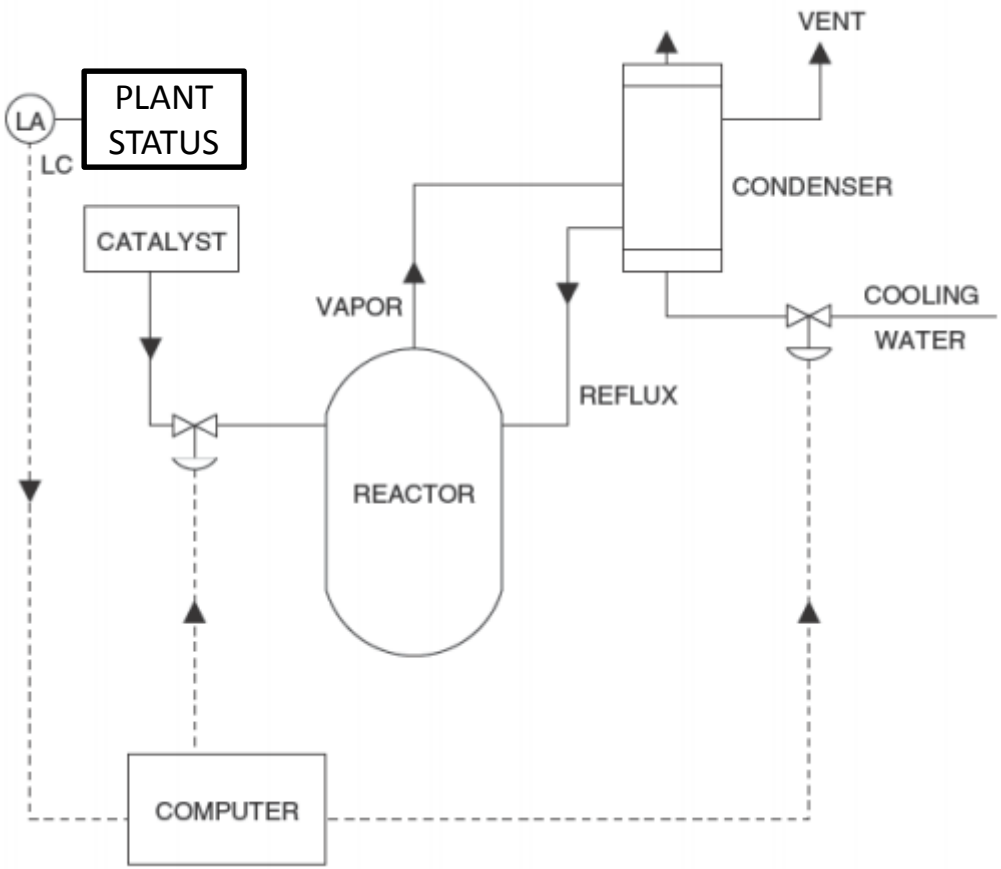
# STAMP/STPA
# Intermediate Tutorial
## Guided Exercise:
## Applying STPA to a real system

Dr. John Thomas
System Engineering Research Laboratory
Massachusetts Institute of Technology

# Chemical Reactor Design

- Toxic catalyst flows into reactor
- Chemical reaction creates heat, pressure
- Water and condenser provide cooling



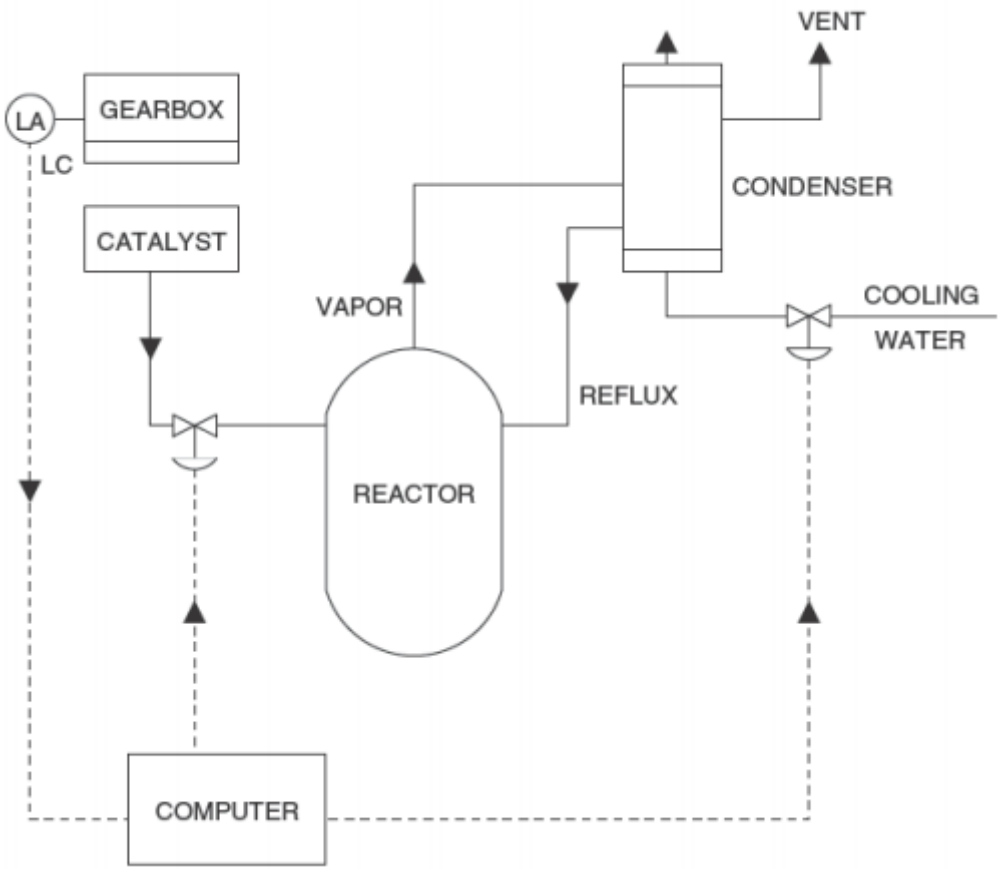

**What are the system losses and system hazards?**

©

# Chemical Reactor Design

- A-1: People die from toxic chemical exposure
- A-2: Economic loss

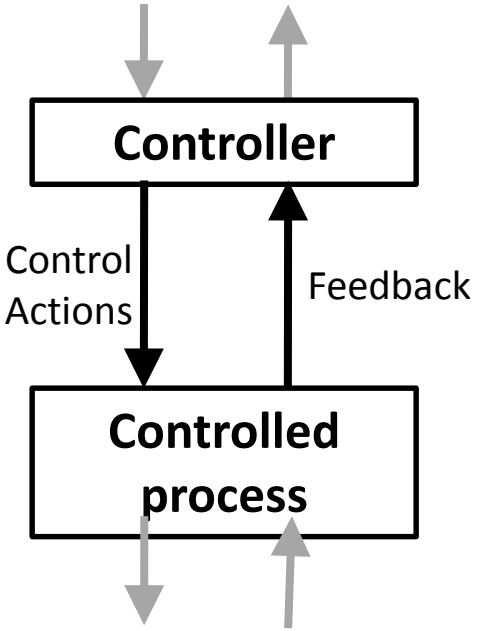
- H-1: Toxic chemical is released
- H-2: Unable to produce chemical X




