Cybersafety Analysis of Industrial Control Systems: Chiller Systems

Shaharyar Khan, Stuart Madnick

Working Paper CISL# 2020-09

January 2020

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

Cybersafety Analysis of Industrial Control Systems: Chiller Systems

Shaharyar Khan
Massachusetts Institute of Technology
shkhan@mit.edu

Stuart Madnick
Massachusetts Institute of Technology
smadnick@mit.edu

Abstract

Recent world events and geopolitics have brought the vulnerability of critical infrastructure to cyberattacks by advanced cyber-adversaries to the forefront. While there has been continued and growing attention to vulnerabilities in our energy generation and distribution systems, there are many other types of industrial control systems, ranging from manufacturing facilities to refineries to water treatment plants, that are also at significant risk based on their unique physical characteristics. In this paper, we take a holistic view of one such complex system – the chiller plant – in an archetypal industrial setting to identify vulnerabilities emerging from interactions between technology, operator actions as well as organizational structure and provide recommendations to mitigate resulting loss scenarios.

1.0 Introduction

Recent events such as the Ukraine cyberattack, targeting the electric grid as well as attacks on oil and gas plants and nuclear facilities in Saudi Arabia and Iran, respectively, have demonstrated not only the *capability* but also the *willingness* of nation-states to disrupt and/or cause damage to an adversary's critical infrastructure (Angle, Madnick, Kirtley, & Khan, 2019). While such attacks are generally classified as matters of *national security* (Loukas, n.d.), requiring nation-state resources to defend against, an equally potent threat with the potential to cause physical damage and/or disruption to our day-to-day lives, lurks much closer to home; centralized heating and cooling, which is enabled by industrial boilers and chillers, is taken for granted in most industrialized nations. In fact, *industrial boilers* and *chillers*, have become embedded within every aspect of our lives – from large commercial and office buildings, hospitals, college campuses to ice rinks, shopping malls and grocery stores. These large, specialized, pieces of equipment along with their control systems are archetypal examples of ICS, which under unsafe control actions can result in catastrophic consequences. For instance, although not cyber-related, the 1997 chiller accident at Los Alamos National Labs costed $3.2 million in damages (Twining, 1998) to the facility and to equipment used for nonproliferation and international security operations in addition to raising concerns about radiological contamination.

In the context of cybersecurity, industrial chillers are of particular significance because over the years (in seeking improved efficiency), their control systems have become increasingly software-dependent, coupled with other systems (including pumps and valves) and in many cases offer the functionality to be controlled directly via the internet. The traditional approach to protecting such systems is to undertake a risk-based, technical perspective that is biased by information security concerns (Loukas, n.d.). However, important differences exist between cyber-physical and traditional IT systems, that make such a narrow approach largely impotent in the face of targeted attacks (Freeman, St Michel, Smith, & Assante, 2016)– underscoring the need for *a systems perspective* of the security problem. In this paper, we use the systems theory-based *cybersafety* method to holistically identify cyber-vulnerabilities and mitigation requirements in a chiller plant. Among other things, it is shown how the functionality of being able to remotely update critical frequency settings in the variable frequency drive (VFD) for the chiller compressor could be attacked to cause damage to the compressor and how the entire system (people, processes and technology) could be leveraged to prevent a loss through such a mechanism.

2.0 Literature Review

Since a breach of security of a cyber-physical system has the potential to impact system safety, a number of hazard analysis frameworks, traditionally employed for safety analysis are adapted for security analysis. An alternative to performing joint analysis of safety and security using extended versions of traditional hazard analysis methods (such as FTA (Altawairqi & Maarek, 2017), FMEA (Schmittner, Gruber, Puschner, & Schoitsch, 2014) etc.), is to use the perspective of modeling using *systems theory*. Leveson (N. G. Leveson

& Thomas, 2018), (N. Leveson, 2012) developed a framework to understand causes of accidents using *systems theory* known as STAMP (System-Theoretic Accident Model and Processes).

STAMP is a framework that treats accidents as a *'dynamic control problem'* emerging from violation of safety *constraints* rather than a *'reliability problem'* aimed at preventing component *failures*. Several analytical methods have been developed based on the STAMP framework such as STPA, CAST etc.

Presented in a concept paper by (Young & Leveson, 2014), STPA-Sec presents a methodology to perform integrated safety and security analysis using systems theory. In addition, (Salim, 2014) analyzed the TJX cyberattack while (Nourian & Madnick, 2018) analyzed the Stuxnet attack using the STAMP framework. However, both the later works were analyzing events that have already occurred. Despite best effort, our literature search did not reveal any detailed published work documenting the application of STPA-Sec to industrial control systems. *Cybersafety* is a further refinement of the STPA-Sec method that presents a robust, repeatable and structured approach to undertake integrated safety and security analysis of an industrial control system, spanning all aspects of the complex system – *technical, human* and *management*.

2.1 Cybersafety Method

The basic steps in the cybersafety method are illustrated in Figure 1. Briefly, the method starts by defining the basis of the analysis which includes identifying the goal of the system, the most critical losses and system-level hazards that can result in those losses. The next step is to identify the *controllers* responsible for enforcing constraints on the processes (i.e. to control the hazards) and their interactions with one another – this results in the development of the *functional control structure*. Next, each control action for each controller is evaluated in the context of the various system and environment states that the system is subject to, in order to identify *hazardous control actions*. And finally, *loss scenarios* are generated by hypothesizing how the interaction between the controllers and missing constraints can be leveraged by an attacker to cause losses to the system. New mitigation requirements are then derived to prevent the hazards from propagating into system-level losses.

