Massachusetts Institute of Technology

# Digital I&C
# Lessons learned across industries

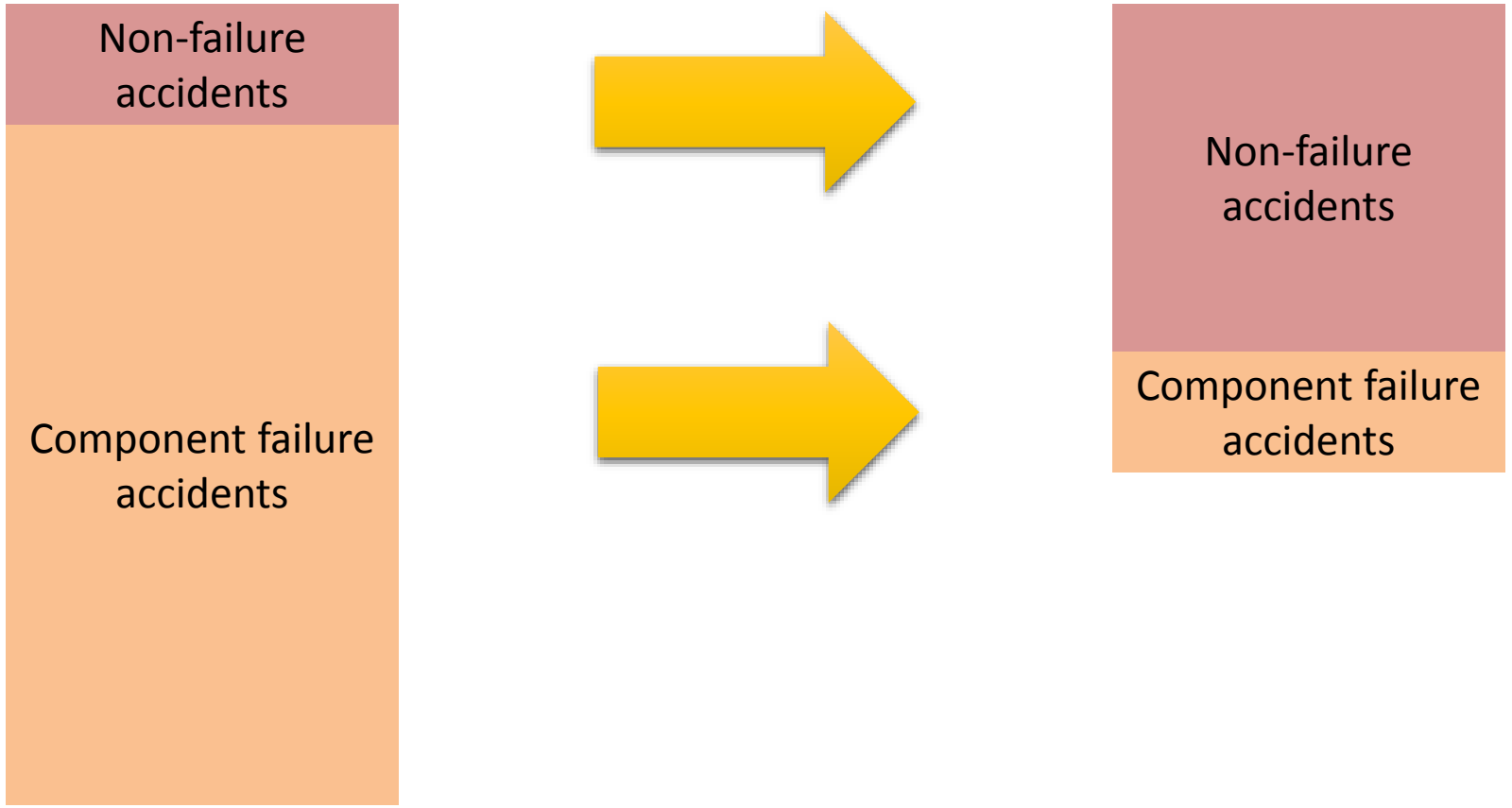
Dr. John Thomas

MIT

## Experiences across industries

(Automotive, Aviation, Space Systems, Chemical, Oil & Gas, Nuclear Power, Defense, Healthcare, Medical Devices, Weapon Systems, etc.)