©

# STPA
# (System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios



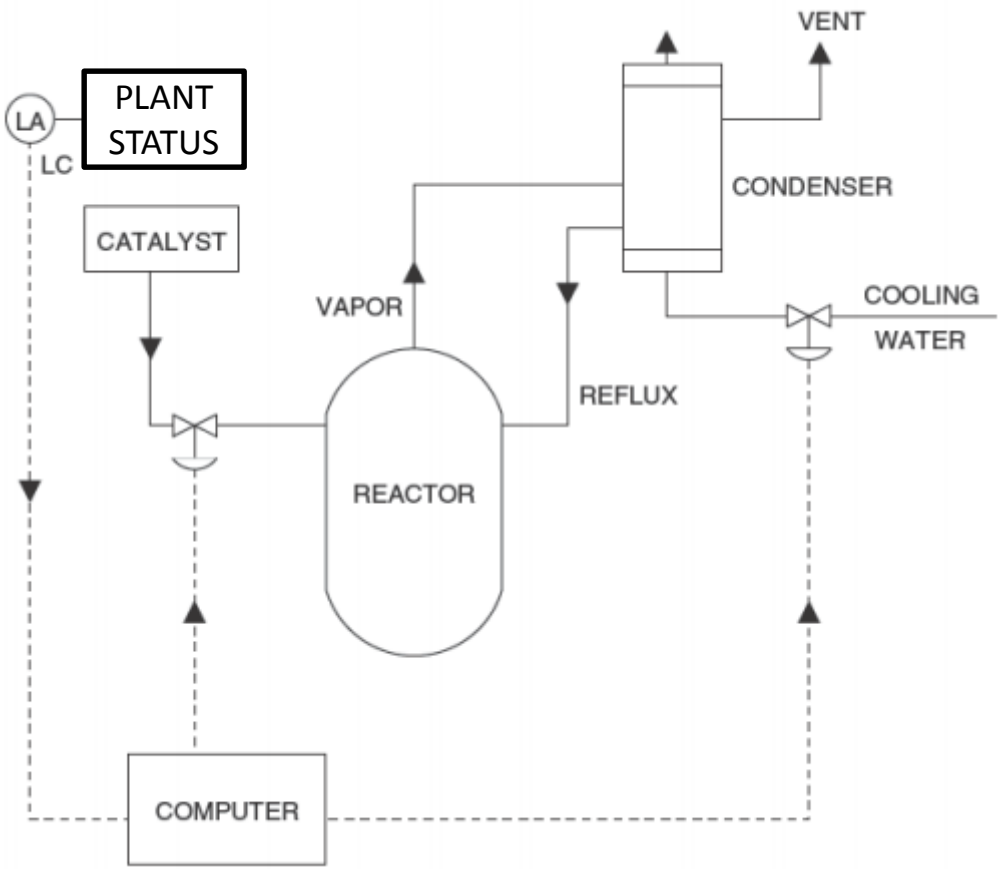

(Leveson, 2012)



©

# Chemical Reactor Design

- Toxic catalyst flows into reactor
- Chemical reaction creates heat, pressure
- Water and condenser provide cooling

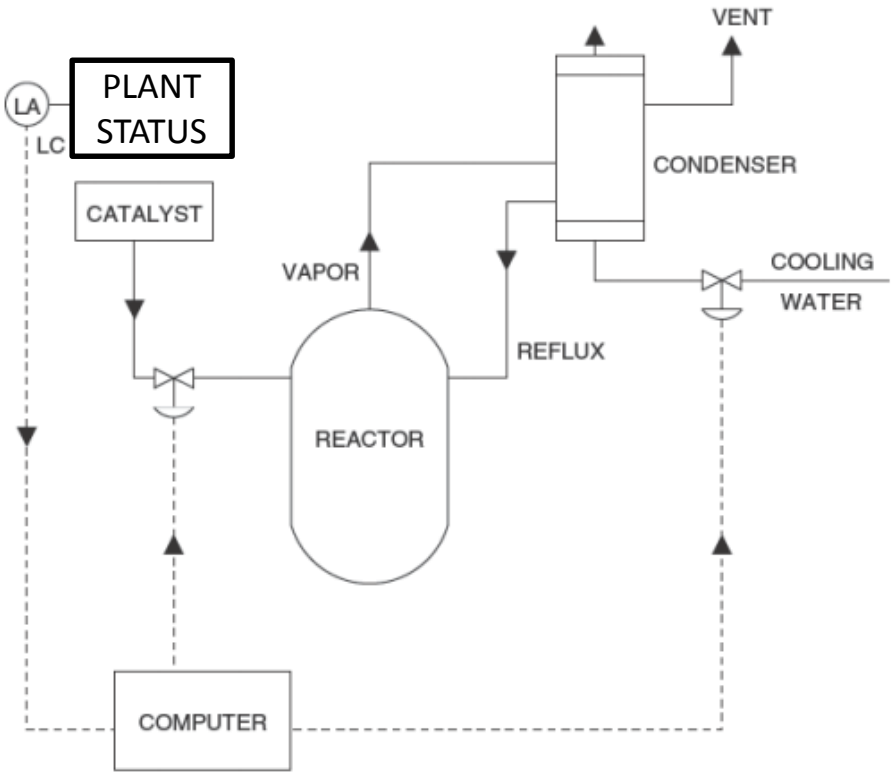


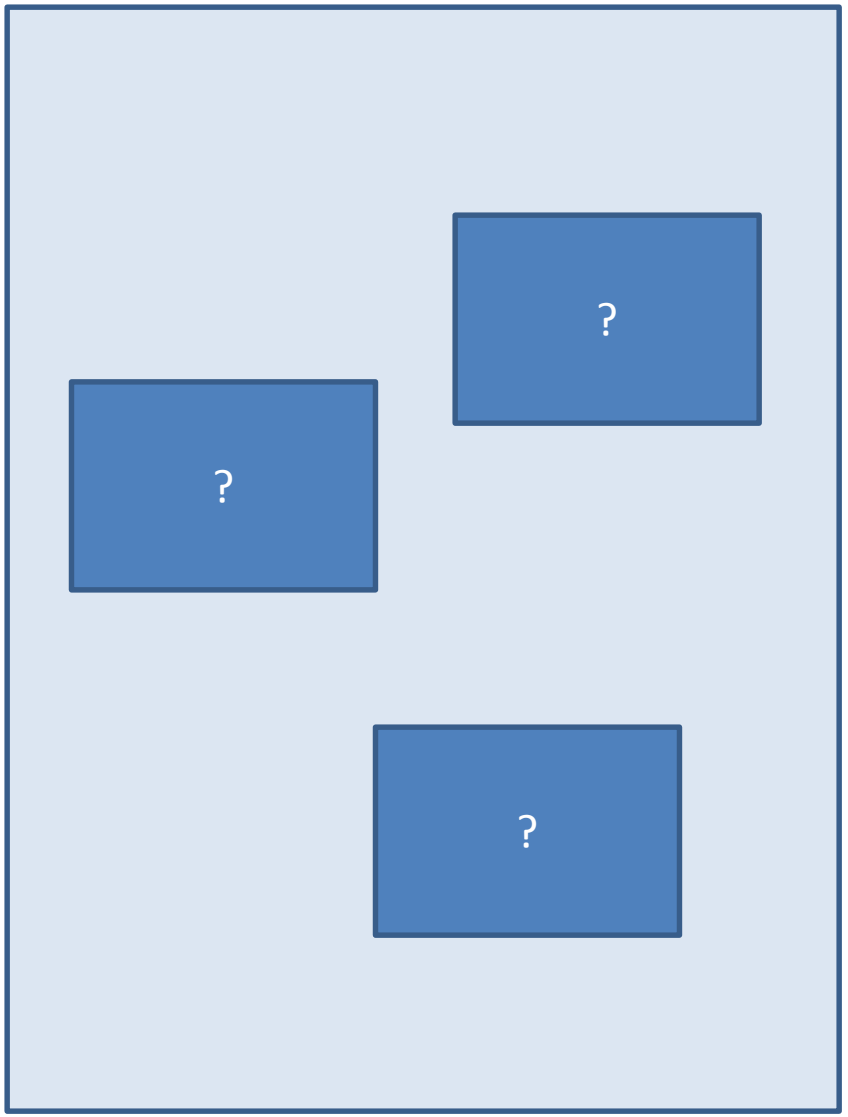

**Create Control Structure**

©

# STPA Analysis

- High-level (simple) Control Structure
  - What are the main parts?

