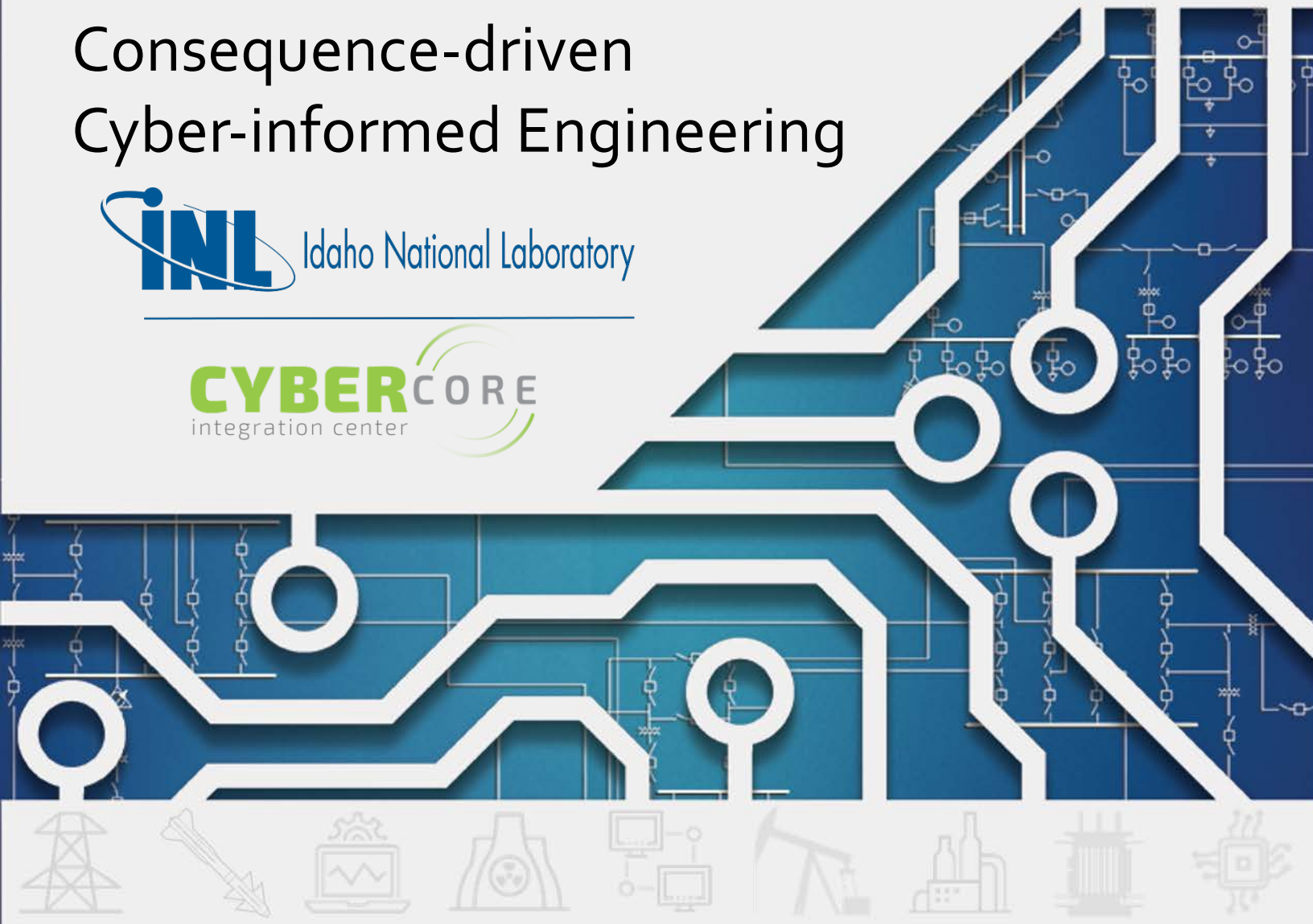
CCE Case Study: Stinky Cheese Company

Consequence-driven Cyber-informed Engineering



Cybercore Integration Center
Idaho National Laboratory

October 6, 2020

Stinky Cheese Company

CCE Case Study

A Cybercore Product

Idaho National Laboratory
Cybercore Integration Center
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of National & Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

Introduction

This document explores how to apply the CCE methodology to identify worst-case functional impacts and determine High Consequence Events (HCEs) in a fictional case study. For this case study, we will examine potential negative production/business impacts of cyber-enabled sabotage against a fictional entity, the Stinky Cheese Company. The following background section captures the type of information a CCE Team would gather from initial open-source research to describe the operations of the Stinky Cheese Company.

DISCLAIMER #1

This case study is a work of fiction. It is the product of the authors' imaginations, written to reinforce the understanding of the CCE methodology. Names, locations, events, corporations, regions, countries, and incidents are fictitious. Any resemblance to actual countries or events is purely coincidental.

DISCLAIMER #2

Any references to specific equipment, vendors, or technologies in this study does not imply increased susceptibility to cyber-attack over other brands or devices. The equipment in this study is "typical" equipment often found in the industry. As a work of fiction, some features were modified to support the narrative.

Background

Stinky Cheese is the nation's largest single-source producer and distributor of fresh cheese, recognized as a trusted and reliable brand since 1956. Located in beautiful Muenster, Montana, Stinky Cheese owns and operates a 15,000-acre farm that includes the Kase Dairy Ranch and the Stinky Cheese's own creamery. Stinky Cheese has over 10,000 happy cows that produce over 50,000 gallons of milk each week. This milk is made into the company's famous fresh cheeses.

Stinky Cheese is committed to providing its customers with fresh, delicious, and sustainable dairy products. Stinky Cheese only sources its dairy from its own Kase Ranch. The company's creamery is a 147-acre industrial complex adjacent to the Kase Ranch. The state-of-the-art creamery includes the Treatment and Pasteurization Facility, Ripening Depot, and Packaging Plant. Expert staff confidently claim that Stinky Cheese's sterile facilities and advanced pasteurization process ensure only the safest cheese products are made at Stink Cheese.

Stinky Cheese focuses on one batch of cheese at a time. The meticulous and undivided attention on each batch ensures the cheese products are exceptional, the impact to the environment is minimal, and the cows stay happy! Stinky Cheese finishes a fresh batch of 1,000 wheels of cheese a week—that's 10 tons of cheese!

Stinky Cheese ships to over 1,000 locations every day. Long-standing customers include national grocery brands such as Trader Flo's, Hole Foods, and Food Liger. Because of the company's renowned quality and safety record, it is also the sole supplier of cheese and milk products to over 500 school districts, 200 hospitals, and nearly 100 federal and state government facilities across the western United States. To find out more about placing a large order or joining the national family of wholesale and bulk customers, please contact Stinky Cheese directly by phone at (555) 867-5309.

Due to the volume of fresh cheese that Stinky Cheese produces every week, 10,000 gallons of milk are pasteurized during a single 10-hour shift to allow time for cheesemaking and packaging activities each day. To accomplish this, Stinky Cheese uses a high-temperature short-time (HTST) pasteurization system called the MU1000. The MU1000 is capable of pasteurizing 1,000 gallons of raw milk per hour.

Also known as "continuous" or "flash" pasteurization, the HTST pasteurization system is designed to heat and hold milk at a set temperature and duration to destroy bacteria and other microbes prior to releasing it for cooldown. The HTST system is highly complex, but it allows a large volume of raw milk to continuously pass through the pasteurization process. As a result, the cheesemaking process is greatly accelerated, allowing for large volumes of product every day to help meet the demand.

Production disruptions of one or two shifts are now able to be "absorbed" through scheduling modifications. Although the upgrade to the new HTST platform was capital intensive (anticipated 2-year ROI), Stinky Cheese stakeholders are fully committed to the advantages of this great new system.

As demonstrated by aligning the entire production process around the HTST, Stinky Cheese is especially focused on the pasteurization process. In the production of Stinky Cheese's cheeses, it is important that pasteurization is done precisely and correctly. The "sweet spot" for milk pasteurization is to raise the temperature to between 162°F and 380°F and hold it there for 20–30 seconds. If the cheese is held between 162°F and 380°F for more than 30 seconds, or if the milk reaches temperatures above 380°F, the quality and shelf life the of the final product will be significantly reduced.

However, if the cheese is held between 162°F and 380°F for less than 15 seconds, bacteria may survive to spoil the cheese prematurely and introduce consumer health concerns. If the milk does not reach 162°F for any amount of time, bacteria will be present and pose significant consumer health risks, in addition to quality/taste degradation of the product. According to the CDC, consuming raw milk and the products made from it can pose severe health risks, including death![1]

Discussing the dangers of consuming raw milk, the CDC states that:

> *Raw milk can cause serious illnesses. Raw milk and raw milk products, including soft cheese, ice cream, and yogurt, can be contaminated with harmful bacteria and other germs that can cause serious illness, hospitalization, or death. These harmful germs include Brucella, Campylobacter, Cryptosporidium, E. coli, Listeria, and Salmonella…. Pasteurization is the process of heating milk to a high enough temperature for a long enough time to kill illness-causing germs. Pasteurized milk is milk that has gone through this process.*[2]

Freshness and taste are super important at Stinky Cheese, but the company understands it is critical they create well-pasteurized, safe products for its customers who rely on Stinky Cheese! The company complies with all Federal and State regulations that define food processing standards. By participating in the annual self-validation program, Stinky Cheese avoids hefty fines and production shutdown (3+ months for re-cert inspection scheduling) that would result from a violation and citation related to food safety. You never have to worry about public health or a safety epidemic with this state-of-the-art pasteurization and highly automated cheesemaking process!

---

[1] To learn more about the dangers of consuming raw milk, see https://www.cdc.gov/foodsafety/rawmilk/raw-milk-index.html.
[2] Ibid.

A controls system vendor will provide digitally connected thermostats, automated control capabilities, and an HMI. The SIMATIC S7 PLC logic and I/O control provides the automation backbone, while the HMI allows operators to monitor and make any necessary adjustments to critical production parameters.

The automation platform provides operators with flow management, remote and local temperature monitoring, high and low temperature alarming, and capabilities for trend analysis. The components and network connectivity provide a complete view of the cheesemaking process—from raw input to final product.

The vendor will also be able to offer 24/7 remote support for instant access, monitoring, and troubleshooting of the system. This allows for proactive corrective maintenance and code development to assist operators with any issue. Additionally, access to diagrams and program code will be available to the customer on a supported server. Quality control issues around food safety would be an exception in terms of “continuous production” support.

Because of the potential business risks, pasteurization issues would require production shutdown and troubleshooting. Disruption would likely impact production for a minimum of 1 week due to the combination of downtime and weekly product inventory discard.

Phase 1: Consequence Prioritization

Objective:

Cause a public health/safety incident that will compromise Stinky Cheese's production capability for at least 3 months.

Scope:

Meet the Objective by focusing on Stinky Cheese's state-of-the-art pasteurization process.

Boundary Condition:

Cause a public health/safety incident by creating a sanitization issue in Stinky Cheese's pasteurization process that will compromise production capability for at least 3 months.

Events:

1. Excessive Pasteurization: The raw milk product reaches 162°F as intended, but the batches are held above that threshold for an amount of time exceeding 30 seconds, significantly reducing the shelf life of the final product.
2. Overheat: The raw milk product reaches temperatures above 380°F during pasteurization, significantly reducing the shelf life of the final product.
3. No Pasteurization: The raw milk product proceeds through the pasteurization process without undergoing pasteurization and proceeds to the separation stage of production. The unpasteurized final product includes harmful germs and is susceptible to early spoilage due to excessive bacteria.
4. Insufficient Pasteurization: The raw milk product reaches the required 162°F as intended, but the product is prematurely returned to room temperature before meeting the minimum of 15 seconds. Some bacterial and germs survive the process. The final cheese product may spoil prematurely and/or include harmful germs.

cyber-Events:

1. Excessive Pasteurization: Adversary gains access to the cheese production control system environment and targets the pasteurization process control/monitoring functions. Malicious modifications focus on the pasteurization temperature control. The controller logic is changed such that pasteurization process temperature thresholds are reached but the duration timing is extended. Display on the HMI appears normal. The milk stays in the pasteurization temperature range for an excessive amount of time.
2. Overheat: Adversary gains access to the cheese production control system environment and targets the pasteurization process control/monitoring functions. Malicious modifications focus on the pasteurization temperature control. The controller logic is changed such that pasteurization process temperature values are significantly higher than those used in control algorithms and as displayed on the HMI. The milk reaches extremely high temperatures.
3. No Pasteurization: Adversary gains access to the cheese production control system environment and targets the pasteurization process control/monitoring functions. Malicious modifications focus on the pasteurization temperature control. The controller logic is changed to ensure that the process temperature never reaches required limits for destroying bacteria and harmful microbes in the milk. Attacker ensures that no indications (HMI) or notifications (alarming) are presented to the system operators.