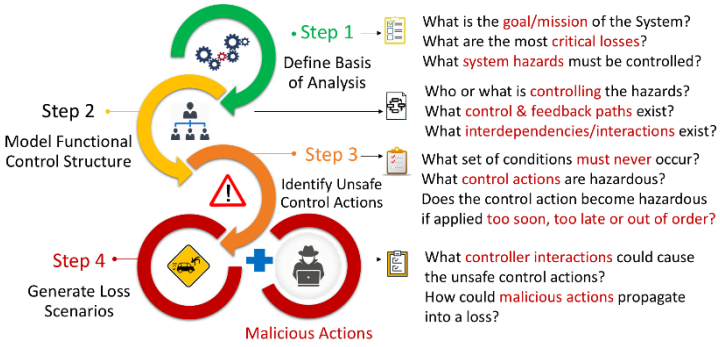


Figure 1 - Overview of the Cybersafety method

3.0 Description of the System

The chiller plant that is the subject of this paper is located inside a typical energy facility with upstream operations that include delivery of fuel (both natural gas and fuel oil) to the facility along with a tie-line connection to the local utility grid as well as a steam-line connection to the local powerplant. The plant's downstream operations include distribution of electricity, steam and chilled water to the facility buildings.

The plant operates a 21 MW Siemens ABB (GT10) gas turbo-generator that provides electricity to the facility buildings; waste heat from the turbine is directed to a Heat Recovery Steam Generator (HRSG) to produce steam. The steam from the HRSG is supplemented with steam from other gas/oil-fired water-tube boilers and is used for heating and other functions such as driving steam-driven chillers. The combined output from the 6 steam-driven chillers is 21 kilotons. This chilled water supply is supplemented with 8 additional electric-driven chillers (with a combined capacity of 13 kilotons) to meet facility demand. The plant consists of a juxtaposition of various types of chillers (e.g. reciprocating, centrifugal, screw-driven etc.), from different manufacturers and of different equipment ages which adds to the complexity of the system. For the purpose of this paper, we focus on electric-driven centrifugal chillers.

Chiller System – Electric-driven Centrifugal Chillers

A chilled water system consists of a chiller or a combination of chillers, air-handling units (AHU), cooling towers as well as auxiliary equipment including pumps, water purification system and piping as shown schematically in Figure 2. The chiller removes heat from a liquid via a vapor-compression cycle which consists of four main components: evaporator, compressor, condenser and expansion device. The basic operation can be described as follows. The refrigerant in the evaporator, absorbs heat from chilled water return line, changing its state to superheated vapor. The temperature and pressure of this superheated refrigerant vapor is increased by the compressor which converts kinetic energy to pressure and pumps the

vapor to the condenser. Here, cool condenser water extracts heat from the refrigerant converting it back to a high pressure, high temperature liquid. A thermal expansion valve is used to reduce the temperature of the liquid by reducing its pressure by passing the liquid refrigerant through a small adjustable orifice. The liquid refrigerant then again absorbs heat from the chilled water return line, turns to vapor and the cycle is repeated (Daikin, n.d.).

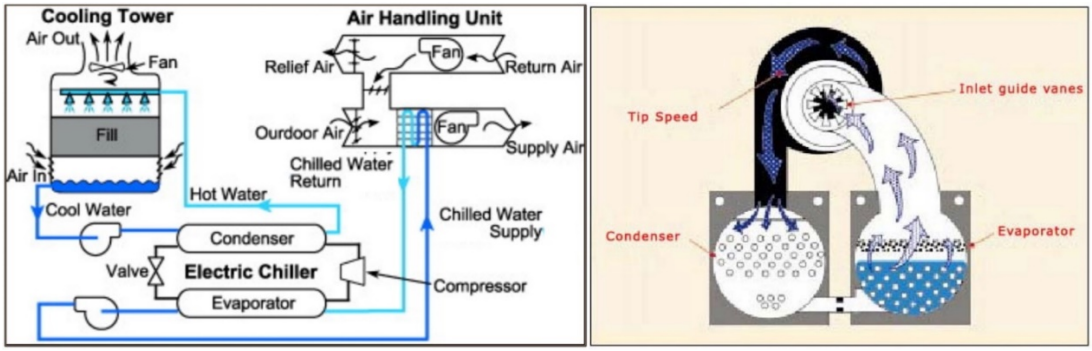


Figure 2 – (a) Schematic of Chiller Plant (b) Chiller cross-section

Note that there are three independent fluid loops which function together to enable delivery of chilled water to the facility; 1) a closed loop water circuit that runs chilled water between the building AHUs and the evaporator, 2) a closed loop refrigerant circuit, which enables transfer of heat from the chilled water loop to the condenser water loop, and 3) an open water loop, which absorbs heat from the refrigerant and rejects it to the atmosphere via cooling towers. Each of these loops have pumps and valves which are operated by the chiller controller or supervisory controllers such as the Distributed Control System (DCS) or the operator based on certain decision rules.

4.0 Analysis

This section provides the bulk of the analysis for the chiller plant. It is divided into subsections where each subsection represents one step in the basic *cybersafety* diagram presented in Figure 1.