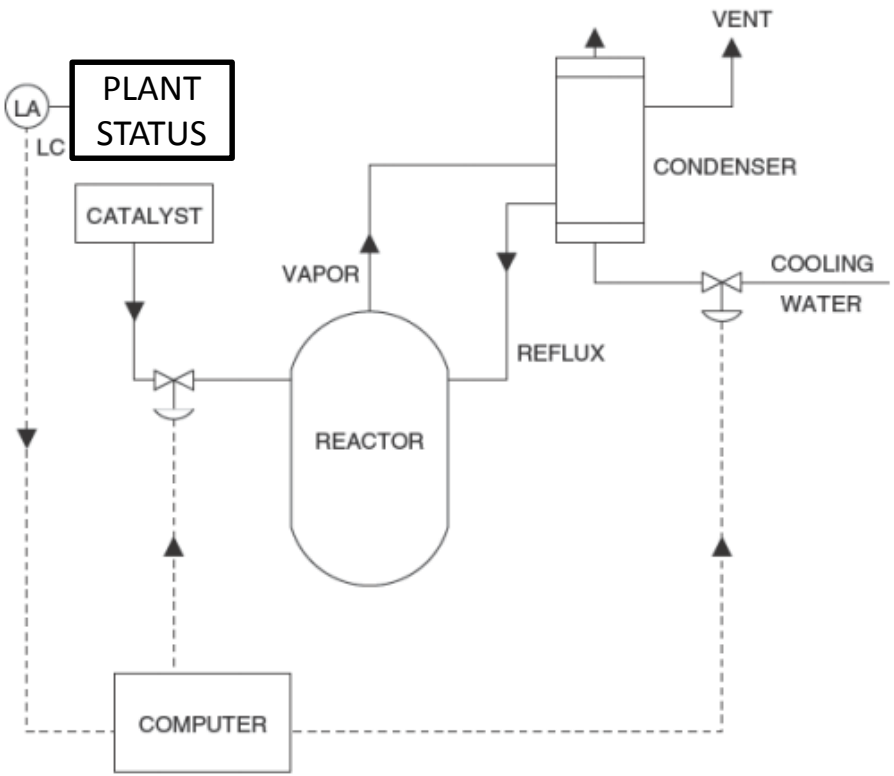


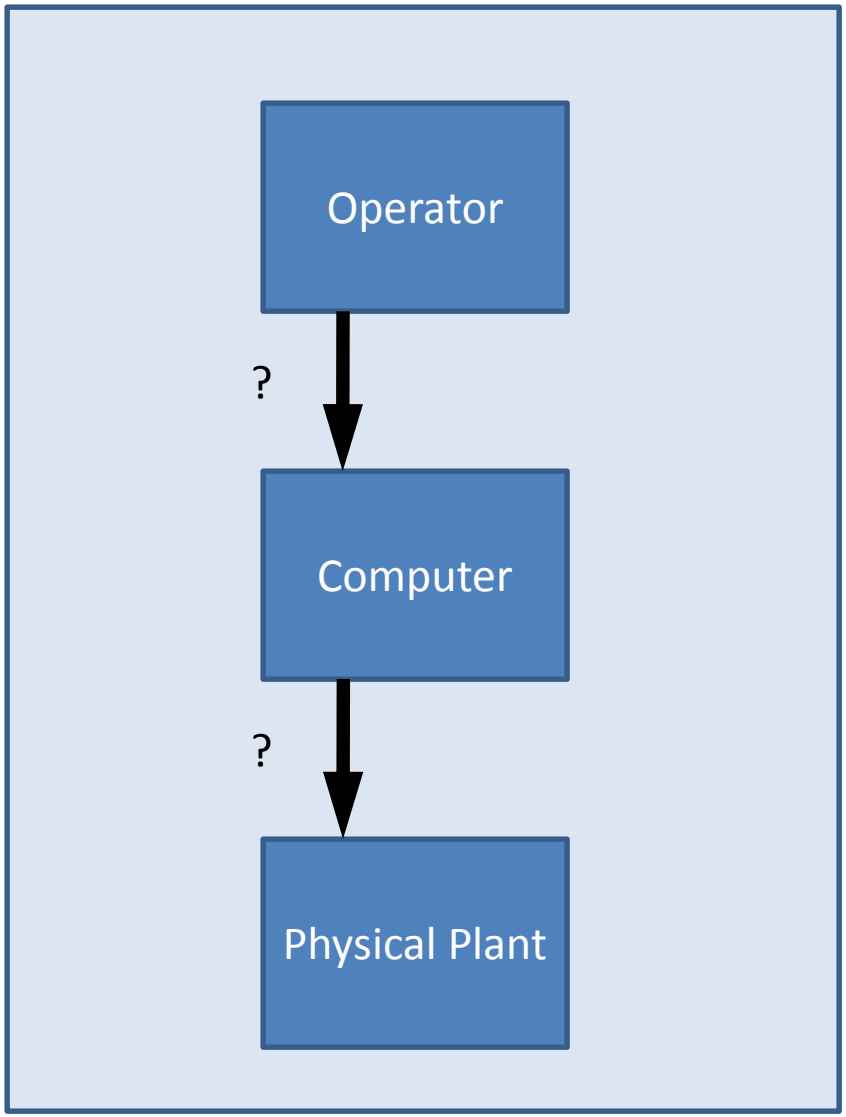




©

# STPA Analysis

- High-level (simple) Control Structure
  - What commands are sent?

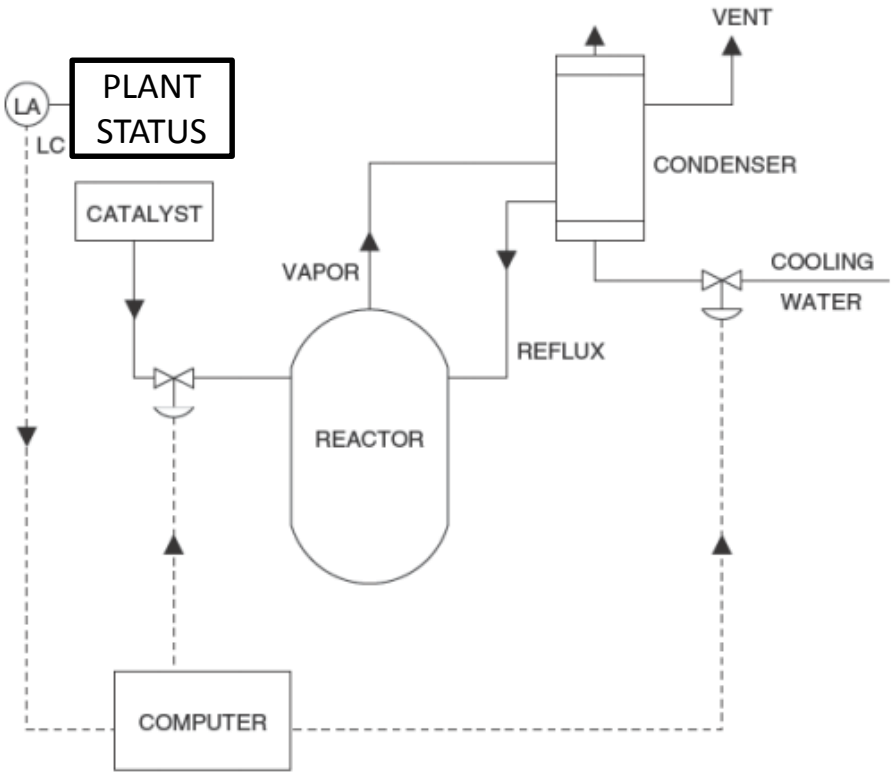


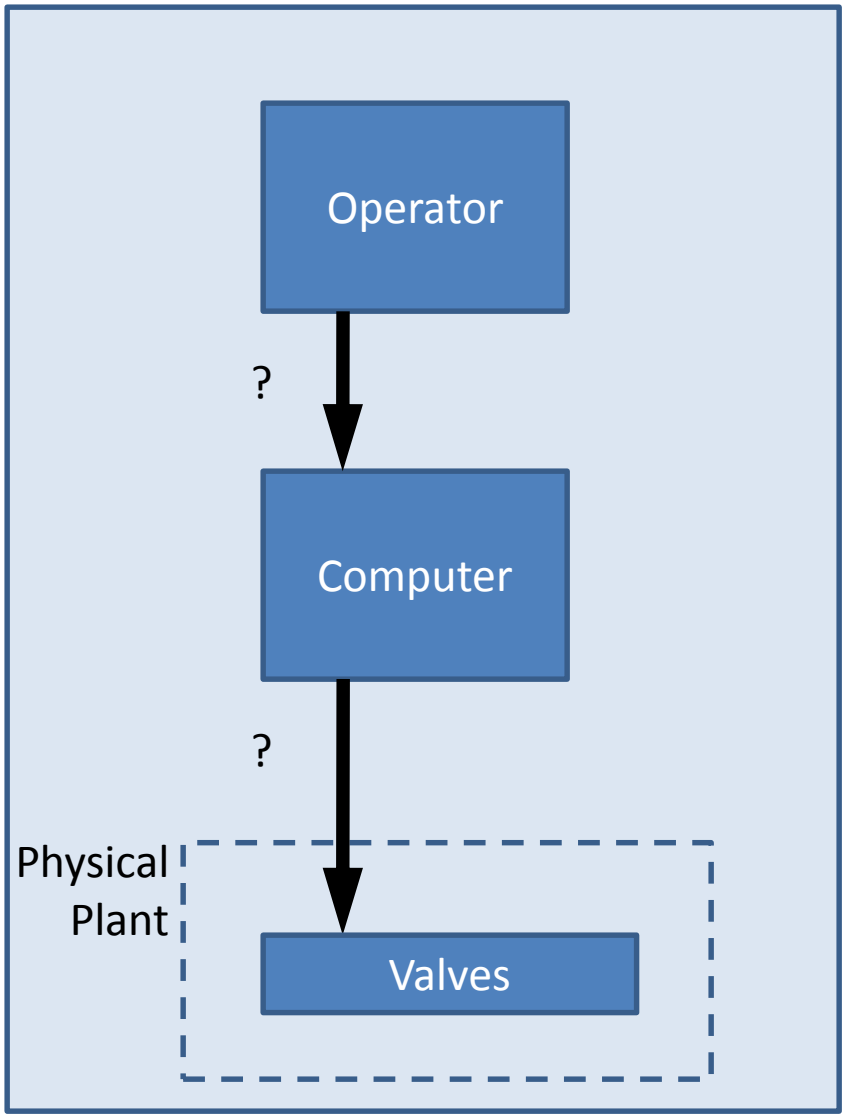




©

# STPA Analysis

- High-level (simple) Control Structure
  - What commands are sent?