4. Insufficient Pasteurization: Adversary gains access to the cheese production control system environment and targets the pasteurization process control/monitoring functions. Malicious modifications focus on the pasteurization temperature control. The controller logic is changed such that the appropriate pasteurization temperature is reached but not sustained long enough to ensure complete destruction of bacteria and harmful microbes in the milk. Attacker ensures that no indications (HMI) or notifications (alarming) are presented to the system operators.

HCE Severity Scoring:

List of potential criteria

- Impact to public safety
- Financial loss
- Disruption of production
- Loss of brand reputation

Criteria Weighting

- Impact to public safety: **HIGH - 3**
- Financial loss: **HIGH - 3**
- Disruption of production: **MEDIUM - 2**
- Loss of brand reputation: **LOW – 1**

Combining the list of criteria with their assigned weighting values, Stinky Cheese develops and agrees on the cyber-Event scoring matrix on the next page.

Table 1. cyber-Event scoring matrix for evaluating each cyber-Event.

		HCE Severity Scoring			
		None (0)	**Low (1)**	**Medium (3)**	**High (5)**
Criteria Weighting	Impact to Public Safety $\alpha = 3$	There is no risk to public safety.	There is a low but definite risk to public safety—a few illnesses but no deaths occur.	Danger to public safety is widespread due to significant numbers of illnesses, but no deaths occur.	Danger to public safety is widespread including significant numbers of illnesses and one or more deaths.
	Financial Loss $\beta = 3$	Financial losses are insignificant or nonexistent.	Financial losses are significant, but well within the company's ability to recover from within 1 year or less.	Financial losses are substantial and will require multiple years to recover from.	Financial losses are substantial and may result in bankruptcy of the company.
	Disruption of Production $\gamma = 2$	Production will not be disrupted.	Production is disrupted for 1 week, leading to shortages, but it can be recuperated within a month or less. Some orders will be delayed.	Production is disrupted for a month, leading to serious shortages requiring up to a year to recuperate. Existing orders are cancelled or significantly delayed.	Production is disrupted for 3+ months. Existing orders are cancelled or significantly delayed. Additional orders are not accepted during disruption.
	Loss of Brand Reputation $\delta = 1$	There is no risk of damage to the brand's reputation.	The brand is slightly damaged but not widely considered untrustworthy. Poor public opinion is minimal and temporary.	The brand is seriously damaged and generally considered untrustworthy but can be restored with significant, sustained effort.	The brand is irreparably damaged and may be considered untrustworthy by wide public consensus.

Table 2. Scoring cyber-Event #1: Excessive Pasteurization.

		HCE Severity Scoring			
		None (0)	Low (1)	Medium (3)	High (5)
Criteria Weighting	Impact to Public Safety α = 3		There is a low but definite risk to public safety—a few illnesses but no deaths occur.		
	Financial Loss β = 3		Financial losses are significant, but well within the company's ability to recover from within 1 year or less.		
	Disruption of Production γ = 2		Production is disrupted for 1 week, leading to shortages, but it can be recuperated within a month or less. Some orders will be delayed.		
	Loss of Brand Reputation δ = 1		The brand is slightly damaged but not widely considered untrustworthy. Poor public opinion is minimal and temporary.		

Score for cyber-Event #1:

$\alpha 1 + \beta 1 + \gamma 1 + \delta 1 =$

$3(1) + 3(1) + 2(1) + 1(1) =$

$3 + 3 + 2 + 1 =$

9

Table 3. Scoring cyber-Event #2: Overheat.

		HCE Severity Scoring			
		None (0)	Low (1)	Medium (3)	High (5)
Criteria Weighting	Impact to Public Safety α = 3		There is a low but definite risk to public safety—a few illnesses but no deaths occur.		
	Financial Loss β = 3		Financial losses are significant, but well within the company's ability to recover from within 1 year or less.		
	Disruption of Production γ = 2		Production is disrupted for 1 week, leading to shortages, but it can be recuperated within a month or less. Some orders will be delayed.		
	Loss of Brand Reputation δ = 1		The brand is slightly damaged but not widely considered untrustworthy. Poor public opinion is minimal and temporary.		

Score for cyber-Event #2:

$\alpha 1 + \beta 1 + \gamma 1 + \delta 1 =$

$3(1) + 3(1) + 2(1) + 1(1) =$

$3 + 3 + 2 + 1 =$

9

Table 4. Scoring cyber-Event #3: No pasteurization.

		HCE Severity Scoring			
		None (0)	Low (1)	Medium (3)	High (5)
Criteria Weighting	Impact to Public Safety α = 3				Danger to public safety is widespread including significant numbers of illnesses and one or more deaths.
	Financial Loss β = 3			Financial losses are substantial and will require multiple years to recover from.	
	Disruption of Production γ = 2				Production is disrupted for 3+ months. Existing orders are cancelled or significantly delayed. Additional orders are not accepted during disruption.
	Loss of Brand Reputation δ = 1			The brand is seriously damaged and generally considered untrustworthy but can be restored with significant, sustained effort.	

Score for cyber-Event #3:

$\alpha 5 + \beta 3 + \gamma 5 + \delta 3 =$

$3(5) + 3(3) + 2(5) + 1(3) =$

$15 + 9 + 10 + 3 =$

37

Table 5. Scoring cyber-Event #4: Insufficient pasteurization.

		HCE Severity Scoring			
		None (0)	Low (1)	Medium (3)	High (5)
Criteria Weighting	Impact to Public Safety α = 3			Danger to public safety widespread due to significant numbers of illnesses, but no deaths occur.	
	Financial Loss β = 3			The financial loss is substantial and will require multiple years to recover from.	
	Disruption of Production γ = 2				Production is disrupted for 3+ months. Existing orders are cancelled or significantly delayed. Additional orders are not accepted during
	Loss of Brand Reputation δ = 1			The brand is seriously damaged and generally considered untrustworthy but can be restored with significant, sustained effort.	

Score for cyber-Event #4:

α3 + β3 + γ5 + δ3 =

3(3) + 3(3) + 2(5) + 1(3) =

9 + 9 + 10 + 3 =

31

Criteria Weighting (1-3)			
Public Safety	Financial Loss	Production Disruption	Brand Reputation
3	3	2	1

		Event Scoring per Criteria (0, 1, 3, or 5)					
Event ID	Event Description	α	β	γ	δ	Severity Score	Severity %
1	Excessive Pasteurization	1	1	1	1	9	20%
2	Overheat	1	1	1	1	9	20%
3	No Pasteurization	5	3	5	3	37	82.2%
4	Insufficient Pasteurization	3	3	5	3	31	68.9%

Figure 1. cyber-Event Scoring Summary

HCE Identification

Given time and resource constraints, Stinky Cheese decided to move forward with only HCE. Using the criteria established previously, **cyber-Event #3 scores the highest.** Since Stinky Cheese will only work on one High Consequence Event during this CCE engagement, "cyber-Event #3: No Pasteurization" **will serve as the HCE**.

Phase 2: System-of-Systems Analysis

Creating an HCE block diagram

The starting point for Phase 2, System-of-Systems Analysis, is the creation of a simple block diagram depicting the HCE from a functional perspective. The HCE block diagram should identify which of the entity's production or business functions an adversary would have to disrupt to cause the HCE. See Figure 2 for Stinky Cheese's HCE block diagram, based off the HCE identified in Phase 1.

High Consequence Event:
The adversary gains access to the cheese production control system environment and targets the pasteurization process control/monitoring functions. Malicious modifications focus on the pasteurization temperature control. The controller logic is changed to ensure that the process temperature never reaches required limits for destroying bacteria and harmful microbes in the milk. Attacker ensures that no indications (HMI) or notifications (alarming) are presented to the system operators.

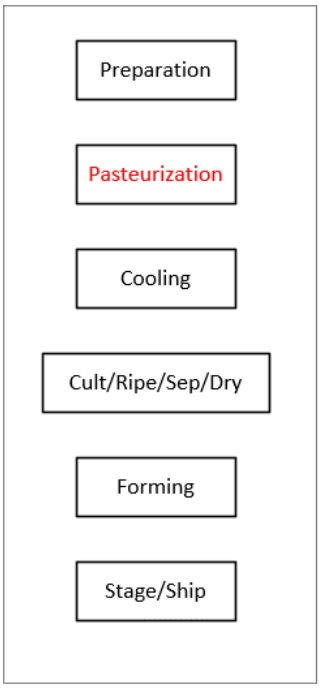


Figure 2: Stinky Cheese's HCE description (above) and HCE block diagram (below).

"Perfect knowledge" and its benefits

Phase 2 continues with a deeper look at the production or business function(s) identified in the HCE block diagram above. The entity (in this case, Stinky Cheese) knows best how it delivers these functions, and CCE leverages that unique and in-depth understanding from a technical and operational perspective.

Stinky Cheese will focus on to identifying, assessing, and categorizing "artifacts" that describe details of the systems, system configurations, system operations, supply chain, and other personnel support activities present in delivery of the pasteurization function that is targeted in the HCE. Stinky Cheese must iteratively consider the following:

- What systems and components are involved in the HCE?
- What documentation is needed to describe interconnected systems and dependencies?
- What relationships with other entities are involved?

Stinky Cheese starts with the system/component that must be affected to cause the HCE and works outward. Success here is measured by developing "perfect knowledge" of the system(s), operations, and support. Artifacts collected should include details of the target system(s), including logical and physical connectivity, system dependencies, controllers, technical and operational manuals, engineering/process/communications diagrams, protocols, access lists, associated manufacturers, trusted relationships, contractors, suppliers, emergency procedures, personnel lists, etc.

Keep in mind, the objective is to identify not only the technical and operational details, but also where the information is documented and stored. Stinky Cheese must determine if the critical information is stored only on internal servers or is also available on public-facing assets.

Establishing "perfect knowledge" is most accurately and efficiently executed through the development and use of a functional taxonomy.

Functional Taxonomy

Background/Purpose
The CCE functional taxonomy is a relational framework used for describing an organization's critical functions, the people, process, technology (PPT) that enable those critical functions, and the artifacts that document an entity's unique implementation for function delivery. Most importantly, the taxonomy maps the organization's critical functions (CFs) and those enabling functions (EF) that support them. The artifacts and their relative location within the taxonomy framework describe the "what", "where", "when", "how," and "who" of the HCE.

Method
Specialized visualization applications like MindManager[3] are effective tools for capturing the hierarchical organization and mapping of relationships between objects. If specialized applications are not available to the CCE Team, taxonomy mapping can also be accomplished using a spreadsheet like Excel.

[3] Visit https://www.mindmanager.com/en/product/mindmanager/ to learn more about MindManager's mind mapping software.

Approach

CCE taxonomy mapping begins by naming the entity (Stinky Cheese) at the root level of the taxonomy structure and creating the Entity Box (see Figure 3). Every object created in the mapping from here forward will describe a part or function of Stinky Cheese (e.g., business, business subsector, etc.).

From here, a CCE taxonomy clearly divides the functional mapping into two halves. The right-hand side are branches of CFs that describe the actions or activities making up Stinky Cheese's primary purpose. If any of these CFs are disrupted by an adversary, it would result in the worst of 'bad days' for Stinky Cheese.

The left-hand side is reserved for mapping EF branches. EFs describe the infrastructure, people, processes, technologies, and systems Stinky Cheese uses to both physically and logically deliver its CFs.

