Testbed Infrastructure Proposal (Center Energy) For Electricity Power Grid And Defence In Depth Practice On The Proposal

İbrahim Özçelik[1] , Murat İskefiyeli[1], Musa Balta[1], Firdevs S. Toker[1]

[1]Computer Engineering, Sakarya University, Sakarya, Turkey
Corresponding Author: mbalta@sakarya.edu.tr

Research Paper Received: 01.03.2022 Revised: 07.04.2022 Accepted: 24.04.2022

Abstract—Nowadays, Industrial Control Systems became more vulnerable because of integration of Information Systems and Operational Systems. And also critical infrastructures, such as energy, water, petrol etc., are more important ICS must be secured for threats. The methods to secure the critical infrastructures may be both by hardware or software. And by the way, the scientist and the engineers are implementing hardware and software solutions for securing. But the problem is how and where to test their solutions. The solutions cannot be tested in real systems, because critical infrastructures are systems that run 24/7 and cannot be stopped. During the test the system may be in fault. The testbeds can be used as modelling tool and they represent the real systems, with same devices, network topologies, processes etc., that means testbeds are realistic hardware and software environment that to test solutions without having the ultimate system. For this purpose, a testbed center called “Center Energy” has been established in order to carry out studies on the critical infrastructure of the electrical power grid for the purposes such as education of security researchers, and the development of national/international attack and defense solutions. In this study, the information about the architectural structure of Center Energy, implemented according to the Purdue model, and the process scope of the substation and distribution center owned by the electricity transmission and distribution companies, SCADA (Supervisory Control and Data Acquisition) and data management are given, as well as the SOC (Security Operation Center) implemented in accordance with the Defense in Depth approach of this architecture. Studies related to its activities are also presented.

Keywords—critical infrastructures, energy management, ICS testbeds, security, SOC

1. Introduction

Critical infrastructures include both Information Technologies (IT) and Operational Technologies (OT) together. It is called critical because of any problem of the process in the critical infrastructure may cause service and public order disruption (security, health, transportation, etc.), large-scale economic loss, prestige loss and even loss of human life [1]. While critical infrastructures such as banking, finance, communication use IT systems, ICS such as energy, water management and transportation use OT systems [2]. The processes of industrial control systems were local at the beginning, but today they are distributed and centrally and/or locally monitored and controlled. For this reason, the cyber security phenomenon, which was not needed at the beginning, has become an important element today [3]. Security experts have focused on and considered about cyber-attacks

on ICS systems such as DCS (Distributed Control Systems) and SCADA (Supervisory Control and Data Acquisition), which have been usually used for monitoring and managing critical infrastructures are vital, since 2001 and in particular since the Stuxnet attack in 2010 [4]. Most systems built in the past or new installations are designed to operate on closed and proprietary networks. However, using common software and operating systems in hardware, the direct or indirect connection of critical infrastructure systems to public communication networks and internet connection creates vital cyber risks, and critical infrastructures designed as closed networks become more vulnerable to cyber-attacks [5]. Also, insufficient information of the end users about the cyber security, misconfigurations of IT staff increase the risk level considerably. Therefore, it is getting more difficult to manage the security processes of critical infrastructure systems, which contain many different devices and protocols such as PLC (Programmable Logic Controller), RTU (Remote Terminal Unit), HMI (Human Machine Interface), SCADA and server systems [5], [6]. When the major attacks on OT systems, such as Stuxnet, Night Dragon, Duqu, Flame, Gauss, Shamoon, Havex, Black Energy, Crashoverride are examined, it is seen that the main reason is that mentioned above and the risks they posed. Increasing the security of systems as critical infrastructure is considered a national priority in all countries, and national strategy plans are published, because of both the risk factor on OT/ICS systems is high and also the major cyber-attacks and their effects in the past are of vital importance. In Turkey, the security of critical infrastructures action became official for the first time with “The National Cyber Security Strategy and 2013-2014 Action Plan” by the decision of the Council of Ministers, dated 20/06/2013 and numbered with 28683. Today, it is revised as ”The 2020-2023 National Cyber Security Strategy and Action Plan” and the first strategic objective in the action plan has been determined as ”Protection and Strengthening of Critical Infrastructures” [1]. On the other hand, Energy Transmission and Distribution systems, in particular of OT/ICS systems, are systems that operate 24/7 by its nature. So, many problems like as process interruption, any device breakdown or protocol incompatibility may occur during the integration of new process or security applications to the system [5], [6], [7]. Eventually, Critical Infrastructures National Testbed Center (CENTER-SAU) is established to both contribute to the strategic goals and objectives in the action plan and working on a real ICS system to discover and resolve critical security vulnerabilities/threats faced by critical infrastructures, to detect cyber-attacks and to develop preventive and mitigation techniques at the point of defense. There are two critical infrastructures are modeled at this center. One of them is Water Management [8] and the other one is Electric Power Grid [9]. In Center-SAU, the Water Management Critical Infrastructure (CENTER-Water) has waste and potable water processes, and they are modeled as real system descripted in reference [8]. And in this study, a detailed information is given about the Electric Power Network Critical Infrastructure (CENTER-Energy), which has a secure architectural infrastructure for the management and security of the energy transmission and distribution systems built within the scope of the same project [9]. Internationally, there are many test centers and laboratories (Table 1) established related to the energy sector and/or ICS security. The prominent one is the National SCADA Testbed (NTSB) laboratory supported by the US Department of Energy [10]. In this context, national laboratories, Idaho [11], Sandia [12], Argonne [13], Los Alamos [14] and Lawrence Berkeley [15] were established. In these laboratories, studies related to the security of energy systems and sectors in the