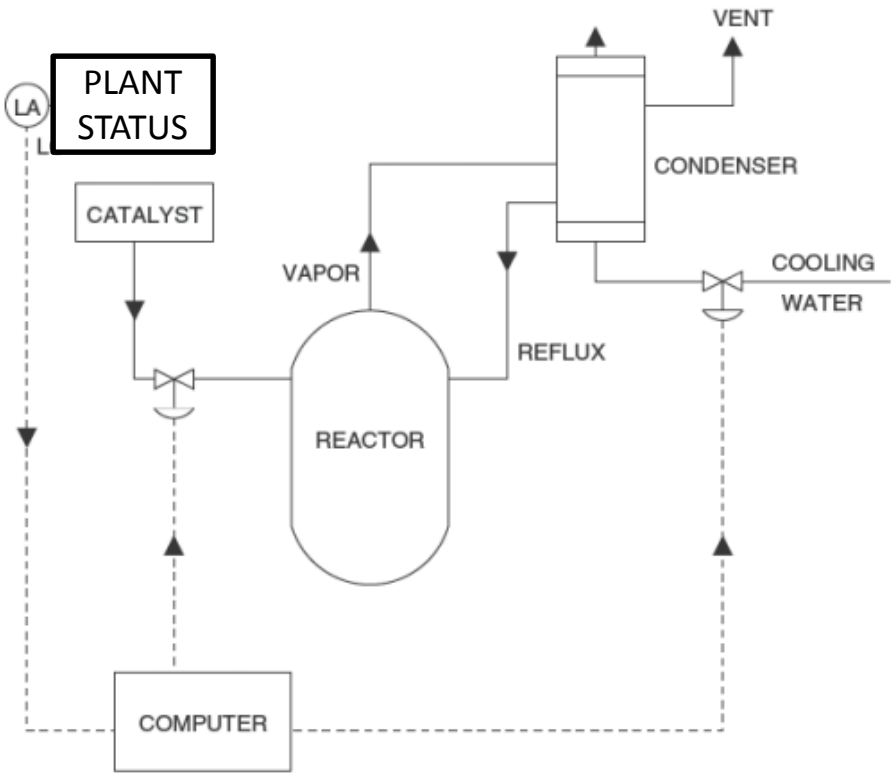


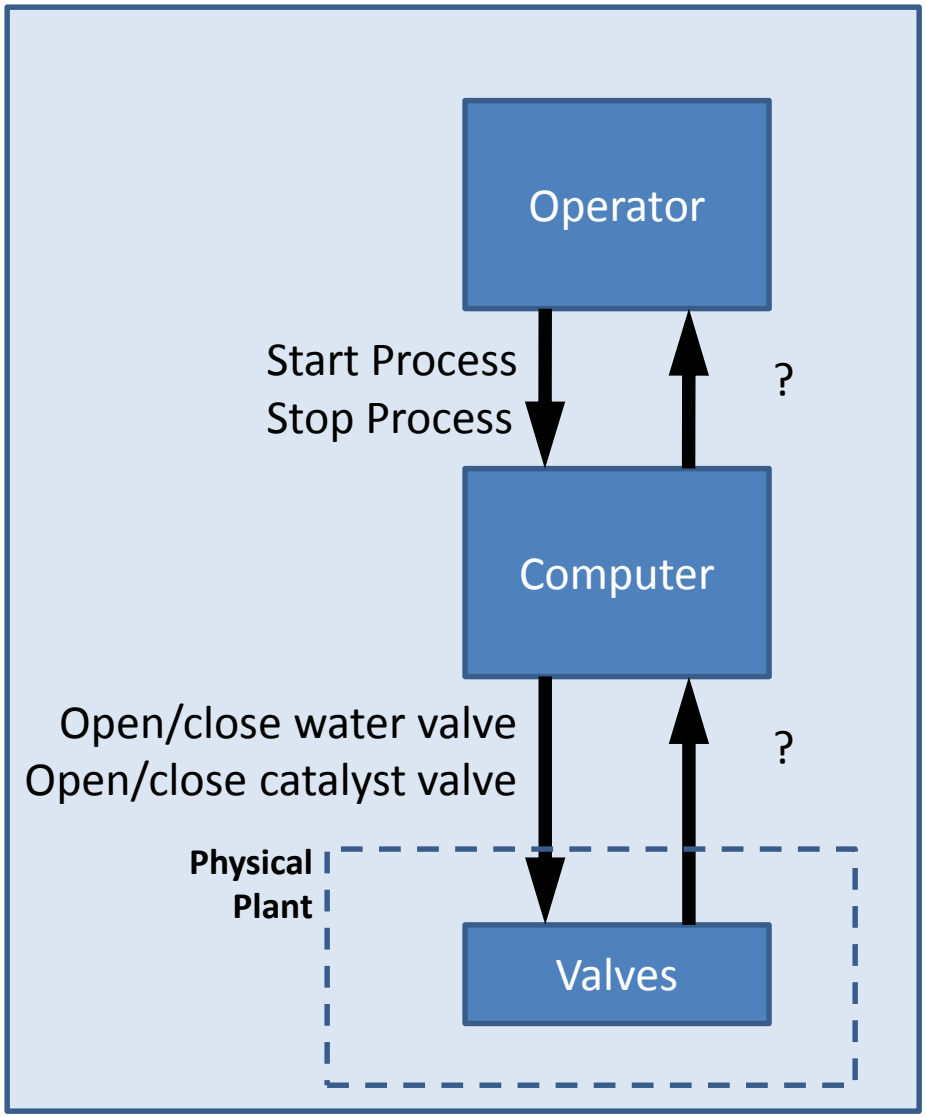




©

# STPA Analysis

- High-level (simple) Control Structure
  - What feedback is sent?

