DRAGOS

Improving OT Defense and Response with Consequence-Driven ICS Cybersecurity Scoping

Abstract

The advent of communication networks within industrial environments has proven to effectively compress decision cycles, increase productivity, and has freed organizations of many resource constraints and increased safety and reliability of operations. The reliance of real-time operational data to drive business decisions has led to significantly increased physical asset connectivity within industrial environments. Over the last 20 years, this increase has opened the way for attackers to potentially compromise process functions through the very communication networks that are depended upon for control and safety. This fact has motivated security professionals to develop a plethora of security assessment frameworks, including frameworks specifically designed to identify vulnerabilities and mitigate the risk of cyber attacks within industrial control systems (ICS).

However, no single assessment framework allows industrial asset owners to scope and prioritize the most critical network assets and processes with their associated network dependencies--the failure of which would result in a loss of the ability to operate. This paper will introduce an easily applied and repeatable scoping model that will help security analysts identify starting points for cyber threat hunts, incident response planning, penetration/vulnerability assessments, and cyber security strategies for ICS environments. This is done through merging traditional IT risk methodologies with historically-proven engineering and process risk methodologies by aligning network assets to known risk metrics within operational environments. We describe this scoping model by laying out a foundational analytic framework that starts with system and functional analysis and leverages completed Process Hazard Analysis (PHA), Piping and Instrumentation Diagram (P&ID) reviews, and their associated control strategies within the industrial environment. We use the results of these analyses to steer and identify control network dependency of critical processes to systematically determine crown jewels, as would be determined by an attacker to affect system functions.

The analytic results involved within this model allow a security analyst to work from the starting point of identified risks to processes. Cyber attackers often assess the feasibility of affecting system functions in a similar fashion. Therefore, a key assumption must be made up front in this analytic process. The position of the highest impact to a system's functional output, which can be defined as the organization's bottom line, should be assumed when trying to determine the most impactful risk of a cyber-attack.

Introduction

For ICS cybersecurity to be effective, organizations must have well-planned and informed requirements for the protection of their operational environments from cyber-attacks. Effective cybersecurity within an ICS environment can be applied throughout a range of measures that span the physical, procedural, and logical areas. However, one truth to any security application is the identification and prioritization of what must be protected. Within ICS environments, identification and prioritization for cybersecurity cannot be done exclusively through the application of traditional IT or OT risk assessments. Common questions seen throughout ICS security scoping include:

- What are the systems and components?
- What integral functions must be maintained for continued operations to occur? How are these systems, their components, and their functions at risk?
- Do I defend the network as a whole, or are certain network segmentations or assets valued higher and thus deserve a higher degree of protection?

The answers to these questions depend on identifying what system(s) contribute most to functional output, the systems' dependencies on the control network(s) to perform tasks, and the prioritization of control network assets.

To frame the risk of cyber attacks occurring within IT or OT environments, organizations have tried to use the classic information security risk equation of Risk = Threat * Vulnerability * Likelihood. There are many variations of this equation, but this equation is speculative due to the inclusion of the Likelihood variable, which relies on identifying when and how often a cyber-attack will occur. Due to the physical nature of ICS environments, a more accurate representation of risk would be Risk = Threat * Vulnerability * Consequence, where consequence is defined as impact to functional output. Fortunately, consequences have already been enumerated to account for potential process upsets due to variable system states. Why not leverage conclusions drawn from PHA and engineering practices and use them to identify what assets or crown jewels are necessary to affect system function through a cyber-attack on the control system? Applying the same engineering methodology to the cyber-attack risk problem identifies functional dependency of the control system, which also identifies the crown jewels of a control network, which informs security posture. This is the same way adversaries analyze systems and system functions to identify the most impactful targets.

Identifying criticality of physical processes and system components is done in much the same method. PHA and risk assessments are often completed using a combination of experienced analyst methodology and quantitative mathematical equations to identify and measure risk to function or risk to life, so that it can be mitigated to its lowest form. In most cases, operational decisions are aligned to the threshold of acceptable risk to the organization's bottom line.

In the past, organizations have hinged risk associated decisions on the most likely and most dangerous scenarios to impact operations. These decisions are informed by reliable engineering and safety methodologies, including PHA. PHA can include Hazard and Operability (HAZOP) studies, Failure Mode and Effects Analysis (FMEA), Criticality Rating assessments, etc., and the application of this analysis often occurs during the initial design of a system or operational environment. Once established, the analytic process is then periodically revisited after an initial design or installation, usually when the system or environment encounters new assets or modifications, or when the acceptable risk threshold has changed for the organization.