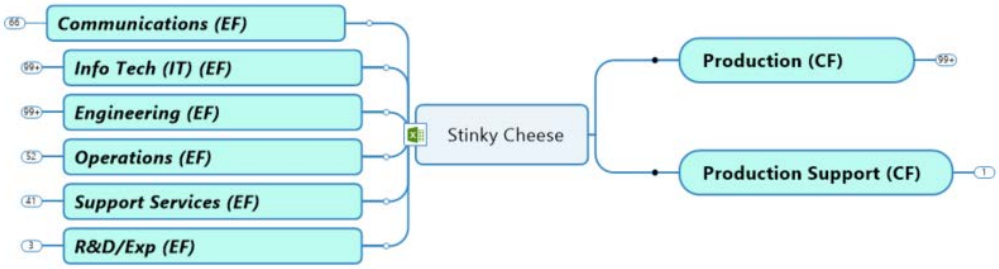


Figure 3: Taxonomy mapping starts by creating the Entity Box and describing high-level CFs and EFs.

Critical and Enabling Functions Mapping

A functional taxonomy mapping for Stinky Cheese is shown in Figures 4 through 9 below. These figures demonstrate how Stinky Cheese has located elements and created branches required to document its critical functions and the delivery of these functions.

As a general note, it is understood that the language used may not be universal and that practitioners (engineers, technicians, operators, etc.) from specific entities and/or sectors may use differing terms.

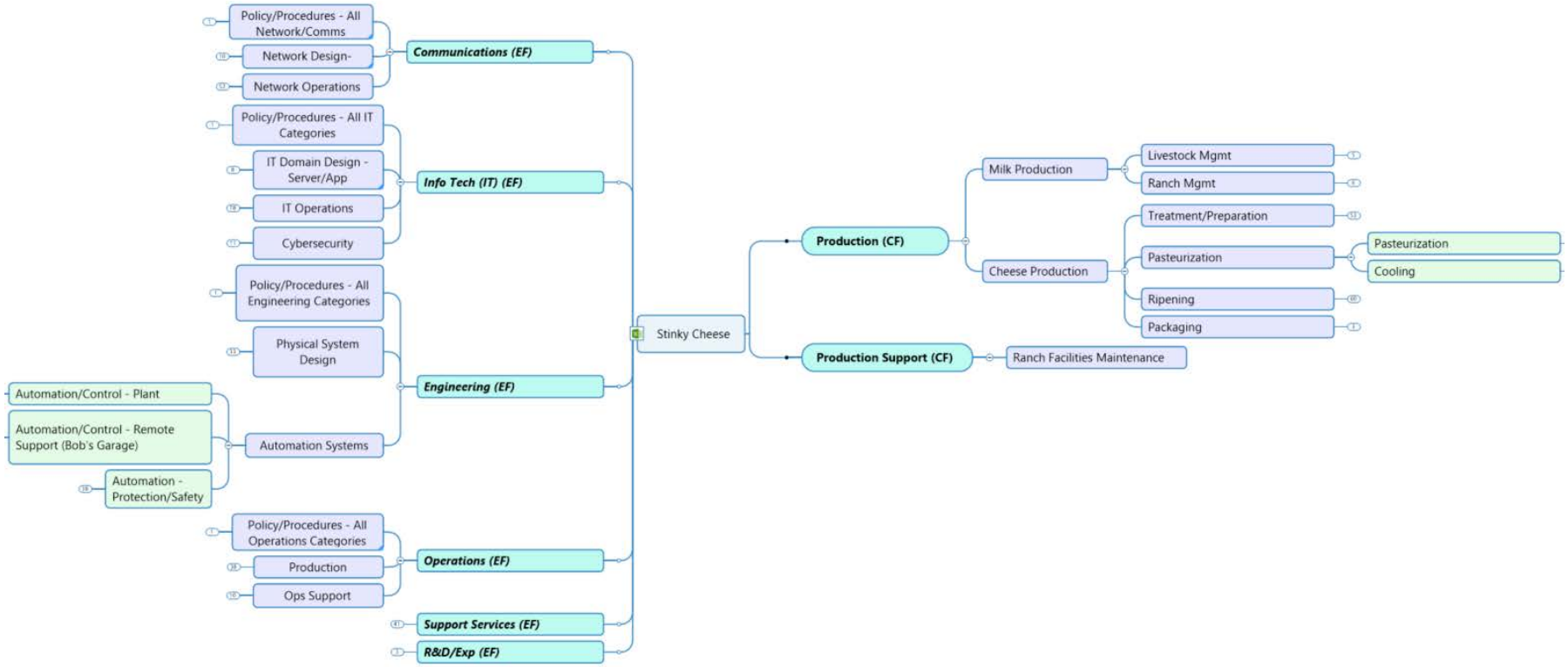


Figure 4: A draft of Stinky Cheese's functional taxonomy with developed **critical functions** (right) and **enabling functions** (left).

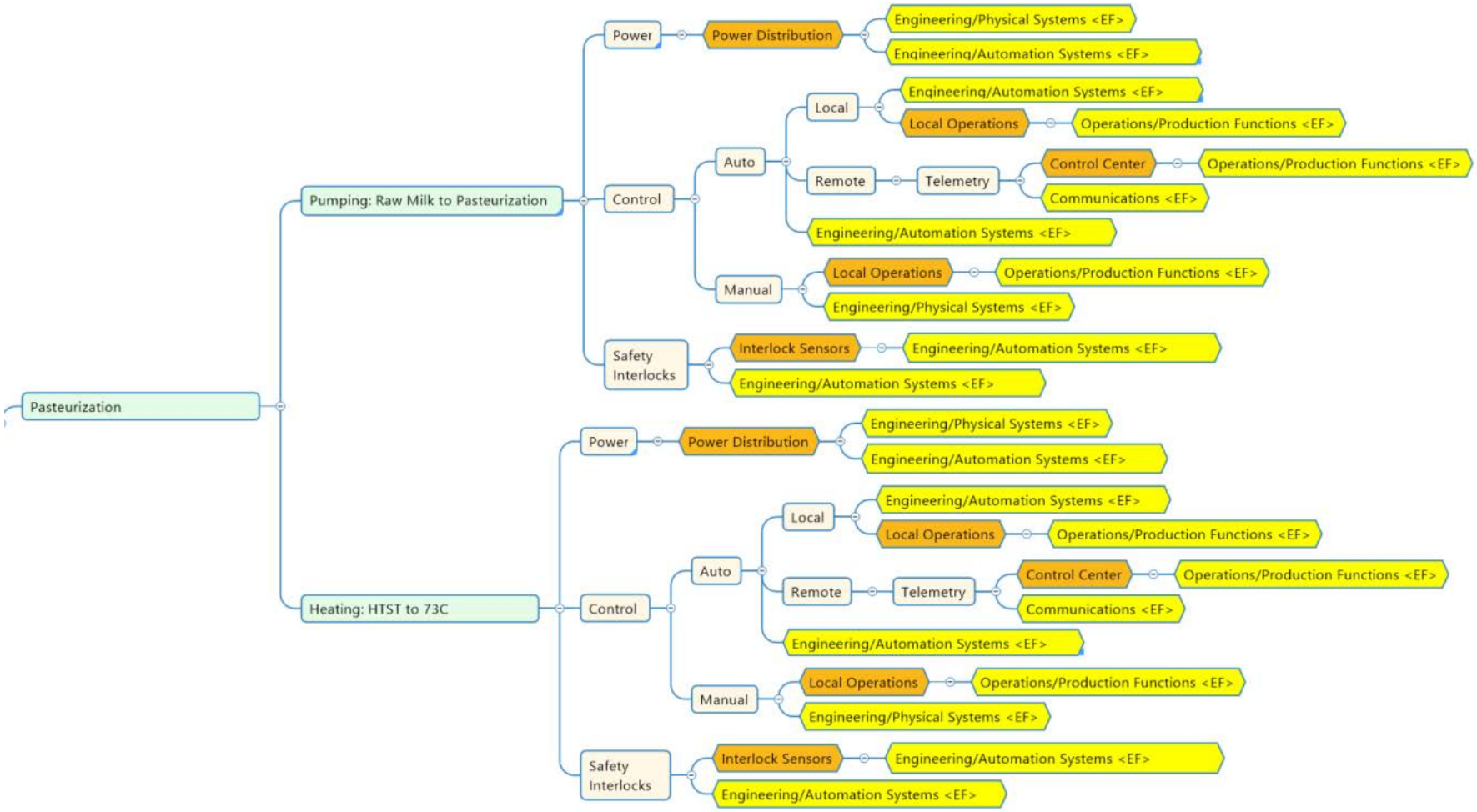


Figure 5: Further expansion of the example right-hand side (CFs) for Stinky Cheese's functional taxonomy.

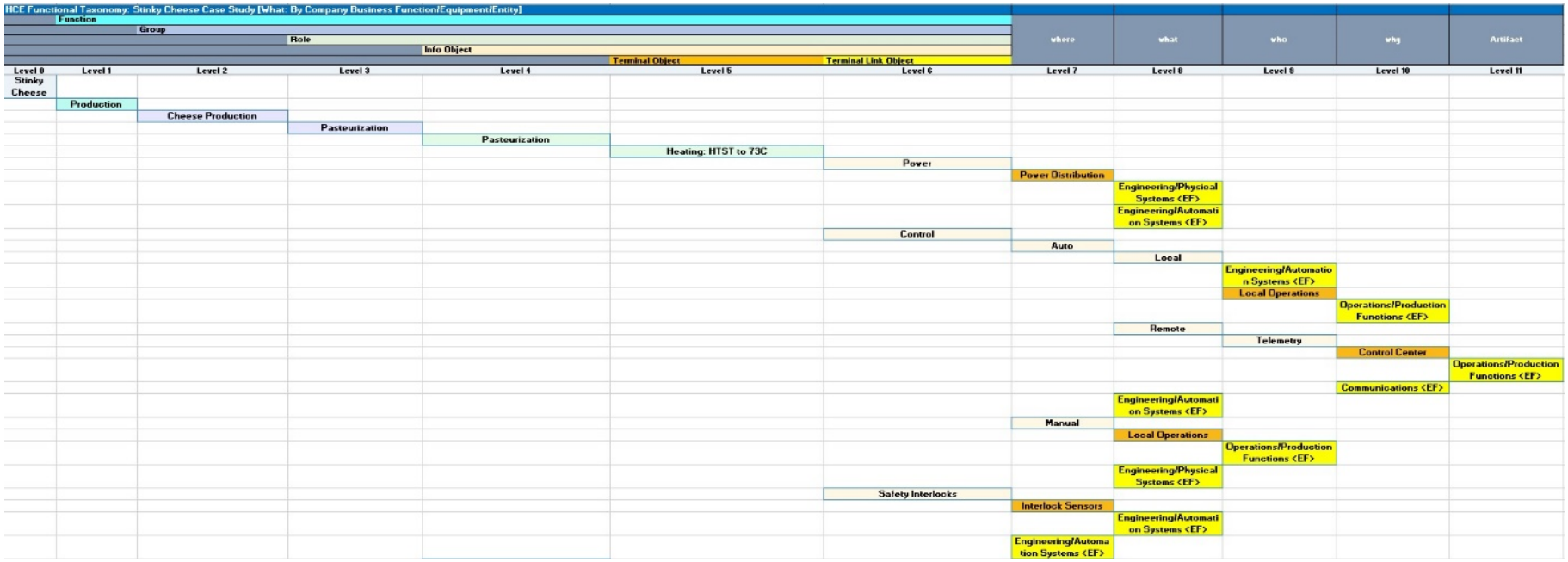


Figure 6: Screenshot of an equivalent “spreadsheet version” of right-hand side (CFs) for Stinky Cheese’s functional taxonomy.

