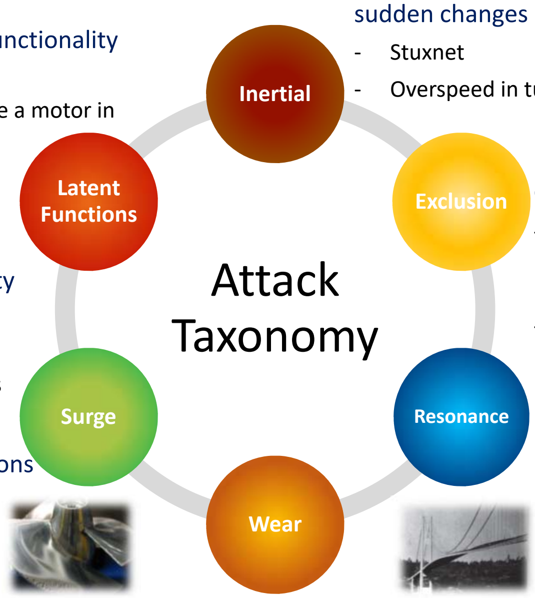
Identification and Mitigation of Cyber Vulnerabilities in Industrial Control Systems using a System Theoretic Design Approach

Shaharyar Khan, Fellow, MIT System Design & Management

Motivation – Personal Experience

1. Project Engineer at a nuclear power plant
2. Plant air-gap breached inadvertently, to get facility up and running
3. Availability and Reliability >> Security

Classes of Physical Damage



Exploiting *unused/unknown* functionality of *off-the-shelf components*

- For instance, ability to operate a motor in reverse via VFD
- Ability to update *Safety Controller* settings remotely

Exceeding *Design Limit* Capacity

- Sending too much gas/fluid through a compressor
- Overheating/melting of cables

Manipulating operating conditions to reduce component life

- Non-uniform cooling of turbine shaft → mechanical vibration
- Cavitation in Pumps

Mechanical Equipment typically doesn't like sudden changes in state

- Stuxnet
- Overspeed in turbines

Order of Operations is critical

- Chiller Compressor must never be operated before lube oil is at correct temp/pressure
- Green light for cars and pedestrians should not light at the same time

Instability in elec/mech systems when applied frequency = natural frequency

- Burning motors by running at critical frequencies → VFD
- Water Hammer in pipes

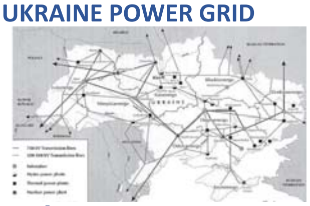
-Inspired by Marina Krotofil's Madrid Workshop
https://www.cci-es.org/documents/10694/124308/Madrid_Workshop_2014_p1_1.pdf/57ea16de-e4c2-4f26-a99b-ccd46f5e8580;jsessionid=80FFB196E9091BB8CE9DC9E74BAF486E?version=1.0

Examples of Physical Damage Cyber-Attacks

AURORA VULNERABILITY

STUXNET

UKRAINE POWER GRID



TURKISH PIPELINE

Different mechanisms employed with similar devastating effect!

TRITON

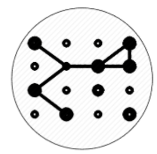
- From "Identifying and Mitigating Cyber Attacks that could cause Physical Damage to Industrial Control Systems", Angle. M et. *Al*
http://web.mit.edu/smadnick/www/wp/2017-14.pdf

New Ground Realities

1 If targeted, you will be **compromised**

2 Cyber-hygiene only protects you against **non-targeted** attacks

3 Critical Infrastructure *Control Systems* are designed to meet engineering requirements, NOT security requirements



4 Control Systems are becoming increasingly **complex, coupled** and **software-dependent**

Coping with Complexity

1. Analytic Reduction – Traditional View
2. The assumptions **DO NOT** always hold in our
   - Tightly coupled
   - Software intensive
   - Complex
   - Socio-technical

   engineered systems

3. Need a new theoretical basis
   - *Systems theory* can provide it

- From Nancy Leveson's 'Engineering a Safer and More Secure World', CREDC, https://cred-c.org/sites/default/files/slides/2016_11-07_CREDC-Seminar_Leveson.pdf

Research Vision

"To develop **software tools** based on the ***Systems Theoretic Design Approach*** for **operators** to identify critical cyber-vulnerabilities and mitigation strategies in **energy systems**."

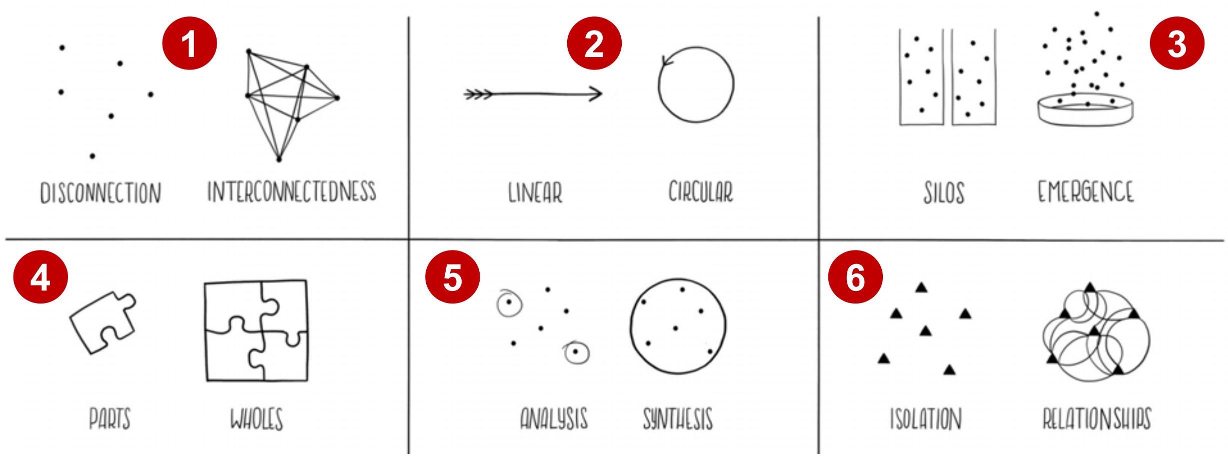
Two-Step Plan

1. Formalize the System-Theoretic Design Method by applying to *real-world* use cases
   - the MIT Central Utilities Plant
2. Develop software tools to assist *operators* to conduct such analysis