# Accidents causes are changing



# Barrier: requirements

- "The hardest single part of building a software system is **deciding precisely what to build**."
  -- Fred Brooks, *The Mythical Man-Month*

- Most software-related accidents have been traced to flaws in the **requirements**
  (Leveson, 2004) (Endres et al., 2003)(Lutz et al., 1993)

- *"As is well known to software engineers, by far the largest class of problems arises from errors made in the eliciting, recording, and analysis of **requirements**"*
  (Jackson et al., 2007)

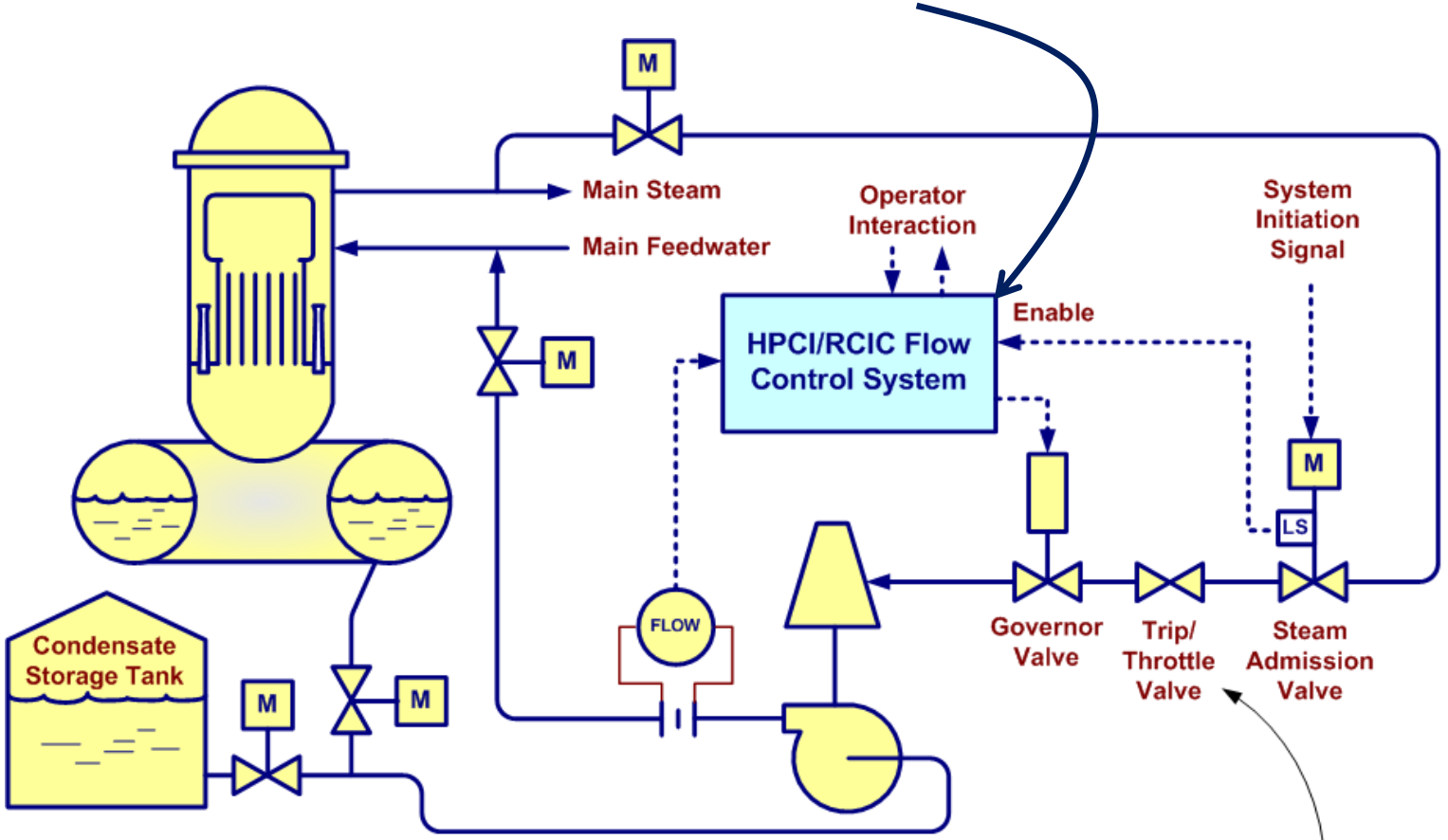
# Insight from Automotive

- “In my experience the **requirements** are much more important than preventing hardware failures. recalls are rarely due to component failures, typically it’s due to missed requirements, requirements never verified, or missed interaction with supplier.”
  - Joseph Miller

# Common pitfalls/mistakes in analysis

4. Incorrect understanding of system architecture → incorrect model of system failures and failure behaviors
5. **Paying more attention to crunching probabilities than to the physics of the problem.**
6. Analyst works alone; no independent validation/verification