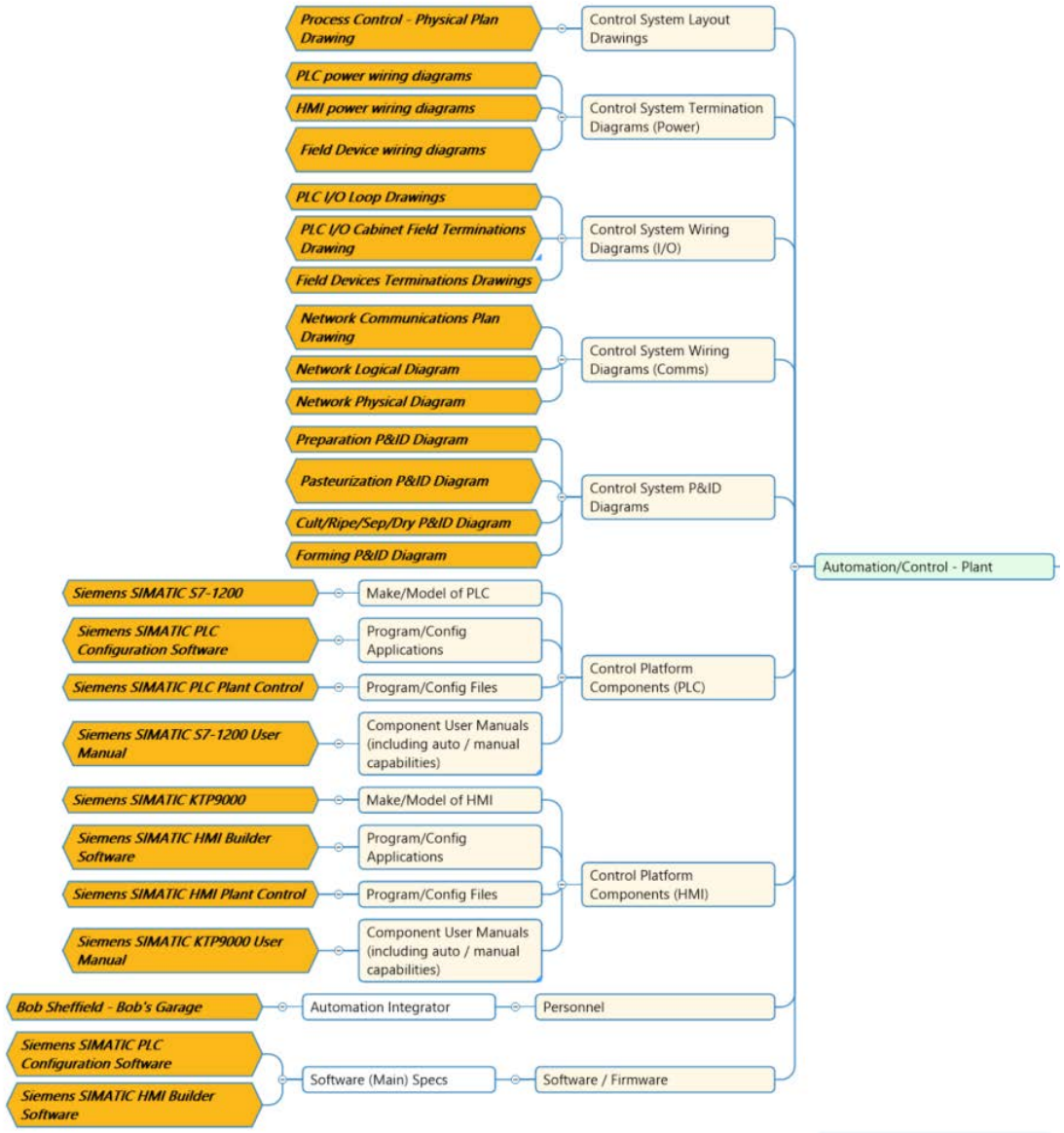


Figure 7: Further expansion of the example left-hand side (EFs) for Stinky Cheese's functional taxonomy.

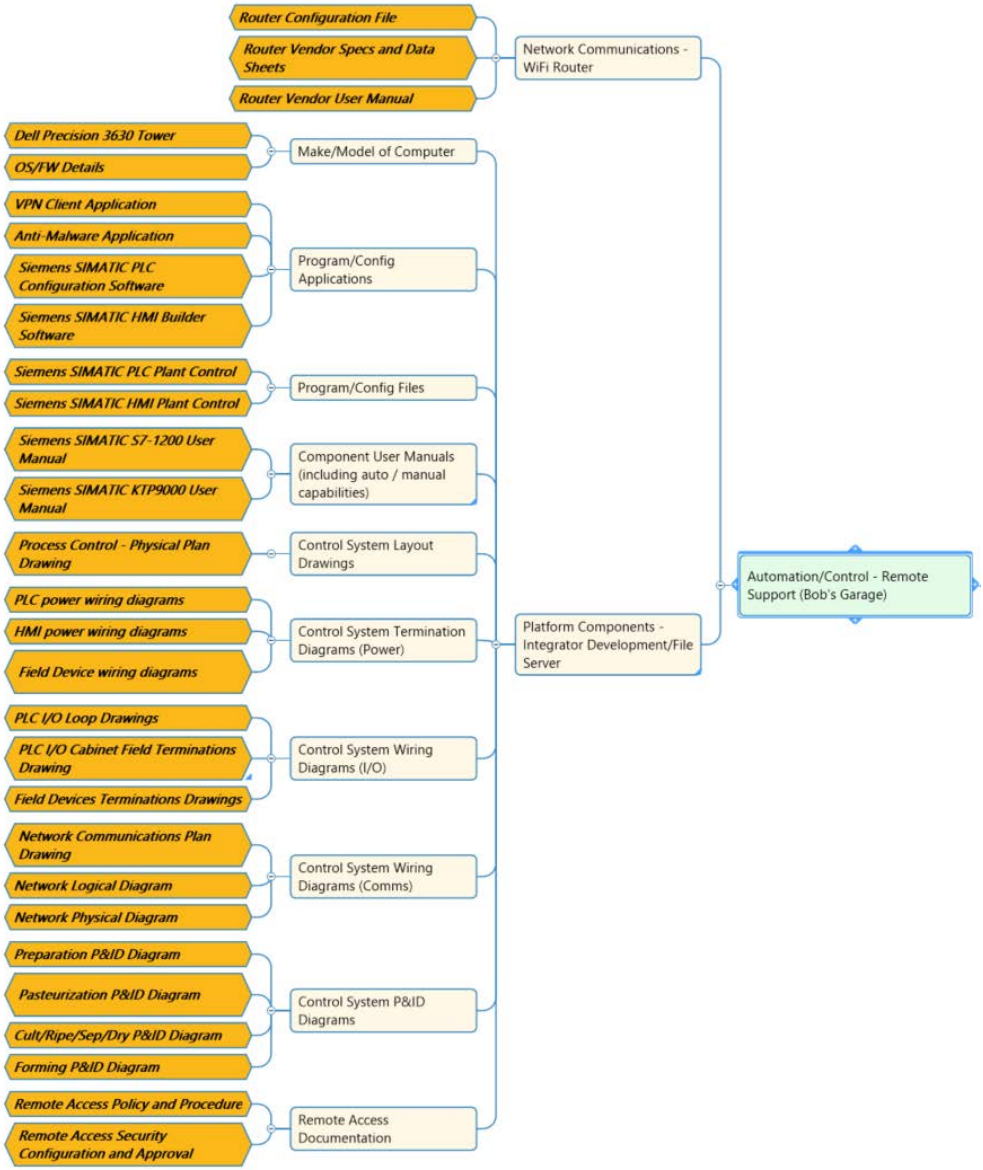


Figure 8: Further expansion of the example left-hand side (EFs) for Stinky Cheese's functional taxonomy (***continued***).

HCE Functional Taxonomy: Stinky Cheese Case Study [What: By Company Business Function/Equipment/Entity]						
	Function					
		Group				
			Role			
				Info Object		
					Terminal Object	Terminal Link Object
Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
Stinky Cheese						
	Engineering					
		Automation Systems				
			Automation/Control – Remote Support (Bob's Garage)			
				Network Communications – WiFi Router		
					Router Configuration File	
					Router Vendor Specs and Data Sheets	
					Router Vendor User Manual	
				Platform Components – Integrator Development/File Server		
					Make/Model of Computer	
						Dell Precision 3630 Tower
						OS/FW Details
					Program/Config Applications	
						VPN Client Application
						Anti-Malware Application
						Siemens SIMATIC PLC Configuration Software
						Siemens SIMATIC HMI Builder Software
					Program/Config Files	
						Siemens SIMATIC PLC Plant Control
						Siemens SIMATIC HMI Plant Control
					Component User Manuals (including auto / manual capabilities)	
						Siemens SIMATIC S7-1200 User Manual
						Siemens SIMATIC KTP9000 User
					Control System Layout Drawings	
						Process Control – Physical Plan
					Control System Termination Diagrams	
						PLC power wiring diagrams
						HMI power wiring diagrams
						Field Device wiring diagrams
					Control System Wiring Diagrams (I/O)	
						PLC I/O Loop Drawings
						PLC I/O Cabinet Field Terminations
						Field Devices Terminations Drawings
					Control System Wiring Diagrams (Comms)	
						Network Communications Plan Drawing
						Network Logical Diagram
						Network Physical Diagram
					Control System P&ID Diagrams	
						Preparation P&ID Diagram
						Pasteruization P&ID Diagram
						Cult/Ripe/Sep/Dry P&ID Diagram
						Forming P&ID Diagram
					Remote Access Documentation	
						Remote Access Policy and Procedure
						Remote Access Security Configuration and Approval

Figure 9: Screenshot of an equivalent "spreadsheet version" of the left-hand side (EFs) for Stinky Cheese's functional taxonomy.

System Description

A System Description is a summary of all the information Stinky Cheese gathered in Phase 2. This description should summarize the functional taxonomy mapping and provide traceability to where all the information resides—as well as who has access to it. This will be the output of Phase 2 and the input to Phase 3. A System Description for this use case is detailed below.

System Description: Cheese Production

Stinky Cheese's creamery is a 147-acre industrial complex adjacent to the Kase Ranch. The state-of-the-art creamery includes the Treatment and Pasteurization Facility, Ripening Depot, and Packaging Plant. Expert staff confidently claim that Stinky Cheese's sterile facilities and advanced pasteurization process ensure only the safest cheese products are made at Stink Cheese.

Stinky Cheese focuses on one batch of cheese at a time. The meticulous and undivided attention on each batch ensures the cheese products are exceptional, the impact to the environment is minimal, and the cows stay happy! Stinky Cheese finishes a fresh batch of 1,000 wheels of cheese a week—that's 10 tons of cheese!

The state-of-the-art production process includes raw milk preparation, pasteurization, cooling, culturing, ripening, separation, drying, forming, staging, and shipping. Figure 10 below is another functional block diagram that identifies the HCE. This more developed version is an extremely useful starting point for building out the System Description.

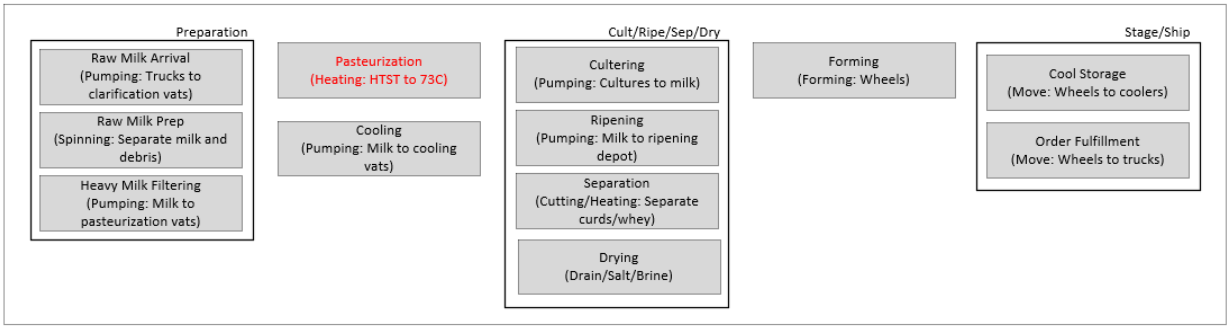


Figure 10. A further developed HCE block diagram showing production details and sequences for the entire cheesemaking process.