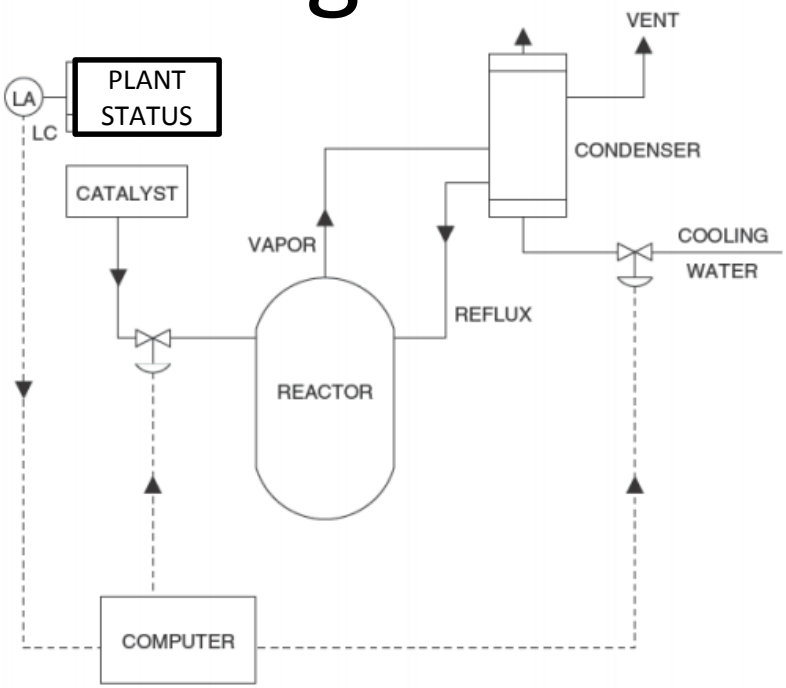


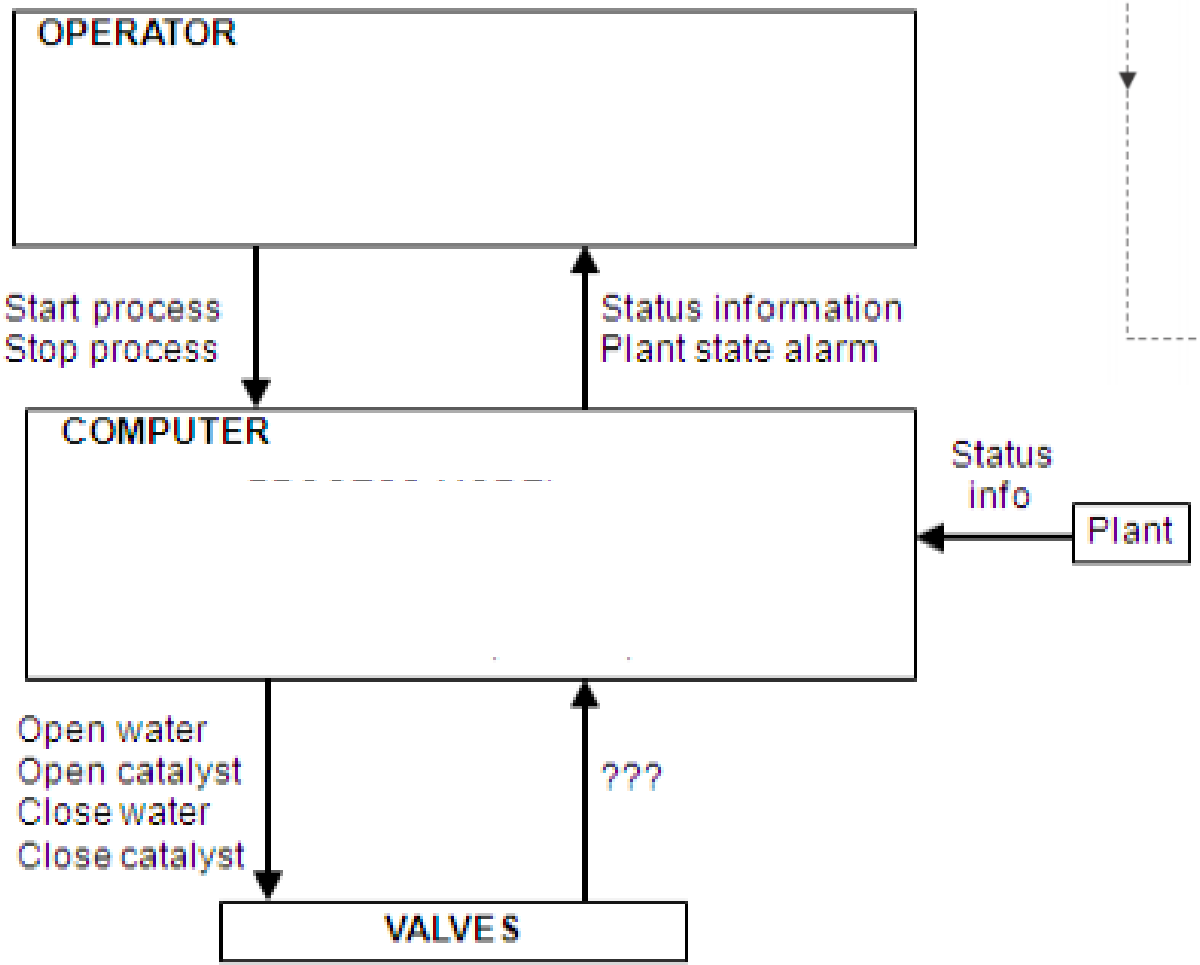




©

# Chemical Reactor Design

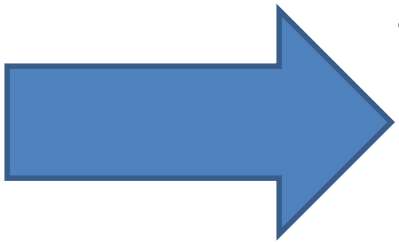
## Control Structure:



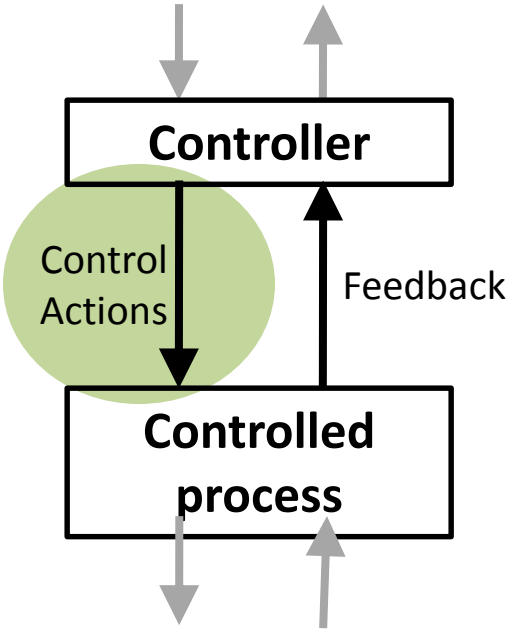




©

# STPA
# (System-Theoretic Process Analysis)



- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios



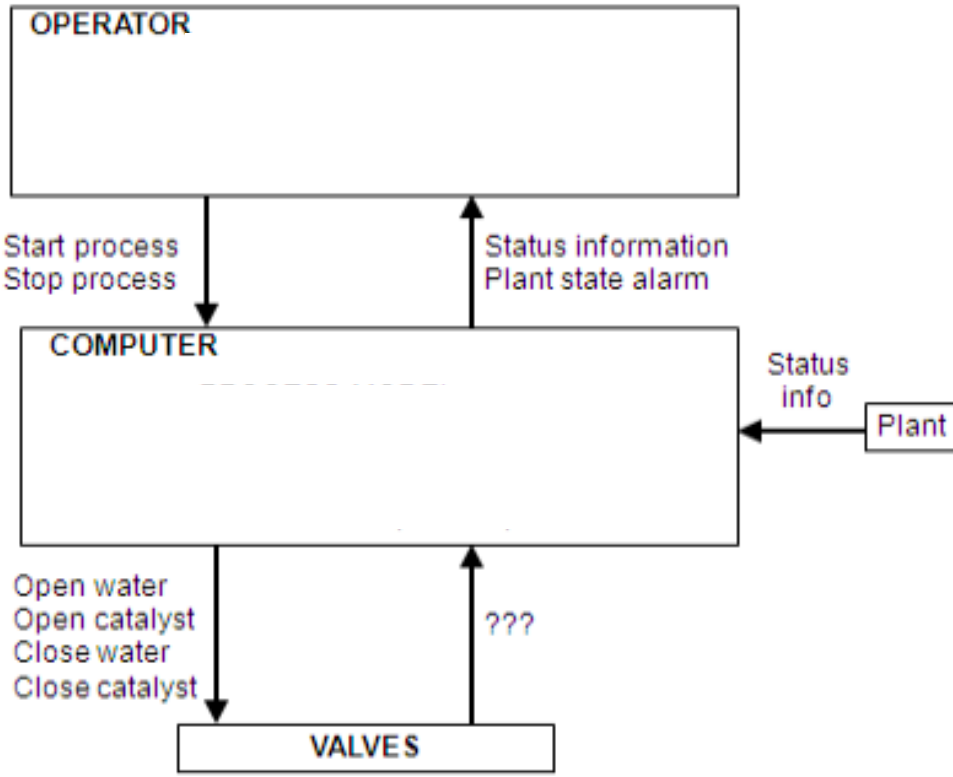

(Leveson, 2012)



©

# Chemical Reactor: Unsafe Control Actions

## Control Structure:

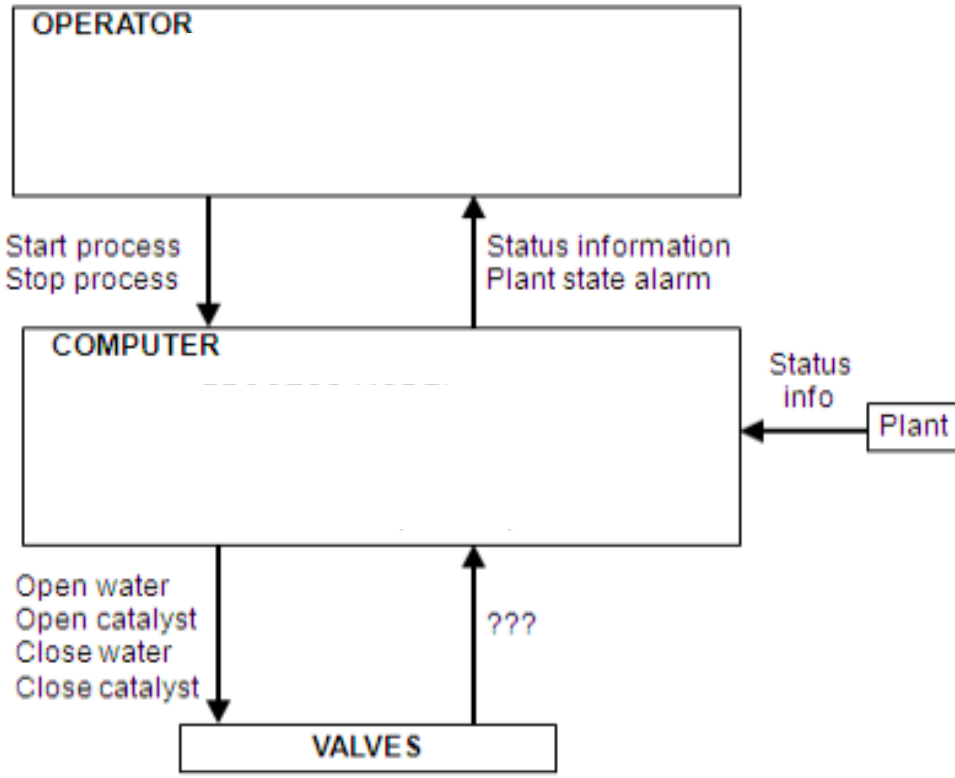



| | ? | ? | ? | ? |
|---|---|---|---|---|
| **Close Water Valve** | | | | |

©

# Chemical Reactor: Unsafe Control Actions

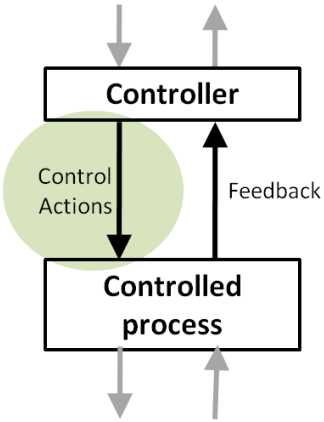
## Control Structure:




| | Not providing causes hazard | Providing causes hazard | Incorrect Timing/ Order | Stopped Too Soon / Applied too long |
|---|---|---|---|---|
| **Close Water Valve** | ? | **Computer provides Close Water cmd while catalyst open** | ? | ? |