Systems-Theoretic View of Cybersecurity

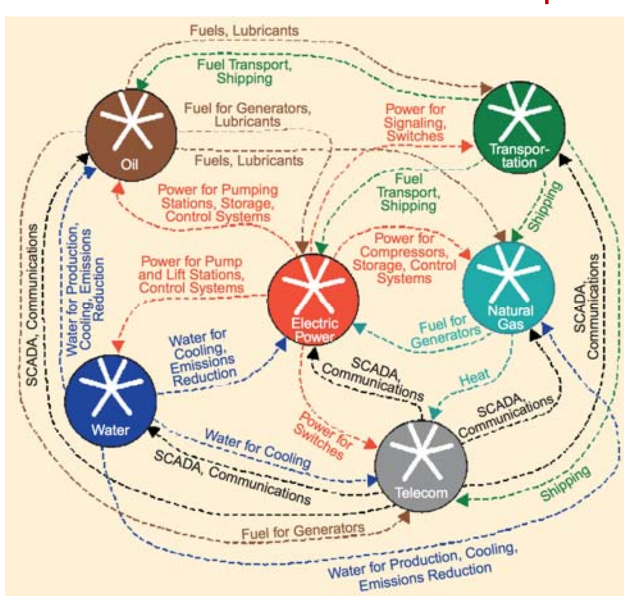
https://medium.com/disruptive-design/tools-for-systems-thinkers-the-6-fundamental-concepts-of-systems-thinking-379cdac3dc6a
https://pdfs.semanticscholar.org/b1b7/d1e0bb39badc3592373427840a4039d9717d.pdf

Systems-Theoretic View of Cybersecurity



https://medium.com/disruptive-design/tools-for-systems-thinkers-the-6-fundamental-concepts-of-systems-thinking-379cdac3dc6a
https://pdfs.semanticscholar.org/b1b7/d1e0bb39badc3592373427840a4039d9717d.pdf

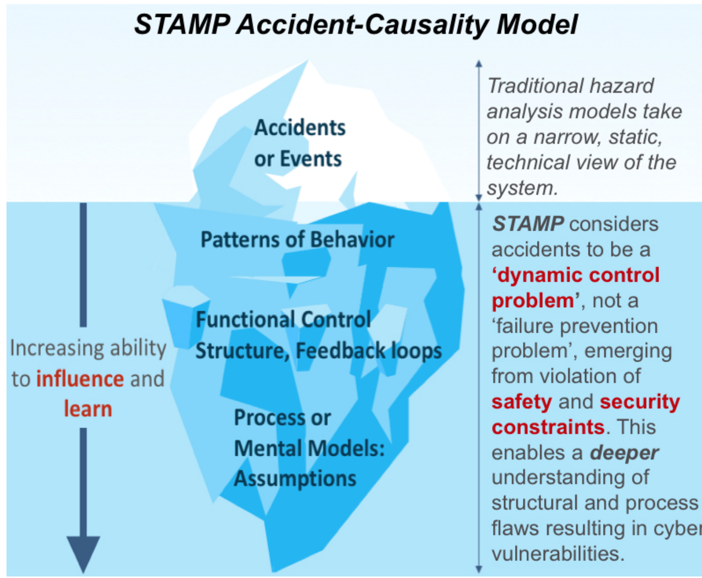
Example of Infrastructure Interdependencies



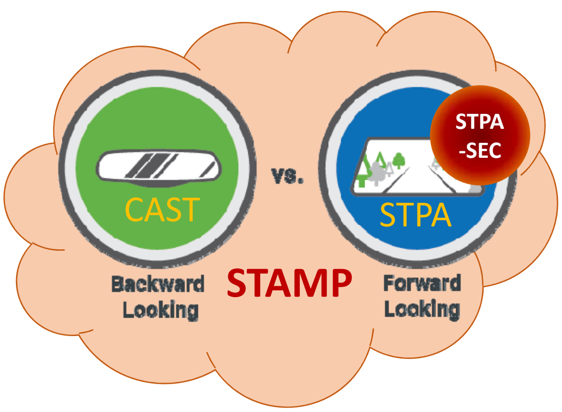
https://pdfs.semanticscholar.org/b1b7/d1e0bb39badc3592373427840a4039d9717d.pdf

STAMP (System-Theoretic Accident Model & Processes)

1. Accident-causality model based on *Systems Theory, developed by **Dr. N. Leveson***
2. Alternative to *Chain-of-Failure* events model (Swiss cheese, dominos etc.)
3. *"All engineers are trained wrong because they are trained to think in terms of the statistical independence of events" – **Dr. S. Madnick***



STAMP-based Methods

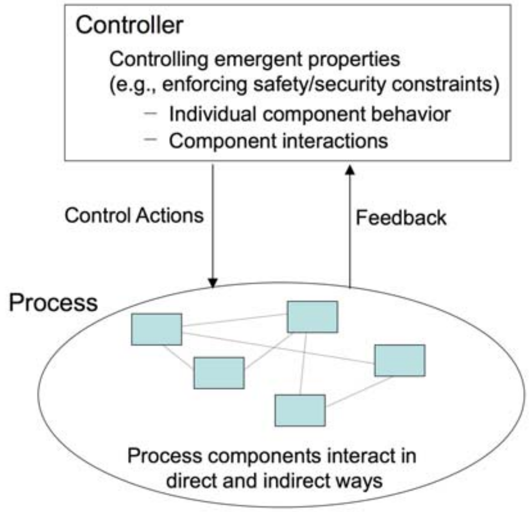


1. CAST → Causal Analysis using Systems Theory
2. STPA → System-Theoretic Process Analysis
3. STPA-Sec is a vulnerability analysis method based on STAMP that focuses on *Security*

Introduction to STPA-SEC

1. **Goal:** Design an effective ***'Control'*** structure that enforces the system *'Security Constraints'*

2. ***'Control'*** could be enforced:
   - through design (interlocks, fail-safe design)
   - through process (procedures etc.)
   - through social controls (regulatory, culture, insurance etc.)