critical infrastructure category are carried out in relation to the scope of the project. Another important testbed is iTrust, in which there are subtest beds such as Water Distribution (WADI), Secure Water Treatment (SWAT), Electric Power and Intelligent Control (EPIC) and Internet of Thing (IoT), established at the University of Singapore [16]. In addition, the relevant university has testbed centers in areas such as water management and IoT [17]. Apart from these testbeds, there are many testbed centers for energy critical infrastructures established for both academic and sectoral purposes [18], [19], [4].

A real-scale system can be built for the testbed requirement. However, it will cost too much to set up a real system, the configuration will be very difficult and the construction site of laboratory will be very wide [20]. In accordance with this purpose, ICS testbeds are divided into four categories: physical simulation, software simulation, semi-physical simulation and virtualized testbed [21]. The aims, objectives and contributions of the Center-Energy critical infrastructure, established as a physical simulation within Sakarya University for the academia or industrial sector, are listed below:

- Providing an environment that can be used both in the laboratory and via remote access to academics and sectoral companies that want to work on the security of critical infrastructures.
- Conducting research studies related to ICS/SCADA Security in the sector, to provide cooperation for companies that want to develop projects and to provide both infrastructure and academic consultancy to the solutions desired to be developed,
- Performing risk management and penetration test studies on the testbed,
- Implementing the secure architectural approaches and system tightening recommended by the internationally published IEC (International Electrotechnical Commission), NIST (National Institute of Standards and Technology), CIS (Center for Internet Security), ISO 27000 (International Organization for Standardization), ISA 99 (International Society of Automation, and NERC CIP (North American Electric Reliability Corporation, Critical Infrastructure Protection) standards and sharing the results with the industry,
- Raising awareness by organizing training activities and special courses for the staff in the sector, since the weakest link in security is human,
- Organizing cyber camps and Capture-the-Flag competitions related to ICS security, ensuring that secure architectures are tested in these events,
- Forming dataset from traffic collected in competitions and events and to use them in academic studies,
- Contributing to increase the cyber resilience of critical infrastructures,
- Increasing the capabilities of our testbed center, expanding its scope, taking part in testing and accreditation processes, becoming a center of excellence, and assisting other similar testbed center setups.

The next parts of the article planned as; in Chapter 2, basic information about the security approaches applied on the Energy critical infrastructure established is given. Then, in Chapter 3, information about the architectural infrastructure of the proposed safe testbed center for energy transmission and distribution, and in Chapter 4, information about the SOC (Security Operation Center) capabilities of this testbed center are given.

Table 1.
Comparisons of energy management test-beds.