©

# Structure of an Unsafe Control Action




Example:

"Computer provides close water valve command when catalyst open"

Source Controller

Type

Control Action

Context

Four parts of an unsafe control action

- Source Controller: the controller that can provide the control action
- Type: whether the control action was provided or not provided
- Control Action: the controller's command that was provided / missing
- Context: conditions for the hazard to occur
  - (system or environmental state in which command is provided)



©

# Chemical Reactor: Unsafe Control Actions (UCA)

| | Not providing causes hazard | Providing causes hazard | Incorrect Timing/ Order | Stopped Too Soon / Applied too long |
|---|---|---|---|---|
| **Close Water Valve** | | **Computer provides Close Water cmd while catalyst open** | **Computer provides Close Water cmd before catalyst closes** | |
| **Open Water Valve** | | | | |
| **Open Catalyst Valve** | | | | |
| **Close Catalyst Valve** | | | | |

©

# Chemical Reactor: Unsafe Control Actions (UCA)

| | Not providing causes hazard | Providing causes hazard | Incorrect Timing/ Order | Stopped Too Soon / Applied too long |
|---|---|---|---|---|
| Close Water Valve | | Computer closes water valve while catalyst open | Computer closes water valve before catalyst closes | |
| Open Water Valve | Computer does not open water valve when catalyst open | | Computer opens water valve more than X seconds after open catalyst | Computer stops opening water valve too soon when catalyst open |
| Open Catalyst Valve | | Computer opens catalyst valve when water valve not open | Computer opens catalyst more than X seconds before open water | |
| Close Catalyst Valve | Computer does not close catalyst when water closed | | Computer closes catalyst more than X seconds after close water | Computer stops closing catalyst too soon when water closed |

©

# Safety Constraints

| Unsafe Control Action | Safety Constraint |
|---|---|
| Computer does not open water valve when catalyst valve open | Computer must open water valve whenever catalyst valve is open |
| Computer opens water valve more than X seconds after catalyst valve open | ? |
| Computer closes water valve while catalyst valve open | ? |
| Computer closes water valve before catalyst valve closes | ? |
| Computer opens catalyst valve when water valve not open | ? |
| Etc. | Etc. |

# Safety Constraints

| Unsafe Control Action | Safety Constraint |
|---|---|
| Computer does not open water valve when catalyst valve open | Computer must open water valve whenever catalyst valve is open |
| Computer opens water valve more than X seconds after catalyst valve open | Computer must open water valve within X seconds of catalyst valve open |
| Computer closes water valve while catalyst valve open | Computer must not close water valve while catalyst valve open |
| Computer closes water valve before catalyst valve closes | Computer must not close water valve before catalyst valve closes |
| Computer opens catalyst valve when water valve not open | Computer must not open catalyst valve when water valve not open |
| Etc. | Etc. |

# Traceability

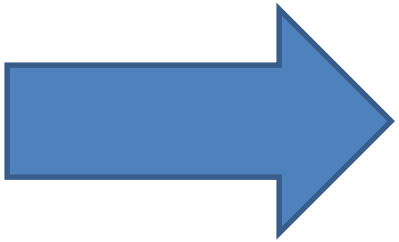
- Always provide traceability information between UCAs and the hazards they cause
  - Same for Safety Constraints
- Two ways:
  - Create one UCA table (or safety constraint list) per hazard, label each table with the hazard
  - Create one UCA table for all hazards, include traceability info at the end of each UCA
    - E.g. **Computer closes water valve while catalyst open [H-1]**

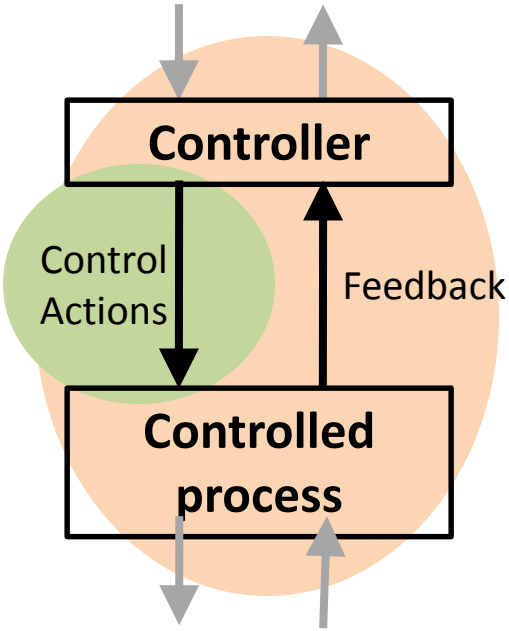
# STPA
# (System-Theoretic Process Analysis)

- Identify accidents and hazards

- Draw the control structure

- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios



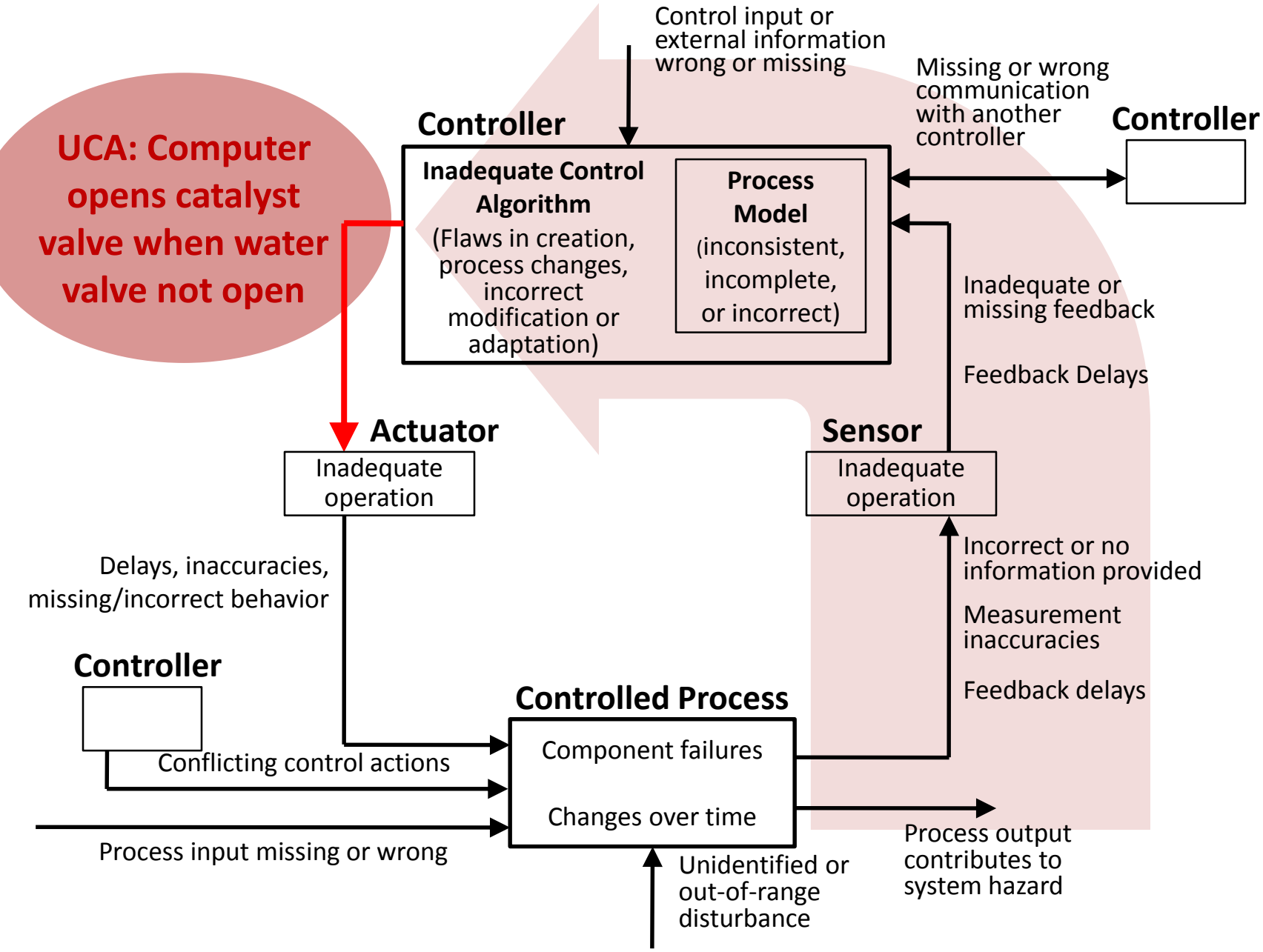



(Leveson, 2012)