- From Nancy Leveson's 'Engineering a Safer and More Secure World', CREDC, https://cred-c.org/sites/default/files/slides/2016_11-07_CREDC-Seminar_Leveson.pdf

STPA-Sec Methodology

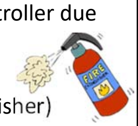
Step 1
- System – Fire Sprinkler System
- Loss – Building catches fire
- Hazard – Fire is not suppressed in time

Step 2
- Controller detects smoke
- Controller *decides* to fight the fire by activating the sprinkler

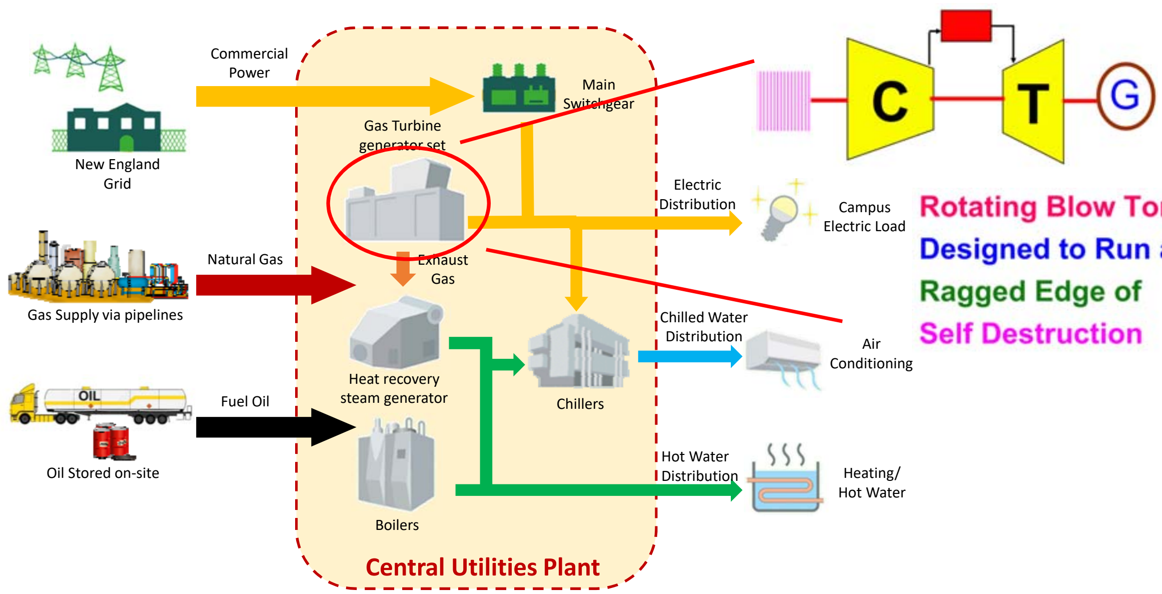
Step 3
- Control action to start sprinkler system is delayed after smoke is detected
  → Hazard (Fire not suppressed in time)

Step 4
- Causal Factor: Malformed process model of controller due to malicious feedback injection

New Requirements
- Provide *out-of-band* control loop (e.g. fire extinguisher)
- Fire extinguisher is rigorously maintained
- Management enforces policy through maintenance staff



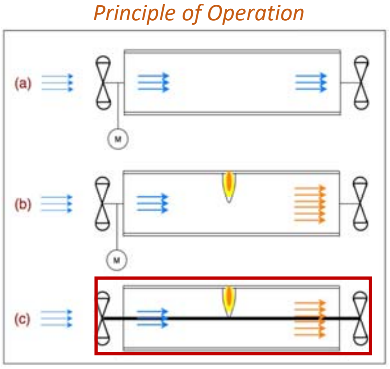
MIT Central Utilities Plant – A Microcosm Energy Facility



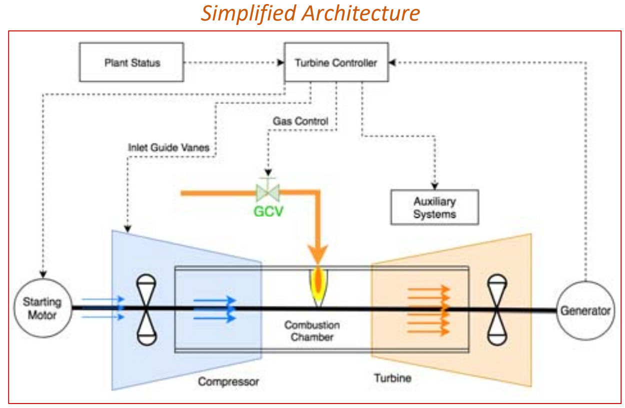
Rotating Blow Torch
Designed to Run at the
Ragged Edge of
Self Destruction

Gas Turbine – Basic Operation and Architecture

Principle of Operation



Simplified Architecture



1. Compressed air flows from the *Compressor* to the *Combustion chamber* where it is ignited
2. *Exhaust gases* accelerate the *Turbine*; the turbine shaft is coupled to the *Generator*
3. By controlling the flow of gas, the speed of the turbine can be controlled

Step 1: Define Purpose of the System (1)

1 *Key Assumption:* The system is already compromised

2 *Question to Ask:*

- What is the goal/mission of the system?
- What is the absolute worst that can happen to the system?
- What aspect of the system is the most critical to its ability to deliver its *primary-value* function?
- What is it that is being protected?

Step 1: Define Purpose of the System (2)

To
- Control Gas turbine output

By
- *Adjusting* gas flow to the turbine

Using
- An automated turbine controller

1 *System Problem Statement* is used to define purpose of the system

2 *Losses* are unacceptable conditions from the stakeholders perspective

3 *Hazards* are system states that can result in a system loss under worst-case environmental conditions

4 System-level constraints are derived by essentially inverting the Hazards

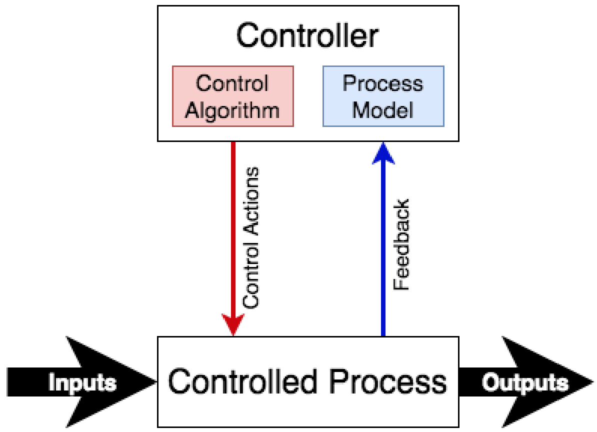
System-Level Losses

L-1: Death, dismemberment or injury to plant personnel
L-2: Loss of equipment (financial/operational)
L-3: Loss of power generation
L-4: Release of environmental pollutants