Location	Objective	Design Approach	Coverage
[10] USA National SCADA Testbed	Education and Training,Attack Analysis, Defense Mechanisms,Test Analysis	Virtualization, Physical Simulation	Physical Process, Fields Devices, Communication Gateways
[11] IDAHO	Vulnerability Analysis, Attack Analysis,Impact Analysis	Software-Based Simulation, Emulation	Physical Process, Fields Devices, Communication Gateways
[12] SANDIA National Laboratory	Education and Training,Attack Analysis ,Defense Mechanisms,Test Analysis	Physical Simulation	Physical Process, Fields Devices, Communication Gateways
[13] Argonne National Laboratory	Education and Training,Attack Analysis, Defense Mechanisms,Test Analysis	Physical Simulation	Physical Process, Fields Devices, Communication Gateways
[14] Los Alamos National Laboratory	Education and Training, Attack Analysis, Defense Mechanisms, Test Analysis	Physical Simulation, Emulation	Physical Process, Fields Devices, Communication Gateways
[15] Lawrence Berkeley National Laboratory	Education and Training, Attack Analysis, Defense Mechanisms, Test Analysis	Software-Based Simulation	Physical Process, Fields Devices, Communication Gateways
[16] EPIC, iTrust	Education and Training, Impact Analysis, Defense Mechanisms Test/Analysis	Physical Simulation	Physical Process, Fields Devices,IoT Communication Gateways
Critical Infrastructures National Testbed Center (CENTER), TR	Attack Analysis, Defense Mechanisms , Test Analysis, Asset Management, Vulnerability Analysis SOC Activities Education and Training	Physical Simulation	Physical Process, Control Centre, Fields Devices, Communication Gateways

2. Security Approaches for ICS

There are common approaches in the design and implementation of cyber solutions that are developed for the facilities despite security researches in energy transmission and distribution systems. In this section, the Purdue Model and Defense in Depth architectures will be explained.

2.1. Purdue Model

The Purdue Enterprise Reference Architecture model was developed by Theodore J. Williams in collaboration with the Purdue University Consortium members in the 1990s. Network security, log management, remote access and access control are the four main critical security areas in ICS. The Purdue reference architecture is used for delivering these basis architectural patterns. The Purdue model uses the concept of zones to divide an ICS network into logical partitions made up of systems that perform similar functions or have similar requirements. It is a model consisting of 6 levels and 4 zones. The levels of Purdue can be defined in below [21];

- Level 5; is where enterprise IT infrastructure systems and applications are located.
- Level 4; It hosts IT systems that deal with

scheduling, capacity planning, inventory management, maintenance and operational management, email, reporting, telephone and print services.

- Level 3; There are assets and services that provide the management of low-level control devices such as remote access services, product reporting systems, engineering computer, at the level where the field production operations and control are made that provide the front entrance to the OT area.
- Level 2; includes production operations equipment including HMI, alarm systems and control room workstations.
- Level 1 includes process control equipment that receives input from sensors, processes the input data using control algorithms, and sends the extracted data to an end element.
- Level 0; includes sensors and actuator elements that directly connect and control the manufacturing process.

2.2. Defence in Depth (DiD)

The Defense-in-Depth concept was firstly designed by the US National Security Agency (NSA). It refers to a cyber security approach that derives its name from a common multi-layered military strategy. A layered defense concept helps organizations to mitigate risks, address threats, and mitigate vulnerabilities. Because of the defense-in-depth approach, if the attacker breaks a defense layer, the next defense layer will detect. With this approach that covers human, process, and technology, it also provides a standard for SOC solutions [22]. The Defence in Depth approach has been handled with the following parameters specifically for ICS:

- Risk management program
- Vendor Management
- Cybersecurity architecture
- ICS Network Architecture
- Physical security
- ICS Network Perimeter Security
- Security Monitoring
- The Human Element
- Host Security

3. The Testbed Infrastructure

The testbed center created for the transmission and distribution systems in the electrical power grid critical infrastructures has a physical environment as in Fig. 1 This environment has been created in a laboratory environment, taking into account the process structure used by electricity transmission and distribution companies in order to increase the success of cyber security studies.