# HPCI Flow Control System

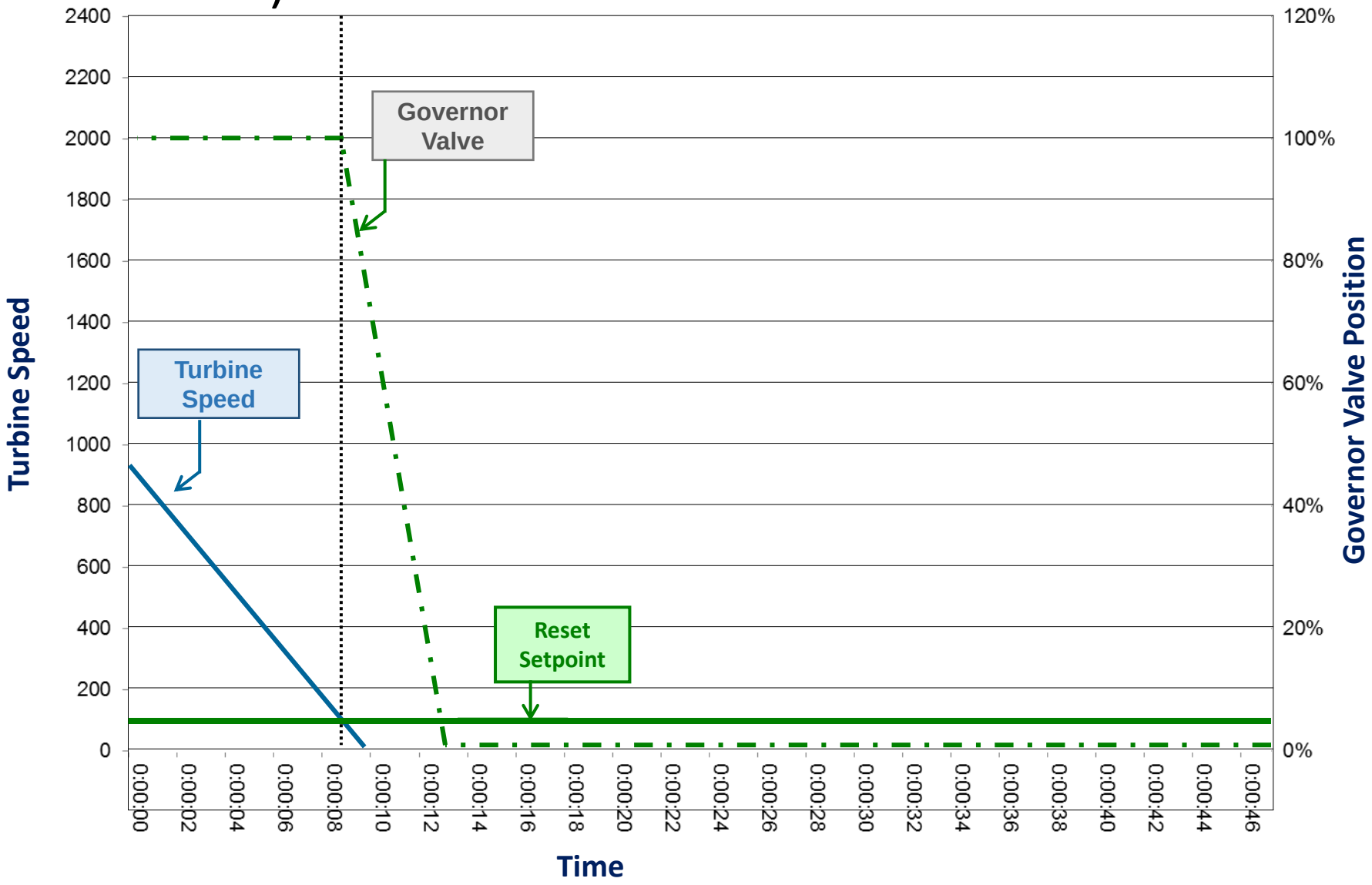



**System Initiation Signals**
(Open Steam Admission Valve & Process Valves)
1. Low Reactor Level (-48")
2. High Drywell Pressure (HPCI only; +2 psig)