System-Level Hazards

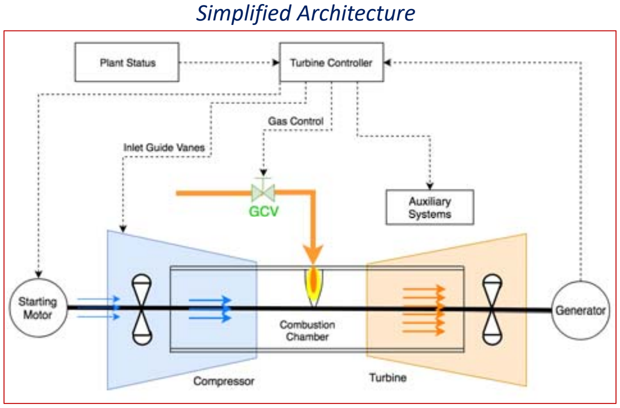
Hazards	Related Losses
H-1: Turbine is operated beyond normal operational limits (Speed, Temperature, Pressure etc.)	L-1, L-2, L-3, L-4
H-2: Turbine violates correct sequence of operation	L-1, L-2, L-3, L-4
H-3: Turbine operates without adequately purging combustible gases	L-1, L-2, L-3
H-4: Turbine loses situational awareness of its operational environment	L-3
H-5: Turbine does not meet load requirements	L-3

Step 2: Model the Functional Control Structure (1)



Step 2: Model the Functional Control Structure (2)

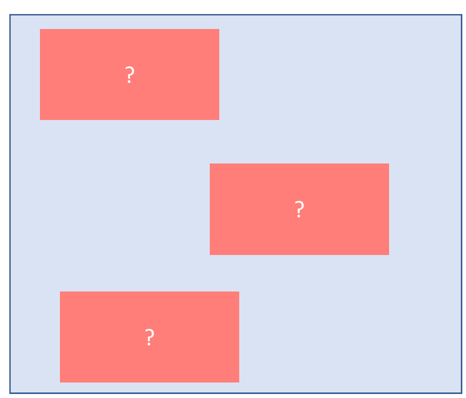
Simplified Architecture



Use the *System-Problem Statement*, to narrow down the key parts and processes of the system

Exercise:

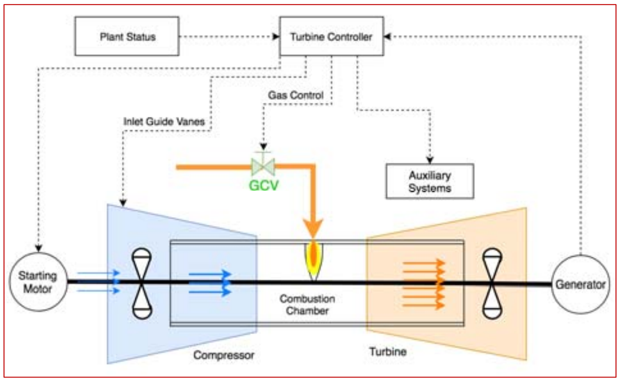
1. *What are the key processes being controlled?*
2. *What are the main parts of the system?*



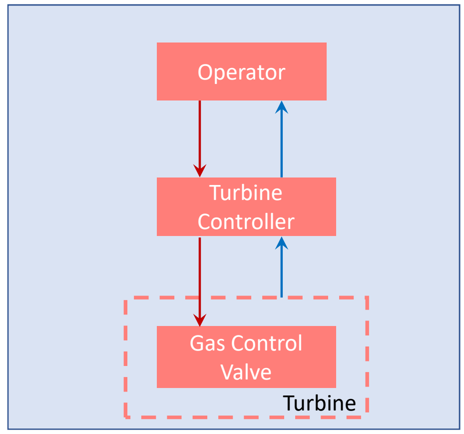
- Adapted from Dr. John Thomas' Basic STPA Exercise, MIT SDM EM.413 Course Presentation

Step 2: Model the Functional Control Structure (3)

Simplified Architecture



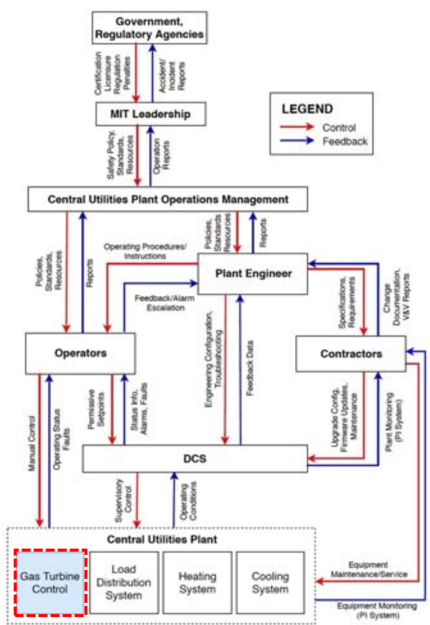
1. *What commands are sent?*
2. *What feedbacks are received?*



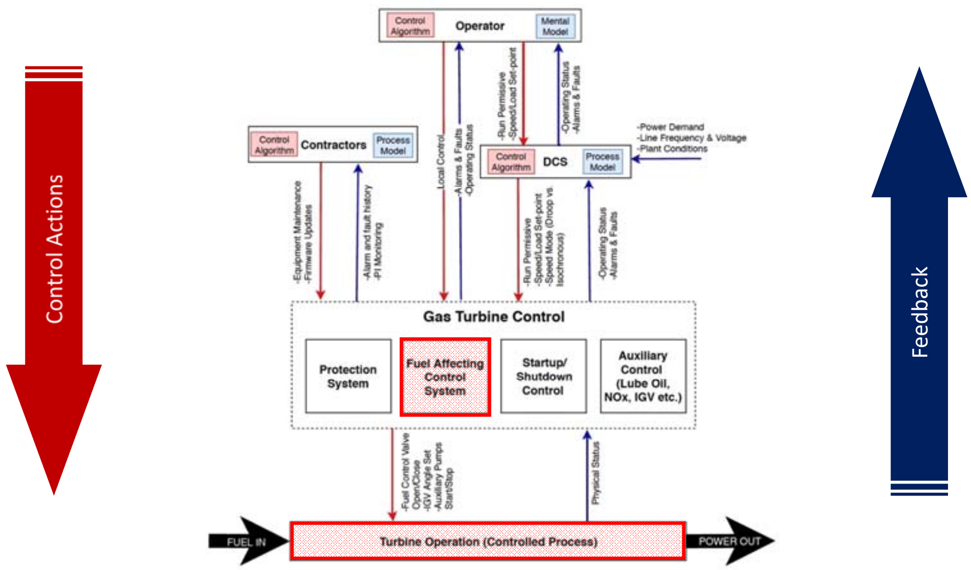
Next: Refine these diagrams to the level of complexity that is appropriate for the analysis

- Adapted from Dr. John Thomas' Basic STPA Exercise, MIT SDM EM.413 Course Presentation