3.1. The Operation of the Process

The architecture in Fig. 2 is the model for the electric power grid that represents power generating, transporting, distributing and consumption of electric both in mimic diagram, mock-up, SCADA screens and flows (Table 2). In model there are different power sources as hydroelectric, wind, thermal and solar energy plants generate electric. To transmit generated energy there are two substations as Substation-1 (Sub-1) and Substation-2 (Sub-2). In addition, to distribute and consume the energy that is transmitted through Sub-1 and Sub-2 there are Distribution and Consumption Centers. The line colours in orange, red, blue and green represent 11 kVs, 154 kVs, 34,5 kVs and 400 Vs respectively. The generated energy from different power sources is at medium voltage level about 11 KVs is fed to Sub-1 through Generator Feeder and transformed to high voltage level about 154 KVs at Sub-1 (Line-1 in Fig. 2). Also, this high voltage is transmitted to Sub-2 through Overhead Line Feeder (Line-2

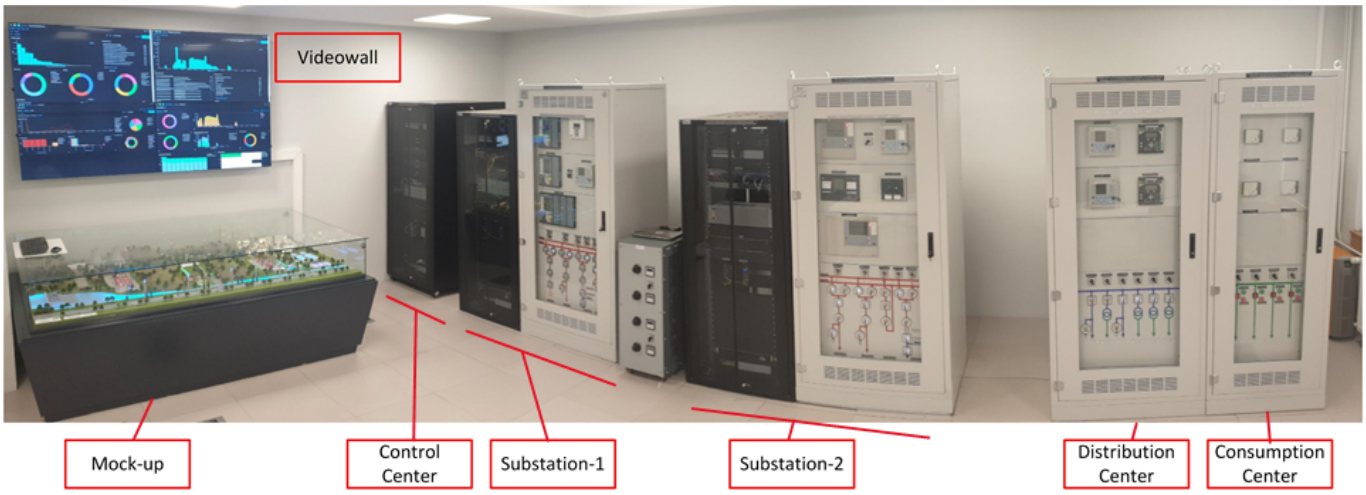


Figure 1. Physical Representation of The Energy Management Testbed Center.

in Fig. 2). At Sub-1, the high voltage transformed to medium voltage for distribution from 154 kVs to 34,5 kVs and transmitted to Distribution Center through Transformer Feeder and Outgoing Feeder (Line-4 in Fig. 2). There is a two-busbar system both at Sub-1 and Sub-2 can be used alternatively or together. To use these two-busbar together, the Coupler Feeders short-circuit the busbars both at Sub-1 and Sub-2. At Sub-2, a Spare Feeder is also available for alternative energy source from power grid (Line-3 in Fig. 2). The high voltage transformed to medium voltage for distribution from 154 kVs to 34,5 kVs and transmitted to Distribution Center through Transformer Feeder and Outgoing Feeder (Line-5 in Fig. 2).