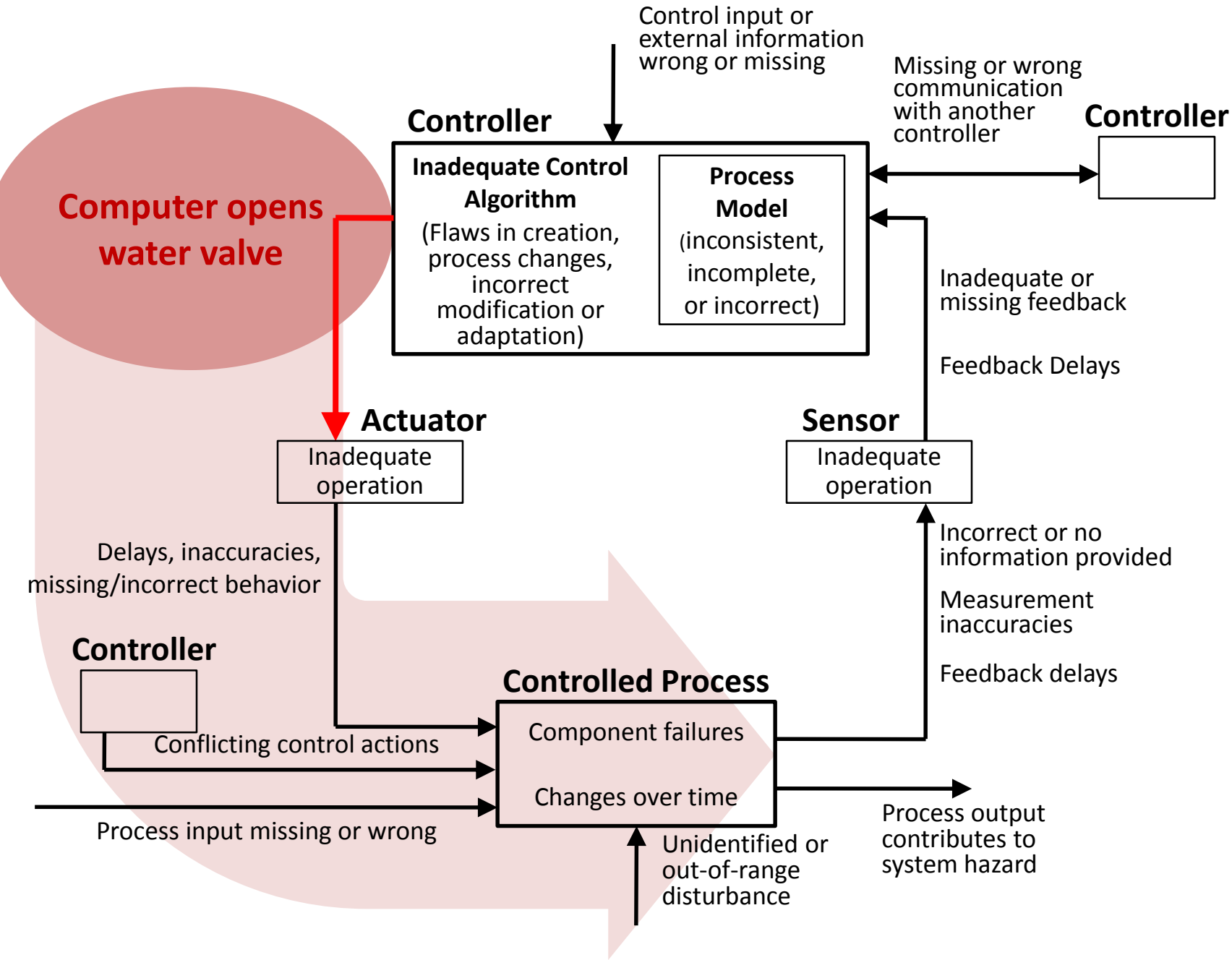


©

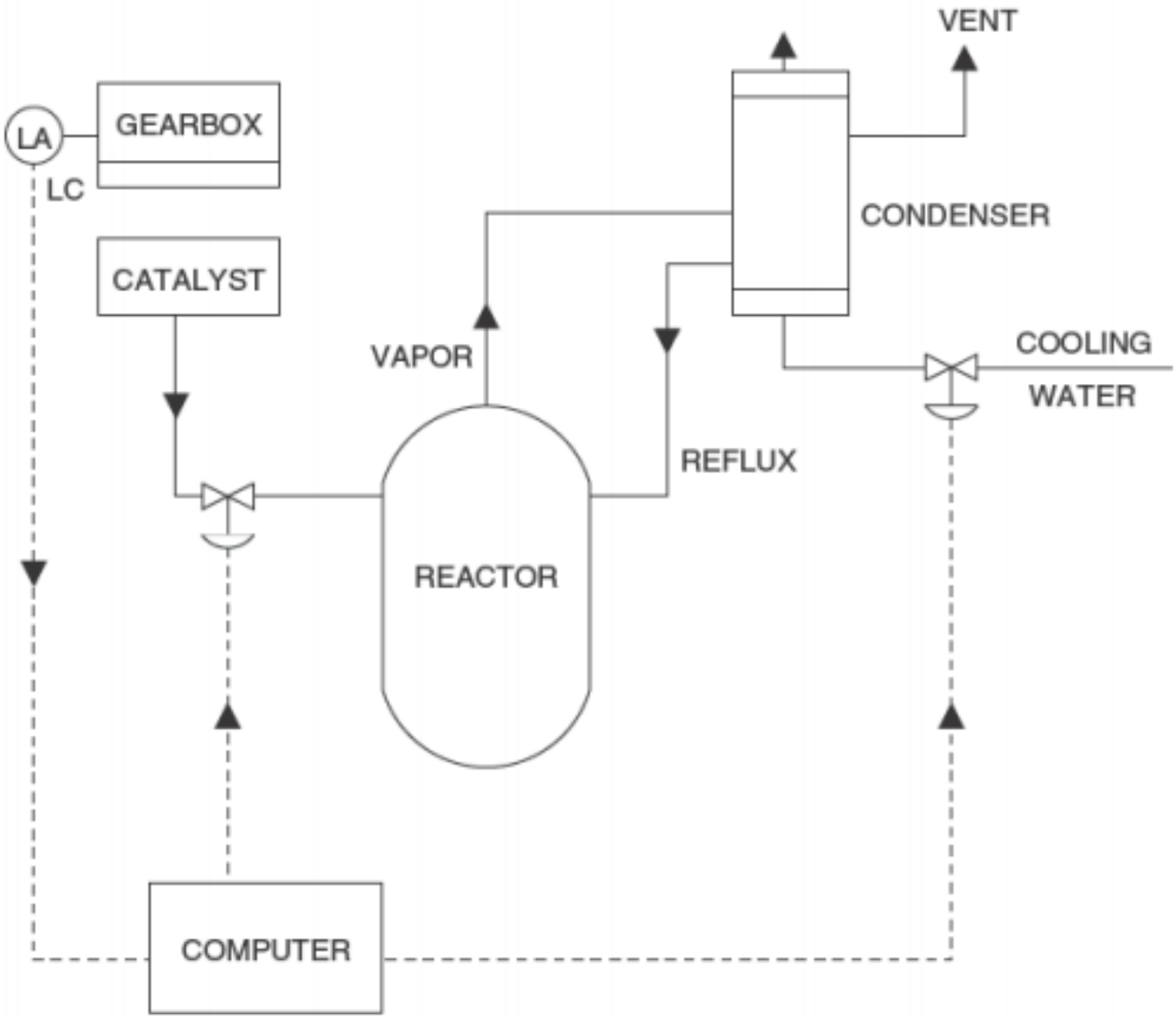
# Step 2A: Potential causes of UCAs



# Step 2B: Potential control actions not followed



# Chemical Reactor: Real accident



# How does STPA compare?

- MIT: TCAS
  - Existing high quality fault tree done by MITRE for FAA
  - MIT comparison: STPA captured everything in fault tree, plus more
- JAXA: HTV
  - Existing fault tree reviewed by NASA
  - JAXA comparison: STPA captured everything in fault tree, plus more
- EPRI: HPCI/RCIC
  - Existing fault tree & FMEA overlooked causes of real accident
  - EPRI comparison: Blind study, only STPA found actual accident scenario
- NRC: Power plant safety systems
  - Proposed design that successfully completed Final Safety Analysis Report
  - STPA found additional issues that had not been considered
- Safeware: U.S. Missile Defense Agency BMDS
  - Existing hazard analysis per U.S. military standards
  - Safeware comparison: STPA captured existing causes plus more
  - STPA took 2 people 3 months, MDA took 6 months to fix problems
- Automotive: EPS
  - Compare STPA results to FMECA using SAE J1739
- MIT: NextGen ITP
  - Existing fault tree & event tree analysis by RTCA
  - MIT comparison: STPA captured everything in fault tree, plus more
- MIT: Blood gas analyzer
  - Existing FMEA found 75 accident causes
  - STPA by S.M. student found 175 accident causes
  - STPA took less effort, found 9 scenarios that led to FDA Class 1 recall