Step 2: Model the Functional Control Structure

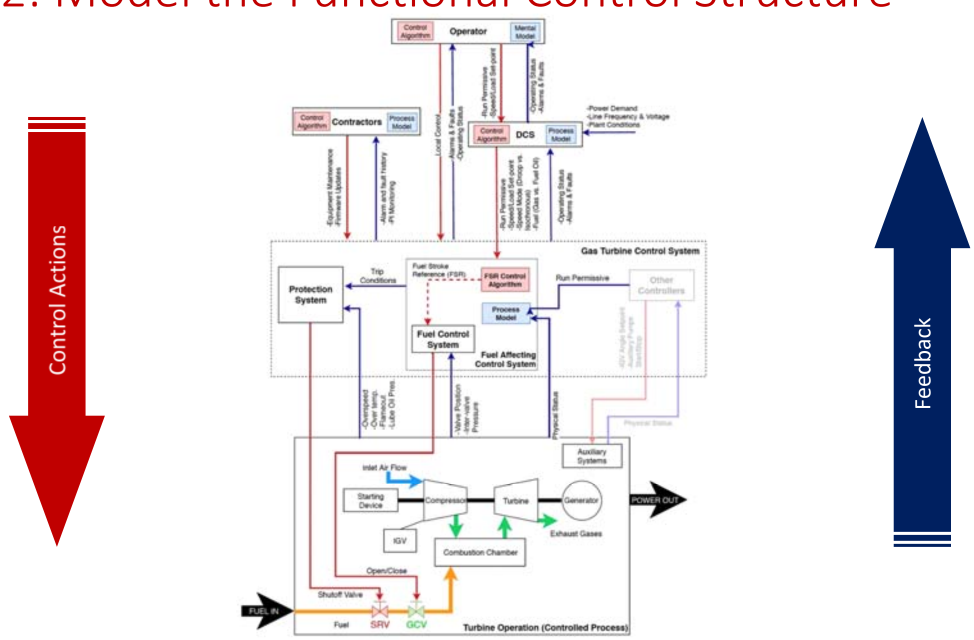


Step 2: Model the Functional Control Structure



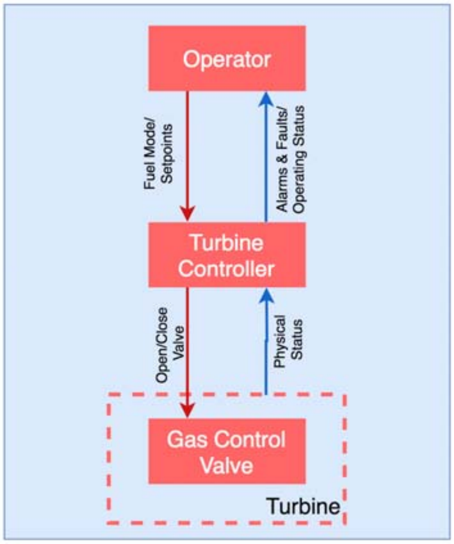
23

Step 2: Model the Functional Control Structure



24

Step 3: Identify Unsafe Control Actions (3)



1 Identify hazardous *Control Actions*

NOTE: Control Actions can be *hazardous* if they are:

a) Not provided at all

b) Provided at any time

c) Provided too soon, too late or out-of-order

d) Applied too long or stopped too soon

Action By	Control Action	Providing Causes Hazard	Not Providing Causes Hazard	Too soon, Too late, Out of order	Stopped too soon, Applied too long
Turbine Controller	Open Gas Control Valve	**UCA-1:** Turbine Controller opens *Gas Control Valve* without permissive function to undertake such an action (violating purge timer, protection system, system enable, liquid-fuel mode permissive functions etc.) --> [H-1, H-2, H-3]	?	?	?

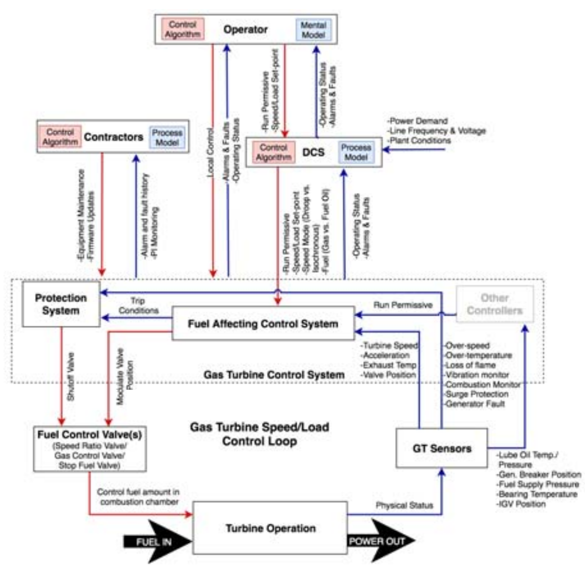
Step 3: How to Generate a Context Table

1 By analyzing all the inputs required by a controller to make a decision about executing a command, we can begin to identify the key process model variables

2 Discrepancy between a Controller's *Process Model* and the *Actual Physical State* can result in execution of unsafe control actions

3 **Physical environment** is a communication media!

- Components can influence each other even if their control loops do not communicate electronically
- *'Unseen state'* of one component may have **hidden** impact



Step 3: Unsafe Control Actions (By Defining Context Table)

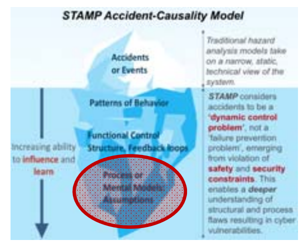
Process Model Variables

#	Name	Values
1	Turbine Sequence	Startup | Shutdown
2	Turbine Speed	Within Limits | Outside Limits
3	Shaft Acceleration	Within Limits | Outside Limits
4	Exhaust Temperature	Within Limits | Outside Limits
5	Operating Mode	Part-Load | Base-Load
6	Permissive Function	Yes | No
7	Fuel Mode	Gas | Fuel Oil | Dual

Context Table

	System Variables	#1	#2	#3	#4	#5	#6	#7	Providing Causes Hazard	Not Providing Causes Hazard	Too Early, Too Late, or Out-of-Order	Applied too long, Stopped too soon	Hazards
Open Gas Control Valve	CA-1	Start	-	-	-	-	-	-	0	1	1	0	H-1, H-2, H-5
	CA-2	S/Down	-	-	-	-	-	-	0	0	1	0	H-2, H-3
	CA-3	-	Out	-	-	-	-	-	1	0	0	1	H-1, H-3
	CA-4	-	-	Out	-	-	-	-	1	0	0	1	H-1, H-3
	CA-5	-	-	-	Out	-	-	-	1	0	0	0	H-1
	CA-6	-	-	-	-	Base	-	-	0	1	0	0	H-5
	CA-7	-	-	-	-	-	No	-	1	0	1	0	H-2, H-3
	CA-8	-	-	-	-	-	Yes	Oil	1	1	1	0	H-1, H-2, H-3, H-5
	CA-9	-	-	-	-	-	-	Dual	0	1	0	1	H-1, H-2, H-3, H-5