System Description: Pasteurization

Due to the volume of fresh cheese that Stinky Cheese produces every week, pasteurization of 10,000 gallons of milk must occur during a single 10-hour shift to allow time for cheesemaking and packaging activities each day. To accomplish this, Stinky Cheese uses a high-temperature short-time (HTST) pasteurization system called the MU1000. This HTST system is capable of pasteurizing 1,000 gallons of raw milk per hour. Also known as "continuous" or "flash" pasteurization, the HTST system is designed to heat and hold milk at a set temperature and duration prior to cooldown to destroy bacteria and other microbes in the milk. The HTST system is highly complex, but it allows a high volume of raw milk to continuously pass through the pasteurization process. As a result, it is a more efficient start to the cheesemaking process.

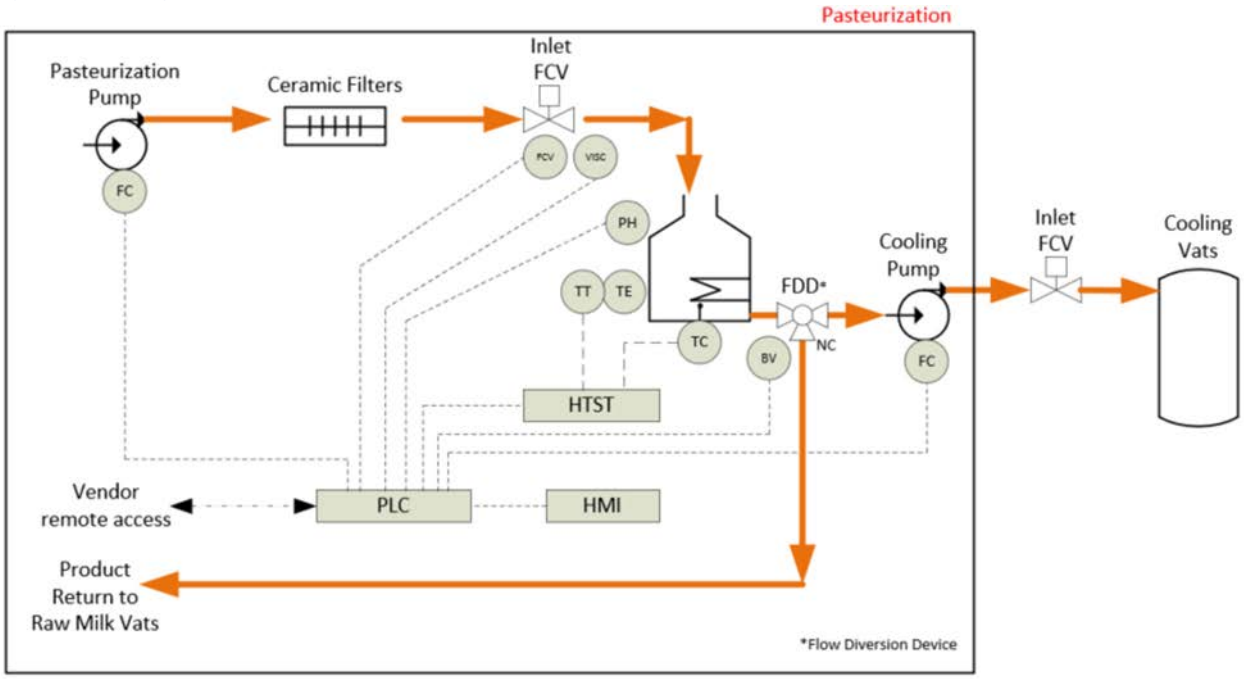


Figure 11. Pasteurization major control elements.

The MU1000 HTST system pasteurizes raw milk at 73°C for 18 seconds. The steps to accomplish this are:

1. Raw milk is pumped from a storage tank into the raw milk regenerator of the MU1000 to warm it to 65°C.
2. Raw milk is then continuously and consistently pumped through closely spaced plates of the MU1000 pasteurization heater. Hot water (83°C) heated by a boiler is pumped alongside both sides of the plates. (See Figure 12)
3. The milk and hot water are pumped through the heater plates for 18 seconds, allowing the hot water to heat the milk to 73°C. (See Figure 13)

Figure 12. Image of the MU1000.

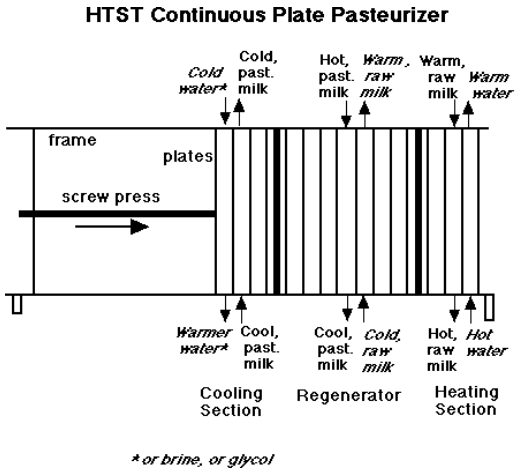


Figure 13. Heater plates.

4. At 73°C and under pressure, the milk passes through and is held in a holding tube for 18 seconds. Meanwhile, the water diverges away from the heater, feeding back into the hot water boiler for reheating.
5. After passing a temperature sensor (indicating thermometer) at the end of the holding tube, milk passes into the flow diversion device (FDD). The FDD assumes a forward-flow position if the milk passes the set temperature control (73°C). The FDD remains in normal position (diverted flow) if milk has not achieved 73°C per the temperature sensor. Improperly heated milk flows back to the raw milk tank. Correctly heated milk flows through the FDD forward flow to the pasteurized milk regenerator while gradually losing heat to reach approximately 50°C.
6. Warm milk then passes through cooling plates, where the milk is cooled to 32°C via coolant flowing along the outsides of the plates.
7. The pasteurized milk then flows through a vacuum breaker (to prevent back-siphoning) to the cheese vat.

System Description: Controls Platforms

The MU1000 system uses a Siemens SIMATIC S7-1200 PLC for pasteurization process control. The operator interface is a Siemens SIMATIC KTP900 HMI.

HMI Temp Control Screenshot

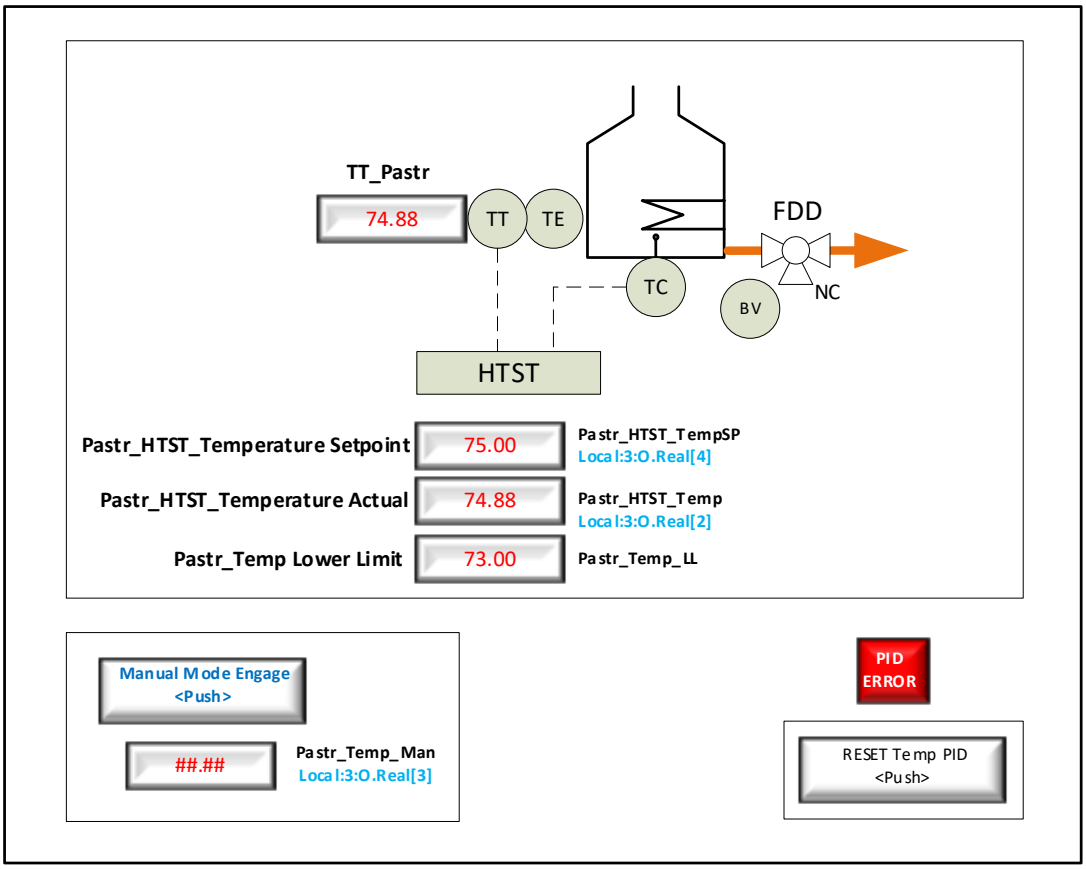


Figure 14. MU1000 Siemens HMI screen.

System Description: Operations

During each 10-hour shift, pasteurization operators are responsible for following a set of operating procedures for the MU1000. These procedures include:

1. Check sensor value setpoints from HMI to ensure they are meeting standard values. Adjust if necessary.
2. Start equipment.
3. Check/record HMI readings of temperature and the statuses on flow rate, pumps, and valves 20 minutes after startup.
4. Conduct equipment walkdown to ensure no physical signs of damage; check manual valves for leakages.
5. Check/record HMI readings of temperature and the statuses on flow rate, pumps, and valves 5 hours after startup.
6. Check/record HMI readings of temperature and the statuses on flow rate, pumps, and valves 20 minutes before process completion.
7. Conduct equipment walkdown to ensure no physical signs of damage; check manual valves for leakages.
8. Initiate an automatic high temperature steam clean sequence.
9. Shutdown equipment.

**If setpoints or readings do not match, the operator must shutdown equipment and contact technician to investigate.*

System Description: Vendor Support

A controls system vendor will provide patented, digitally connected thermostats, remote controllers, and HMIs that allow for local and remote monitoring of temperatures critical to the cheesemaking process. Component designs—which use the SIMATIC S7 backbone—and programming allow operators to monitor temperature values within the flash pasteurization process locally and remotely. Operators can also use this technology to make adjustments as needed throughout the process.

The program provides operators with flow management, remote and local temperature monitoring, high/low temperature alarms, trend analysis for future maintenance, and integrated network connectivity, resulting in a complete, digital view of the cheesemaking process from raw milk to final product. In addition to the local and remote monitoring of the system by operators, vendors will also be able to offer 24/7 remote support for instant access, monitoring, and troubleshooting of system components. This allows for proactive corrective maintenance and code development to assist operators with any issues. Additionally, access to diagrams and program code will be available to the customer on a supported server.

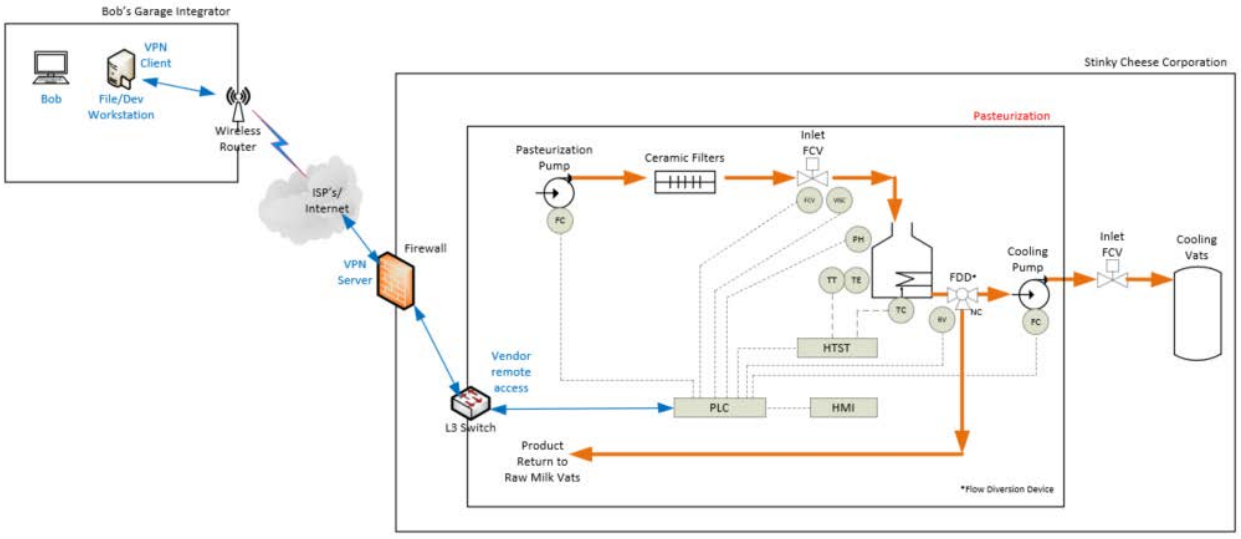


Figure 15. Network connectivity allowing vendor support to pasteurization process.