# Who has been using STPA?

Automotive:












*US silicon valley companies

# MIT March Workshop (free)

**Industries**:
Automotive
Oil and Gas
Space
Aviation
Defense
Nuclear
Healthcare and Healthcare IT
Medical Devices
Academia
Insurance
Academia (Education)
Hydropower
Chemicals
Software/Computing
Government
Industrial Automation
Electric Utility
Security
Think Tank
Transportation
Maritime (security)
Environmental
Pharmaceuticals
Internet

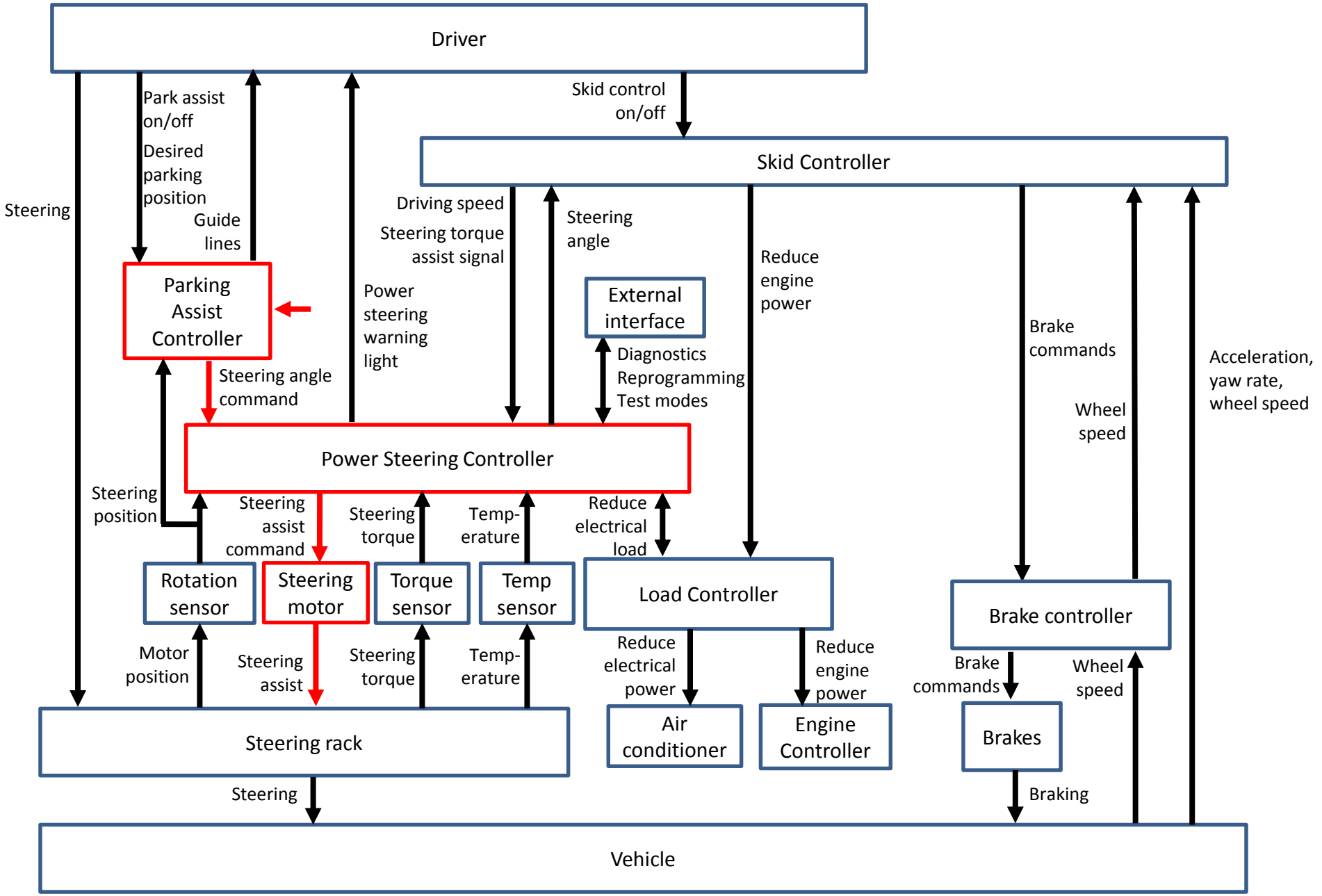
**Organizations**:
General Motors
Ford
Nissan Motor Company
Toyota
Draper Lab
Volpe National Transportation Research Center
The Boeing Company
Boeing Environment Health and Safety
Boeing Engineering and Operations
Embraer
U.S. Nuclear Regulatory Commission
U.S. Army
GE Aviation
Sikorsky
Thoratec Corporation
University of Alabama in Huntsville
Liberty Mutual Safety Research Institute
ITA (Instituto Tecnologico de Aeronautica)
Jeppesen
Beijing Institute of Technology
TEGMA Gestao Logistica S.A.
Amsterdam University of Applied Sciences
Dutch Safety Agency
University of Stuttgart
BC Hydro
Therapeutic Goods Administration
Institute of Aeronautics and Space (IAE), Brazil
Shell Oil
University of Braunschweig
Stiki
Reykjavik University
National Nuclear Energy Commission, Brazil
FAA
U.S. Department of Transportation
U.S. Air Force
U.S. Navy
IPEV (Institute for Research and Flight Testing), Brazil
Japan Aerospace Exploration Agency (JAXA)
U.S. Department of Energy
Rockwell Automation
Democritus University of Thrace
Dependable Management
ILF Consulting Engineers
JETRO (Japan)
Alliance for Clinical Research Excellence and Safety
Washington CORE
Florida Institute of Technology
U.S. Navy Strategic Systems Programs
IPEN (Institute for Nuclear and Energy Research), Brazil
Duke Energy
Synensis
Japan MOT Society
Tufts University
Southern Company
U.S. Army Aviation Engineering
U.S. Army Corps of Engineers (Kansas City District)
University of Houston, Clear Lake
Lincoln Lab
Hanscom AFB
U.S. Army Research, Development, and Engineering Command
McMaster University
Bechtel
Kyushu University (Japan)
Analog Devices
Cummins
University of Massachusetts Dartmouth
Syracuse Safety Research
National Civil Aviation Agency (ANAC0, Brazil
State Nuclear Power Automation System Engineering Company (China)
Toyota Central R&D Labs
Massachusetts General Hospital
AstraZeneca
STM (Defense Technology Engineering and Trading Corp., Turkey)
Varian Medical Systems
Fort Hill Group
TUBITAK-UZAY (Scientific and Technological Research Council of TURKEY-Space Technologies Research Institute)
Cranfield University (U.K.)
U.S. Air Force Test Pilot School
NASA/Bastion Technologies
U.S. Customs and Border Protection
Second Curve Systems
Vequria
Akamai Technologies
Canadian Dept. of Defense (DND)
University of Virginia
MSAG
Novartis
U.S. Coast Guard
EPRI (Electric Power Research Institute)
Sandia National Laboratories
Lawrence Livermore National Laboratories
Tapestry Solutions
Kansas State University
Systems Planning and Analysis
Zurich University of Applied Sciences
IBM
Lawrence Berkeley National Laboratory (LBNL)
U.S. Navy School of Aviation Safety
JAMSS (Japanese Manned Space Systems)
U.S. Chemical Safety Board

[mit.edu/psas](mit.edu/psas)



**Countries**: USA, Brazil, Japan, China, Netherlands, Germany, Canada, Australia, Iceland, Greece, United Kingdom, Turkey, Estonia, Australia

# Works for security too!



# Feedback!

- Did you like the tutorial?
- Any comments or questions?
- Email me!

jthomas4@mit.edu