Cybersafety Analysis of Industrial Control System for Gas Turbines

Shaharyar Khan, Stuart Madnick, and Allen Moulton

Working Paper CISL# 2018-12

October 2018
(revised April 28, 2019)

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Cybersafety Analysis of Industrial Control System for Gas Turbines

Shaharyar Khan, Stuart Madnick, Allen Moulton

***Abstract*-- As Industrial Control Systems (ICS) become increasingly software-intensive and more complex, the traditional approaches to cybersecurity that undertake a narrow, static technical view of the system are proving to be increasingly inept in the face of new threat vectors and vulnerabilities. To date, most attacks on Energy Systems have targeted either the IT infrastructure (e.g., the Aramco Shamoo attack) or Circuit breakers of Operational Technology (e.g., the Ukraine attack.). In such cases, recovery is usually rather fast – either by rebooting computers or resetting breakers. But, if the Operation Technology equipment, especially the important, large, customized equipment, is physically damaged, recovery can take weeks or even months. In this paper, we demonstrate the use of the *Systems-Theoretic Process Analysis for Security (STPA-Sec) method* to identify cyber vulnerabilities that have the potential to cause physical damage in industrial control systems using a gas turbine as a use-case. This analysis does not attempt to perform a complete analysis of the entire plant or the gas turbine; rather, it lays the foundation for the exercise in a rigorous, systematic fashion that could be emulated to perform a complete analysis. Several new requirements are identified to make the system more resilient which do not only span the technical aspects of the system but also the broader socio-organizational system.**

I. INTRODUCTION

Cyber-Physical systems are electronic control systems that control physical processes and machines such as, motors and valves, in an industrial plant using Information and Communication Technologies (ICT). They can be thought of as the central nervous system of a plant that enable monitoring and control of all operations of a plant. The advances in computing power and network transmission speeds, coupled with a decrease in hardware cost, has enabled new applications of ICT in industrial settings to improve efficiency of the underlying physical processes. The resulting displacement of traditional analog and mechanical devices with complex, software-intensive Industrial Control Systems (ICS), has inadvertently intertwined the architecture of physical processes with cyberspace; thus, exposing them to new threat vectors and vulnerabilities.

ICSs monitor and control industrial processes across a wide spectrum of industries; from critical infrastructures such as electric grids, nuclear power plants, gas and water distribution pipelines and oil refineries to standalone cogeneration power plants and Building Management Systems (BMS) in hospitals, universities, malls and commercial buildings. Despite the diversity of scale and application across industries, their system architecture is fairly identical. Typically, these control systems rely on sensors, limit switches and metering devices to acquire data from controlled processes, which is then fed back to Programmable Logic Controllers (PLC) in conjunction with some kind of a Supervisory Control and Data Acquisition (SCADA) system, to control the physical processes through actuators, motors and valves.

While security (of data) has been a primary concern for traditional Information Technology (IT) systems since their inception, it is a rather recent phenomenon for ICSs; the traditional top priority for ICS being the

reliability and *availability* of physical devices. This lack of urgency or attention to security risks exposes ICS to potential cyberattacks that can cause actual physical damage or disruption of critical infrastructure or services. The 2009 Stuxnet cyberattack that partially destroyed a third of the centrifuges at a uranium enrichment facility in Natanz, Iran, demonstrated the unprecedented capabilities of such attacks on ICS, ushering a new era in cyber warfare.

Current approaches to examining cybersecurity of cyber-physical systems are often based on analysis of ICT protocols or network configurations; they undertake a narrow technical view that is biased by information security concerns [7]. In reality, security (and by extension cybersecurity), like safety, is an *emergent* property of a system where the interactions of simple components produce complex behaviors which cannot be predicted by linearly analyzing the individual components in isolation. Instead, a top-down, *systems thinking* approach is required that examines not only the components on their own but also holistically considers the functional interactions between components, people and management as a whole.

System Theoretic Accident Model & Processes (STAMP) is an accident causality model originally developed to address *safety* of complex systems. The actual method based on the STAMP accident model is called System Theoretic Process Analysis (STPA). Young and Levenson [2] adapted the STPA method to security; the new method is called STPA-Sec. The key idea that distinguishes STPA-Sec from other hazard and vulnerability analysis methods is that it is assumed, right at the onset of the analysis, that the control system has already been compromised; the analysis then starts with identification of high-level, worst-case loss scenarios for the system. It then systematically attempts to identify what control actions throughout the hierarchical functional control structure would move the system into a hazardous state, which under worst case environmental conditions could be exploited to result in a loss scenario. Finally, new requirements are derived from the analysis that prescribe new constraints that would prevent the system from entering an unsafe/unsecure state that could result in a loss.

In this paper, we perform a limited STPA-Sec analysis on a gas turbine to demonstrate the use of the method for an archetypal industrial control system. The gas turbine control system provides an illustrative example of a modern-day, software intensive, cyber-physical system. In this paper, a robust analysis of a single control loop (the turbine *Fuel Affecting Control Loop*) is used to illustrate how a cyberattack at a component level can propagate into system-level losses and how such losses can be mitigated through implementation of control measures both at the technical level as well as at the broader socio-organizational level.

II. BACKGROUND

The plant studied, operates a 20 MW gas turbine generator that provides electricity; waste heat from the turbine is directed to a Heat Recovery Steam Generator (HRSG) to produce steam. The steam along with other gas/oil-fired water-tube boilers is used for heating and other functions such as driving steam-driven chillers. The plant has been designed to provide near 100 percent reliability through maintaining standby units at all times, as the steam, chilled water and electrical power generated is used to maintain critical research facilities and laboratories. A loop-connection electric distribution system is used (as opposed to a radial-connection distribution system) designed with redundancy to provide a high level of service continuity and operating flexibility.

The power generated by the gas turbine meets only about 60 percent of the electricity demand; the shortfall is drawn from the local utility tie-line via six 13.8 kV service connections feeding into the main switchgear in addition to the gas turbine which also produces power at 13.8 kV. The plant is set up to optimize operating expense by throttling generation capacity to most economically supply power based on fluctuating electricity and natural gas prices. The throttle settings are changed up to three times per day to take advantage of electric and gas price fluctuations.

In addition to the electric and gas price fluctuations, the power demand (both real and reactive power) varies throughout the day. Reactive power, which does not produce any useful work but supports the voltage that must be controlled for system stability, affects line currents, bus voltages as well as the power factor of the tie-line bringing power into the plant from the local utility. Low power factors are penalized by the local utility as it impacts system efficiency. Stable system operation requires that bus voltages are maintained within assigned limits, transformers and connecting cables are not overloaded and the generators are operated within their reactive capabilities.

In order to control and manage the devices that affect the electric generation and distribution, along with other plant equipment, including turbine, boilers, chillers, and other ancillary equipment, a Distributed Control System, shown in Figure 1, is implemented which is supervised by operators 24/7. The DCS provides supervisory level control over geographically distributed control elements. Process control is achieved by deploying feedback or feedforward control loops whereby key process conditions are automatically maintained around a desired set point using Programmable Logic Controllers (PLCs) [8]. The control architecture differs from centralized control system wherein a single controller at a central location handles the control function; in DCS, each process element or machine or group of machines is controlled by a dedicated controller.

The DCS uses MODBUS TCP/IP protocols to communicate with the various PLCs, I/O modules and gateways. MODBUS is a serial communications protocol for PLCs which is the de-facto standard communication protocol for connecting industrial control devices. A high-level system architecture implementation for a generic DCS is shown in Figure 2; it shows several controllers (PLCs, machine controllers, process controllers etc.) connected to an integrated supervisory control system (DCS) annotated as the *Control Server*.

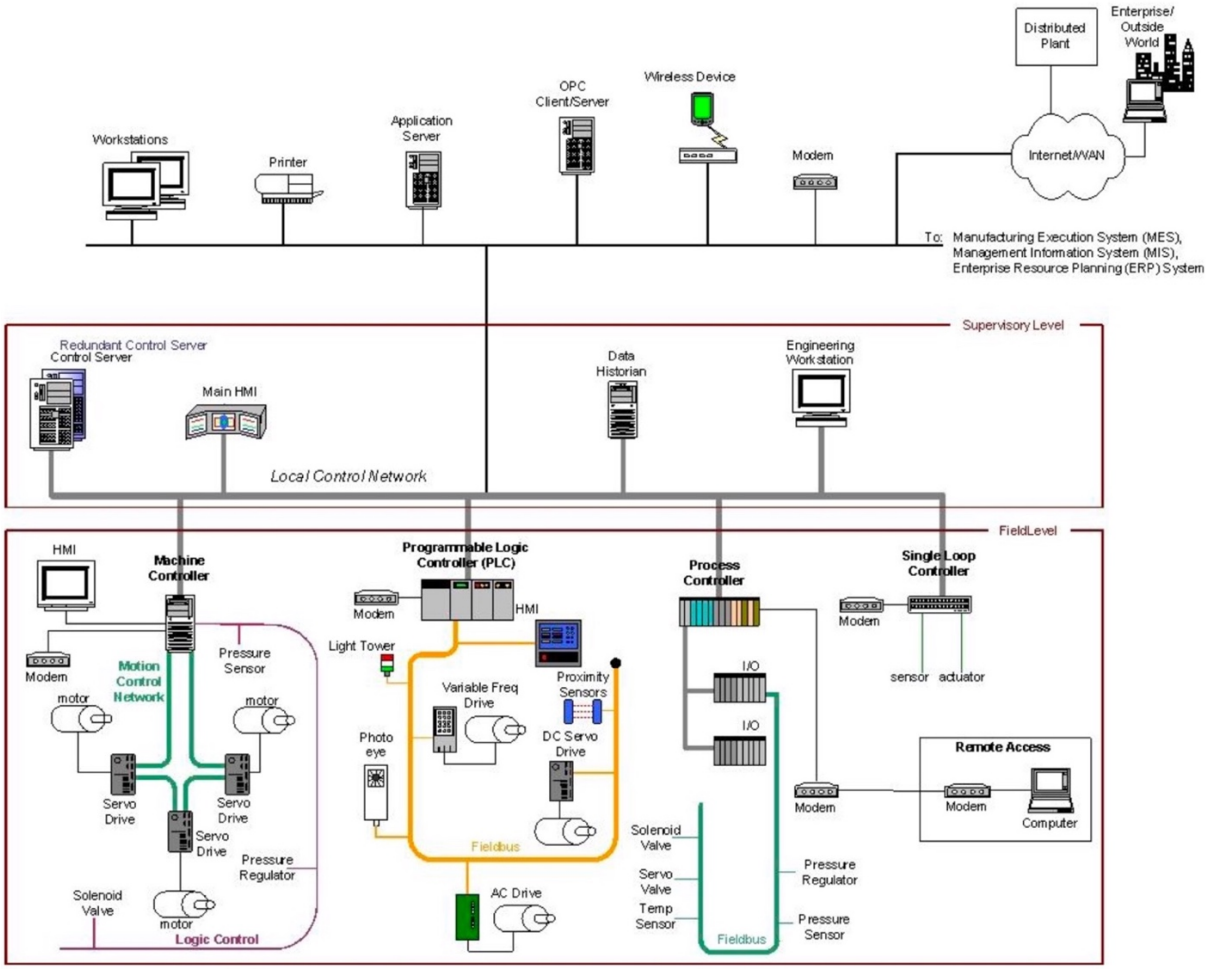

Figure 1 - DCS System Architecture Example [8]

The figure also shows the *Main HMI* (Human-Machine Interface) which serves as the primary interface between the operator and the various control elements throughout the plant. Figure 2 further shows example HMI screens for the gas turbine, boilers, chillers and electric distribution system. As can be observed from the figure, operating status of the various pumps, valves, breakers distributed throughout the plant is readily available to the operator in real-time through the DCS HMI.

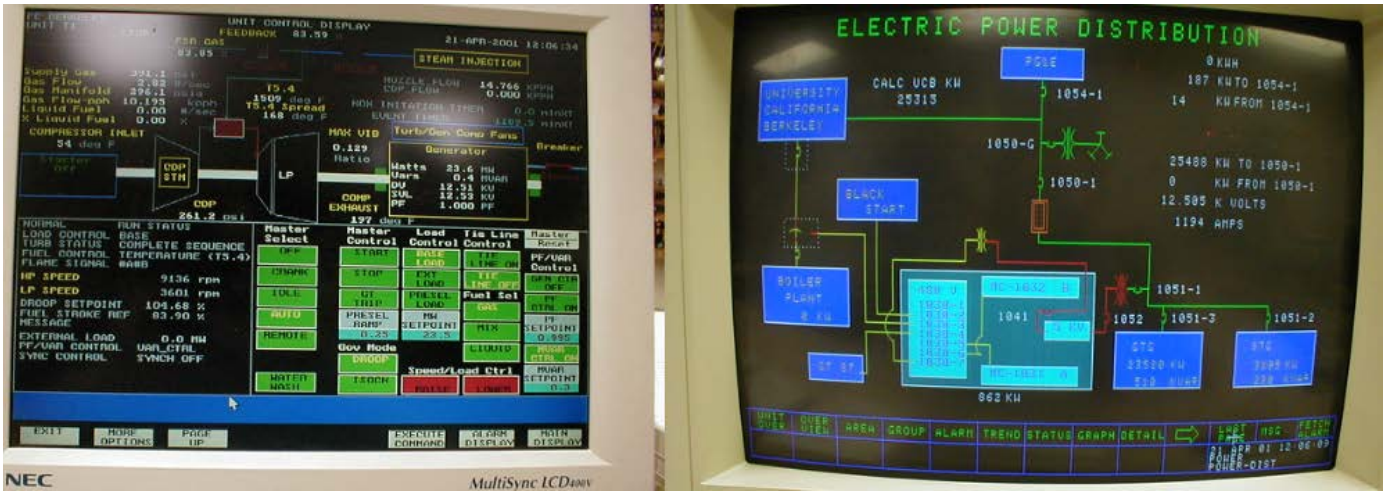

Figure 2 –Sample screenshots of a plant's DCS System [19]

We will now briefly describe the STPA-Sec method.