The Distribution Center have two Input Feeders and four Outlet Feeders. The first Input Feeder is supplied by Sub-1's Outgoing Feeder (Transformer Feeder) and the second one is supplied by Sub-2's Outgoing Feeder (Transformer Feeder). The Outlet Feeders have transformers to transform the 34,5 kVs medium voltage level to 400 Vs low voltage level. The first Outlet Feeder is connected to the Consumption Center's first Input Feeder (Line-6 in Fig. 2) and the second Outlet Feeder is connected to the Consumption Center's second Input Feeder (Line-7 in Fig. 2) similarly. Third and fourth Outlet Feeders are spares and can be used when expansion needed. The voltage level at the Consumption Center is 400 Vs and center has two Input Feeder, supplied by Distribution Center, and two Outlet Feeder to supply the consumption zones, Zone-1 and Zone-2 (Line-6 and Line-7 at Output Feeders in Fig. 2). At substations there are many IEDs (Intelligent Electronic Device) that commands, controls and monitors the system. The IEDs are differential relays, distance relays, over current relays, BCUs (Bay Control Unit), RTUs and have different vendors as Siemens, ABB, Schneider and GE. To monitor and control the line events on high and low voltage feeders, differential, distance control and over current relays are used and configured for protection. To model each of the transformers, circuit-breaker, disconnector field signals auxiliary relays are used at substations and distribution centers. These auxiliary relays are connected as an input to the protection relays and data from these inputs are used both at alarms and latching logics. In addition, a model system (Mock-up)

Table 2.
Flow of energy at power lines.

Power Line	From	To
1	Energy Source	Substation-1 Generator Feeder
2	Substation-1 Feeder Line	Substation-2 Feeder Line-1
3	Alternative Feeder Line	Substation-2 Feeder Line-2
4	Substation-1 Distributor Line	Distribution Center Input Feeder-1
5	Substation-2 Distributor Line	Distribution Center Input Feeder-2
6	Distributor Center Output Feeder-1	Consumption Center Input Feeder-1 and Consumption Zone-1
7	Distributor Center Output Feeder-2	Consumption Center Input Feeder-2 and Consumption Zone-2

specific to the testbed center has been developed to visualize and make intelligible the scenarios realized on the transmission and distribution processes in the national testbed center. The bird's eye view of the mock-up is in the upper left corner of Fig. 2. The energy suppliers, substations, distribution centers, consumption centers and consumption zones can be seen in figure. Also colored lines have same codes as in mimic diagrams. The mock-up is integrated with Sub-1, Sub-2, Distribution and Consumption Centers through auxiliary relays. This integration enables turning on/off the LEDs simultaneously on the mock-up according to the action taken on a mimic diagram manually or taken on local/remote SCADA. All of the circuit breakers and disconnectors actions, energy transmission represented by LEDs. A videowall of four monitor is located 2 by 2 on the wall as in Fig. 1 (panorama). It can be used as four independent monitors or a single monitor. There are different video sources as SCADA application screens, Wazuh HIDS (Host-based Intrusion Detection) security application screens, any server or PC remote desktop connection screens etc. In the CENTER Energy model, in Substation-1, SICAM SCC SCADA is used as a Scada software to model the monitoring, command and controlling the generation, transmission and distribution (high voltage side) processes in Automation and Process Zone. Siemens, ABB and GE relays are used as IEDs, and Siemens RTU is used for communication with Load Dispatching Center. In parallel to Sub-1; ABB MicroSCADA is used as a SCADA software. ABB, Schneider relays are used as IEDs and ABB RTU is used for communication. SICAM SCC and MicroSCADA software are designed as local SCADA and in Fig. 2 there are screenshots of them under the substations' mimic diagrams. And also, there is a central remote Scada software at Load Dispatching Center (Control Center), called Copa Zenon SCADA, to monitor and manage the substations centrally. The screenshot of the remote SCADA is in Fig. 2 divided to zones as in yellow blocks that correspond Sub-1, Sub-2, Distribution Center and Consumption Center. The choice of different vendors' production for SCADA, IED and RTU devices is to ensure and test the interoperability of the devices in the testbed center and to ensure that the testbed center is studied by different scope of products in energy sector. In the CENTER Energy infrastructure, where devices and protocols from many different manufacturers are used, transmission, distribution and consumption systems can

work together, as well as an infrastructure and architecture that can work independently, in order to provide a rich and flexible infrastructure for academic and sectoral studies.