1. A more systematic and ruggedized approach can be followed to identify ***Unsafe Control Actions***
   - Creating a *Context Table*
2. Identifying the *Process Model Variables* is a key step in the method
3. This is where the *widely-held assumptions* are challenged



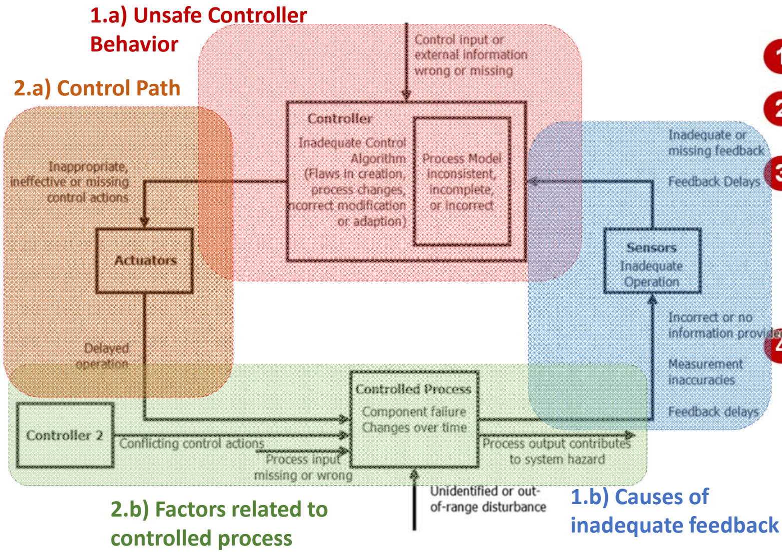
Step 3: Unsafe Control Actions

Action By	Control Action	Providing Causes Hazard	Not Providing Causes Hazard	Too soon, Too late, Out of order	Stopped too soon, Applied too long
Fuel Affecting Control System (FACS)	Open Gas Control Valve	**UCA-1:** FACS opens *Gas Control Valve* without permissive function to undertake such an action (violating purge timer, protection system, system enable, liquid-fuel mode permissive functions etc.) --> [H-1, H-2, H-3]	**UCA-4:** FACS does not open the *Gas Control Valve* during firing sequence (no ignition) --> [H-5]	**UCA-7:** FACS ramps up *Gas Control Valve* too quickly during Startup sequence (leading to uncontrolled ignition) --> [H-1; H-2]	**UCA-10:** FACS does not keep *Gas Control Valve* open above the minimum value required to prevent flameout during sudden rejection of load or generator fault (leading to accumulation of combustible gases) --> [H-3]
		UCA-2: FACS opens *Gas Control Valve* when there is a sudden loss of load or generator fault, driving the turbine to overspeed conditions --> [H-1]	**UCA-5:** FACS does not open the *Gas Control Valve* during fuel changeover (loss of synchronization) --> [H-5]	**UCA-8:** FACS opens *Gas Control Valve*, out-of-order, after flameout --> [H-2; H-3]	**UCA-11:** FACS opens the *Gas Control Valve* for too long or modulates the fuel rates incorrectly during fuel changeover (leading to internal fire, explosion) --> [H-1, H-2, H-3]
		UCA-3: FACS opens *Gas Control Valve* when operating at design temperature limit (leading to overtemperature conditions) --> [H-1]	**UCA-6:** FACS does not open the *Gas Control Valve* during frequency excursion when operating at base-load (loss of synchronization) --> [H-5]	**UCA-9:** FACS opens *Gas Control Valve* prior to receiving permissive function to undertake such action (such as purge timer, protection system, auxilary pumps etc.) --> [H-2, H-3]	

1. UCAs are control actions that put the system in a hazardous state
2. Derived from the context table by *abstracting* out common system states

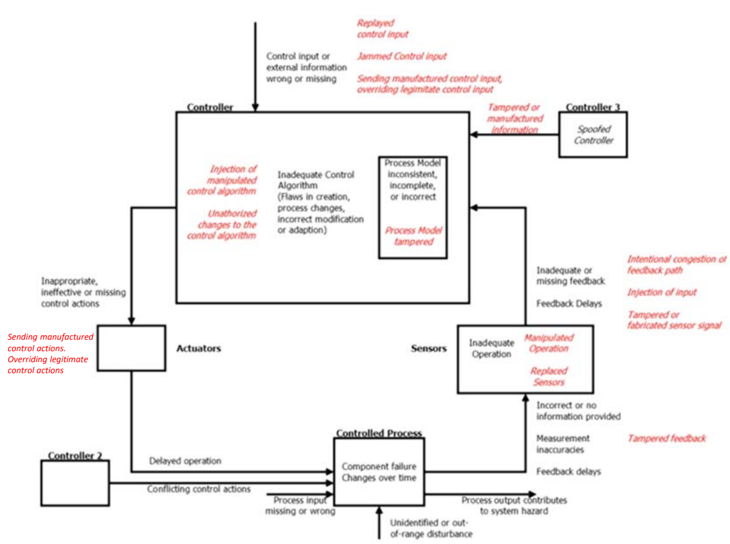
UCA-2: FACS opens the *Gas Control Valve* when there is a sudden loss of load or generator fault, driving the turbine to overspeed conditions → [H-1]

Step 4: Loss Scenarios



1. Hypothesize a loss scenario based on an UCA
2. Use a CAST type of analysis to work backwards to determine causal factors
3. Two type of *causal scenarios*
   - → Scenarios that lead to unsafe control actions
   - → Scenarios in which control actions are improperly executed or not executed at all
4. Map malicious actions to the causal scenarios
   - → Command injection or manipulation
   - → Feedback injection or manipulation
   - → Node availability
   - → Communication delays/drops

Step 4: Loss Scenarios



1. Hypothesize a loss scenario based on an UCA
2. Use a CAST type of analysis to work backwards to determine causal factors
3. Two type of *causal scenarios*
   - → Scenarios that lead to unsafe control actions
   - → Scenarios in which control actions are improperly executed or not executed at all
4. Map malicious actions to the causal scenarios
   - → Command injection or manipulation
   - → Feedback injection or manipulation
   - → Node availability
   - → Communication delays/drops

Step 4: Loss Scenarios (CUP Use-Case)