This quantitative approach to assessing operational risk includes identifying, valuing, and prioritizing assets based on their contribution to total system function. Once the threshold and impact of failure is determined, process and safety measures are applied as needed or required to lower risk to an acceptable threshold that is aligned to the organization's bottom line. This methodology has historically provided definitive risk thresholds that are grounded to engineering principles and facts, and it is generally applied to every process, reaction, rotating machine, etc., within an industrial environment to help ensure safe, reliable, and harmonious operations and control.

When a process upset does occur, the applied risk analysis, mitigation strategies, and safeguards are often first examined when trying to identify the root cause of an event. However, when applying this type of analysis, organizations have historically not needed to account for the purposeful compromise of the availability, integrity, or confidentiality of control systems through a cyber-attack, but the same analytic approach can and should be considered as a starting point for identifying potential root causes and impacts of a cyber-attack within an industrial space. When risk analysis is extended beyond the functional dependency of physical components to the dependency of control network architecture, patterns of network criticality become evident and control network crown jewels become defendable objects that risk mitigation strategies can be applied to.

ICS Convergence

In their authoritative paper, "The Industrial Control System Cyber Kill Chain," Michael J. Assante and Robert M. Lee state, "ICS-custom cyber attacks capable of significant process or equipment impact require the actor to become intimately aware of the processes being automated and the engineering decisions and design of the ICS and safety system or safeguards."[1] Gaining such knowledge enables an attacker to learn the systems well enough to identify where weapons may be applied to cause predictable effects on systems in ways that circumvent or impact safety mechanisms and achieve a true cyber-physical effect on the function of the system. The attackers are basing their campaign to attack a target on the fact that they are intimately informed of the functional dependency of the system. That's not a qualitative approach to measuring attack success. It is a systematic approach to identify and target a critical process and its dependency on control network assets within an operational environment.

Based on this, it can also be said that attackers must identify consequential impacts, or effects, on systems and align those effects to objectives in order to achieve favorable outcomes of attacking a target. The consequence of the impact, or effects, of any cyber event can therefore be calculated and linked to the system's functional dependency on the control network target. Applying this method to a large complex system, like an industrial environment, allows a security professional to draw definitive conclusions and identify crown jewels within control networks that an attacker MUST leverage in order to successfully apply a cyber-physical effect on a system function.

Once identified, the functional value of that control network asset is already aligned with established risk thresholds because PHA is used as a starting point and defensive measures may be placed to ensure the availability, integrity, and confidentiality of critical network assets is maintained. While the unknown nature of attacker motivations and timing seemingly gives them the positional advantage, application of attacker mindset by those more intimately familiar with the complex integration of their systems turns the tables to give defense the high ground.

[1] "The Industrial Control System Cyber Kill Chain," Michael J Assante and Robert M Lee, 25 October 2015: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

The Model

Functional Output

Functional output is a system or system owner's primary purpose. With most asset owners, functional output will be tied to their bottom line, but this can also incorporate safety, environmental, or public image. Functional output can be impacted through the following effects of a cyber-attack:

- Unintended, catastrophic process failures
- Unintended exposure (population or environment)
- Loss of control system availability
- Loss of confidence in the system
- Product recall
- Regulatory fines
- Sustained process inefficiency
- Loss of public confidence

Understanding and aligning the analytic methodology to the functional output, or primary purpose, of the system is crucial to isolating and capturing the most likely and most dangerous attack scenarios an environment could possibly face. However, without intelligence, it would be very difficult to define attacker objectives and effects. What we can identify are the dependencies of function that would most likely be attacked based on a scenario. Once a functional output has been selected, we can move on to identifying the dependencies of the system to sustain the functional output, including the dependency of the control system.

Functional Dependency

Functional dependency is the reliance of one system on other systems to fulfill its functional output. After analyzing and accounting for the largest functional output, determining the overall inputs and outputs of a system to capture the dependencies on each other will allow for alternate attack paths to be enumerated. If the system with the largest functional output also has the most controls around it, effects on a combination of different inputs could nullify the prioritized system with similar efficiency.

System Owner - A leading or specific provider within an industry discipline, geographic region, or demographic which may be targeted.

Critical System or Sub-system

A critical system or sub-system is a collection of assets, facilities, networks, and/or operators that provide a specific collective function and output. These critical systems are also the heart of a system owner, of which the organization's bottom line is most dependent. These determine your starting position within a functional organization. While the methodology can be used to holistically determine where a motivated attacker would attempt to cause an effect on an entire organization, it could also be used with a specific plant, unit, or individual processes within a unit as a basis.

Critical Function or Sub-Function

Critical functions or sub-functions are characterized as the required principal tasks of a system, such as heating, cooling, exchanging, pumping, separating, compressing, distributing, storing, etc. This is where previous risk assessment data becomes a requisite for determining critical points in a process. Repeated functional dependency analysis through understanding the engineering principles will provide a roadmap for developing expertise and more efficient model progression.