IV. THE METHOD

STPA-Sec is an analytical method that finds its theoretical basis in an accident causality model based on *Systems Theory* called STAMP (System-Theoretic Accident Model and Processes). STAMP treats *safety* (and by extension, *security*) as a 'dynamic control problem' rather than a 'failure prevention problem'. Traditional causality models used for safety analysis, attribute accidents to an initial component failure or human error that cascades through a set of other components. Such models are adequate for systems with limited complexity, or systems that exhibit linear interactions and simple cause-and-effect linkages [2, 7].

More complex, software-intensive systems, that are increasingly becoming commonplace in industrial settings, present new challenges in the form of losses caused not only by component failure, but also unsafe interactions among components (none of which may have failed), system requirements and design errors and indirect sociotechnical interactions resulting in unidentified common-cause failures of barriers [2, 7]. For such complex systems, STAMP offers a more robust and comprehensive accident causality model because of the following reasons [2]:

- It works top-down, rather than bottom up i.e. instead of using *external threats*, it uses *outcomes* to derive security requirements
- It includes software, humans, organizations, safety culture, etc. as causal factors in accidents and other types of losses without having to treat them differently or separately.
- It enables creation of powerful tools, such as STPA, Causal Analysis using Systems Theory (CAST) etc.

It should be noted, however, that STAMP is not an analysis method; rather it is a model or set of assumptions about how accidents occur [2]. The two most widely used STAMP-based tools that provide an analytical method are STPA (System-Theoretic Process Analysis) and CAST (Causal Analysis based on STAMP). STPA is *forward-looking* (i.e. a tool for hazard analysis) while CAST is backward-looking (i.e. a tool for analyzing loss events that have already occurred). The basic steps in STPA are shown in Figure 3.

Figure 3 - Overview of the Basic STPA Method

The goal of STPA is to identify how safety constraints may be violated as a result of loss of control due to inadequate or malformed process models or design flaws which under worst-case environmental factors would result in a system-level loss. STPA starts with defining the purpose of the analysis by defining system-level losses that the analysis aims to prevent (*Step 1* in Figure 3). The next step (*Step 2* in Figure 3) is to build a hierarchical functional control structure that captures the functional relationships and interactions by modeling the system as a set of feedback control loops. In the control structure, each level of the structure enforces the required constraints on the behavior of the components at the next lower level. Missing or lack of enforcement of relevant constraints can lead to elevated risks, which may result in a loss event(s) under worst-case environmental conditions [2].

The third step (*Step 3* in Figure 3) is to analyze control actions in the control structure to examine how they could lead to unacceptable losses identified in the first step. These *unsafe control actions* are used to create functional requirements and constraints for the system. Finally, the last step (*Step 4* in Figure 3) identifies reasons why unsafe control actions might occur. Scenarios are created to explain [2]:

1. How incorrect feedback, inadequate requirements, design errors, component failures, and other factors could cause *unsafe* control actions and ultimately lead to losses.
2. How *safe* control actions might be provided but not followed or executed properly, leading to a loss.

STPA-Sec is an extension to STPA to include security analysis. The initial steps in the analysis are identical to those for safety: identifying the losses to be considered, identifying system hazards or security vulnerabilities, drawing the system functional control structure, and identifying unsafe, or in this case, insecure, control actions. The only difference is the addition of intentional actions in the generation of the causal scenarios, in the last step in the process [7].

According to Young [7], use of a systems-theoretic approach to security, *"requires a reframing of the usual security problem…into one of strategy rather than tactics. In practice, this reframing involves shifting the majority of security analysis away from guarding against attacks (tactics) and more toward design of the broader socio-technical system (strategy)"*. This means, that instead of focusing on threats from adversaries which are outside the control of the system, security efforts should be focused on controlling system vulnerabilities. This would prevent not only disruptions from known threats, but also disruptions introduced by unknown threats, such as insider-attacks. In other words, in STPA-Sec, the source of the disruption does not matter; what matters is identifying and controlling the inherent system vulnerabilities [7].

According to Young [7], the STPA-Sec method does not circumvent a formal threat analysis but proposes to perform the threat analysis only after developing a deeper systemic understanding of the context under which the threats may operate and the disruptions that could actually lead to critical loss events.

We will now provide a high-level description of the system under analysis (i.e. the gas turbine).

V. GAS TURBINE OPERATION

A gas turbine which is sometimes, frivolously, described as a *'rotating blow torch, designed to run at the ragged edge of self-destruction'*, is an internal combustion engine, designed to accelerate a stream of gas to produce mechanical power to turn a load. In the case of power generation, the turbine shaft is coupled to a synchronous generator where the rotational energy supplied by the turbine is converted to 3-phase electrical power.

The operation of a simplified gas turbine is depicted in Figure 4. Figure 4(a) shows a cylindrical cross-section with a fan on each end. If the fan on the left is started via an electric motor, it will draw air inside the cylinder which will cause the fan on the right to rotate at the same speed as the fan on the left (ignoring frictional losses). If a flame is introduced inside the cylinder (as shown in Figure 4(b)), it will increase the temperature of the air as it passes through the flame as well as increase its specific volume. This will cause the fan on the right to rotate even faster than the fan on the left (because the increase in temperature increases the volumetric flow rate). Now, if the electric motor running the fan on the left is disconnected and instead the two fans are coupled via a shaft (as shown in Figure 4(c)), the rotation of the right-hand fan is adequate to support the rotation of the left-hand side fan. This, in fact, is the basic principle of operation of a gas turbine, known as the *Brayton cycle* in thermodynamics.

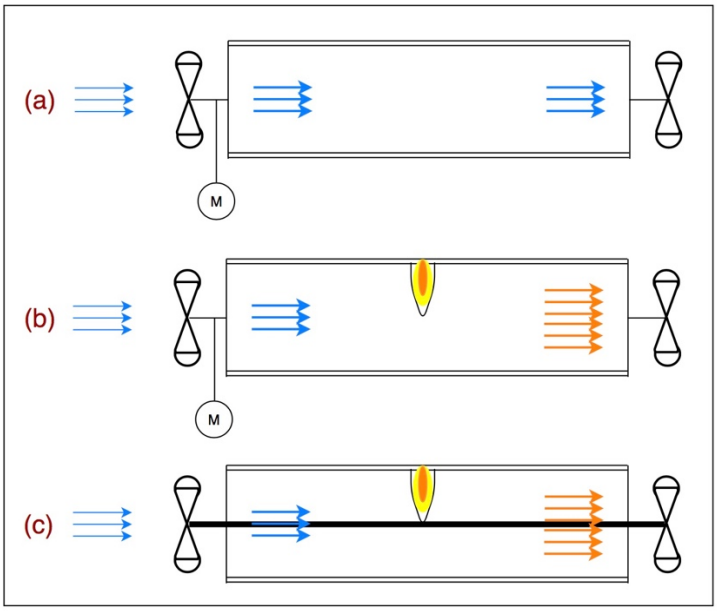

Figure 4 - Simplified Gas Turbine

As schematically shown in Figure 5, the gas turbine system is composed primarily of a starting device, a compressor, a combustion chamber, a turbine, an electric generator and the auxiliary systems such as fuel system, lube oil system, startup system etc. The starting device is a diesel engine (or an electric motor) which *cranks* the turbine shaft to overcome inertia and to accelerate the gas turbine up to the ignition speed.

The figure also shows the P-v (pressure vs. specific volume) and T-s (temperature vs. specific entropy) characteristics of the *idealized* Brayton cycle. It basically consists of four stages:

a) Stage 1-2 – Ambient air is drawn into the axial compressor where it is pressurized.
b) Stage 2-3 – The compressed air then runs through the combustion chamber where fuel is burned, heating the air. This is a constant-pressure process, since the chamber is open and allows the air to flow in and out.
c) Stage 3-4 – The high temperature, high pressure exhaust gases are expanded in turbine stages to rotate the unit, thereby losing energy (shown by the decrease in temperature and pressure in the diagrams). The electric generator which is mechanically coupled to the turbine generates electricity while some of the work extracted by the turbine is used to drive the compressor.
d) Stage 4-1 – Heat is rejected to the atmosphere. In the case of the co-generation plant, the heat is passed onto the HRSG where it is extracted to generate steam.

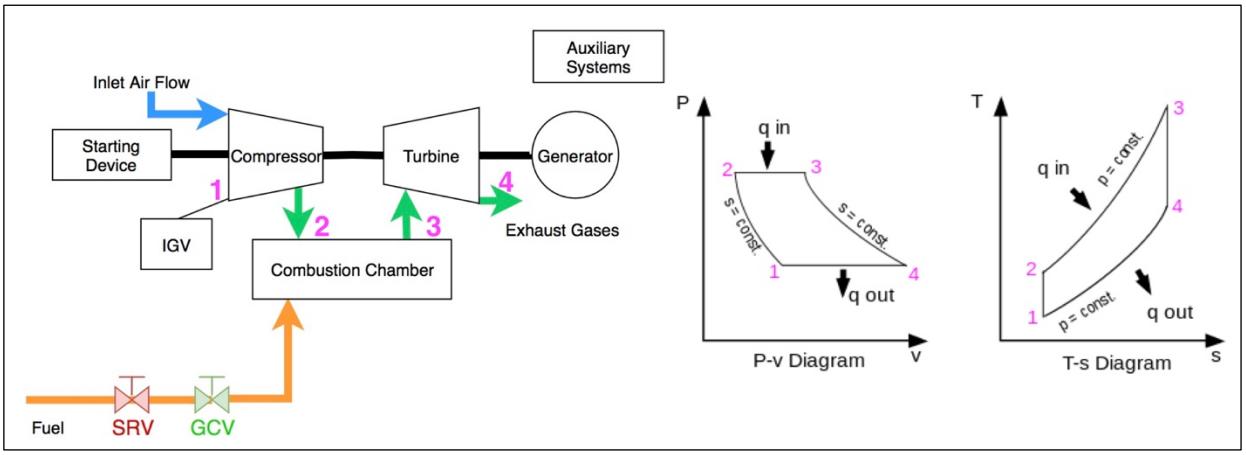

Figure 5 - Overview of the Gas Turbine System

Building upon the simplified gas turbine schematics, Figure 6 shows a detailed view of the various systems of a Siemens gas turbine unit [4]. The figure shows the various auxiliary subsystems including the pumps, motors and valves that are required for the smooth operation of the turbine. These include the lube oil system, the ventilation system, the fuel oil system, compressor cleaning unit etc. Figure 7 shows an outside 3D view of the gas turbine system and is provided primarily to provide some context of location and size of the various subsystems.