4.1 – Define Basis of Analysis

Being a top-down, consequence-driven method, the first step in the *cybersafety* method is to establish the system boundaries by defining the goal/primary mission of the target system i.e. the Chiller Plant. The *system problem statement* provides a convenient framework for establishing the goal and critical functions of the system as demonstrated in Figure 3. Note that there are three critical functions identified in the *system problem statement* – *controlling* chiller capacity, *managing* chilled water distribution and *rejecting* waste heat to the environment – that enable the system to achieve its primary value function.

Next, with the boundaries of the target system established, *unacceptable* system-level losses are determined; these are unacceptable consequences from the primary stakeholder's (plant owner) perspective as itemized in Table 1.

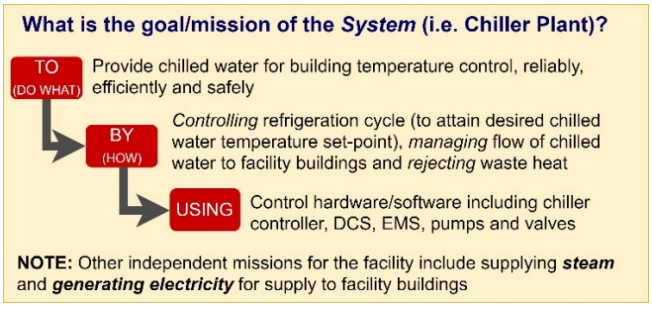


Figure 3 – System Problem Statement

Table 1 – List of Unacceptable Losses

Unacceptable System-Level Losses	
L-1	Physical damage to critical equipment
L-2	Loss of mission i.e. inability to provide chilled water

The *cybersafety* method, being based on the STAMP framework (N. Leveson, 2012), establishes a clear distinction between *unacceptable losses* and *system-level hazards*. *System-level hazards* are those system-states that are within the control of the system, which if not controlled, would result in losses. The goal of

the analysis is to establish *constraints* on the system that prevent the hazards from translating into losses. As a first approximation, by inverting the system-level hazards, we arrive at a first set of constraints; these constraints are progressively refined, throughout the analysis. Table 2 presents *system-level hazards*, along with corresponding *constraints* and their mapping to *unacceptable losses*.

Table 2 - System-level Hazards and Constraints

System-Level Hazards	Related Losses	System-Level Constraints
H-1: Chiller system is operated beyond normal operational limits	L-1, L-2	SC-1: Chiller system must not be operated beyond normal operational limits
H-1.1: Operated at a temperature that is too low (potential for freezing)	L-1, L-2	SC-1.1: Must be operated within temperature limits
H-1.2: Operated at a pressure that is too high or too low (potential for catastrophic failure due to over-pressure or in the case of low pressure, could lead to cavitation or freezing)	L-1, L-2	SC-1.2: Must be operated within pressure limits
H-1.3: Operated to meet a load that is beyond capacity	L-2	SC-1.3: Must be operated within capacity limits
H-1.4: Operated at a flow that is too high or too low (potential for freezing, or tube failure due to erosion or poor performance due to fouling)	L-1, L-2	SC-1.4: Must be operated within flow limits
H-2: Chiller system violates correct sequence of operation (opening/closing of valves, start-up of pumps, fans)	L-1, L-2	SC-2: Chiller system must not violate correct sequence of operation
H-3: Chiller system violates timing constraints (for instance during start-up, causing compressor burnout (overheating) or compressor seizure (lube oil not at correct temperature/pressure)	L-1, L-2	SC-3: Chiller system must not violate timing constraints

4.2 – Model the *Functional Control Structure*

In this subsection, we model *how* the constraints identified in the previous subsection are enforced on the target system via a hierarchy of controllers known as the *functional control structure*. Figure 4 presents the functional control structure for the chiller plant.

The control of the chiller plant consists of not only managing the combined cooling capacity of the chillers, but also the auxiliary equipment to enable *distribution* of chilled water to facility buildings as well as *rejection* of waste heat to the environment via cooling towers. While individual control of chiller compressors, chilled water pump motors and valves, cooling tower fans etc. is implemented via PLCs, the overall control logic for system operation is managed by the DCS. The DCS, through a *Human-Machine Interface* (HMI) provides the plant operator with a birds-eye view of all the equipment in the plant and enables supervisory control of field equipment by transferring settings, operator permissive functions and manual override commands to field controllers.

Note that the plant's mandate is limited to maintaining chilled water supply at a certain temperature, pressure and flowrate; the control of building automation systems (BAS) is beyond its mandate and is in fact controlled by a different group of operators, referred to as *Facilities Operators* in the *functional control structure*. The plant operator actions, in turn, are controlled via operating procedures and instructions by Plant Engineers. Both Plant Engineers and operators report to *Plant's Operations Management* which enforces the company leadership's enterprise-level goals and vision through policies and standards. The leadership team, in turn, is controlled by municipal, state and federal regulations enforced via certificates and licensure for operating the plant.

The chiller plant does not operate in isolation; in fact, it is closely coupled with other systems in the plant, notably the electric generation and boiler systems. The operation of the chiller plant is contingent on decisions such as what combination of chillers should be run to achieve the desired cooling capacity, what is the desired chilled water setpoint and flow-rate, how many pumps should be operated and at what capacity, and which cooling towers should be operated and at what capacity. These decisions are highly dependent on environmental factors such as weather conditions, energy costs for electricity, gas, steam (imported from neighboring power plant) as well as cooling load (dependent on time of day and building occupancy).