Phase 3: Consequence-based Targeting

The System Description developed in Phase 2 will be the starting point for Phase 3 as we examine the system from an adversarial perspective. We will try to determine what elements of the system the adversary needs to manipulate to achieve the HCE.

For any given HCE, there are likely many paths an adversary could take to achieve a particular outcome. Thus, a primary goal of Phase 3 is identifying any points that an adversary ***must*** access or traverse—known as "choke points." Choke points are ideal locations to implement potential mitigations and protections, as they effectively provide a way to cut off (or at least detect) the adversary's progress.

For the purposes of Phase 3, we will consider two stages of adversary activity: payload development and payload deployment. For this HCE, and for each of these stages, we use Phase 2's System Description (and supporting documentation as needed) to help identify the adversary's:

1) **System Targeting Description**: Combination of the System Description and the system analysis for targeting.
2) **Technical Approach**: What the adversary must do to cause the HCE.
3) **Target Details:** Detailed description of the system component(s) the adversary needs to manipulate to cause the HCE.

Development Stage

System Targeting Description

High Consequence Event: Adversary gains access to the cheese production control system environment and targets the pasteurization process control/monitoring functions. Malicious modifications focus on the pasteurization temperature control. The controller logic is changed such that pasteurization temperature is rendered inadequate for destroying bacteria and harmful microbes in the milk. Attacker ensures that no indications (HMI) or notifications (alarming) are presented to the system operators.

Stinky Cheese Production Facility: Physical Location, Process Subsystems, and Distribution Breadth

System Description: Cheese Production

The company's creamery is a 147-acre industrial complex adjacent to the Kase Ranch. The state-of-the-art creamery includes the Treatment and Pasteurization Facility, Ripening Depot, and Packaging Plant. Expert staff confidently claim that Stinky Cheese's sterile facilities and advanced pasteurization process ensure only the safest cheese products are made at Stink Cheese.

Stinky Cheese focuses on one batch of cheese at a time. The meticulous and undivided attention on each batch ensures the cheese products are exceptional, the impact to the environment is minimal, and the cows stay happy! Stinky Cheese finishes a fresh batch of 1,000 wheels of cheese a week—that's 10 tons of cheese!

The state-of-the-art production process includes raw milk preparation, pasteurization, cooling, culturing, ripening, separation, drying, forming, staging, and shipping.

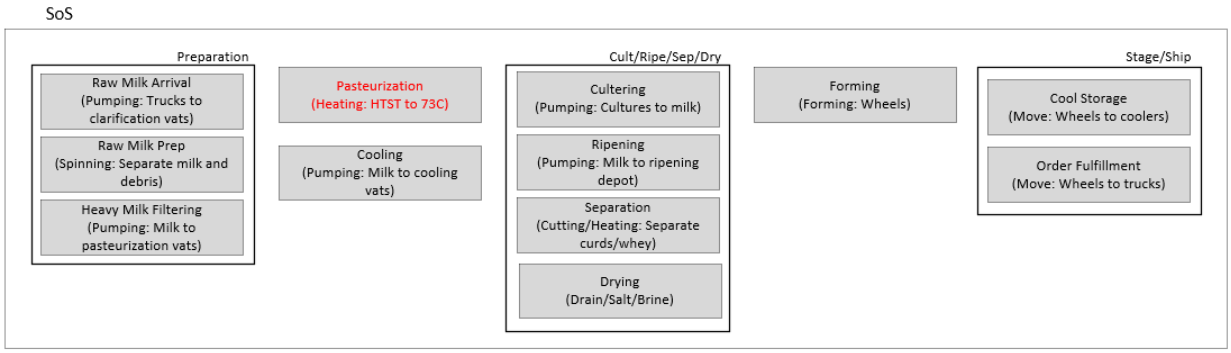


Figure 16. From Phase 2 (SoS Analysis) – Example highly developed HCE block diagram showing production details and sequences for the entire cheesemaking process.

Production Process: Critical Subsystem and Major Control Elements

System Description: Pasteurization

Due to the volume of fresh cheese that Stinky Cheese produces every week, pasteurization of 10,000 gallons of milk must occur during a single 10-hour shift to allow time for cheesemaking and packaging activities each day. To accomplish this, Stinky Cheese uses a high-temperature short-time (HTST) pasteurization system called the MU1000. This HTST system is capable of pasteurizing 1,000 gallons of raw milk per hour. Also known as “continuous” or “flash” pasteurization, the HTST system is designed to heat and hold milk at a set temperature and duration prior to cooldown to destroy bacteria and other microbes in the milk. The HTST system is highly complex, but it allows a high volume of raw milk to continuously pass through the pasteurization process. As a result, it is a more efficient start to the cheesemaking process.

Critical Subsystem Process: Sequencing, Major Control Elements, Critical Parameters for Control

System Description: Pasteurization System Process Control

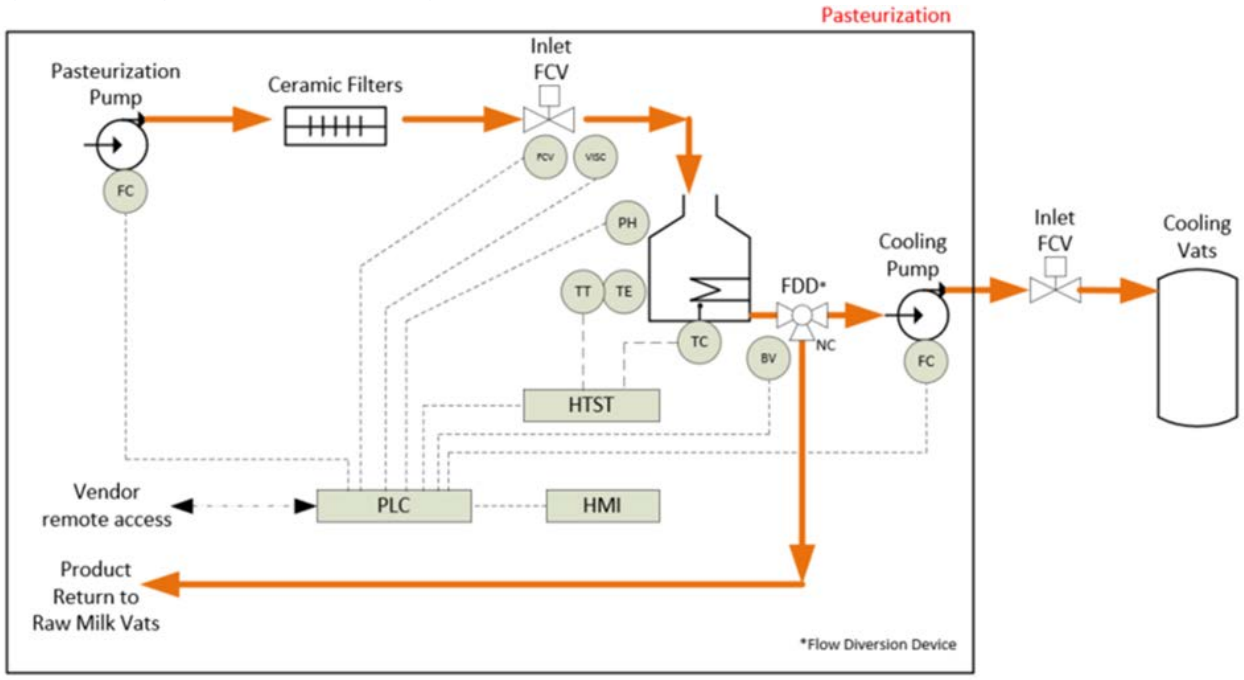


Figure 17. Pasteurization major control elements.

The MU1000 HTST system pasteurizes raw milk at 73°C for 18 seconds. The steps to accomplish this are:

1. Raw milk is pumped from a storage tank into the raw milk regenerator of the MU1000 to warm it to 65°C.
2. Raw milk is then continuously and consistently pumped through closely spaced plates of the MU1000 pasteurization heater. Hot water (83°C) heated by a boiler is pumped alongside both sides of the plates. (See Figure 18)
3. The milk and hot water are pumped through the heater plates for 18 seconds, allowing the hot water to heat the milk to 73°C. (See Figure 19)

Figure 18. Image of the MU1000.

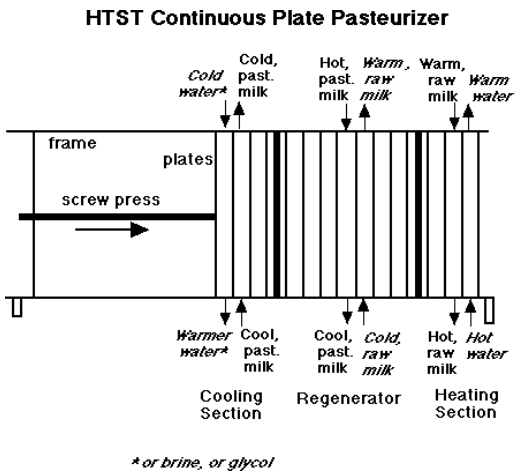


Figure 19. Heater plates

4. At 73°C and under pressure, the milk passes through and is held in a holding tube for 18 seconds. Meanwhile, the water diverges away from the heater, feeding back into the hot water boiler for reheating.
5. After passing a temperature sensor (indicating thermometer) at the end of the holding tube, milk passes into the flow diversion device (FDD). The FDD assumes a forward-flow position if the milk passes the set temperature control (73°C). The FDD remains in normal position (diverted flow) if milk has not achieved 73°C per the temperature sensor. Improperly heated milk flows back to the raw milk tank. Correctly heated milk flows through the FDD forward flow to the pasteurized milk regenerator while gradually losing heat to reach approximately 50°C.
6. Warm milk then passes through cooling plates, where the milk is cooled to 32°C via coolant flowing along the outsides of the plates.
7. The pasteurized milk then flows through a vacuum breaker (to prevent back-siphoning) to the cheese vat.

Critical Subsystem Process Control: Controller and HMI Identification, Process Screenshot (HMI)

System Description: Pasteurization System Controls Platforms

The MU1000 system uses a Siemens SIMATIC S7-1200 PLC to automate and monitor the pasteurization process. The PLC includes an integrated I/O interface to communicate and control based on sensor data from the pasteurization process. To view system status and change system state, the MU1000 features a Siemens SIMATIC HMI KTP900 basic HMI. Controller details include – Vendor: Siemens; Model: SIMATIC S7-1200; Function: Pasteurization Process Controller; and Supported Protocols: Ethernet, Modbus TCP. HMI details include - Vendor: Siemens; Model: SIMATIC KTP9000; Function: Pasteurization Process – Operator Interface; and Supported Protocols: Ethernet, Modbus TCP.