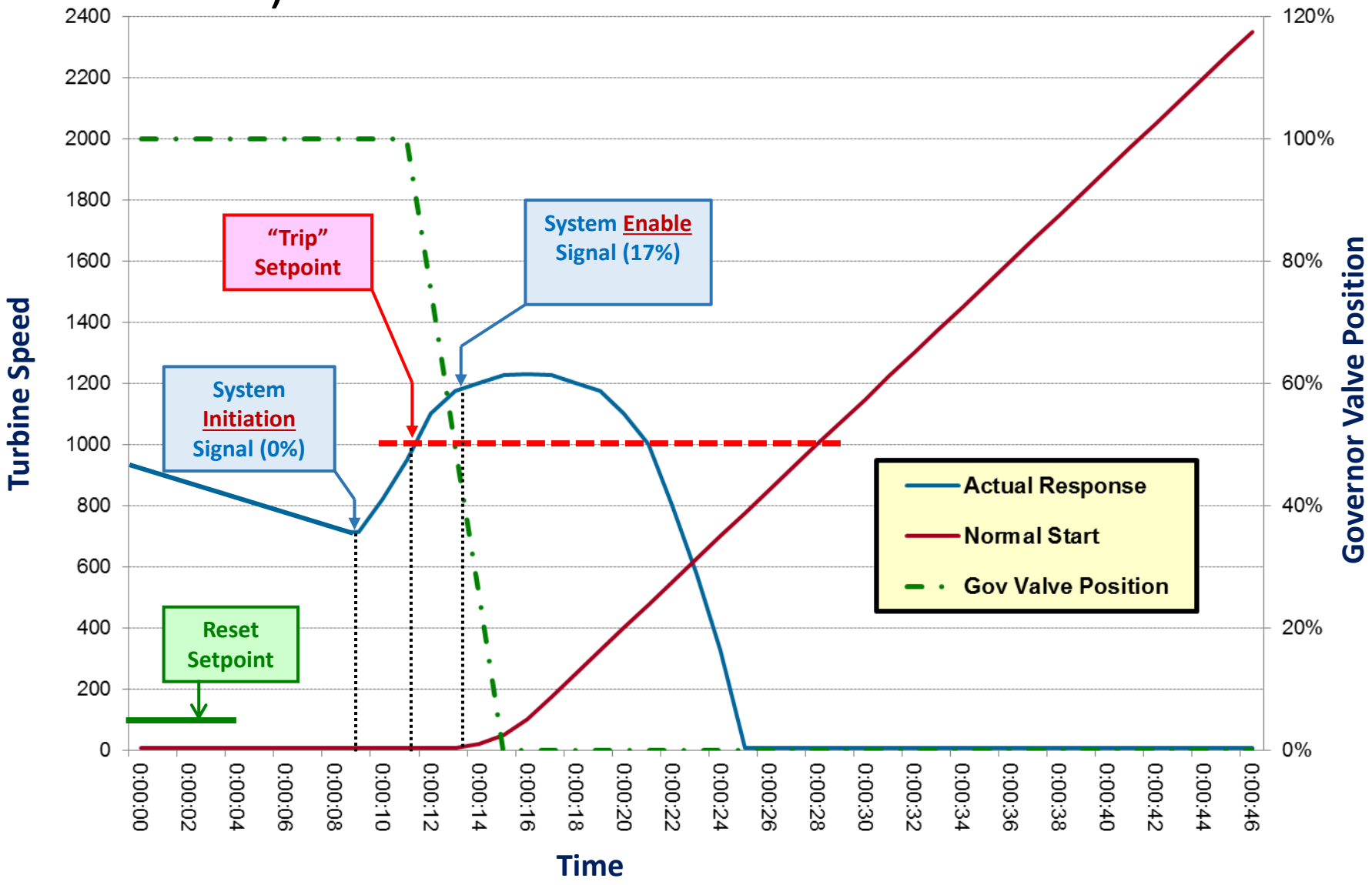
**System Isolation Signals**
(Trip Turbine & Close Process Valves)
1. High Steam Line Flow
2. High Area Temperature
3. Low Steam Line Pressure (HPCI only)
4. Low Reactor Pressure (RCIC only)
5. Manual