Although each of the field devices are operated as individual components, they together interact in indirect ways to produce complex, *emergent* behavior that is greater than the sum of the parts. Each control decision

is made in such a way so as to achieve a global optimum for the plant in order to maximize efficiency. An energy management system (EMS) service provider is contracted to provide recommendations for optimum integrated performance. The EMS combines aggregated data from the plant's DCS and real-time market, weather and fuel prices with predictive analytics to recommend operating points that maximize efficiency for the plant.

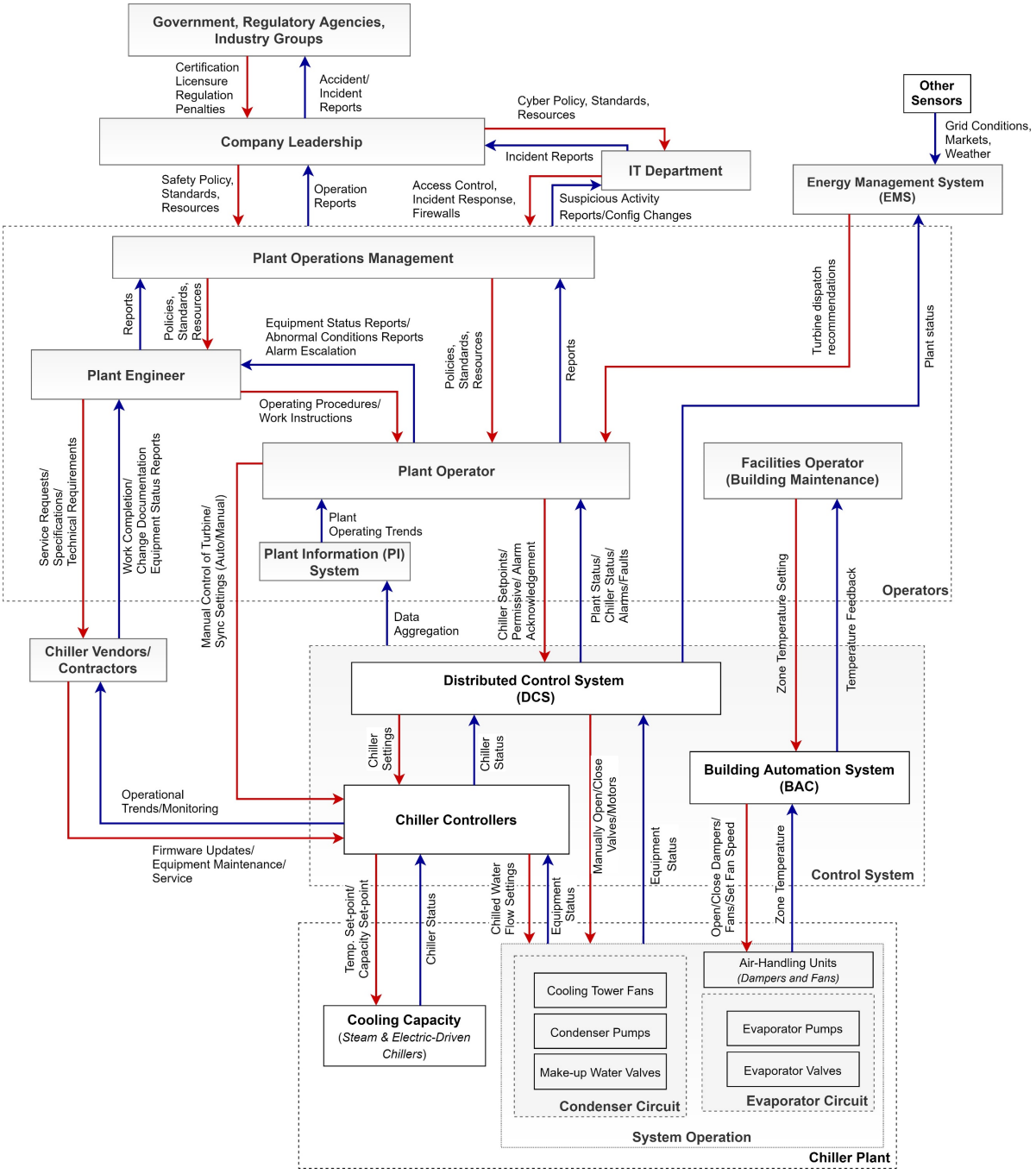


Figure 4 – Detailed Hierarchical Functional Control Structure for the Chiller Plant

For the purpose of this paper, we limit our focus to *chiller cooling capacity control loop*. The electric-driven chillers at the plant are equipped with a Programmable Logic Controller (PLC), which regulates the cooling capacity of the chiller in response to chilled water temperature deviation from the set-point by adjusting the speed of the compressor motor (Daikin, n.d.). The PLC receives feedback from several sensors monitoring various physical processes, including refrigerant discharge and suction temperatures and pressures, condenser and evaporator water temperatures, pressures and flows, compressor lube oil

temperature and pressure, guide vane position etc., and computes the required compressor speed which is then implemented by sending required signals to a variable frequency drive (VFD).

4.3 – Identify Unsafe Control Actions

The next step in the *Cybersafety* method is to identify *Unsafe Control Actions*. We begin by identifying the *primary functions*, *safety responsibilities* and associated *control actions* for the main controllers in the *functional control structure* as presented in Table 3. Note that a particular *control action* in of itself is not *unsafe*, rather the *context* in which it is performed, makes it *safe* or *unsafe*. A systematic method to identify the various contextual environmental and system states of significance, is to formulate the *process model* for each controller. The *process model* is the model that the controller uses to determine what control actions are *safe* or *needed* in order to keep the controlled process within certain constraints and could be potentially targeted by an *attacker* to cause the controller to issue hazardous control actions. The *process model* for the chiller controller is presented in Table 4.