HMI Temp Control Screenshot

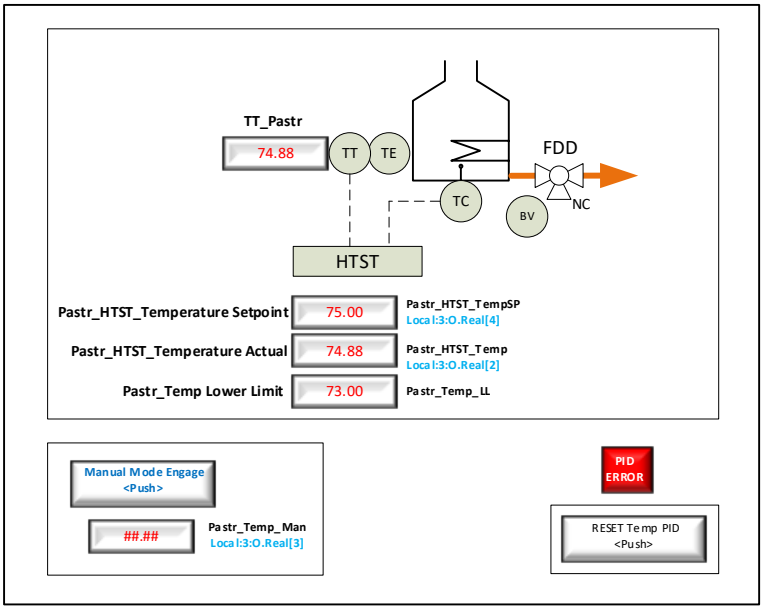


Figure 20. MU1000 Siemens HMI screen.

Critical Subsystem Operations: Process Parameter Monitoring and Process Visibility Source

System Description: Operations

During each 10-hour shift, pasteurization operators are responsible for following a set of operating procedures for the MU1000. These procedures include:

1. Check sensor value setpoints from HMI to ensure they are meeting standard values. Adjust if necessary.
2. Start equipment.
3. Check/record HMI readings of temperature and the statuses on flow rate, pumps, and valves 20 minutes after startup.
4. Conduct equipment walkdown to ensure no physical signs of damage; check manual valves for leakages.
5. Check/record HMI readings of temperature and the statuses on flow rate, pumps, and valves 5 hours after startup.
6. Check/record HMI readings of temperature and the statuses on flow rate, pumps, and valves 20 minutes before process completion.
7. Conduct equipment walkdown to ensure no physical signs of damage; check manual valves for leakages.
8. Initiate an automatic high temperature steam clean sequence.
9. Shutdown equipment.

**If setpoints or readings do not match, the operator must shutdown equipment and contact technician to investigate.*

Production Automation: Vendor Technical Support (Engr, Programming) and Remote Access Capabilities.

System Description: Vendor Support for Pasteurization Controls System

A controls system vendor will provide patented, digitally connected thermostats, remote controllers, and HMIs that allow for local and remote monitoring of temperatures critical to the cheesemaking process. Component designs—which use the SIMATIC S7 backbone—and programming allow operators to monitor temperature values within the flash pasteurization process locally and remotely. Operators can also use this technology to make adjustments as needed throughout the process.

The program provides operators with flow management, remote and local temperature monitoring, high/low temperature alarms, trend analysis for future maintenance, and integrated network connectivity, resulting in a complete, digital view of the cheesemaking process from raw milk to final product. In addition to the local and remote monitoring of the system by operators, vendors will also be able to offer 24/7 remote support for instant access, monitoring, and troubleshooting of system components. This allows for proactive corrective maintenance and code development to assist operators with any issues. Additionally, access to diagrams and program code will be available to the customer on a supported server.

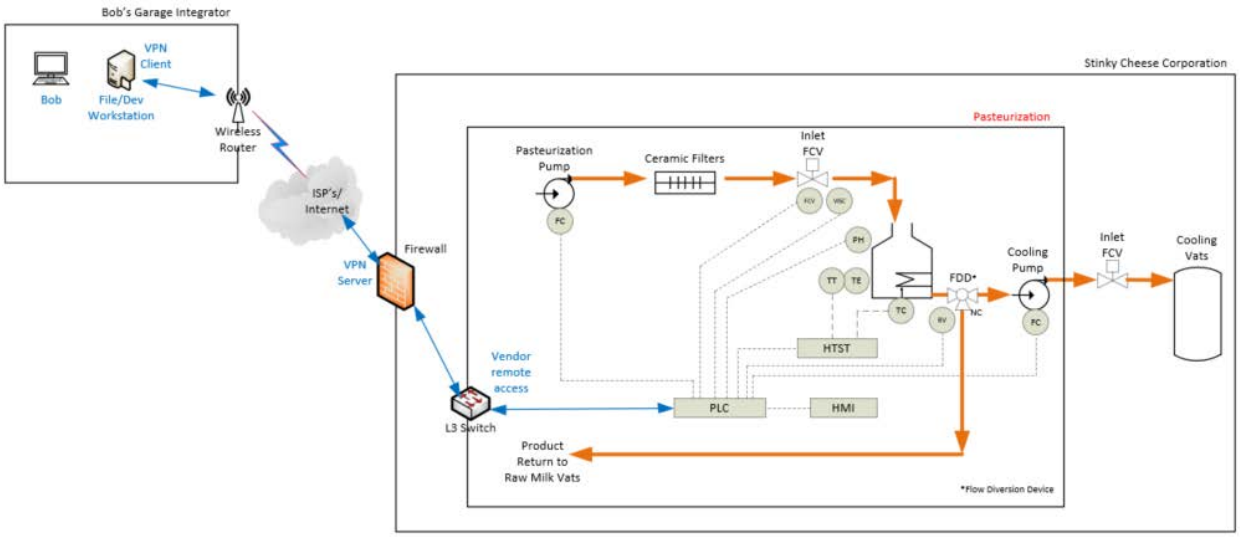


Figure 21. Network connectivity allowing vendor support to pasteurization process.

Critical Subsystem (Pasteurization): Process/Safety Requirement

Safety: Food Safety

Quality control issues around food safety would be an exception in terms of "continuous production" support. Because of the potential business risks, pasteurization issues would require production shutdown and troubleshooting. Disruption would likely impact production for 1 week minimum due to the combination of downtime and weekly product inventory discard.

System Analysis for Targeting

Additional analysis of key systems, components, people, processes, digital connectivity, and data flows that "fill in the gaps" and enable an adversary to assemble a relationally contiguous System Targeting Description for attack.

Key Additional Targeting Information and Steps (Reconnaissance – open source and target environment)

Technical Support: Vendor

Newspaper article (Muenster Instant News/Billings Nickel Post) identifies Stinky Cheese's process automation support vendor by name (Bob Sheffield – Bob's Garage). Online research provides his profile on LinkedIn. Open-source research produces the employee's home address. Social engineering confirms his ISP and further reconnaissance provides his home router Wi-Fi network ID and access credentials.

Vendor Development/File Workstation

Investigation of available documentation on the development/file host produces a "remote access procedure" for automation support, Stinky Cheese production network access credentials, production system P&ID, wiring, engineering drawings, control system device specs, configuration files, and the automation applications (Siemens SIMATIC PLC Configuration Software, Siemens SIMATIC HMI Builder Software). Details readily available on Bob's workstation (at time of targeting analysis) include –

Host

Vendor: Dell; Model: Precision 3630 Tower; OS/Misc.: x64, Windows 10 Enterprise; and Supported Protocols: TCP/IP/Ethernet, SSH, SNMP, HTTPS, HTTP.

Software
Vendor: Siemens; Name: SIMATIC PLC Configuration Software; Function: SIMATIC S7-1200 Configuration

Remote Connectivity: Targeted Pasteurization Process Controller

With the creation of a free online account at the control device vendor website (Siemens), "anonymous" review of technical documentation reveals a software application platform feature common to automation products that caches previously configured network communication paths. The communication paths are typically created by the technical support personnel as part of remote online controller engagement. The feature is utilized out of convenience because it eliminates the need to remember and reconfigure complex network location/IP specifics each time.

Technical Approach

Target 1 (T1): Bob's Garage Development/File Workstation
Access: Leveraging poor network security configuration (open broadcast of SSID, no MAC filter, default router credentials, unpatched firmware, etc.) on Bob's home Wi-Fi router, the adversary can compromise Bob's workstation using the persistent connection to home Wi-Fi network.
Timing/Triggering: Immediately upon access to Bob's home Wi-Fi network and connected workstation.
Action/Payload: The malware payload is installed on the workstation. The malware will target, compromise, and modify logic in the Stinky Cheese pasteurization process PLC the next time Bob establishes a remote network connection to the production environment.

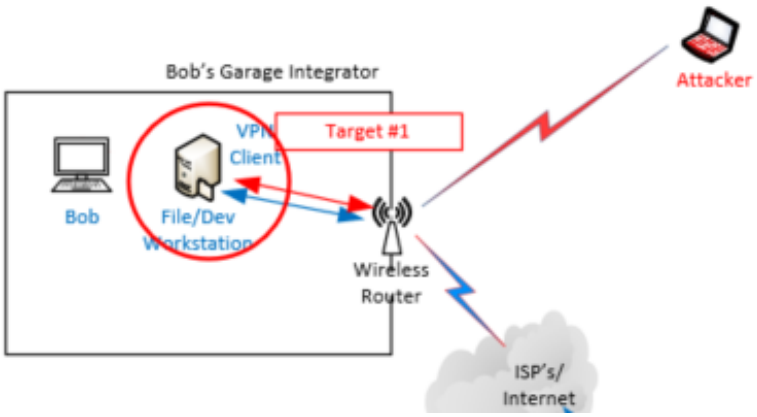


Figure 22. Access to Target #1.

Target 2 (T2): Process Controller: Siemens SIMATIC S7-1200 PLC
Access: Access is established through trusted remote connectivity from Bob's workstation via certificate-based authentication and VPN server configuration at Stinky Cheese's company firewall. Leveraging Bob's account (escalated privileges)—and the production environment's flat network architecture, as well as the absence of secondary independent authentication requirement—Bob's workstation quickly establishes a secure session with the pasteurization PLC.
Timing/Triggering: Immediately when Bob's workstation VPN establishes a connection to the Stinky Cheese production network.

Action/Payload: The Action involves changing temperature setpoints in the Siemens PLC to a temperature range below pasteurization needs. In the PLC, the adversary will modify PID coefficients to produce a targeted (23°C to 25°C) setpoint (tagname: **Pastr_HTST_TempSP**), which is communicated to the HTST. Supporting temperature tags (**e.g., Pastr_HTST_Temp**) will be modified to static "acceptable range" values before being communicated to the HMI. Tags related to normal FDD control communications will also be modified to static "acceptable range" values.

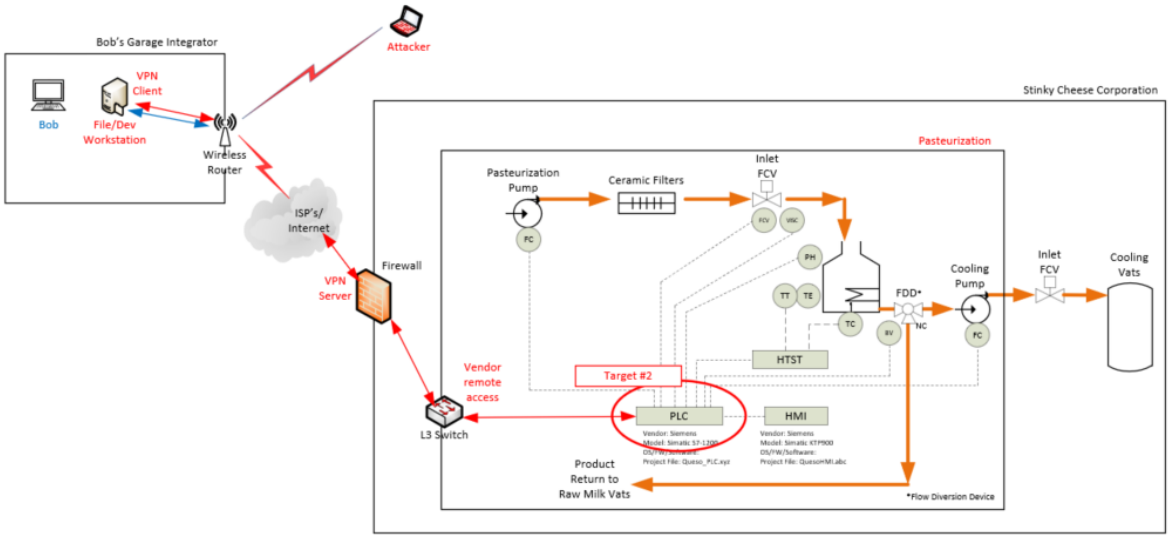


Figure 23. Access to Target #2.