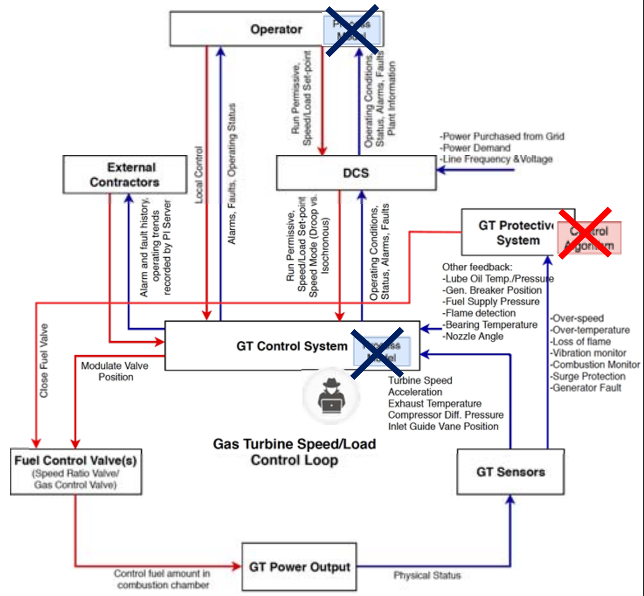
Scenario #1

1 **UCA →** GT Controller opens *Gas Control Valve* when there is a sudden loss of load or generator fault, driving the turbine to overspeed conditions.

2 **Loss Scenario →** *GT Controller interprets correct feedback incorrectly and opens the Gas Control Valve. Protection System is disabled.*

While synchronized to the grid and operating at part- or base-load, generator breaker is inadvertently tripped; GT controller and Protection System fail to act to reduce speed.

Rotational speed of the turbine exceeds safe operating limits, causing the main shaft and impeller wheels to be pulled out by centrifugal force to catastrophic failure.



Step 4: Loss Scenarios (CUP Use-Case)

Scenario #2

1 **UCA →** GT Controller opens *Gas Control Valve, out of order, after flame-out.*

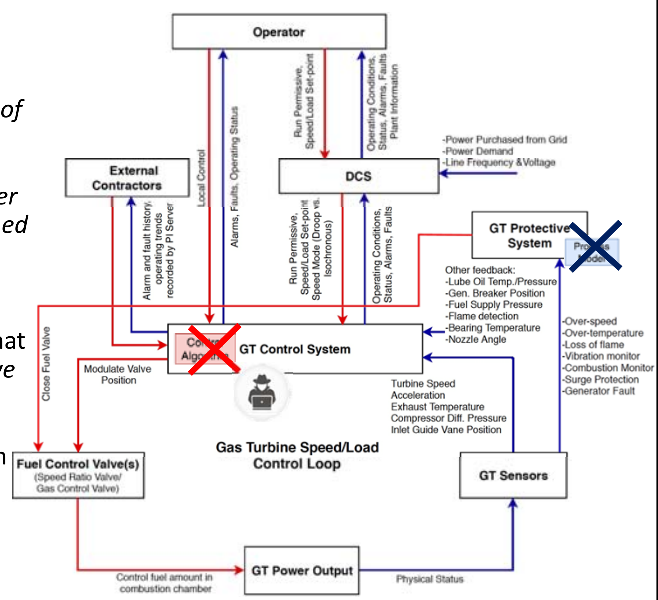
2 **Loss Scenario →** *Controller is reprogrammed to enter unsafe state that the protective system is not designed to prevent*

During a controlled (fired) shutdown of the gas turbine, the shutdown sequence is modified such that after the flame is extinguished, the *Gas Control Valve* instead of being closed shut, is opened.

A flammable mixture of gas accumulates resulting in an internal explosion.

GT Controller – Malformed Control Algorithm

Protection System – Inadequate Process Model



Step 4: Loss Scenarios (CUP Use-Case)

Scenario #3

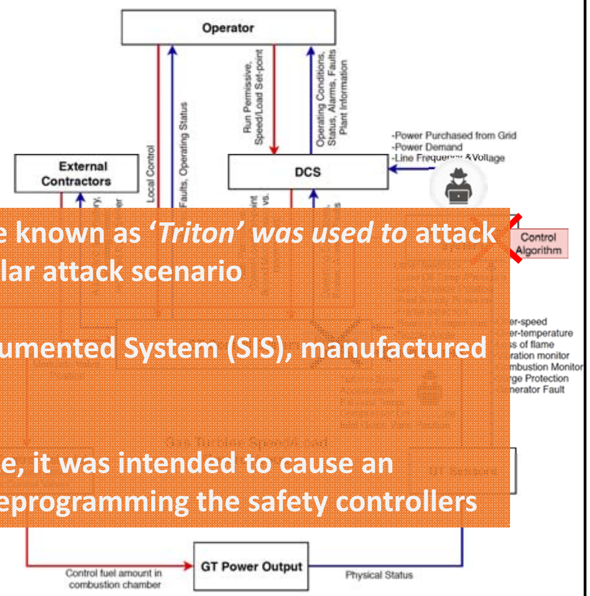
1 **UCA →** GT Controller opens *Gas Control Valve* when operating at design temperature limit (leading to over-temperature conditions)

2 **Loss Scenario →** *Protection system is reprogrammed to a[illegible] creates conditions for the [illegible] state*

During part-load operation, the GT controller unsafely ope[illegible] tem[illegible] fails to act [illegible] despite the existence of the trip conditions, the Protection System does not intervene to shut off the fuel control valv[illegible]

Protective System → Malformed Control Algorithm (i.e. incorrect temperature limits)