Table 3 - List of Controllers, Safety Responsibilities & Control Actions

Controller	Function Performed	Safety Responsibilities	Control Actions
Operator	Perform day-to-day tasks to run equipment including the turbine, boilers and chillers in response to real-time demand variations from the facility	-Dispatch chillers, boilers to meet cooling load -Monitor system operation for abnormalities -Emergency Shutdown of equipment -Respond to alarms and faults and take corrective actions -Provide permissive functions/command overrides	-Select chillers and manually start/stop chillers -Set CW set-point, capacity -Manually open/close pumps/valves -Shutdown process during emergencies
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/troubleshoot -Ensure procedural compliance and training	-Approve operating procedures -Provide technical specifications and requirements to contractors/ vendors -Approve equipment change/modification requests
Distributed Control System (DCS)	Provide operator with supervisory control and monitoring of all automated controllers distributed throughout the plant	-Raise alarms and faults for system abnormalities -Aggregate data and provide accurate information -Ensure necessary pumps/valves are open/ closed	-Start/stop cooling tower fans -Open/close evaporator/condenser valves -Start/stop pumps
Energy Management System	Combine real-time market and grid conditions along with predictive analytics to recommend operating points that maximize efficiency	-Provide recommendations within the generator capability limits	-Provide turbine dispatch recommendations
IT Department	Primarily responsible for enterprise network management	- Provide onboarding and access control to IT systems at the plant to new employees -Employee cyber-awareness and training -Perform IT functions, such as deploying firewalls, DMZ, etc.	-Deploy patches -Authenticate users -Setup Firewalls and DMZ
Chiller Controller	Control chiller cooling capacity to achieve desired chilled water temperature setpoint	-Ensure necessary safety permissive functions are received for safe operation -Emergency shutdown	-Increase/decrease compressor speed -Open/close metering device -Open/close guide vanes -Open/close condenser/evaporator valves

Table 4 – Process Model Variables for the AVR and their possible values

#	Chiller Controller Process Model Variables	Process Model States
1	Chilled Water Temperature	Below | At Setpoint | Above
2	Compressor Differential Pressure	Within Limits | Outside Limits
3	Lube Oil Permissive	Available | Not Available
4	Evaporator Flow	Within Limits | Outside Limits
5	Condenser Flow	Within Limits | Outside Limits
6	Compressor Motor Speed	Within Limits | Outside Limits
7	Compressor Motor Temperature	Within Limits | Outside Limits
8	Refrigerant Superheat	Within Limits | Outside Limits

Unsafe control actions (UCA) can be identified by enumerating various combinations of the process model variables (Thomas, 2012). Several UCAs for the chiller controller are listed in Table 5, some of which are described next.

Motor Critical Speed & Reverse Rotation

The compressor motor has certain *critical* speeds at which mechanical resonance can occur. Typically, the VFD is programmed to skip over these resonant frequencies (Emerson Application Engineering Bulletin, 2018). However, operating the motor at its critical speed, can cause considerable damage to *'the bearings*

and (the) motor shaft' (Zetter, n.d.) **[UCA-1]**. Another unsafe condition for the compressor motor is reverse rotation; the VFD can be easily toggled to change the direction of rotation. Although reversing the direction of rotation would not change the direction of fluid flow through the compressor, it would cause significant damage to the compressor due to vibrations **[UCA-4]**.

Lubrication Oil

A Centrifugal compressor needs oil forced around its internal components (such as gears, thrust bearings etc.) to provide lubrication and remove heat caused by friction. The lubrication oil has to be at the correct temperature and pressure for it to perform its intended function; it must be thin enough to lubricate properly at high speeds of rotation but also thick enough to handle the heat and refrigerant contamination that can occur. If the lubrication oil conditions is not at the correct temperature and pressure, it can destroy the compressor in the matter of a few minutes because of the excessive heat build-up through friction in the internal components (Evans, 2017) **[UCA-6]**.

Motor Burnout

If a compressor motor is operating at its temperature or current limit, a command to increase motor speed would result in overheating; excessive heat can lead to premature loss of motor winding insulation, resulting in the motor burning itself out **[UCA-5, UCA-8]**.

Surging

Another characteristic hazardous condition for centrifugal chillers is surging. This can occur when the compressor differential pressure exceeds design limits, particularly during *low-load* operation; it is caused when the required lift exceeds the systems pumping capacity. It may be caused by either increasing the condenser temperature and pressure or reducing the evaporator temperature and pressure – both could be caused by reducing water flows in the condenser or evaporator at low load conditions. Once surge occurs, the output pressure of the compressor is drastically reduced, resulting in flow reversal within the compressor. The flow reversal applies significant dynamic forces on the impeller which subjects the compressor components (such as thrust bearings, bearings, casing) to large axial force changes due to the rotor rocking back and forth. If not controlled it can cause tight-tolerance compressor internals to be permanently damaged due to asymmetric thermal expansion and subsequent friction damage (Mechanical Engineering Site, 2017) **[UCA-3]**.