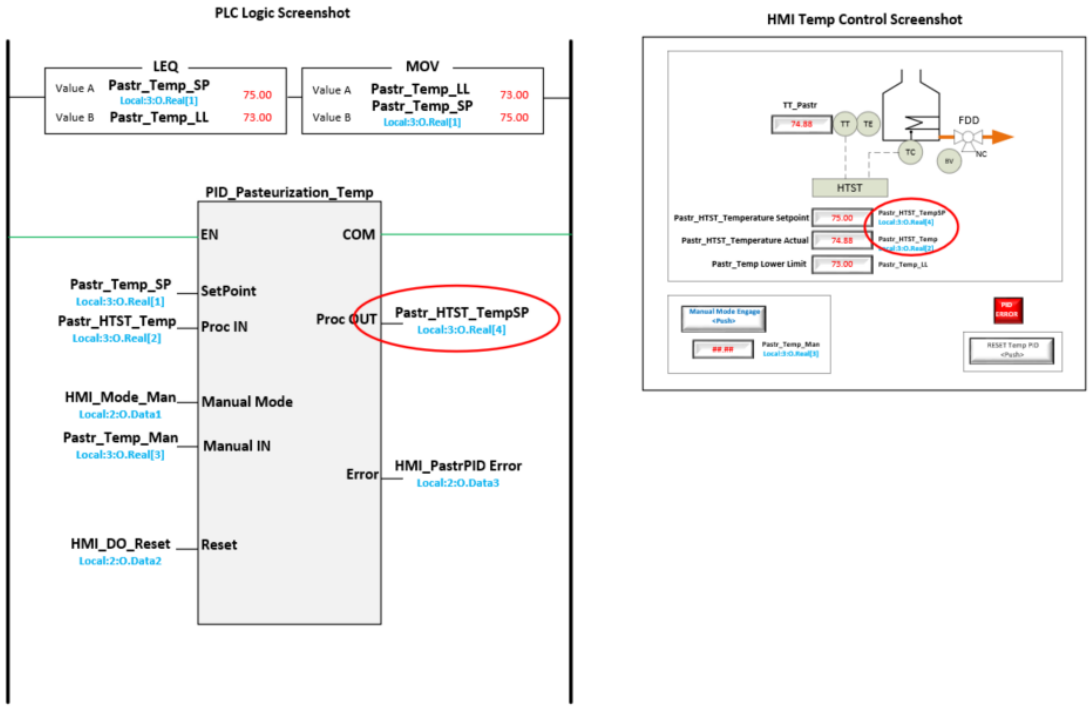


Figure 24. Target #2: PLC logic and HMI display.

Target Details

The Technical Approach described above identifies components that are integral and critical to carrying out the HCE attack. These components provide access, control, and monitoring for the pasteurization system (see Figure 25).

Recall, Bob's workstation was the first target (Target #1), where the attacker's payload is installed. When Bob connected remotely to the Stinky Cheese production system network, the payload immediately initiated and established trusted ("unverified") communications with the pasteurization process PLC (Target #2). The software platform leveraged for remote interaction was the Siemens SIMATIC Configuration Application.

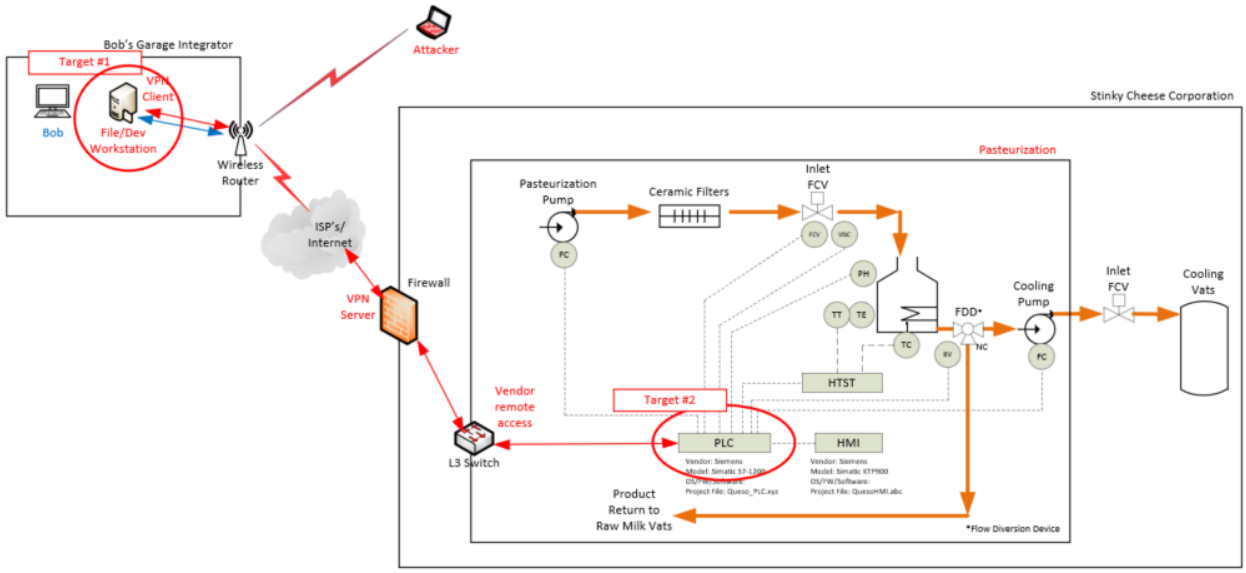


Figure 25. Updated targeting access path.

Adversary efforts to expand understanding of these critical systems and devices would involve development of a critical component list (see Table 6, below) providing technical details about each targeted element. Notice that the components list is a subset of taxonomy line items from Phase 2. In this case study example, the list would include details available via open-source vendor literature that were not provided already on the compromised workstation.

Table 6. Critical Components List with Target Details.

Bob's Engineering Workstation	Name	Dell Laptop
	Function	SCADA Engineer App/Data Host
	Vendor	Dell
	Model	Precision 3630 Tower
	OS/Misc.	x64, Windows 10 Enterprise
	Protocols	TCP/IP/Ethernet, SSH, SNMP, HTTPS, HTTP
Pasteurization Process Controller	Name	Pasteurization Process PLC
	Function	Pasteurization Process Controller
	Vendor	Siemens
	Model	SIMATIC S7-1200
	Protocols	Ethernet, Modbus TCP
Pasteurization Process HMI	Name	Pasteurization Process HMI
	Function	Pasteurization Process – Operator Interface
	Vendor	Siemens
	Model	SIMATIC KTP9000
	Protocols	Ethernet, Modbus TCP
Siemens SIMATIC PLC Configuration Software	Name	SIMATIC PLC Configuration Software
	Function	SIMATIC S7-1200 Configuration
	Vendor	Siemens
Bob's Garage Wi-Fi Router	Name	Bob's Wi-Fi Router
	Function	Home Wi-Fi Network Router
	Vendor	Vendor X
	Model	Model X
	Protocols	Ethernet

Critical Needs for Development

To develop the attack that delivers the HCE, an adversary would need to understand the detailed functionality of each critical component, as well as the operational context for use of the technologies. Documentation providing these functional and contextual details would be part of the adversary's Critical Needs. Table 7 provides an example Critical Needs list including likely artifact location.

Table 7: Component Critical Needs for Development.

Component	Critical Needs for Development	Location/Availability
Bob's Garage Wi-Fi Router	Vendor specs / data sheets	Open source
	Vendor Ops Manual	Vendor Website
	Configuration File	On board, available at initial compromise
Siemens SIMATIC S7-1200 PLC	Vendor specs / data sheets	Open source
	Vendor Ops Manual	Vendor Website
	Vendor I/O Module Pinouts/Wiring Diagrams	Vendor Website
	Stinky Cheese PLC project file	Bob's Garage workstation; company data/file server
Siemens SIMATIC KTP9000 HMI	Vendor specs / data sheets	Open source
	Vendor Ops Manual	Vendor Website
	Stinky Cheese HMI project file	Bob's Garage workstation; company data/file server.
Software: Siemens SIMATIC PLC Configuration	Software and associated install documentation	Purchase
	Vendor programming literature	Vendor Website
Software: Siemens SIMATIC HMI Screen Builder	Software and associated install documentation	Purchase
	Vendor programming literature	Vendor Website
Bob's Garage Workstation	Vendor specs / data sheets	Open source
	Operating system	Open source
	VPN	On board, available at initial compromise

Critical Needs for Deployment

The only additional element required for payload deployment is access to Bob's home Wi-Fi network (see Technical Support Vendor, System Analysis for Targeting, earlier in Phase 3). Everything else required for deployment is in the payload already.

Phase 4: Mitigations and Protections

Phase 4 is Mitigations and Protections. Recall the framework from the lesson plan as shown in Figure 26. Using this framework, we will provide protection and mitigation recommendations in anticipation of the HCE scenario.

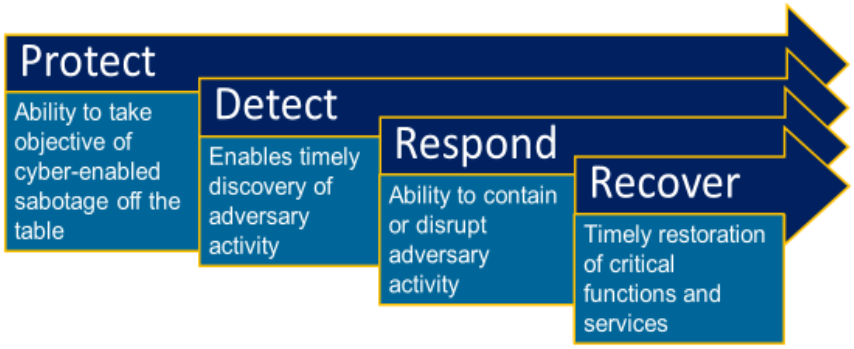


Figure 26: Mitigation and Protection Framework.

PROTECT

Process Control/Monitoring: Independent Pasteurization Temperature Measurement

- Standalone temperature probe/transducer installed.
- Transducer features local temperature readout display.
- Probe/transducer does not provide remote connectivity for configuration.

DETECT

Measurement Validation

- New Operations Procedure - “Pasteurization Temperature Measurement Validation”
- Procedure tasks include manually recording both HMI and standalone transducer temperature values in a log and comparing. Repeat 3x daily.
- Observed temperature variances within a recorded pair that exceed engineered tolerances require operator response described in RESPOND below.

RESPOND

Operations: Pasteurization Temperature Observed Variance (reference DETECT above).

- Operator takes immediate actions per “Pasteurization Temperature Measurement Validation - Temperature Variances” response procedure.
- Steps include the following: immediate process shutdown, contacting technician to investigate probe placement, configuration (transducer, PLC, HMI), power continuity, and communications continuity, reporting technician findings to operations supervisor. Operator also initiates cybersecurity response and troubleshooting protocol.

Incident Response and Management - General

- Fully developed Incident Response (IR) and Management Plans for operations and business environments
- Annual hands-on practice of IR and Management Plans
- Operations personnel on staff to support manual operations
- Out-of-band communications infrastructure, operable and available 24/7 to support Ops staff
- Establish chain of command in advance of emergencies
- Open communication channels between OT and IT (and corporate)

RECOVER

Operations: Pasteurization Temperature Measurement Restoration (reference RESPOND from above).

- Depending on conditions discovered during response activities, possibly replace standalone probe and/or transducer, reassign/relocate temperature I/O point termination in PLC analog input module, or replace analog I/O module.
- Full recovery concludes with measurement re-validation.

Incident Recovery - General

- Fully developed Recovery Plan for operations and business environments
- Annual hands-on practice of Recovery Plan
- Operations personnel on staff to support manual operations
- Out-of-band communications infrastructure operable and available 24/7 to support Ops staff
- Maintain local manual control capabilities for substation components
- Ensure configuration data backups
- Tested recovery (dry run)
- Encrypted storage for sensitive files