3.2. SCADA and Data Management

At the National Testbed Center for Critical Infrastructures there are three SCADA server and application systems. The Siemens SICAM SCC is for Sub-1, the ABB Micro SCADA is for Sub-2 and the COPA Zenon SCADA is for Control Center (Load Dispatching Center). Both of them are used to monitor and control the energy processes. According to Purdue architecture, both of the SCADA servers and applications for Sub-1 and Sub-2 are defined at Layer-2 and also configured and programmed as Local HMIs. At substations, the communication between SCADA applications and IED devices is provided over IEC 61850 MMS (Manufacturing Message Specification) and GOOSE (Generic Object Oriented Substation Event) protocols. Therefore, the access lists have been created between two separate zones on the firewall to ensure that the SCADA application communicate with only the relevant IED devices. Also, according to the IEC 61850 data structure, SCADA applications are configured as clients and IED devices as servers. Analogue values such as current, voltage, power in the substation, state (Open/Close) of the circuit breaker and disconnector devices, command signals of the circuit breaker and disconnector, specific signals of the transformer and circuit breaker, and field signals related to communication are defined in the datasets and applied to both Local HMI SCADA software and the RTU devices through report control blocks in the substation. The RTU devices in the substations convert the signals into IEC 104 protocol data structure that they received over the IEC 61850 protocol and transmit them to the COPA Zenon SCADA application in the Control Center and act as a gateway device. The measurement values, open/close states, commands and field signals in the Distribution Center were also transferred to the COPA Zenon SCADA application in the control center via IEC 61850 protocol. The COPA Zenon SCADA application receives IEC 104 data from Substations via RTU, and IEC 61850 data from Distribution Center. In the CENTER Energy architecture, the measurement values, open/close states and field signals received from the substations and distribution center were transferred to the COPA Zenon SCADA Application in the Control Center (Load Dispatching Center) over an alternative second line with the IEC 60870-5-101 protocol. This transported data can only be used for monitoring purposes from the SCADA application.

4. CENTER Energy Network Architecture and Defence in Depth Practice

4.1. CENTER Energy Purdue Model Architecture

According to the literature, the first step to create a secure ICS architecture is to model the network architecture according to the Purdue reference model [10], [11], [12], [13], [14]. The Purdue architecture needs some name changes, revisions and acceptances for energy critical infrastructures due to its development for manufacturing systems. Accordingly, CENTER Energy critical infrastructure is modeled in an architecture in Fig. 3, taking into account both the Purdue architecture and the terminology and needs of the energy critical infrastructures. According to the architecture;

- Layer 0 is considered as the process level and contains switchyard devices and signals such as breaker, disconnector, transformer (in Fig. 2). In