Table 5 - List of Unsafe Control Actions

Action By	Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too soon, Too late, Out of order	Stopped too soon, Applied too long
Chiller Controller	Increase Compressor Speed	**UCA-1:** Chiller Controller does not increase speed when compressor is operating at critical speed --> [H-1]	**UCA-3:** Chiller Controller increases compressor speed when the required lift (pressure differential) is too high (suction pressure too low or discharge pressure too high) --> [H-1.2]	**UCA-6:** Chiller controller increases compressor speed before lube oil permissive function is available --> [H-2, H-3]	**UCA-9:** Chiller controller continues to increases compressor speed when refrigerant superheat is too low --> [H-1]
		UCA-2: Chiller Controller does not increase compressor speed when chilled water temp is below setpoint --> [H-1.3]	**UCA-4:** Chiller controller increases compressor speed when configured for rotation in reverse direction --> [H-1]	**UCA-7:** Chiller controller increases compressor speed before evaporator flow is established --> [H-2]	**UCA-10:** Chiller controller increases compressor speed for too long after discharge pressure is beyond high-pressure cut-out --> [H-1.2]
			UCA-5: Chiller controller increases compressor speed when compressor motor is overheated --> [H-1.2]	**UCA-8:** Chiller controller increases compressor speed when timer permissive function is unavailable --> [H-3]	

While there are several other hazardous control actions, we selected a small subset to demonstrate the application of the *cybersafety* method following a systematic approach.

4.4 – Generate loss scenarios

In this subsection, we determine causal factors that enable the issuance of the earlier identified unsafe control actions. According to Leveson (N. G. Leveson & Thomas, 2018), two types of causal scenarios must be considered:

a) Scenarios that lead to the issuance of unsafe control actions; these could be a result of (1) *unsafe controller behavior* or (2) *inadequate/malformed feedback*.
b) Scenarios in which safe control actions are improperly executed or not executed altogether; these could be a result of issues along the (1) *control path* or the (1) *controlled process* itself.

For illustration purposes, we zoom into the functional control structure for the chiller controller from Figure 4 and superimpose it with guidewords from (Schmittner, Ma, & Puschner, 2016) signifying sample attack scenarios; the simplified control structure is presented in Figure 5. By going around the control loop and hypothesizing why a controller may issue a hazardous control action while considering the actions and motivations of malicious actors, we can generate a list causal factors for loss scenarios. A few loss scenarios along with potential causal factors and associated safety/security constraints are presented in Table 6 which is followed by a discussion of some of the key findings.

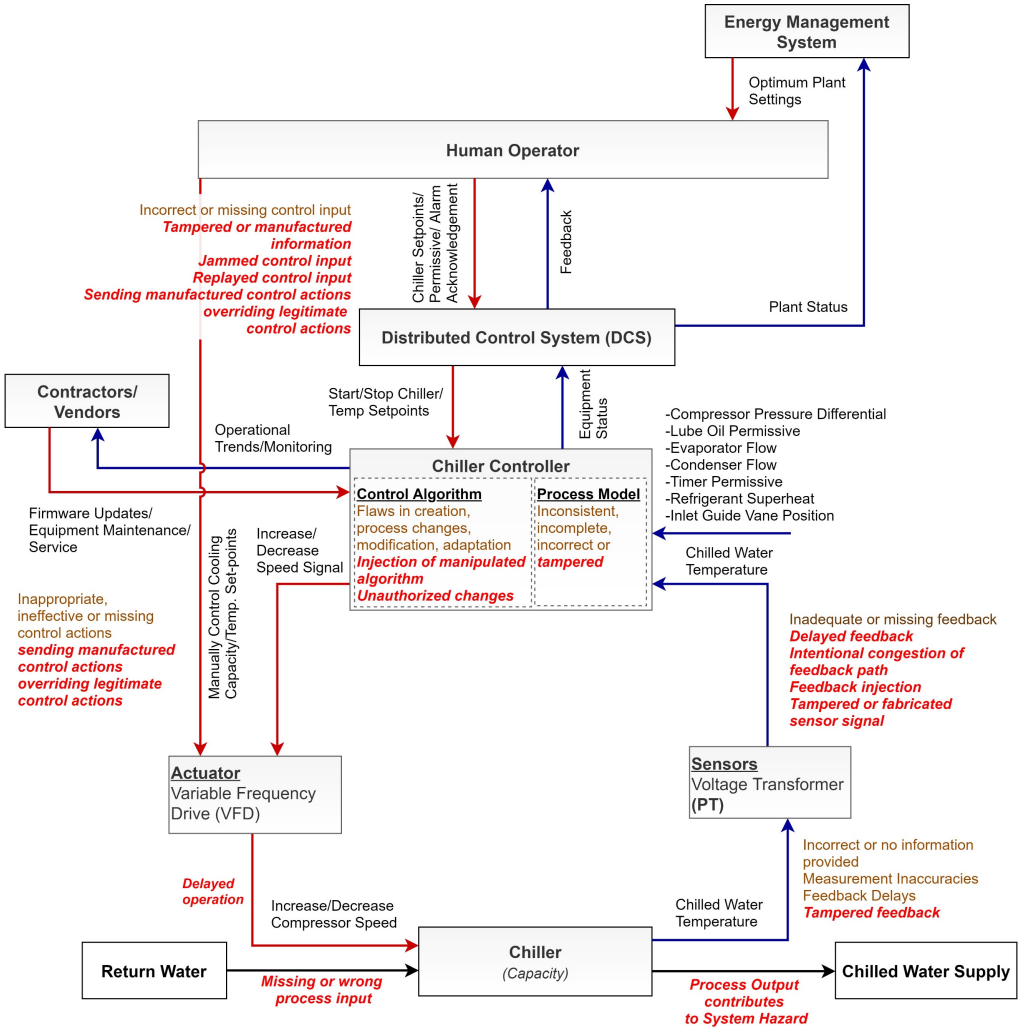


Figure 5 - Simplified Control Structure for Chiller Control Loop with Sample Attack Scenarios