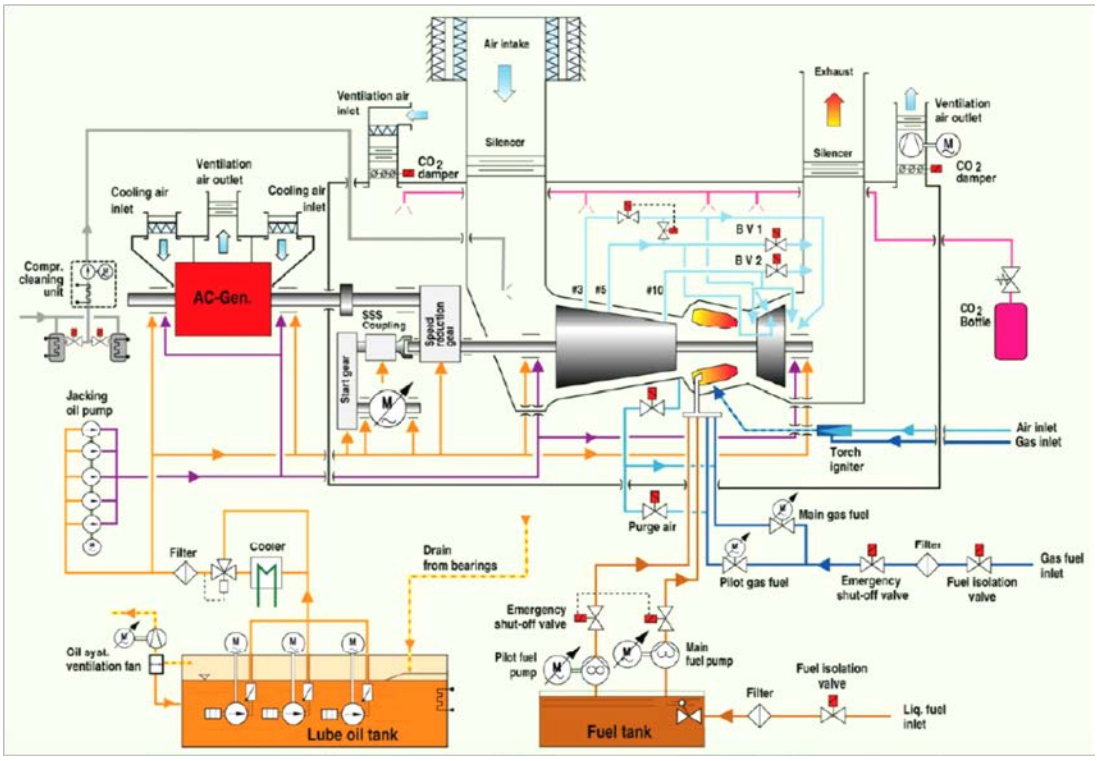

Figure 6 - Auxiliary Systems of a gas turbine

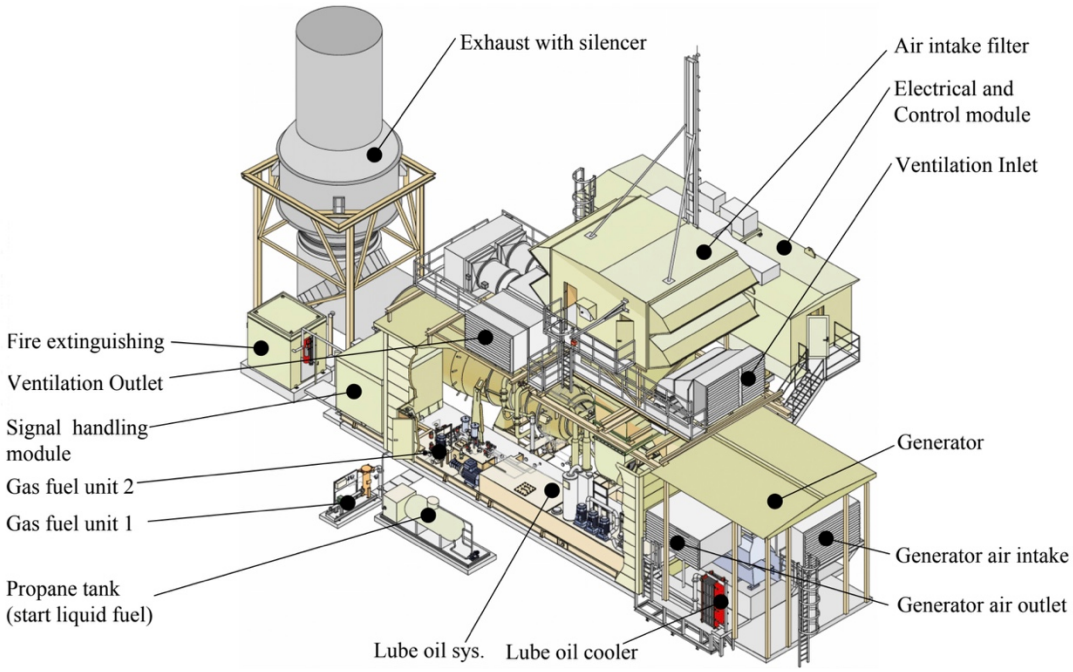

Figure 7 – 3D view of auxiliary systems of an illustrative gas turbine unit [4]

VI. ANALYSIS

In this section, we demonstrate the application of the STPA-Sec method to the gas turbine use case. This section is divided into subsections where each subsection represents one step in the basic STPA-Sec diagram as presented in Figure 3. The hazard scenarios generated in this section are used to guide an in-depth security analysis and derive mitigation strategies presented later.

Step 1 – Define Purpose of Analysis

We define the system under analysis as the *control of the Gas Turbine in its various system states*. Since the STPA-Sec method uses a *top-down* approach, the first step in the method is to identify system-level losses and hazards. System-level losses are defined as any loss that would be considered unacceptable from the stakeholder's perspective. The fundamental questions that are asked to guide this step are:

- 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?

Table 1 provides a prioritized list of system losses. Here, (**L-2***) loss of equipment*, is given higher preference over (**L-3**) *loss of power generation*, which is the *primary-value function* of the system. The justification for this prioritization is based on impact severity; an equipment loss would potentially result in a longer-term loss of function of the system than loss of power. These *losses* are deemed as critical to the system and serve as a focus for the analysis.

Table 1 - 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

Table 2 - 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

Based on system losses, system hazards are listed in Table 2. System hazards are conditions or system states that will result in a system loss under worst-case environmental conditions. For instance, falling off a flight of stairs is an accident or loss whereas poor lighting, lack of hand-rail, lack of skid-resistant surface etc., are

system hazards which under worst-case environmental factors such as wet surface, distracted agent etc., could result in a trip or fall (accident or loss).

Based on system hazards, system-level constraints are derived by essentially inverting the system hazards as presented in Table 3. For instance, if a system-level hazard is defined as 'turbine is operating beyond normal operational limits', a system-level constraint can be defined as 'the turbine must not operate beyond normal operational limits'. The key idea is to specify system conditions or behaviors that need to be satisfied in order to prevent the system from moving into a hazardous state that could result in a system loss under worst case environmental conditions. In the current use case, no specific security-related system constraints are defined. Instead, overall system operation is considered from a *top-down* perspective without specifying a singular approach or solution to prevent hazards in order to enable a broader exploration of the solution space further down the analysis. These constraints are ultimately refined during the analysis to comprehensively encapsulate safety and security needs.

Table 3 - System-Level Constraints

Hazards	**Related Losses**	**Constraints**
H-1: Turbine is operating beyond normal operational limits	L-1, L-2, L-3	SC-1.1: Turbine must not operate beyond normal operational limits SC-1.2: If turbine is operating outside limits, then provisions must be in place to detect the violation and limit such operation
H-2: Turbine violates correct sequence of operation	L-1, L-2, L-3	SC-2: Turbine must not violate correct sequence of operations
H-3: Turbine operates without adequately purging combustible gases	L-1, L-2, L-3	SC-3: Turbine must ensure adequate purging of combustible gases
H-4: Turbine loses situational awareness of its operational environment	L-3	SC-4.1: Turbine must not lose situational awareness of its operational environment SC-4.2: If turbine lose situational awareness, alternative sources must be present by design to prevent damage to critical loads due to loss of electrical supply
H-5: Turbine does not meet load requirements	L-3	SC-5.1: Turbine must be adequately sized to meet load requirements SC-5.2: Adequate reserve or backup capacity should be designed for in order to meet load requirements

Step 2 – Model and Control Structure

The next step in the STPA-Sec method is to model the hierarchical functional control structure. At its most fundamental level, the control structure models *control loops* comprised of *controlled processes* and *controllers.* The *controllers* receive *feedback* about the *controlled process,* and then based on some *control algorithm* or logic provide *control actions* to adjust the process. Figure 8 shows a generic form of a control loop; it shows that the controller consists of a *control algorithm* and a *process model.*

Every controller has a model of the process it is controlling – it gives the controller situational awareness of the state of the process it is controlling and enables it to determine the control actions necessary to fulfil its responsibilities; in human controllers, this is the mental model. According to Leveson [2], accidents are sometimes a result of incorrect or malformed process models; a controller takes actions believing a certain state of the controlled process, when in reality the actual state is different than the process model. Therefore, the process model must contain the information necessary for the controller to make *safe* decisions.

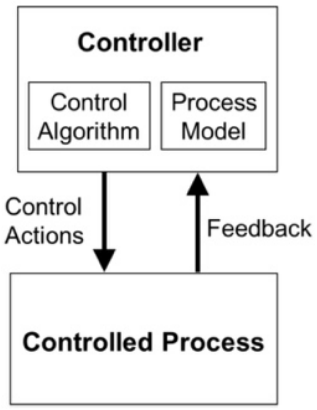

Figure 8 - Generic Control Loop [2]

The STPA-Sec control structure enables modeling not only physical processes, but also human operations, including control of procedures, information and policies. This makes STPA-Sec extremely versatile for cybersecurity applications because it provides visibility of complex functional interactions between the physical systems as well as information flows between control systems, operators, management and even government and regulatory bodies as a whole. Due to the complexity of the system, not every controlled process is modeled in the control structure; instead, abstraction of the physical model is used to convey the essence of the flow of *control actions* and *feedback.*

Figure 9 illustrates the high-level hierarchical functional control structure. In this view, the system under analysis i.e. the turbine and associated equipment, is abstracted as *turbine control* under the boundary of the plant. The figure also illustrates how the operators have the ability to control the plant through both the DCS as well as the equipment's local *Human-Machine Interface* (HMI) screen. The operator actions, in turn, are controlled via operating procedures and instructions by Plant Engineers. Both Plant Engineers and operators report to Operations Management which enforces leadership's enterprise level goals and vision through policies and standards. The leadership, in turn, is controlled by municipal, state and federal regulations enforced via certificates and licensure for operating the plant.

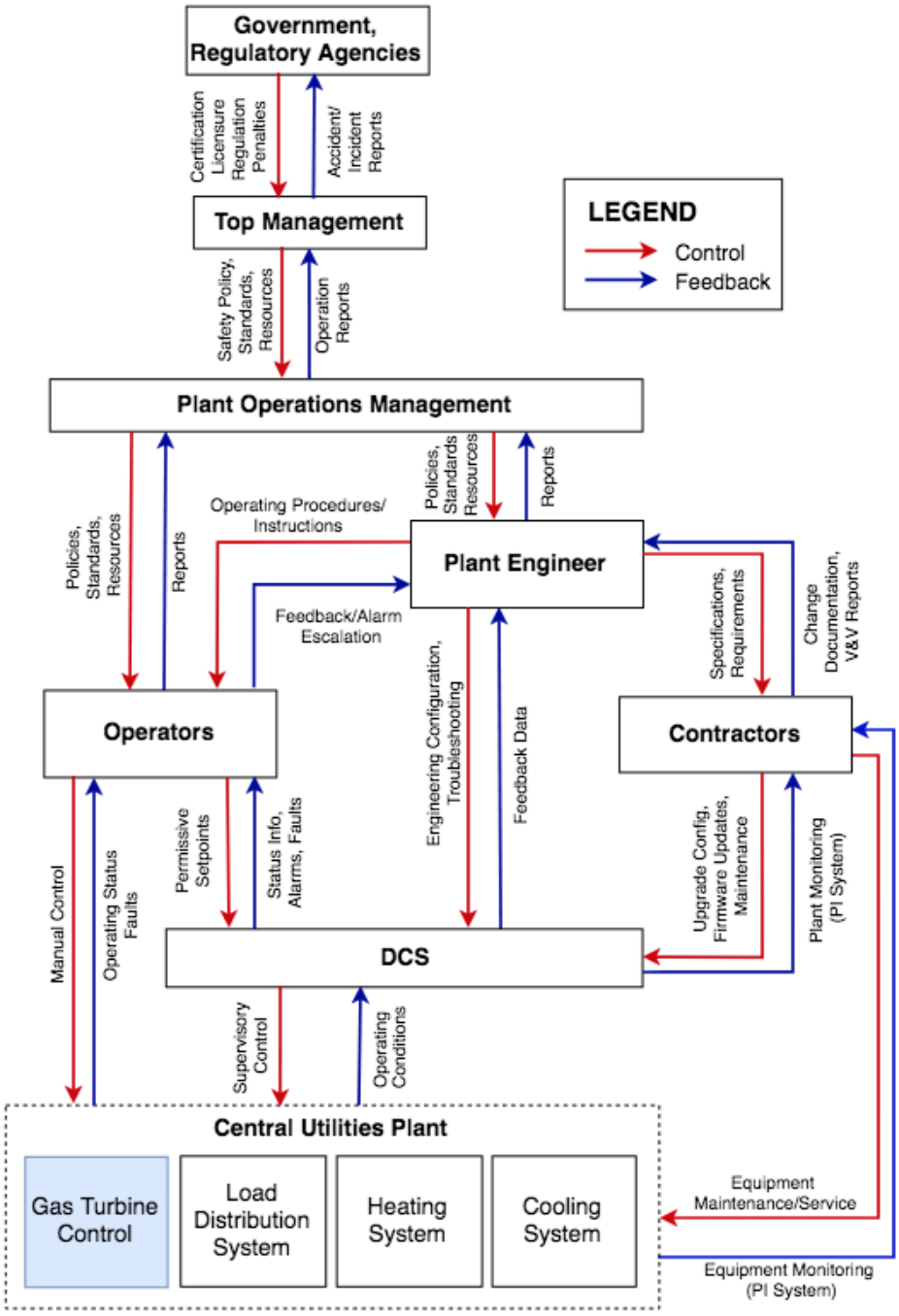

Figure 9 – Overall plant functional control structure

For the purpose of this analysis, we use the *GE Speedtronic Control System* as an illustrative example of turbine controlled processes; it is *assumed* that the plant uses a similar automated system to control turbine operations. We gradually *unpack* the *Gas Turbine Control system* in Figure 10 to uncover more details of the system under analysis. The turbine control system primarily consists of 4 major functions:

1. Fuel Affecting Control
2. Startup/Shutdown Sequence
3. Auxiliary and Special Control (Lube oil, IGV, NOx etc.)
4. Protection System (speed, temperature, pressure etc.)