GT Controller → Malformed Process Model



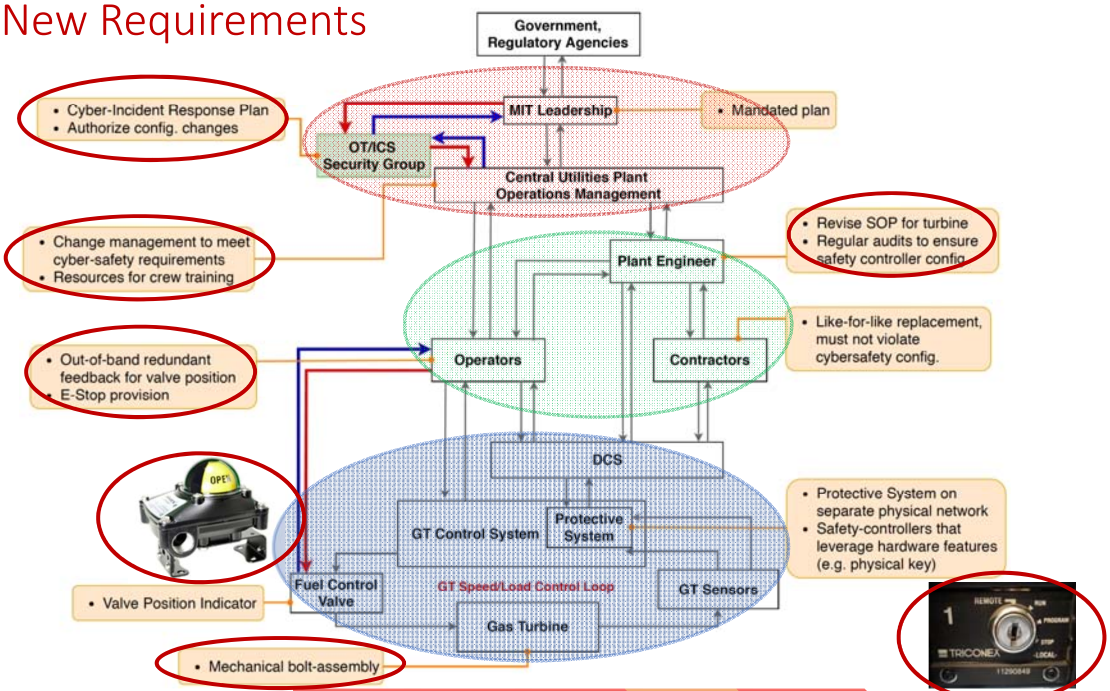
- **Publicly disclosed in Dec 2017, malware known as '*Triton*' *was used to* attack Saudi industrial facility following a similar attack scenario**
- **Malware targeted Triconex Safety Instrumented System (SIS), manufactured by Schnieder Electric**
- **Although the attack failed to materialize, it was intended to cause an explosion at the industrial plant after reprogramming the safety controllers**

Engineer out a Solution

"Think like a hacker, but act like an engineer"

- Marty Edwards, former Director, ICS-CERT

New Requirements



Good Engineering can be Mistakenly Characterized as Backwards

THE HILL

Lawmakers look to 'dumb down' smart grid

Nextgov

DATA CYBERSECURITY EMERGING TECH IT MODERNIZATION CIO BRIEFI

TRENDING // CLOUD // PROCUREMENT // CUSTOMER EXPERIENCE // ARTIFICIAL INTELLIGENCE // WORKFORCE

Senators Want Dumber Tech For Energy Grid Cybersecurity

-From Idaho National Lab's Consequence-Based Cyber Informed Engineering Presentation

https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1521570876.pdf

Conclusion:
How can we help you, and How can you help us?

Using the top-down *Systems Thinking* approach:

1. Provides a structured method to deal with complexity of cyber-physical systems
2. Enables strategic focus on cyber-vulnerabilities and mitigations most critical to the success of the organization/mission/system

Using the *functional control structure*:

3. Enables consideration of interactions between organizational, human and automated controllers in a single diagram
4. Enables natural discovery of key leverage points within the system that can be used to enforce 'control' over the system to prevent hazardous system states

Next Steps

STPA-Sec Software Tool

1. Demonstrated the Analysis for a single controller, for a single control action
2. Imagine repeating the analysis for multiple controllers and multiple control actions

Controller	Function Performed	Safety Responsibilities	Control Actions
Central Utilities Plant Operations Management Team	The Ops management team sets productivity goals for the department, develops and implements policies, standards and procedures	• Ensure that the department is delivering utility services (electricity, chilled water and steam) while meeting safety performance targets • Ensure that policies and procedures are documented and accessible • Ensure that the department has sufficient resources to meet its performance goals • Ensure the department follows a safety culture • Ensure training of personnel	• Set performance expectations • Approve standard operating procedures • Allocate staff and equipment resources • Create and maintain department culture
Plant Engineer	The plant engineer is the technical lead for plant operations	• Ensure the operators have correct procedures • Ensure safety hazards are identified and mitigated • Verify equipment is functioning properly during operation • Ensure procedural compliance and training	• Provide operating procedures • Approve standard operating procedures • Provide technical specifications and requirements to contractors/ vendors • Approve equipment change/modification requests
Operator	The operator performs day-to-day tasks to run equipment including the turbine, boilers and chillers in response to real-time demand variations from the MIT Campus	• Ensure equipment is functioning properly during operation • Observe and identify anomalous equipment behavior and notify plant engineer	• Startup/Shutdown turbine • Specify set-points for speed, temperature, power • Specify ramp function, operation mode (droop or isochronous) • Specify generator synchronization mode (manual or auto) • Specify fuel type and/or fuel-splitting distribution • Acknowledge and resolve equipment alarms and faults • Override permissive for manual control • Manual Control; Increase/decrease speed reference
Distributed Control System (DCS)	The DCS provides the operator with supervisory control and monitoring of all automated controllers distributed through the plant	• Ensure availability of information about the physical processes to the operator via Human-Machine Interface (HMI) • Ensure accessibility of physical devices via HMI (for instance overriding operating parameters)	• Specify operational sequence and set-points • Override operating parameters • Override permissive • Turn equipment (pumps, motors valves) on or off
Fuel Affecting Control System	Fuel Affecting Control System consists of the Speed/Stop Ratio Valve and the Gas Control Valve. In dual fuel systems, it also consists of Fuel Stop Valve. The basic function is to maintain desired fuel flow to the turbine	• Ensure fuel control valves are modulated such that gas turbine safety constraints are not violated (turbine speed, temperatures, acceleration etc.)	• Close/**Open Gas Control Valve (GCV)*** • Close/Open Speed/Stop Ratio Valve (SRV) • Open/Close Fuel Stop Valve (FSV) for liquid fuel control • Specify Fuel Stroke Reference (FSR) value
Protection System	Protection system acts through a trip-oil actuated dump-relay to shutoff fuel supply	• Ensure turbine trip conditions are detected and turbine is tripped to prevent equipment damage	• De-energize dump relay to close Speed/Stop Ratio Valve (SRV) and Fuel Stop Valve (FSR)
Other Controllers	For the purpose of this analysis, other equally important controllers that are part of the Gas Turbine Control System are abstracted out as 'Other Controllers'. Notably these include the Generator Synchronization Circuit Breakers, Startup/Shutdown controllers and Auxiliary Equipment controllers.	• Ensure sequence of operation is not violated	• Start/Stop Auxiliary pumps (lube oil, fuel oil, water etc.) • Modulate Inlet Guide Vane (IGV) position • Start/Stop Starting Motor or diesel generator • Open/Close circuit breaker contacts • Energize/De-energize clutch

Contact Details:

shkhan@mit.edu Shaharyar Khan

tandrews@mit.edu Taylor Andrews

smadnick@mit.edu Dr. Stuart Madnick

Funding Acknowledgement and Disclaimer

Acknowledgment:
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

Disclaimer:
This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Thank you.

Questions?