, step 4, that piece makes complete sense.“
- “This is mind-blowing process, much better than what we do now.”
- “An hour spent on this is much more beneficial than an hour spent on RTM (requirements traceability matrix), where you are just hunting through 100s of detailed pages/requirements without much structure.”





Conclusions

- 2013: STPA does find the overlooked digital I&C and common-cause issues!
- 2019: Professional engineers can use STPA!

Future work: 2020 and beyond

- More workshops at 3 utilities, followed by more validation workshops
- Focus on integration of STPA outputs into downstream processes (e.g. HAZCADS Part 2, DRAM, TAM, etc)