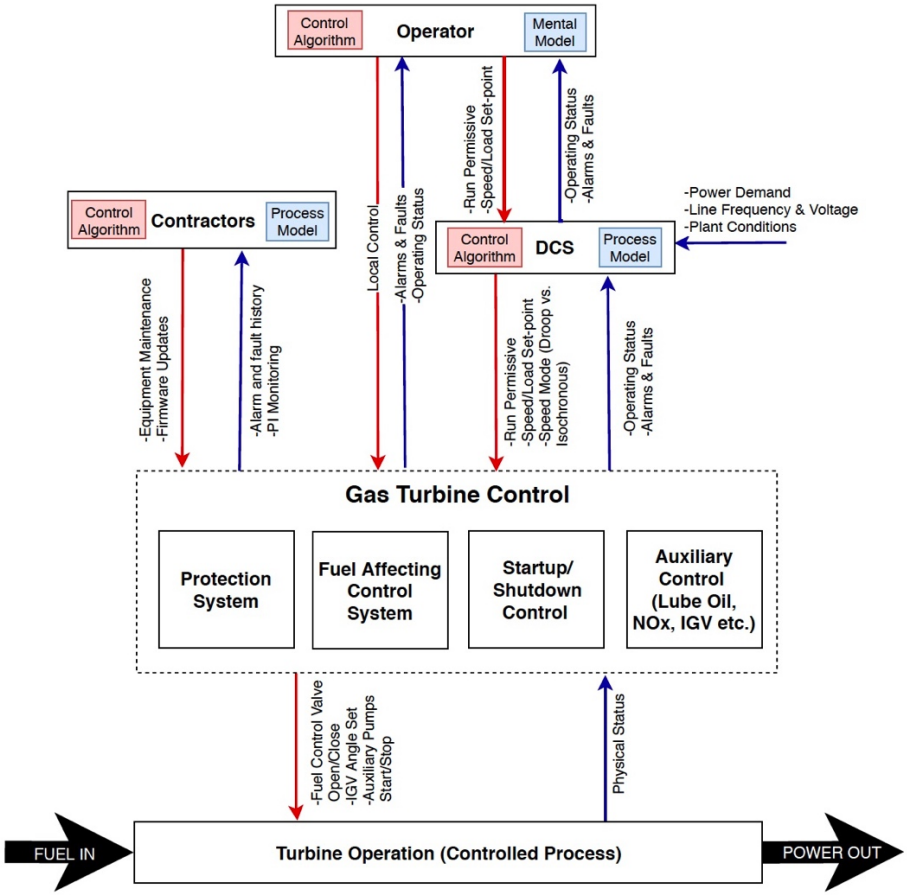

Figure 101 – Gas Turbine Control Loop 'unpacked'

For the purpose of this paper, we focus our attention on a single control loop – the *Fuel Affecting Control System* – and its interaction with the different logical components in the system for analysis. Figure 11 adds additional refinement to the *Fuel Affecting Control System* while abstracting out the *Startup/Shutdown Sequence* and *Auxiliary Control System* under *Other Controllers.*

As the name implies, the *Fuel Affecting Control System* basically modulates the amount of fuel that enters the combustion chamber. It makes this decision by selecting the minimum *Fuel Stroke Reference (FSR)* value from six independent fuel flow *control algorithms* that continuously determine the required amount of fuel that should enter the combustion chamber. The six control algorithms are *startup, acceleration, speed, temperature, shutdown, and manual* control functions as illustrated in Figure 12 [10]; these six independent control algorithms are abstracted out as a *single control algorithm* in Figure 11 inside the *Fuel Affecting Control System,* designated as *'FSR Control Algorithm'*. The function of each of the six control algorithms is summarized in Table 4.

Sensors continuously monitor turbine speed, exhaust temperature, compressor discharge pressure, and other parameters to determine the operating conditions of the unit. This information forms the *process model* of the *Fuel Affecting Control System.* When it is necessary to alter the turbine operating conditions because of changes in load or ambient conditions, the controller modulates the flow of fuel to the gas turbine. For example, if the exhaust temperature tends to exceed its allowable value for a given operating condition, the temperature control system reduces the fuel supplied to the turbine and thereby limits the exhaust temperature [10].

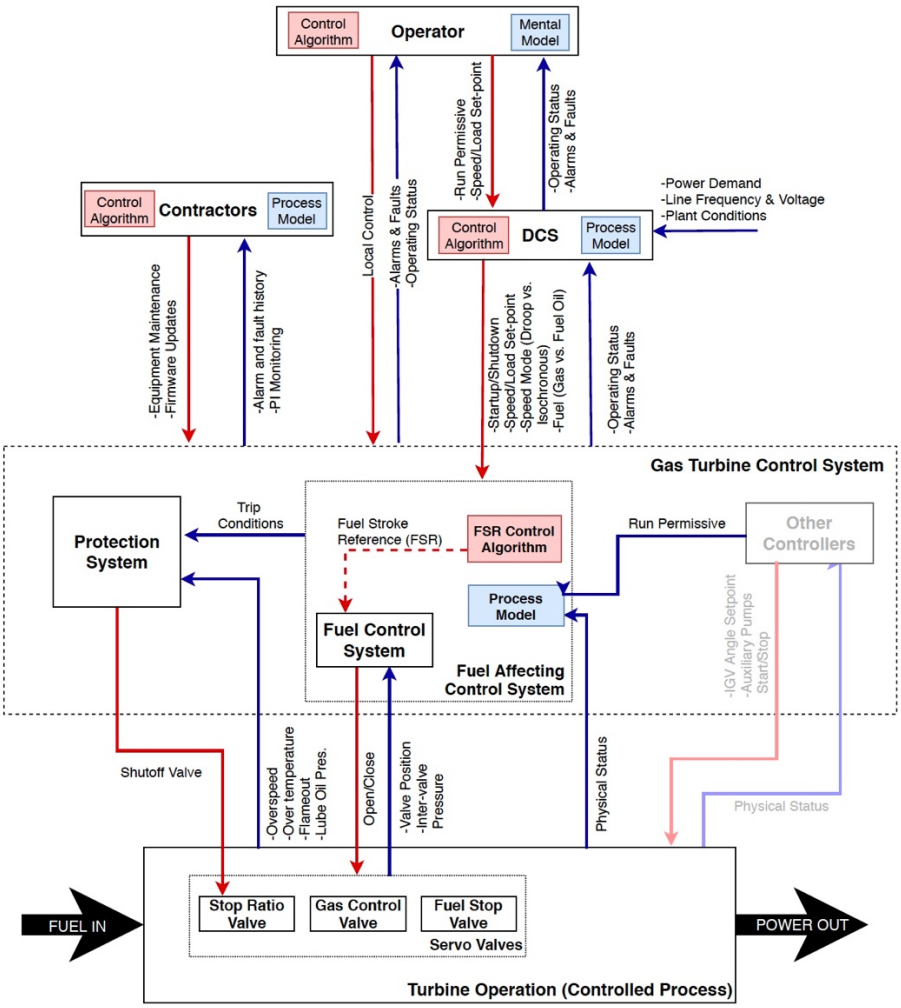

Figure 11 - Overview of the Chiller PLC Controlling Compressor Speed via VFD

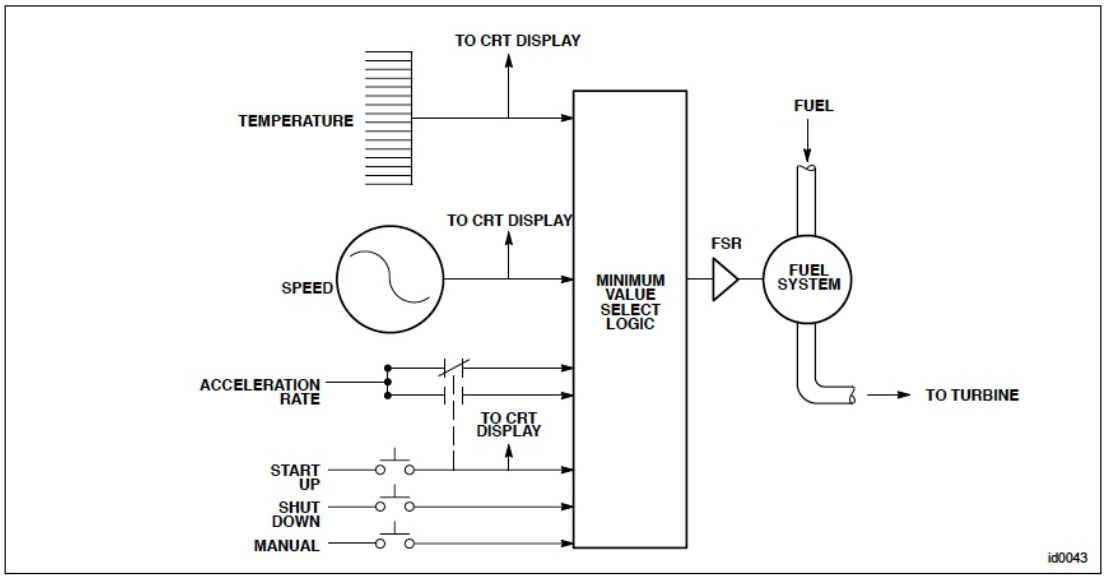

Figure 12 - Simplified Control Schematic [10]

Table 4 - Brief overview of major control algorithms inside the Fuel Affecting Control System [10]

Control Algorithm	**Function**
Start-up Control	This control comprises the ignition, warm up, and the gradual rise of fuel flow to the acceleration.
Speed/Load Control	Fuel flow is adjusted by the speed control loop in such a way that the load demand is maintained.
Acceleration Control	This reduces the fuel flow in case of a too high acceleration of the rotor, Ex. Caused by loss of full load. This prevents excessive vibration.
Temperature Control	This control reduces the fuel flow to prevent overheating of the GT
Shutdown Control	This control reduces the fuel flow during a normal stop (i.e. from the moment that the generator breaker has opened until flame has extinguished).
Manual Control	The operator can enter a value of manually (FSRMAN) in this mode. *In this way, an upper limit for FSR (Fuel Stroke Reference) is established. *If this mode is not used that means FSRMAN = 100 % is the default value.

As previously mentioned, the gas turbine is capable of running on both No. 6 fuel oil (*Bunker C*) as well as natural gas. The *fuel stroke reference (FSR)* value generated by the control algorithm basically consists of two values (*FSR1* and *FSR2*), which is based on operator input for the preference of each fuel (for instance 80% gas and 20% liquid fuel). The *fuel affecting control system,* then sends commands to the respective servo-valve position controllers for the *gas control valve* and the *fuel oil stop valve* based on the calculated ratios as shown in Figure 11. These controllers receive feedback signals about the valve position from the respective linear valve differential transformers (LVDT) and adjust the valve position to match the set-point i.e. FSR value.

There is an additional valve upstream of the *Gas Control Valve*, known as the *Speed/Stop Ratio Valve* (SRV). The SRV has two primary functions – 1) to shut off fuel supply to the combustion chamber in case of a trip condition, and 2) to maintain a constant downstream gas pressure at the gas control valve. The first function is actuated by the *Protection system* on detection of any trip conditions (such as loss of flame, over-temperature, over-speed, low lube oil pressure or surge conditions). The second function is performed by the *Fuel Affecting Control System* by modulating servo position based on turbine reference speed and inter-valve pressure between the SRV and GCV. Figure 13 illustrates this point using a schematic diagram of the gas turbine.

After developing a deeper understanding of the control algorithms and process models of the *Fuel Affecting Control System,* we now abstract out all that detail and present a simplified functional model in Figure 15. The point of this exercise is to understand how the internal processes of a controller interact that cause the higher-level value functions to *emerge*. This approach is known as the *'2 Down, 1 up'* approach in *Systems Theory* and is useful in understanding *emergence* of functions of a system.

Finally, in Table 5, we list each of the controllers that make up the *functional control structure*, along with their primary functions and responsibilities and associated control actions. For the remainder of this analysis, we will focus on a single control action from one controller. The method that is presented below can be emulated for each of the remaining control actions listed in Table 5 for a complete analysis of the turbine.