**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)

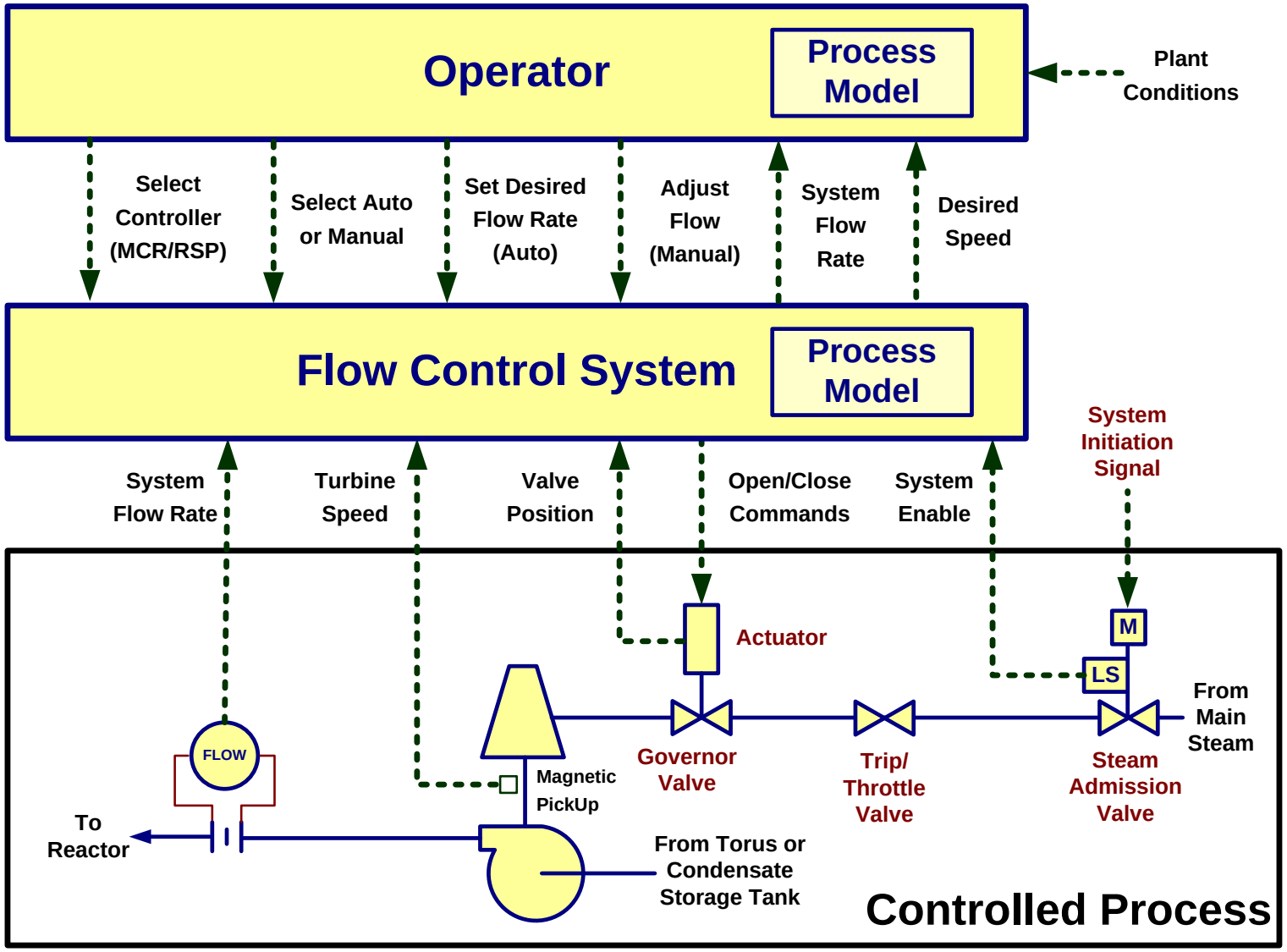
# Operating Experience (No Component Failures)