Critical Components

Critical components are physical assets required to complete a system critical function. Examples of components would be pumps, valves, motors, piping, suction screens, inlets, etc. required to perform the function of pumping. Components are the physical half of the cyber-physical interconnection.

Controllers

The "cyber" half of the cyber-physical interconnection, controllers exercise control over components to complete principal tasks or functions. Controllers are represented by their direct interconnection between the cyber or logical realm and the physical realm. Programmable Logic Controllers (PLCs), and Remote Terminal Units (RTUs) fall under this category.

Crown Jewels

Crown jewels are critical data, logical assets, communication paths, and/or control interfaces that are required to exercise control over components, and thus, functions. These include Human Machine Interfaces (HMIs), engineering and operator workstations, gateways, controllers, etc. An attacker's objective is to identify specific crown jewels associated with an attack approach and manipulate or subvert their normal function, therefore affecting the functionally dependent system states. The attacker's desired system states take into account the human element of process control and operator responses to process upsets. A determined actor will attempt to mitigate the effectiveness of an operator and the pre-configured logical responses to states.

The mechanism for an analyst to move through different levels of the model is by asking and answering the following questions: What element(s) and component(s) are critical to functional output? What functional dependencies do different elements within each layer have? Where is the greatest cyber exposure?

The Case Study

County (A)'s Critical Water Reclamation Facility

Although the information that is used for this case study is actual data, the system owner, system names, functions, components, controllers, and crown jewels have been changed to protect the system.

System Owner: County (A) Public Utility Department, A-City, USA

The County (A) Public Utility Department provides water, wastewater, reclaimed water, and solid waste services for residents of the unincorporated County (A). It is important to note that the functional output of the Public Utility Department is to provide services, as this will help determine what is functionally critical to the bottom line of the organization.

Critical System or Systems: The Water Reclamation Division

There are several organizational systems and subsystems within the County (A) Public Utility Department: the Engineering Division, Customer Service Division, Fiscal and Operational Support Division, Field Services Division, Solid Waste Division, Water Division, and Water Reclamation Division. However, only the system's **Solid Waste, Water,** and **Water Reclamation Divisions** are considered critically dependent by the functional output or bottom line of the system owner. Of the three identified critical systems (Solid Waste, Water, and Water Reclamation), we will concentrate on Water Reclamation for this case study; but we recognize that each of these three systems are relied upon by the system owner to achieve the overall functional output of the organization. The rest of the organization supports these systems and their functional outputs.

The **Water Reclamation Division** provides wastewater treatment through the operation and maintenance of water reclamation facilities and reclaimed water systems, administers environmental compliance, and administers a biosolids program for agricultural use within the surrounding community. Within the Water Reclamation Division, there are three water reclamation facilities that contribute to the Water Reclamation Division's function. The (A) Water Reclamation Facility, the (B) Water Reclamation Facility, and the (C) Water Reclamation Facility.

Critical Subsystems: The (A) Water Reclamation Facility and the Modified Step-fed Biological Nutrient Removal (BNR) Train

Of the three water reclamation facilities, the (A) Water Reclamation Facility has a treatment capacity of 43 Million Gallons Daily (MGD), the (B) Water Reclamation Facility has a treatment capacity of 19 MGD, and the (C) Water Reclamation Facility has a treatment capacity of 10.5 MGD. If we combine the total water output of the three water reclamation facilities, we get 72.5 MGD total processing capacity. If we convert facility (A)'s output to percentage of system capacity, we find that the facility is responsible for 59% of the total water reclamation system output. Therefore, it can be stated that the system, (A) Public Utility Department - Water Reclamation Division, is most functionally dependent upon the (A) Water Reclamation Facility.

The (A) Water Reclamation Facility is permitted as a 43.0 MGD design capacity activated sludge treatment facility, with flow equalization, chemical feed facilities, tertiary filtration, and high-level disinfection. The facility consists of three process trains: a 15 MGD train with Modified Ludzank-Ettinger (MLE) process, a 7.5 MGD train with Carrousel oxidation ditch treatment process, and a 20.5 MGD train with modified step-feed treatment BNR process.

If we go a step further and apply the same process at the sub-system level, we can isolate the subsystem responsible for the largest functional impact to the facility. Facility (A) consists of three process trains totaling 43 MGD output, with the 20.5 MGD BNR train making up the largest portion of output, roughly 47.5 % percent of subsystem capacity. This single train process accounts for over 25% of the total Water Reclamation Division's output. Therefore, it can be stated that the subsystem, the (A) Water Reclamation Facility, is most functionally dependent upon its modified step-fed BNR train.