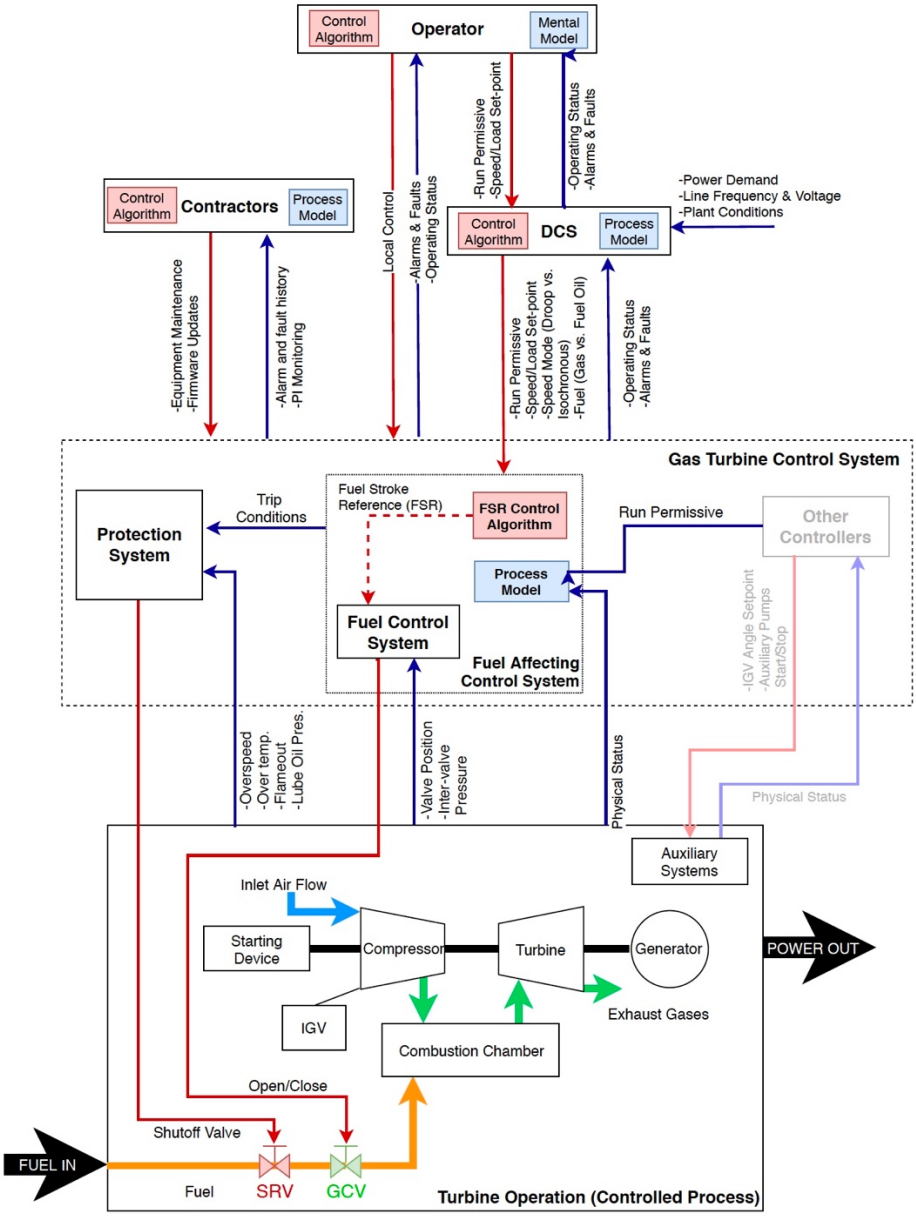

Figure 13 – Zooming into Chiller Controller

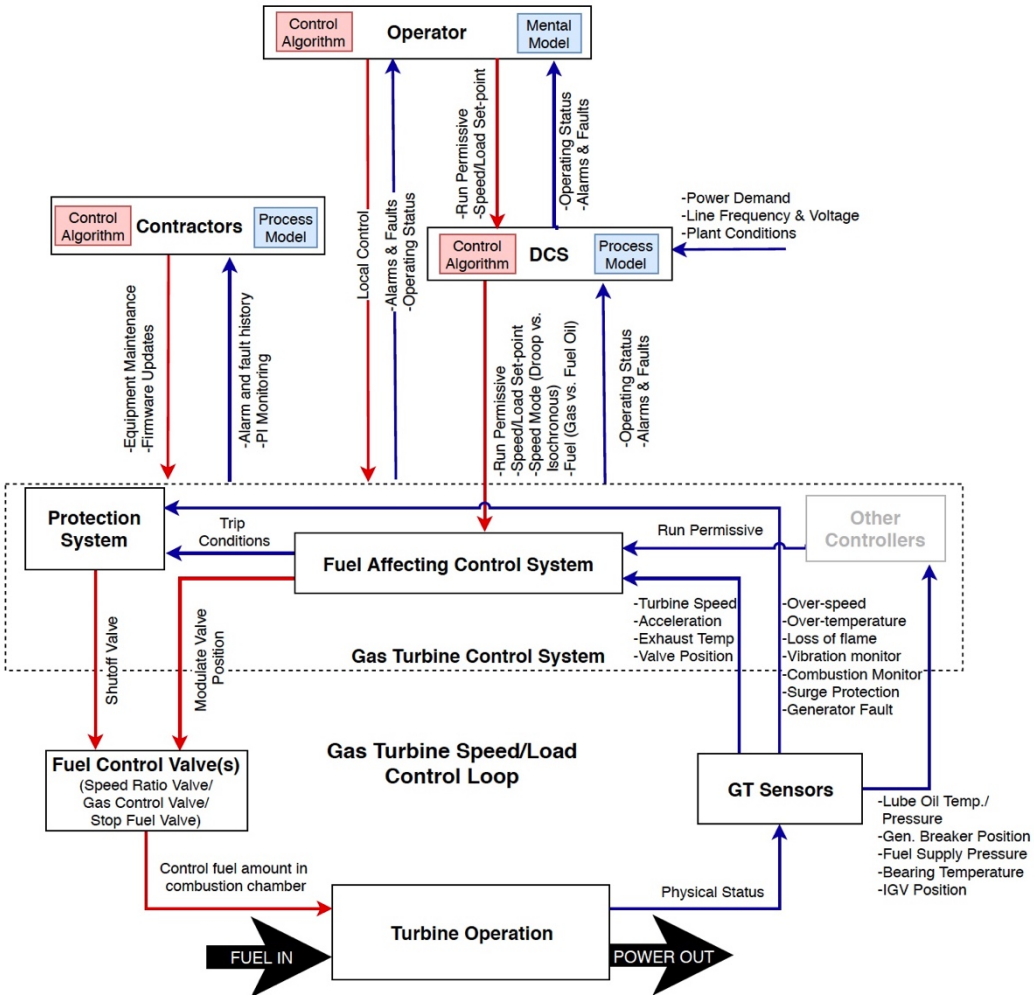

Figure 14 - Gas Turbine Speed/Load Control Loop

Table 5 - List of Controllers, Job functions, Responsibilities and Control Actions

Controller	Function Performed	Safety Responsibilities	Control Actions
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	• 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 duel 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

*This control action is analyzed in the remainder of the paper.

Step 3 – Identify Unsafe Control Actions

The next step in the STPA-Sec method is to identify *Unsafe Control Actions*. The assumption here is that the *control action* in of itself is not unsafe, rather the context in which it is performed, makes it *safe* or *unsafe*. In order to follow a systematic approach in identifying all possible contextual situations where a specific control action would be unsafe, we construct a context table.

We begin by identifying the *process model variables* that the *Fuel Affecting Control System* (i.e. the controller) needs to be aware of, in order to make *safe* decisions. The control action that has been selected for analysis from Table 5 is *'Open Gas Control Valve'*. Based on the information provided in the previous section, Table 6 lists all the relevant process model variables that the controller must account for in making a decision about its control action (i.e. close GCV).

Table 6
System Variables that are relevant for the correct operation of the Chiller Controller and their possible values

#	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

The next step in the analysis is to determine whether the selected control action is hazardous in a given system state or not. A control action can be hazardous if (i) it is not provided, (ii) it is applied at all, (iii) it is applied too early, too late or out of order or (iv) if it is stopped too soon or too late in a given system state [6]. Table 6 shows a *subset* of all possible permutations of the process model variables that are identified as hazardous. Note that this is not an exhaustive list.

Table 7
Control Actions by different system states. A '-' indicates that the status of the variable is irrelevant for the hazardous behavior of the highlighted control action. A control action can be unsafe at any time it is performed in a given state, or only if provided too early or too late or not at all. '1' indicates control action is unsafe in the given state and '0' indicates vice versa.

	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

We will now discuss the selected control action in the context of the various system states shown in the context table. At this stage, we will not take credit for any protective schemes used by the plant; the point is to enumerate all possible vulnerabilities so that a comprehensive understanding of the attack surface and impact severity can be developed.

Startup Sequence

The Startup and Shutdown sequences, unlike speed or temperature control loops, are feedforward control sequences i.e. the gas control valve is opened or closed at preset values during various stages of the startup and shutdown sequence. The *GE Speedtronic* control system typically uses the following speed detectors and speed relays [10]:

–L14HR Zero–Speed (approx. 0% speed)
–L14HM Minimum Speed (approx. 16% speed)
–L14HA Accelerating Speed (approx. 50% speed)
–L14HS Operating Speed (approx. 95% speed)

The speed of the turbine is sensed by magnetic pickups that send a digital '1' or '0' signal to the controller; as the turbine passes through the various speed settings, permissive functions are generated for further actions by the controller. For instance, during startup, the minimum speed detector (L14HM) indicates that the turbine has reached the minimum *firing* speed and initiates a purge cycle prior to the introduction of fuel and ignition. During shutdown, the dropout of the same relay (L14HM) provides several permissive functions for starting various pumps and valves.

Similarly, the high–speed sensor (L14HS) pickup indicates the end of the accelerating sequence and attainment of operating speed, providing the logic for stopping auxiliary lube oil pumps and starting turbine shell/exhaust frame blowers. If there is an under-frequency situation during operation, the L14HS drops out at the under-frequency speed setting, which triggers the generator breaker to open and reset the turbine reference speed to 100.3% (the synchronizing speed) [10].

The point is that the automated controller takes actions based on what it 'perceives' as the current state of the system. If during Startup, the controller does not open the fuel valve upon reaching the designated speed and ignition does not occur, the controller automatically enters a purge sequence and then attempts to re-fire; if it is still unsuccessful, it initiates shutdown [13]. No physical damage occurs in this case; however, the turbine is unable to generate power and deliver its primary-value function *(Hazard H-5).*

The startup sequence is designed to moderate the highest firing temperature produced during acceleration phase. If the controller ramps up fuel flow to the combustors too quickly, it could result in a thermal shock or non-uniform temperature distribution throughout the turbine, causing cracks on turbine casing due to increased thermal fatigue duty on the hot gas path parts *(Hazard H-1, H-2)* [3].

Shutdown Sequence

When normal shutdown is initiated by the operator, the turbine is gradually unloaded by reducing fuel flow to the combustors. At about 5% negative power, the main generator breaker is opened by the reverse power relay which signals to the *Fuel Affecting Controller* to reduce the fuel flow to a minimum value sufficient to maintain flame, but not turbine speed [13]. When turbine speed drops below a defined threshold, the fuel valve position is ramped down to a blowout of one flame detector. The controller remembers which flame detectors were functional when the main generator breaker opened. When any of the functional flame detectors senses a loss of flame, the valve position is decreased at a higher rate until flame–out occurs, at which point fuel flow is completely stopped.

This method of shutdown is known as 'fired' shutdown which is different from a 'trip' shutdown; by maintaining flame down to a lower speed, there is significant reduction in thermal fatigue duty imposed on the hot-gas path parts. In previous generation control systems, the drop out of the minimum speed magnetic pickup (L14HM) would trigger fuel shutoff [10], but it would come at a cost of higher thermal fatigue for the unit.

During a ‘fired’ shutdown, if the fuel control valve is opened after flameout, there is a potential for accumulation of flammable gasses. Such an accumulation could result in internal fires or explosion in the combustor, downstream in the turbine section or in the exhaust ducts *(Hazard H-2, H-3)* [11].

It may be argued that upstream of the *Gas Control Valve (GCV)*, there is the *Speed/Stop Ratio Valve* (SRV) which is what is triggered to shut-off at flameout, instead of the GCV. However, as pointed out by Angle [1], unlike traditional reliability failures, cyber-induced failures are statistically independent; the same cyberattack disrupting the functionality of one valve has the potential to coincidentally disrupt the functionality of an adjacent valve. Hence, inadvertent introduction of fuel to the combustors during shutdown is considered a valid hazardous system state at this stage of the analysis.

Permissive Function (Protection System/Purge Timer etc.)

As illustrated in Figures 11 through 15, the turbine controller has an independent protective system module that protects against over-speed, over-temperature, loss of flame, loss of lube oil and high-vibration conditions. The *Protection System* uses a host of sensors to form its *process model* including magnetic pickups, thermocouples, pressure transducers etc. In the event that anomalous conditions are detected, the *Protection System* trips the SRV or Fuel Stop Valve (in case of liquid fuel), cutting off fuel supply to the turbine.

The implementation of the protective system in GE Speedtronic control systems is such that due to hardware features, the SRV defaults to *‘closed shutoff’* position. It is only when the protective ‘*dump relay’* is energized (by maintaining ‘trip oil’ at a certain pressure) that the servo-valve can control the SRV valve position. When the trip oil pressure is low, the dump valve spring shifts a spool valve to a position which dumps the high-pressure hydraulic oil in the SRV valve actuating cylinder to a lube oil reservoir, enabling the closing spring on top of the valve plug to instantly shut off the valve [10].

Therefore, the availability of *Protection System* permissive function is predicated on the physical availability of the trip function – it cannot be falsified. This is not to suggest that the Protection System controller is incapable of taking unsafe control actions (due to incorrect information or malformed control logic). The point is that in this particular implementation of the *Protection System*, it is inconceivable to have a situation where the controller receives a *protective system* permissive, without the protective system being available in an ‘energized state’. However, other permissive functions are sometimes only implemented in software, which presents a vulnerability as they can be violated or overridden.

Prior to actuating the fuel control valve, the automated controller checks for permissive functions. For instance, when operating in gas fuel-mode, the control system checks for *Protection System, Purge Timer* and *Liquid Fuel Stop Valve* permissive functions [10]. Theoretically, it is only if all three permissive functions are true, that the system allows opening of the GCV.

The *Speedtronic Manual* [5] notes the following *alarm messages* as *‘typical’* in describing the *Fuel Control System*:

1. L60FSGH: Excessive fuel flow on start–up
2. L3GRVFB: Loss of LVDT feedback on the SRV
3. L3GRVO: SRV open prior to permissive to open
4. L3GRVSC: Servo current to SRV detected prior to permissive to open
5. L3GCVFB: Loss of LVDT feedback on the GCV
6. L3GCVO: GCV open prior to permissive to open
7. L3GCVSC: Servo current to GCV detected prior to permissive to open
8. L3GFIVP: Intervalve (P2) pressure low

If we carefully review *alarms* #3, #4, #6 and #7, it may be inferred that it is conceivable that permissive functions are sometimes violated. If, for instance, the gas control valve is opened, violating the *purge timer permissive*, an internal explosion can occur due to accumulation of combustible gases *(Hazard H-2, H-3).*

Operating Mode and Over-firing

Once the generator main breaker is closed onto the power grid, the speed of the turbine is essentially held constant by the grid frequency. Fuel flow to the turbine combustors in excess of that necessary to maintain Full-Speed No-Load (FSNL) condition, results in increased power produced by the generator. At any load lower than the *Base Load* or rated power output of the turbine (i.e. at *Part Load* conditions), the turbine is operating under *Speed Control*; at or above *Base Load,* the turbine is operating under *Temperature Control (see Figure 16).* Under *Speed Control,* the *Fuel Affecting Control System* uses the error signal between the turbine reference speed (or called-for speed) and turbine actual speed to calculate the amount of fuel introduced into the combustor. Thus, the speed control loop becomes a *load control* loop [10].