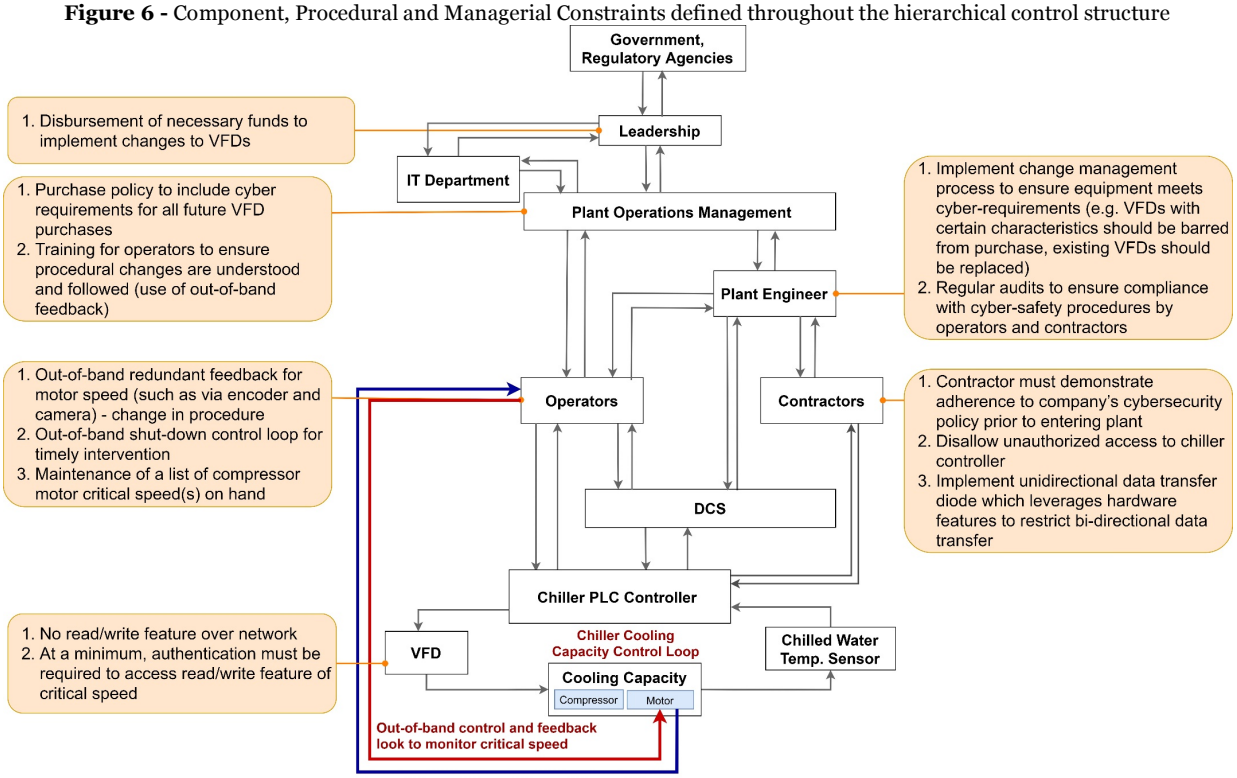
Table 6 – List of Loss Scenarios

Chiller	**UCA-1**		
Chiller controller does not increase speed when compressor is operating at critical speed --> [H-1] **– (Cooling Capacity Control Loop)**			
	Scenarios	**Associated Causal Factors**	**Safety/Security Constraints**
1	**Malformed actuator implementation** During startup or loading of the chiller, the chiller controller does not increase the compressor speed to skip over critical speeds leading to mechanical resonance and physical damage to compressor	1. The specific VFD used allows read/write functionality of critical speeds over network; malicious agent reprograms VFD with incorrect critical speeds	1. VFD must not allow read/write functionality over network
2	**Incorrect control input from higher-level controller – contractor** During routine maintenance, contractor inadvertently uploads malware that causes nominal speed operation to reset to operate at critical speeds	1. Contractor/vendor uses removable media (USBs, Laptop) without scanning for malware, thereby inadvertently uploading malicious firmware during routine maintenance 2. Vendor collects trend monitoring data over internet where the unidirectionality is implemented in software (which is hacked by attacker to deploy malware)	1. Contractor must demonstrate adherence to company's cybersecurity policy prior to entering plant (demonstrate up-to-date virus definitions, malware scans) 2. Disallow unauthorized access to chiller controller 3. Implement unidirectional data transfer diode which leverages hardware features to restrict bi-directional data transfer
3	**Overriding legitimate control actions** During normal operation, operator's legitimate control actions (speed setpoints) are overridden with speed settings that cause mechanical resonance without operator knowledge	1. Operator does is not aware of critical speeds of specific chillers and hence does not take corrective action 2. Operator only relies on a single source (HMI) to monitor plant equipment; the feedback on the HMI is manipulated 3. Operator has a list, but it is corrupted by malicious actor because it was stored online – no hard copy in control room	1. Operator must be provided adequate training to know critical speeds of equipment in the plant. 2. Operator must be provided with a hard-copy of critical speeds for all equipment 3. Operator must have independent out-of-band feedback of compressor speed

5.0 Discussion

A review of the loss scenarios and associated causal factors in the previous section illustrates the discovery of vulnerabilities throughout the larger socio-organizational system – not only technical vulnerabilities. In the *cybersafety* method, it is the violation of *safety* and *security* constraints that results in losses and these constraints are enforced by an entire structure that goes beyond the reliability or security of individual components. Figure 6 shows some additional mitigation requirements that are recommended to be implemented throughout the control structure to make the system more safe and secure.