Critical Function or Sub-Function: Pumping, Treating, Aerating

This step in the analytic process is where referencing PHAs, HAZOPs, engineering design and drawings, and control logic reviews becomes very important to identify the critical functions and components depended upon by the systems or subsystems to perform its functional output. In this case the critical functions of the biological nutrient removal (BNR) process was selected as the most impactful process on the subsystem's, (A) Water Reclamation Facility, functional output of 43 MGD of treated water. Within the BNR process, the sub-functions of pumping, treating, and aerating are critically depended upon to sustain the functional output of 43 MGD of treated water.

Treating removes solids from the wastewater and may include screens, grit removal tanks, and clarifiers as components of the function. Clarification would also be considered a critical function and is essentially a collection of large basins where low turbulence allows solids to settle to the bottom for removal to additional treatment. In this study, clarification is combined with the function of treating. Aerating involves a basin where microorganisms (sludge), a food source (pollutants in the wastewater flow), and oxygen are brought together under a controlled environment. This results in controlled metabolism of the pollutants. The oxygen is typically supplied by blowers, another critical component, and the air is bubbled into the bottom of the basin. From the aeration basin, the wastewater flows into another set of clarifiers. Treated wastewater is passed on for additional treatment and/or disinfection and most of the settled microorganisms are returned to the aeration basins to continue metabolizing pollutants. Finally, pumps (another critical component) are required to direct and control the flow of wastewater from stage to stage in the process.

For the purpose of brevity and to maintain the security of the system involved in the case study, we have chosen only to show a single functional subset, aerating, and its critical components. Should we decide to, this analytic methodology would be continued and repetitively applied to the identified critical functions of pumping and treating as well.

Critical Components: Blowers and Electricity

The air supplied by the four blowers to the aeration basin serve several purposes. The first main purpose is to supply oxygen needed for metabolizing organic compounds in the wastewater. The oxygen must be dissolved in the wastewater in order to be used by the microorganisms. The second purpose, blowers create turbulence in the mixture within the aeration basin to maintain the sludge in suspension. Mixing through the application of forced air turbulence also keeps the contents of the aeration basin homogeneous.

Because the BNR train process demand for air is so high and blowers rely on a steady electrical power demand, Blower (1) through Blower (4) and the electric power transmission assets Switchgear (B), (B1), and (B2) have been deemed as the most critical components depended upon by the Aerating Function.

Controllers: PLC-07A and PLC-15C/D/E/F

The critical aerating components depend on controllers to exercise control over the tasks each component performs to achieve the function of aerating. In this use case, Blower (1) through Blower (4) all depend on individual PLCs, PLC-15C/D/E/F for their tasking, and Switchgear (B), (B1), and (B2) depend on PLC-07A for tasking. These controllers exercise control over components to complete principal tasks or functions. Controllers are represented by their direct interconnection between the cyber or logical realm and the physical realm.

Crown Jewels - Workstation 1A/1B (Primary/Backup), PLC-07A, and PLC(s)-15C/D/E/F

The controllers that exercise control over the critical components also rely on communication paths and/or control interfaces to be configured and to function properly. In this case, the controllers and their interface are considered the critical crown jewels of the (A) Water Reclamation Facility's BNR process train aerating function.

Record and Analyze Data for Scenario

The above use case was developed purely through open source intelligence. Attackers will use the most efficient resources at their disposal, and often process data is treated less critical while standard IT security elements are not. Process information stores can often give attackers the system understanding they need to engineer an effective solution and should be limited in their exposure. Whatever security effort the scoping feeds in to, the following questions should be answered using data collected from progression through the model: What data was required to understand the system's dependencies to function? Where is that data located? What efforts would an attacker need to go through to mount a successful attack on the system's functions?

After identification of crown jewels, the data collected can be used to map to different elements of the kill chain. The scenario of "an attacker has pivoted into the OT network" quickly becomes "an attacker leveraging open source information mounts a spear phishing campaign to a specific user group tied to the control of a unique, high-impact process and would leverage these ICS/OT crown jewels to carry out an attack on the process function." Creating prioritized scenarios based on the realism generated from model progression that map to the attacker kill chain and known threat actor TTPs allow greater buy-in from different stakeholders and more realistic defendable positions.

Conclusion

This research defined a formal model for the scoping of cyber threat hunts, incident response plans, penetration/vulnerability assessments, and cyber security strategies for ICS environments. The resulting model consists of a series of increasingly-specific levels of scoping with progression criteria for traversing to different levels. The model flow shows the iterative nature of scoping through functional dependency analysis as the core principle for bridging IT and OT cybersecurity strategies and gaining specificity within a complex control network. A use case is provided that details the analysis methodology as it relates to consequence driven cyber security. By using the formal scoping model, the overall results of the security exercises and strategies better track to the adversary mindset and objectives to generate more valuable outputs.