The temperature that is of interest to the control system is known as the 'firing temperature' – the temperature of the combustion gases as they exit the first stage turbine nozzles. When operating at part-load conditions, the Inlet Guide Vanes (IGV) are used to control this temperature; by modulating IGV, airflow can be increased or decreased to affect 'firing' temperature. At *base-load*, however, the IGV are fully open – hence, 'firing' temperatures can only be controlled by affecting fuel flow to the combustors; this is called *Temperature Control.*

Gas turbines, in general, are operated at the upper limits of operating temperature design limits of the hot gas path parts in order to maximize efficiency. If the operating temperature design limits are exceeded, the unit parts wear out more rapidly and could completely deteriorate, causing severe damage to the turbine. Therefore, opening the fuel control valve when the turbine is operating close to its design temperature limit can have a significant adverse effect on turbine life *(Hazard H-1).* Under normal operating conditions, the exhaust temperature control system acts to control fuel flow when the firing temperature limit is reached. If the exhaust temperature and fuel flow exceed the control limits (to a point 40° F above the temperature control reference), the over-temperature protection system trips the turbine.

Note that the airflow through axial compressors is greatly affected by speed fluctuations; as the compressor speed decreases, air flow decreases and consequently, critical temperatures increase. If while operating at rated power (i.e. Base load), the grid experiences a decrease in frequency, the compressor speed concurrently decreases which reduces airflow, in turn increasing the critical temperatures. Because the unit is operating under temperature control, the *Fuel Affecting Control system* would then reduce fuel flow in order to counteract the temperature increase which is the opposite of what is required during low-frequency excursions (i.e. an increase in power output is required to correct the frequency excursion). Therefore, when running at base load, not providing the open-valve command (to over-fire the turbine at a cost to unit life) when subjected to a low-frequency excursion can result in loss of power incident due to opening of the under-frequency protective relays *(Hazard H-5).*

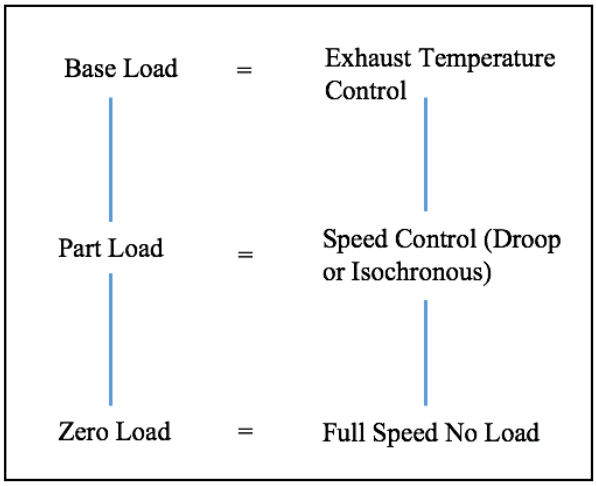

Figure 2 - Different between FSNL, Part Load and Base Load

Turbine Speed and Acceleration

When synchronized with the grid, if there is a sudden loss of load or generator fault, the turbine experiences a sudden increase in speed. If the rotational speed of the turbine exceeds the safe operating limits of the unit, the main shaft and impeller wheels can be pulled apart by centrifugal force. According to McGraorty [12], *"in the worst case, the disintegrating parts can break through the turbine housing, flinging hot, fast-moving shards of metal in all directions. The results of such a failure are always very costly and can be fatal to personnel in the area" (Hazard H-1).*

In a *loss of load* transient, the *Fuel Affecting Control System* reduces the Fuel Stroke Reference (FSR) to the minimum value required to maintain flame. If the over-speed condition is not arrested by ramping down the gas valve position, the *Protection System* trips the turbine by shutting off fuel supply to the combustors. If on the other hand, FSR is ramped down to a flameout which is not detected by the *Protection System*, combustible gases can accumulate in pockets downstream of the combustors which could result in internal explosion or fires *(Hazard H-3).*

Older generation gas-turbines, including the one operated at the plant, are equipped with a further protective device against over-speed – a mechanical bolt assembly. In this setup, a bolt assembly actuated by centrifugal force, overcomes the spring force to activate the hydraulic trip mechanism.

It should be noted that newer gas turbine control systems are replacing the mechanical bolt assembly over-speed protection with additional electronic over-speed protection schemes. As advertised by ABB [16], *"there are significant advantages to the use of electronic overspeed protection system when compared to mechanical trip bolts…a failure during a mechanical bolt test is 3 times more likely than during normal operation…"*

Fuel Mode

As described earlier, the gas turbine at the plant is designed to operate on both liquid and gaseous fuel and is equipped with controls to enable transfer from one fuel to the other on operator command while the unit is online. The unit is capable of mixed-fuel operation. For either mixed-fuel operation or fuel changeover, based on operator input settings, the *Fuel Stroke Reference (FSR)* calculated by the *Fuel Affecting Control Algorithm* is passed onto a *fuel splitter* which divides it into two signals and passes it on to the respective

liquid and gas servo-valves. Figure 16 shows implementation of fuel transfer operation by the GE Speedtronic control system.

For illustrative purposes, the sequence of operations for a *liquid-to-gas* transfer can be briefly described as follows (a similar algorithm is followed for *gas-to-liquid* transfer as well).

- Operator changes fuel selection to *gas* on the control panel
- Control system checks if permissive functions for providing the transfer as well as gas valve operation are true
- FSR for liquid fuel remains constant at initial value, but FSR for gas is increased to a value slightly above 0% to bleed down the inter-valve volume in case a high pressure was entrained
- A time delay of 30 seconds is applied to fill the gas supply line
- The FSR for gas is ramped up while the FSR for liquid fuel is ramped down; completed in ~30 seconds
- Fuel oil stop valve is closed and liquid purge sequence is initiated to prevent coking of the liquid fuel nozzles while operating on gas fuel

If during fuel changeover, the *gas control valve* fails to open after the pre-programmed purge timer expires, the decrease in liquid fuel FSR would initially result in a decrease in load and if not corrected by the operator, would result in the turbine slowing down and losing synchronization with the grid *(Hazard H-5)*. If the gas control valve opens before the purge timer expires, a load spike would occur. If the turbine is already operating at rated base-load conditions, a load spike would result in over-firing the turbine, reducing unit life, deteriorating turbine blades etc. If during fuel changeover, the flow-rates of the fuels are not controlled properly, internal fire or explosions could occur in the combustor, downstream turbine section or exhaust duct *(Hazard H-1, H-2, H-3)* [11].

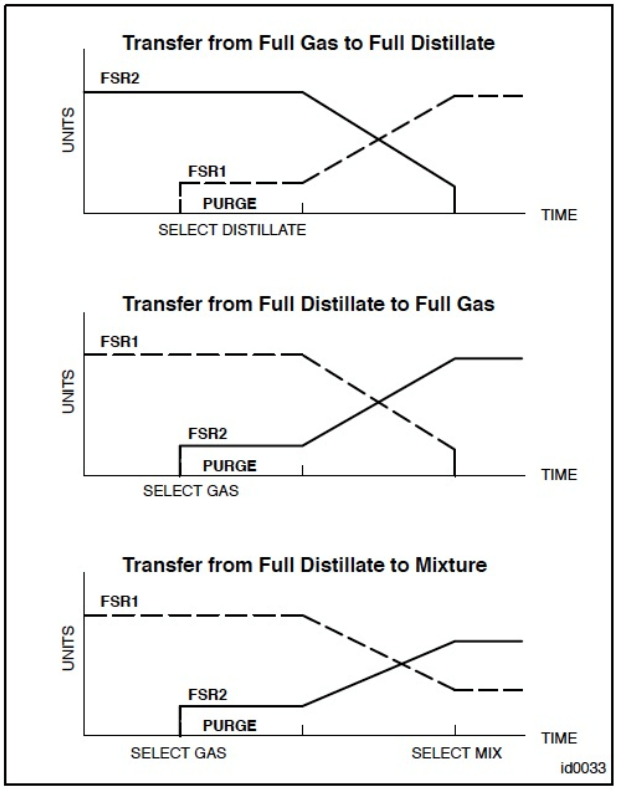

Figure 16 - GE Speedtronic Mark V Fuel Transfer operations

By constructing the context table, we systematically analyzed a single control action (i.e. open gas control valve) in the context of various system states as identified by the controller's process model. We are now in a position to generate a set of *unsafe control actions* as listed in Table 8.

Table 8
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]	

Step 4 – Identify Loss Scenarios

In the previous subsection, we contextualized how under various system states a given control action can become hazardous; essentially, we identified the set of constraints that, if violated, would move the system into a hazardous state. In this section, we identify the factors that would *cause* the constraints to be violated. This is done by generating a *hierarchical* list of *loss scenarios* i.e. a textual representation of causal factors that can lead to *unsafe control actions* resulting in hazardous system states that can potentially culminate into system losses. According to Levenson [2], two types of loss scenarios must be considered:

A. Scenarios that lead to *unsafe control actions*
B. Scenarios in which *safe* control actions are improperly executed or not executed altogether

Scenarios leading to *unsafe control actions* could be a result of *Unsafe controller behavior* or *inadequate feedback;* alternatively, scenarios leading to improperly executed or altogether ignored *control actions* could be a result of the *control path* or the *controlled process* itself as listed in Table 9 and illustrated schematically in Figure 17 [2]:

Table 9 - Generation of Loss Scenarios [2]

A. Identifying Scenarios that lead to Unsafe Control Actions

1. *Unsafe Controller Behavior*

- **a.** Failure involving controller
- **b.** Inadequate Control Algorithm
  - **i.** Flawed implementation of the specified control algorithm
  - **ii.** Specified control algorithm is flawed
  - **iii.** Specified control algorithm becomes flawed over time due to changes/degradation
- **c.** Inadequate process model
  - **i.** Controller receives incorrect feedback/information
  - **ii.** Controller receives correct feedback/information but interprets it incorrectly or ignores it
  - **iii.** Controller does not receive feedback/information when needed (Delayed or never received)
  - **iv.** Necessary controller feedback/information does not exist
- **d.** Unsafe Control input (from another controller)

2. *Inadequate Feedback and information*

- **a.** Feedback or information not received
  - **i.** Feedback/info sent by sensor but not received by controller
  - **ii.** Feedback/info is not sent by sensor but is received by controller
  - **iii.** Feedback/info is not received or applied to sensor
  - **iv.** Feedback/info does not exist in control structure or sensor does not exist
- **b.** Inadequate feedback is received
  - **i.** Sensor responds adequately but controller receives inadequate feedback/info
  - **ii.** Sensor responds inadequately to feedback/info that is received or applied to sensor
  - **iii.** Sensor is not capable or not designed to provide necessary feedback/info

B. Identifying Scenarios in which control actions are improperly executed or not executed

3. *Scenarios involving the Control Path*

- **a.** Control Action not executed
  - **i.** Control action is sent by controller but not received by actuator
  - **ii.** Control action is received by actuator but actuator does not respond
  - **iii.** Actuator responds but the control action is not applied to or received by the controlled process
- **b.** Control Action improperly executed
  - **i.** Control action is sent by controller but received improperly by actuators
  - **ii.** Control action is received correctly by actuator but actuator responds inadequately
  - **iii.** Actuator responds adequately, but the control action is applied improperly at the controlled process
  - **iv.** Control action is not sent by controller, but actuators or other elements respond as if it had been sent

4. *Scenarios related to the Controlled Process*

- **a.** Control action not executed
  - **i.** Control action is applied or received by the controlled process but the controlled process does not respond
- **b.** Control action improperly executed
  - **i.** Control action is applied or received by the controlled process but the controlled process responds improperly
  - **ii.** Control action is not applied or received by the controlled process but the process responds as if the control action had been applied or received

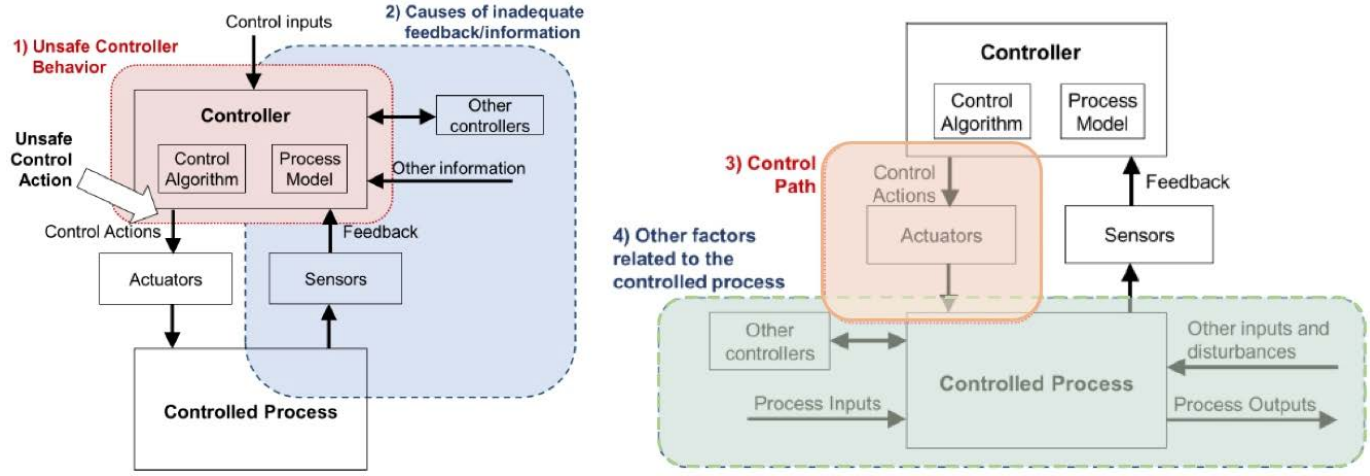

Figure 17 – Factors that can result in a) unsafe control actions b) control actions not or improperly executed [2]

A list of *Loss Scenarios* is presented in Table 12. Due to space limitation, we only present 3 loss scenarios. The first loss scenario describes how a flawed implementation of the *Fuel Affecting Control System* algorithm coupled with an inadequate *process model* of the *Protection System* could result in a fire or explosion leading to death, dismemberment, loss of equipment as well as loss of power generation.