Figure 6 - Component, Procedural and Managerial Constraints defined throughout the hierarchical control structure



For instance, the hazardous control action of operating the motor at its critical speed is enabled by the fact that the VFD used at the plant is of a type that allows remote update of *critical frequencies*. However, taking a *systems perspective*, this vulnerability exists because of a management decision to *allow* use of this type of VFD. In fact, every controller in the functional control structure has a role to play; it either fails to take the necessary decision or control action at the correct time to prevent a loss scenario or its elevated access or privileges are somehow leveraged by the attacker to cause a loss to the critical process.

The requirements summarized in Figure 6 span not only technical constraints, such as restriction on the type of VFD that is used in the plant, but also constraints on processes and procedures as well as constraints on operator actions and management decisions. For instance, the diagram shows that the functional control structure should be changed to include an out-of-band control and feedback loop for the operator (such as via an encoder and camera trained at the encoder readout). But this change must be complemented with a change in procedure where the operator is required to verify compressor speed with the out-of-band feedback loop and must keep a list of critical speeds for chiller compressor motor on hand (physical copy) and implement emergency shutdown in the event of a discrepancy. Likewise, new constraints are also defined for the contractor's access to the chiller controller via the trend monitoring system or for firmware updates etc. The decision to use off-site trend monitoring is again a management decision, but it is highlighted here as a potential source of vulnerability.

6.0 Conclusion

In conclusion, even with a very limited application of the *cybersafety* methodology, we have demonstrated that the method is a well-guided and structured approach that can be effectively utilized to holistically identify vulnerabilities and mitigation requirements in complex systems. The scope of the identified vulnerabilities and mitigation requirements span not only the technical aspects of the system but also the larger socio-organizational system that must enforce safety and security constraints on the system.

References

Altawairqi, A., & Maarek, M. (2017). *Attack Modeling for System Security Analysis*. https://doi.org/10.1007/978-3-319-66284-8_8

Angle, M. G., Madnick, S., Kirtley, J. L., & Khan, S. (2019). Identifying and Anticipating Cyberattacks That Could Cause Physical Damage to Industrial Control Systems. *IEEE Power and Energy Technology Systems Journal*, *6*(4), 172–182. https://doi.org/10.1109/jpets.2019.2923970

Daikin. (n.d.). *Centrifugal Chiller Fundamentals*. Retrieved from www.DaikinApplied.com

Emerson Application Engineering Bulletin. (2018). *Use of Variable Frequency Drives (VFDs) With Copeland Scroll and Copeland Discus in Fixed Capacity Compressors in Refrigeration Applications*.

Evans, P. (2017). Chiller Oil Lubrication Circuit - The Engineering Mindset. Retrieved January 15, 2020, from https://theengineeringmindset.com/chiller-oil-lubrication-circuit/

Freeman, S. G., St Michel, C., Smith, R., & Assante, M. (2016). *Consequence-driven cyber-informed engineering (CCE)*. https://doi.org/10.2172/1341416

Leveson, N. (2012). *Engineering a safer world : systems thinking applied to safety*. The MIT Press.

Leveson, N. G., & Thomas, J. P. (2018). *STPA Handbook*. Retrieved from http://psas.scripts.mit.edu/home/

Loukas, G. (n.d.). *Cyber-physical attacks : a growing invisible threat*.

Mechanical Engineering Site. (2017). Centrifugal Compressor Surge-Basics, Mechanism - Mechanical Engineering Site. Retrieved January 15, 2020, from http://www.mechanicalengineeringsite.com/centrifugal-compressor-surge-basics-mechanism/

Nourian, A., & Madnick, S. (2018). A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. *IEEE Transactions on Dependable and Secure Computing*, *15*(1), 2–13. https://doi.org/10.1109/TDSC.2015.2509994

Salim, H. M. (2014). *Cyber safety : a systems thinking and systems theory approach to managing cyber security risks*. Retrieved from https://dspace.mit.edu/handle/1721.1/90804

Schmittner, C., Gruber, T., Puschner, P., & Schoitsch, E. (2014). *Security Application of Failure Mode and Effect Analysis (FMEA)*. https://doi.org/10.1007/978-3-319-10506-2_21

Schmittner, C., Ma, Z., & Puschner, P. (2016). *Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis*. https://doi.org/10.1007/978-3-319-45480-1_16

Thomas, J. (2012). *Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis*. Retrieved from http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

Twining, B. G. (1998). *Final Report Type B Accident Investigation Board Report Chiller Line Rupture at Technical Area 35, Building 27 Los Alamos National Laboratory Albuquerque Operations Office*.

Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM*, *57*(2), 31–35. https://doi.org/10.1145/2556938

Zetter, K. (n.d.). *An Easy Way for Hackers to Remotely Burn Industrial Motors | WIRED*. Retrieved from https://www.wired.com/2016/01/an-easy-way-for-hackers-to-remotely-burn-industrial-motors/