# Operating Experience (No Component Failures)



# Blind test of STPA



# Blind test: STPA identified the problem

| |
|---|
| **Hazard: Equipment Operated Beyond Limits (H3)** |
| **Controller: HPCI-RCIC Flow Control System** |
| **Hazardous Control Action No. 2: "Increase governor valve position" command is <u>provided</u> when: there is an accident and turbine speed is too high, regardless of system flow** |
| |
| **Inadequate, Missing or Delayed Feedback** |
| **Enable signal sent to controller before there is a valid demand on HPCI/RCIC** |
| **enable provided when steam admission valve is not open (broken or misaligned LS)** |
| **steam admission valve commanded open when there is no demand on HPCI/RCIC (spurious ESFAS signal)** |
| **Enable signal sent to controller when there is a demand on HPCI/RCIC, but delayed** |
| **enable provided when steam admission valve is opened, but too late (misaligned LS or LS setpoint too high)** |
| **Steam admission valve opens too slowly when commanded by ESFAS Initiation Signal (excessive stem thrust)** |
| **steam admission valve commanded open too late when there is a demand on HPCI/RCIC (ESFAS delay)** |
| **HPCI/RCIC pump flow rate signal to controller is missing, delayed, incorrect, too infrequent, or has inadequate resolution** |
| **Signal corrupted during transmission** |
| **sensor failure** |
| **sensor design flaw** |
| **sensor operates correctly but actual flow rate is outside sensor's operating range** |
| **fluid type is not as expected (water vs. steam?)** |
| **Governor valve position signal to controller is missing, delayed, incorrect, too infrequent, or has inadequate resolution** |
| **Problems with communication path** |
| **actual position is beyond sensor's range** |
| **sensor reports actuator position and it doesn't match valve position** |
| **sensor correctly reports valve position but position doesn't match assumed area/shape** |

# Industry standards to solve this problem

- ISO/PAS 21448: Safety of the Intended Functionality (SOTIF)
  - STPA used assess safety of digital systems
- ASTM WK60748
  - “Standard Guide for Application of STPA to Aircraft”
- SAE AIR6913
  - “Using STPA during Development and Safety Assessment of Civil Aircraft”
- RTCA DO-356A
  - “Airworthiness Security Methods and Considerations”
  - STPA-sec used for cybersecurity of digital systems
- SAE JXXXX
  - “Recommended Practice for STPA in Automotive Safety Critical Systems”

(Last Slide)