The second scenario describes how a malformed control algorithm of the *Protection System* coupled with a malformed process model of the *Fuel Affecting Control System* could in fact lead to over-firing of the gas-turbine which would result in failure of turbine blades by creep rupture over time, greatly reducing unit life; such a loss scenario would manifest itself slowly over time, in contrast to the first scenario which would manifest itself in an instantaneous, catastrophic fashion.

Finally, the third scenario describes how a 'trigger' event (such as opening of the generator breaker), coupled with a malformed process model of the *Fuel Affecting Control System* (that deceives the controller into 'believing' that it needs to increase speed when in reality it is required to reduce speed) and a malformed control algorithm of the *Protection System* (i.e. a re-programming of critical speed set-points) can result in over-speeding the turbine, resulting in catastrophic failure. Note that for each *unsafe control action* identified in Table 8, several attack scenarios can be generated by systematically following the *causal factors list* provided in Table 9.

Table 10 - Loss Scenarios for Chiller PLC Control Loop

UCA-8: FACS opens Gas Control Valve, out-of-order, after flameout --> [H-2, H-3]

	Loss Scenario	Associated Causal Factors	Rationale	
1.0	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. The *Protection System* does not intervene to shut off the valve despite recording flameout condition.	1. Malformed control algorithm: - Flawed implementation of the specified control algorithm (LS-1.b.i)	-Malicious command manipulation on FACS (N-1) modifies the controllers auto shutdown sequence to undertake unsafe actions i.e. open fuel control valve when the opposite is required	Unsafe Controller Behaviour
		2. Inadequate process model: - Protection system (controller) receives correct feedback (i.e. loss of flame) but ignores it or interprets it incorrectly (LS-1.c.ii)	-The protection system is programmed to issue a trip command for flameout condition during operation. However, during *shutdown sequence, loss of flame* condition is expected and hence the protection system considers this as routine occurance	

System Loss: Depending on how long the *Gas Control Valve* stays open after flameout, a fire or explosion would ensue causing significant damage to the gas turbine from excessive temperatures or thermal/mechanical shock. Such a scenario would result in potentially death, dismemberment, loss of equipment, loss of power generation as well as loss of revenue.

UCA-3: FACS opens *Gas Control Valve* when operating at design temperature limit (leading to overtemperature conditions) --> [H-1].

	Loss Scenario	Associated Causal Factors	Rationale	
2.0	During part-load operation, FACS unsafely opens the *Gas Control Valve* beyond design temperature limit. The IGV control fails to act to control temperature. Despite the existence of the over-temperature trip condition, the *Protection System* does not intervene to shut off the fuel control valve.	1. Malformed process model: - FACS receives correct feedback/information but interprets it incorrectly or ignores it (LS-1.c.ii), thus unsafely opening *Gas Control Valve* when unit is operating at design limit	-Malicious feedback manipulation at FACS from sensors causes the controller to assume incorrect state and hence unsafely opens the *Gas Control Valve* . For instance, incorrect actual and reference temperatures are fed to the controller, causing it to believe it has 'room' to open the control valve	Unsafe Controller Behaviour
		- IGV controller receives correct feedback/information but interprets it incorrectly or ignores it (LS-1.c.ii) i.e. incorrectly believes unit is operating at base-load, and hence IGV are fully open and cannot be used to control temperature when in reality, they should be used since the unit is operatin in part-load	-Malicious feedback manipulation at IGV controller causes controller to assume incorrect operating mode	
		2. Malformed Control Algorithm: - Protection System's specified control algorithm is flawed (LS-1.b.ii); the controller's reference over-temperature limit is much higher than the design temperature limit	-The protection system controller is also simultaneously compromised; 'trip' values are maliciously modified to disable safety-critical control action when trip conditions occur. This is possible because the specific safety controller used in this application allows remote access and reprogramming of 'trip' values stored in memory	

System Loss: If operation at elevated temperatures is not arrested, gas turbine blades would experience creep rupture near mid-span. Such a scenario would result in loss of equipment, loss of revenue as well as loss of power generation ability. According to Eshati, over-firing the gas turbine is extremely detrimental to blade creep life and translates into a 70% reduction in creep life. Depending on the temperature that is achieved, such a loss scenario, typically, does not manifest itself instantaneously, rather would insidiously impact plant life, over the course of several months.

UCA-6: FACS opens *Gas Control Valve* when there is a sudden loss of load or generator fault, driving the turbine to overspeed conditions --> [H-1]

	Scenario	Associated Causal Factors	Rationale	
3.0	While synchronized to the grid and operating at part- or base-load, generator breaker is 'inadvertently' tripped; FACS, instead of closing the *Gas Control Valve*, opens the valve further, driving the turbine to overspeed conditions. *Protection System* does not intervene to arrest the overspeed trip condition.	1. Unsafe Control input (LS-2.d): - Generator Breaker is opened from the DCS	-Malicious command injection by Man-in-the-middle threat actor sends command to open generator breaker.	Unsafe Controller Behaviour
		2. Malformed process model: - FACS receives correct feedback/information but interprets it incorrectly or ignores it (LS-1.c.ii), thus unsafely opening *Gas Control Valve* when the generator breaker is opened	-Malicious feedback manipulation at FACS from sensors causes the controller to assume incorrect state and hence unsafely opens the *Gas Control Valve* . For instance, incorrect actual and reference speed are fed to the controller, causing it to believe it has 'room' to open the control valve	
		3. Malformed Control Algorithm: - Protection System's specified control algorithm is flawed (LS-1.b.ii); the controller's reference over-speed limit is much higher than the design speed limit	-The protection system controller is also simultaneously compromised; 'trip' values are maliciously modified to disable safety-critical control action when trip conditions occur. This is possible because the specific safety controller used in this application allows remote access and reprogramming of 'trip' values stored in memory	

System Loss: Such a scenario would cause the rotational speed of the turbine to exceed safe operating limits, causing the main shaft and impeller wheels to be pulled out by centrifugal force to catastrophic failure. In the worst case, the disintegrating parts would break through the turbine housing, flinging hot, fast-moving shards of metal in all directions. According to Herschberger & Blanchard [15], during an overspeed event, operators only have 10 milliseconds to react and trip the bolt.

VII. DISCUSSION

In the previous section, we identified scenarios under which *unsafe control actions* violate constraints that move the system into a hazardous state, culminating into system-level losses. We will now analyze how new technical as well as socio-organizational constraints can be defined systematically and enforced at various levels of the hierarchical control structure to prevent *unsafe control actions* from manifesting into system-level losses.

Recall that the underlying assumption in the analysis is that the turbine control system and/or DCS has the potential to be infiltrated by malicious actors at will, despite the existence and implementation of 'typical' network security features, such as *air-gapping* the control system from the public internet, using firewalls, De-militarized Zone (DMZ) routers to isolate the control system etc. Therefore, the proposed mitigation strategies do not focus on the network architecture of the control system; instead, they focus on eliminating the hazards and vulnerabilities or managing the impact of the hazards.

Scenario 1 Mitigation Strategies – *Valve Position Indicator*

Scenario 1 (from Table 10) is a result of malicious manipulation of the shutdown control sequence of the turbine controller, such that the *gas control valve* is left open, undetected, until uncontrolled combustion results in a fire or explosion. Such a scenario can be prevented by active, independent, monitoring of the gas control valve during operation. The recommendation is to install a *valve position indicator* on the *gas control valve* that provide a visual reference to the operator during operation, such as a LED activated by a proximity sensor (or by other completely mechanical methods) when the valve position is fully opened or closed. Figure 19 shows an example of one such visual valve indicator.

Figure 3 - Valworx Valve Position Indicators

Looking at the functional control structure in Figure 19, one can easily identify critical nodes and feedback loops where additional constraints are required beyond the technical layer to prevent the system from entering a hazardous state. For instance, a *valve position indicator* installation has to be coupled with a real-time camera feed to the operator's console along with the operators ability to take corrective action (to shut off the valve) once an anomalous condition is observed. In addition, the operating procedure needs to be revised by the *Plant Engineer* to include a visual confirmation by the operator that the valve is in the correct position (indicating valve closure) *prior* to de-energization of the trip circuit (which would physically prevent spurious reopening of the valve) during shutdown sequence.

In addition, Operations Management needs to ensure the addition of new equipment is coupled with training of the crew in operating the new equipment. It also needs to enforce procedural compliance through spot checks and audits. *Plant Engineer* needs to incorporate verification and validation testing as well as maintenance activities for the new equipment into the standard operating procedures. In some cases, the validation testing would require the unit to be brought offline; this would have a financial impact which has

to be sanctioned, approved and supported by the operational management. The operational management may have conflicting priorities between reduction of operational costs and security; there may be situations where, in an effort to reduce costs, some maintenance activities (such as valve indicator testing) are considered superfluous and consequently waived by management; but such actions would dwindle the operational readiness of such systems.

Therefore, in order to enforce controls on the plant management, leadership has a responsibility to install an independent functional group with the mandate to oversee and audit all cybersecurity policies and standards and ensure that they are not violated in the interest of operations. This is similar to the function of *Quality Assurance* in many corporations, where the Director of Quality Assurance functionally reports directly to the CEO and is hierarchically at the same level as the Director of Engineering or Director of Operations; the reason for doing this is so that quality is not compromised and the Quality Engineers are able to dispense their responsibilities without undue operational pressure; a similar mandate for *cybersecurity* is required.

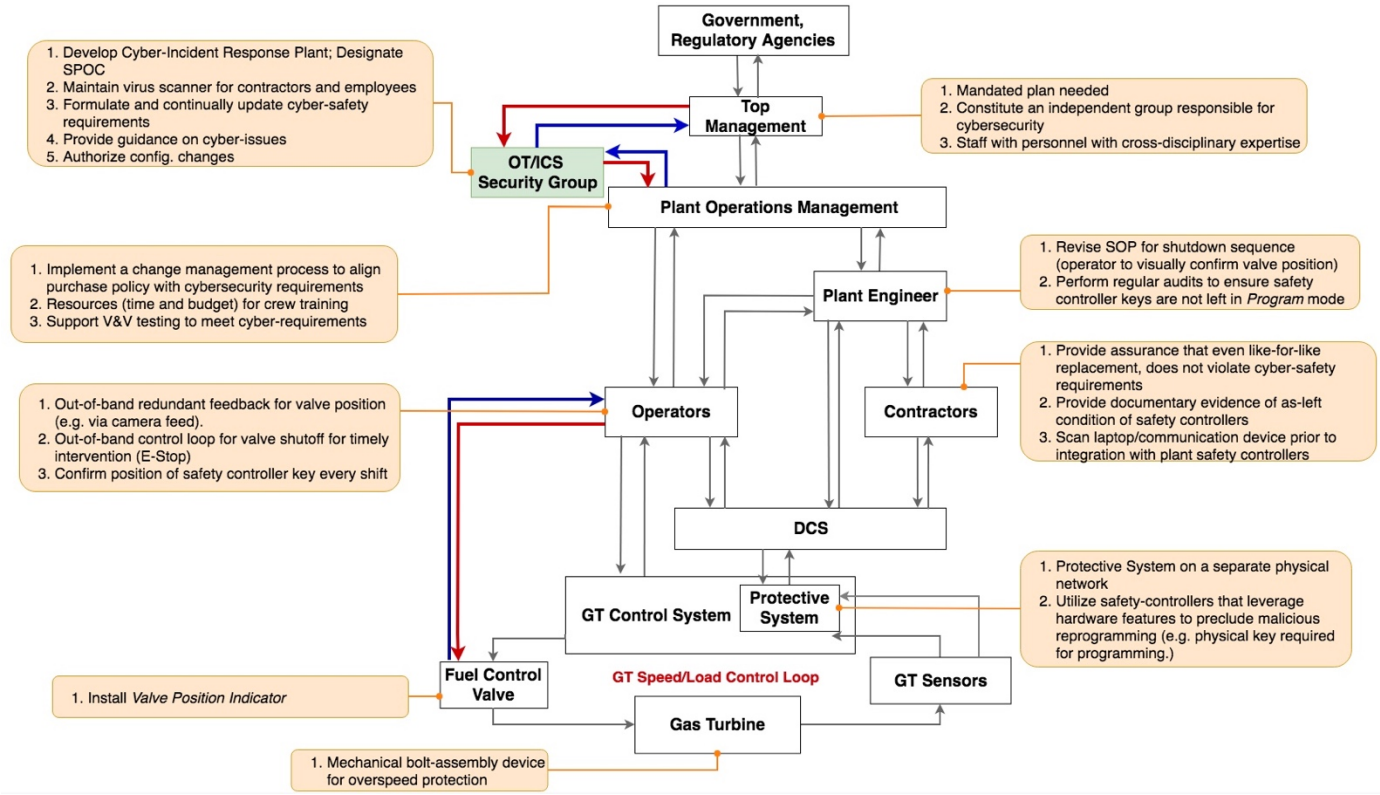

Figure 19– Summary of new requirements superimposed on the simplified control structure

Figure 19 shows a summary of the proposed mitigation strategies superimposed on the hierarchical control structure of the gas turbine *Fuel Control Loop*. Some of these requirements may appear obvious and some may already have been implemented at the plant as a safety measure to ensure equipment *reliability and availability*. However, it is important to reimagine these requirements in the context of *cybersecurity*. A vendor or contractor may not see the implication of replacing some mechanical safety feature with an equivalent software interlock, but such an action would violate the cyber-safety constraint that could result in a loss.

Scenario 2 Mitigation Strategies – *Safety-Controllers*

Scenario 2 (Table 12) is a result of a malformed turbine controller process model which *deceives* the controller (into *assuming* an incorrect process state) while the protection system is emasculated by reprogramming of over-temperature 'trip' set-points; it fails to act even on detection of unsafe operating temperature limits. This scenario is modeled after the *Triton Malware* attack that targeted the Safety Instrumented System (SIS) controllers at a Saudi Industrial facility in 2017 and brought about the shutdown of a critical infrastructure organization [9].

In order to prevent such a loss scenario, it is recommended to leverage hardware features that provide physical control over ability to program safety controllers. For instance, utilize controllers that require a physical key to manipulate program settings as shown in Figure 20 [9]. But note that this technical constraint would be unsuccessful in thwarting a cyberattack if the *controller key* is left in the *PROGRAM* mode.

Therefore, at the next level of control above the turbine automated controller (i.e. at the operator level), new requirements need to be enforced through procedures that require operators to visually confirm every shift that the controllers have not inadvertently been left in the *PROGRAM* mode. As in the previous mitigation plan, the next higher-level controller (i.e. the *Plant Engineer*) needs to *regularly* audit and inspect the safety controllers to correct *key* configuration.

The functional control structure also shows *contractors* interfacing with the turbine controls. As with any other large power plant or process control facility, contractors play a key role in maintaining equipment because of their domain expertise. However, different contractors and vendors maintain different components of the system and their expertise are not always cross-functional; it is at the *interfaces* between contractors where the largest potential for errors and miscommunications exist. We define two requirements for contractors to prevent unsafe behavior of the safety controllers:

1) At the completion of work on a safety system, the contractor must provide documentary evidence that the controller is left in a *safe* state (i.e. controller key in the safe position)
2) Prior to interfacing with the safety controller, the contractor must prove that the laptop being used has been scanned for viruses, malware etc., using the asset owner's equipment

Figure 20 - Schneider Electric Triconex Safety Controller [9]

In the previous subsection, we proposed mandating an independent entity (OT/ICS Security Group) that takes ownership of ICS security at the plant. A new requirement for this group would be to maintain the *virus scanner* (with the latest virus definitions) for use by the contractors. Finally, Operations Management would be responsible for instituting a formal Change-Management program to replace all safety controllers with new controllers that leverage physical features for preventing reprogramming of trip-setting etc. All the requirements described above are summarized in Figure 21 below.

Scenario 3 Mitigation Strategies – Mechanical Bolt Assembly

Scenario 3 is a result of an unmitigated *overspeed* condition, resulting from a sudden loss of load. According to Herschberger & Blanchard [14], operators only have 10 milliseconds to react and trip the bolt in case of an overspeed condition. The gas turbine operated at the plant, currently employs an older-generation, mechanical-bolt assembly overspeed device. Note that this mechanical device is a backup to the turbine protection system, which is a backup to the turbine control system i.e. third line of defense.

However, there is a general trend in the industry towards discontinuation and even replacement of the mechanical bolt assembly with a redundant digital protection system [14, 15, 16]. Several reasons are stated for this trend, such as:

1) Regular maintenance is required on the mechanical device which is costly
2) Turbine has to be taken offline for the test
3) Catastrophic failures occur during overspeed trip tests – according to R. Torok [16], insurance industry estimates that 50% of catastrophic overspeed events occur when the mechanical overspeed system is being tested

However, the recommendation here is to treat the mechanical backup as a cyber-requirement. Earlier, we stated that some of the mitigation strategies may appear redundant to OT personnel, but they have to re-imagined from the context of cybersecurity, not availability or reliability.

This highlights another key requirement; based on the earlier proposed organizational change to mandate *OT/ICS Security group* as the single body responsible for ensuring cybersecurity, it is further proposed that all configuration changes (such as replacing the backup mechanical bolt) must be expressly approved by the *OT/ICS Security group*. Unlike traditional organizations where OT security is delegated to IT professionals, a new generation of cross-disciplinary security professionals is required who intimately understand OT as well as IT security. If staffed correctly, such a group would not an impediment to plant operations, rather an enabler of good cyber-practices and culture.

Finally, the mitigation strategies and requirements discussed for Scenarios #1 and #2 collectively apply to Scenario #3 as well. If the *valve position indicator* is not in the closed position after a sudden loss of load transient, the operator should use the manual E-Stop to shutoff the fuel control valve. Similarly, if the safety controllers are configured as described in the previous subsection, it is unlikely for the overspeed trip set-points to be maliciously reprogrammed.

It is important to recognize that even with a limited STPA-Sec analysis, we have derived key targeted requirements which prevent system-level losses. Note also, that by reimagining *losses* as a *'loss of control'* problem, we systematically derived new requirements by analyzing *unsafe control actions* in the context of the *hierarchical control structure*. The new requirements affect system design, ultimately making it more resilient against cyber-physical attacks, which was the goal of the analysis.

VIII. CONCLUSION

In this paper, we analyzed a single representative control loop (the fuel control loop) of an archetypal industrial control system (i.e. the gas turbine) at a small-sized power plant in the context of cybersecurity using a vulnerability analysis method based on *Systems Thinking*. Starting with *system-level losses* and hazards we traced the functional control structure of the plant and abstracted out the gas turbine fuel affecting control loop for a detailed analysis of a single control action under various system states. We then generated loss scenarios under which *unsafe control actions* would result in *system-level losses*. Finally, we proposed new constraints at various layers of the functional control structure (starting at the process layer and going all the way back up to the enterprise level) to prevent the system from entering *unsafe* system states.

In the process of performing this analysis, we uncovered several insights about the system (i.e. the gas turbine) which were not obvious at the onset of the analysis; such as, the selection of a component at the process layer, is ultimately linked to a policy level decision at the enterprise level. For instance, the selection of *safety controllers* of certain types (such as controllers with ability to be reprogrammed over network), though improves convenience through increased functionality, simultaneously introduces new vulnerabilities for the system. Successful elimination of this vulnerability requires an organizational change management process that not only ensures that existing *safety controllers* meet the cyber-safety specification, but that new purchases are systematically vetted out for such vulnerabilities. In this way, the success of the proposed constraint requires the support and cooperation of additional office functions, such as approval by a dedicated *OT/ICS Security Group*. Typical hazard or vulnerability analysis methods focus primarily on the technical aspect of the system, rather than taking a broader view of the system as a whole.

In addition, the analysis highlighted missing feedback loops both for components (e.g. independent *valve position feedback* to operator via camera feed) as well as for processes (e.g. re-validation of the security architecture of the plant due to reconfiguration or changes to plant equipment). By analyzing *unsafe control actions* in the context of the *hierarchical control structure*, insights and mitigation strategies *emerged almost naturally*. This is because the *hierarchical control structure* provided a bird's eye view of the entire system by combining organizational, human and technical controllers in a single diagram, enabling a broader view of the system along with key leverage points for enforcement of the proposed constraints.

Using a top-down approach and starting with system-level losses, the analysis always stays focused on the bottom-line i.e. what constraints, if violated, would result in the system entering an unsafe state that could propagate into system-level losses. This enables the STPA-Sec method to be more strategic in identifying the most critical vulnerabilities. Furthermore, since each step of the analysis is always tied back to system-level losses, the method provides traceability between recommendations and losses. This helps to communicate with policy and decision-makers who can more clearly see the link between recommendations and vulnerabilities and how the vulnerabilities are linked to system-level losses.

In conclusion, using the analogy of the human body, just as it is impossible to avoid all contact with infections and never catch a disease, it is impossible for an industrial control system to be under constant cyberattack and never have its network defenses breached. Therefore, the system has to be designed so that it is resilient against the effects of the attack. STPA-Sec provides a well-guided and structured analytical method to identify vulnerabilities and derive requirements to improve resilience against attacks.

ACKNOWLEDGEMENTS

We greatly appreciate the cooperation and information provided by the operators at the plant studied.

This research was supported, in part, by the US Department of Energy under Award Number DE-OE0000780, the MIT Energy Initiative Seed Fund Program, and members of the Cybersecurity at MIT Sloan consortium.

IX. REFERENCES

[1] M. Angle, "Identifying and Anticipating Cyber Attacks that could cause Physical Damage to Industrial Control Systems", August 2017, [Online]. Available: http://web.mit.edu/smadnick/www/wp/2017-14.pdf (Last Accessed: July 30, 2018)

[2] N. Levenson, STPA Handbook, March 2018

[3] Poursaeidi, E & Taheri, Morteza & Farhangi, A. (2014). "Non-uniform temperature distribution of turbine casing and its effect on turbine casing distortion", Applied Thermal Engineering. 71. 433–444. 10.1016/j.applthermaleng.2014.07.019.

[4] T. Strand, "Industrial Gas Turbine Control", April 2006, Siemens [Online]. Available. http://energy.kth.se/courses/4a1626/ahpt2006/GTcontrol.pdf (Last Accessed: Sep 22, 2018)

[5] E. Colbert, "Security of Cyber-Physical Systems", Journal of Cyber Security and Information Systems, Volume 5, Number: 1 – Cyber Science & Technology at the Army Research Laboratory (ARL), January 2017. [Online]. Available: https://www.csiac.org/journal-article/security-of-cyber-physical-systems/ (Last Accessed: July 30, 2018)

[6] I. Friedberg, "STPA-SafeSec: Safety and security analysis for cyber-physical systems", Journal of Information Security and Applications, June 2016, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212616300850 (Last Accessed: July 30, 2018)

[7] W. Young, NG. Levenson, "An integrated approach to safe and security based on systems theory", Commn ACM 57 (2), pp. 31-35, Feb 2014, [Online]. Available: https://cacm.acm.org/magazines/2014/2/171683-an-integrated-approach-to-safety-and-security-based-on-systems-theory/abstract (Last Accessed: July 30, 2018)

[8] K. Stouffer et. Al., "Guide to Industrial Control Systems (ICS) Security", Rev. 2, NIST Special Publication 800-82, May 2015, [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-82r2

[9] B. Johnson et. Al, "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure", FireEye, Dec 2017, [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (Last Accessed: Sep 27, 2018)

[10] "Speedtronic Mark V GT Fundamentals", A00023, Rev. A, 1993, GE Power Systems, [Online]. Available: https://www.slideshare.net/masabqadir/01-tab-01 (Last Accessed: Sep 22, 2018)

[11] R. Dundas, "A Statistical Study of Gas Turbine Losses and Analysis of Causes and Optimum Methods of Prevention", ASME Journal 94-GT-279, 1994, [Online]. Available: http://proceedings.asmedigitalcollection.asme.org/proceeding.aspx?articleid=2145410 (Last Accessed: Sep 22, 2018)

[12] J. S. McGroarty, "Mechanical or Electrical trip system testing", Jan 2013, [Online]. Available: https://www.plantservices.com/articles/2012/12-overspeed-failure/ (Last Accessed: Sep 22, 2018)

[13] D. Johnson et. Al., "Speedtronic Mark V Gas Turbine Control System", GE Power Systems, [Online]. Available: https://www.ge.com/content/dam/gepower-pgdp/global/en_US/documents/technical/ger/ger-3658d-speedtronic-mark-v-gas-turbine-control-system.pdf (Last Accessed: Sep 22, 2018)

[14] D. Herschberger & J. Blanchard, "Pushing machines to the limit: Transitioning to digital overspeed protection", Control Engineering, Dec 2013, [Online]. Available: https://www.controleng.com/single-article/pushing-machines-to-the-limit-transitioning-to-digital-overspeed-protection/9229e43977a9d21bd9707fe18d112ec9.html (Last Accessed: Sep 22, 2018)

[15] R. Torok, "Turbine Overspeed Trip Modernization", Technical Report, EPRI, Nov 2006, [Online]. Available https://www.epri.com/#/pages/product/000000000001013461/?lang=en (Last Accessed: Sep 27, 2018)

[16] "Mechanical Overspeed Bolt Replacement", ABB, [Online]. Available: https://library.e.abb.com/public/aba0dd5cb69e871dc1257cd00047f600/Overspeed%20Bolt-9AKK106103A4895.pdf (Last Accessed: Sep 27, 2018)

[17] "Fire and gas detection monitoring system in gas turbines", Turbomachinery International, [Online]. Available: https://www.turbomachinerymag.com/fire-and-gas-detection-monitoring-system-in-gas-turbines/ (Last Accessed: Sep 27, 2018)

[18] Valve Monitor/Limit Switch IP67/NEMA 4X Specification Sheet, Valworx, [Online]. Available: https://www.valworx.com/product/valve-monitorlimit-switch-ip67nema-4x/valve-limit-switches-valve-monitors?gclid=EAIaIQobChMI9trul_7q3QIVg8hkCh1AxgrREAQYASABEgKdDvD_BwE (Last Accessed: Sep 27, 2018)

[19] A look inside Berkeley's Cogeneration Facility, [Online]. Available: https://www.ocf.berkeley.edu/~fricke/cogen/ (Last Accessed: Sep 27, 2018)