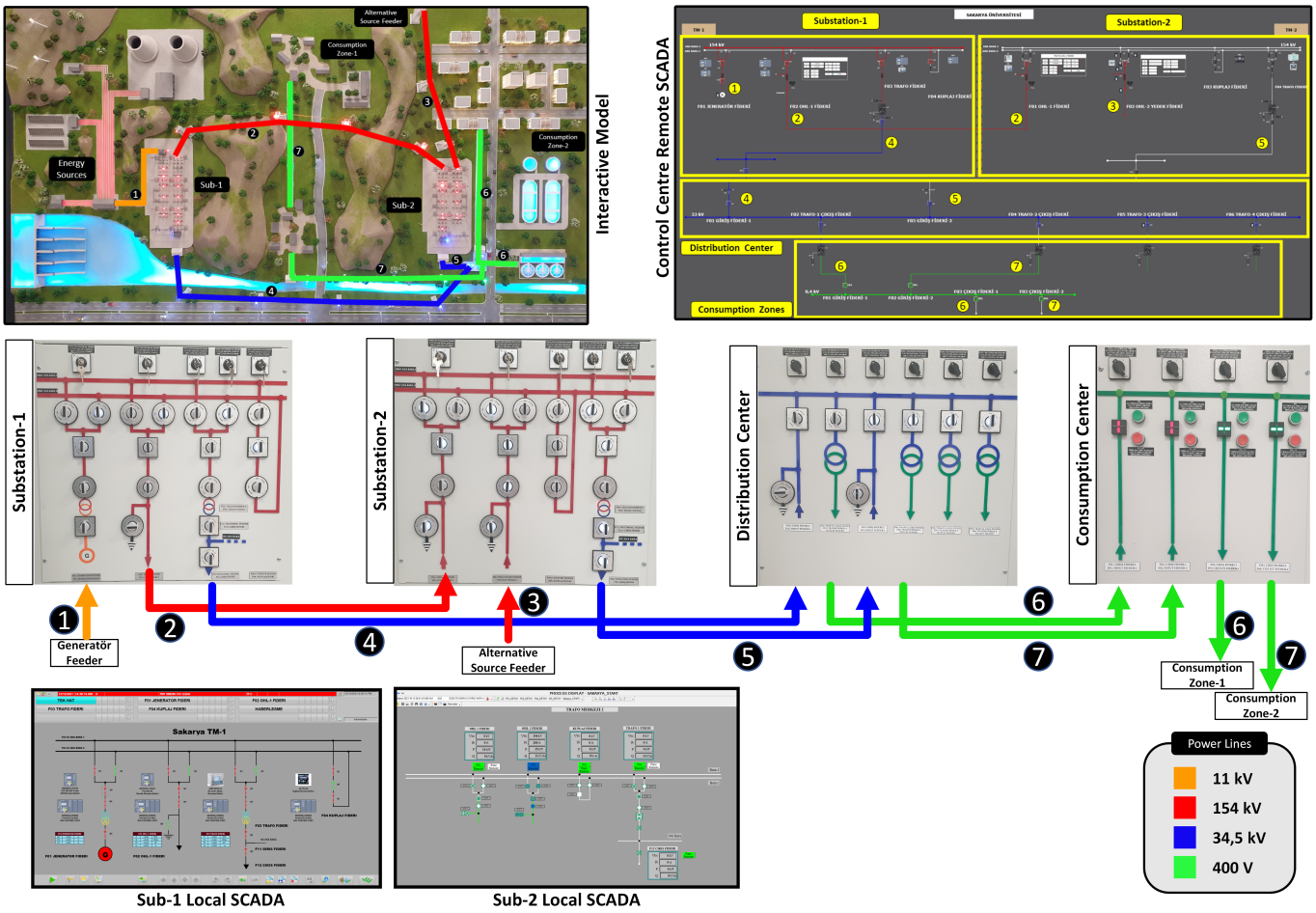


Figure 2. Process Architecture Topology of The Electric Energy Management Testbed Center.

particular, schrack relays are used for breaker, transformer, and communication signals; these relays are moved to control and protection IED devices, field signals are created and are used as logic in locking circuits.

- Since the field signals defined in Layer 0 are physically connected to the IED devices, a zone definition has not been made at the network perimeter point.
- Layer 1 is defined as Bay/Field level and contains control devices such as IED and RTU. While IED devices are defined in the process bus zone, RTU device are defined in the Automation Zone. No RTU device is used in the distribution part.
- Layer 2, on the other hand, is defined as Station Level and contains Local Supervisory devices in order to model the substation located in different locations and to make local inspections. The devices in Layer 2 are considered in two categories. While servers such as Local HMI and OPC (Open Platform Communications) are used to collect, monitor and control data from the process of the Electricity Energy network, servers such as Log Server, Wazuh and ELK (Elasticsearch Logstash Kibana) are used to monitor cyber events within the relevant substation. Layer 2 is not defined on the distribution

side, so there is no local SCADA software.

- In Layer 1 and Layer 2, the automation zone and the process zone are defined together as a transformer control zone. Both substations are configured as two separate zones on the Firewall over different ports. In the distribution part, a Distribution Control Zone was created and terminated on a separate port on the Firewall, as in other substation zones. It is configured so that there is no communication and access between the defined Substation zones and the Distribution zone.
- In Layer 2, substation-specific DMZ (Demilitarized Zone) zones are created for remote access to IED, RTU, and local SCADA devices in each substation zone. Each DMZ zone can only access its substation. For IED devices with RBAC (Role-Based Access Control) support, necessary configurations have been made on the RBAC (RADIUS) and AD servers. Necessary permissions are given between zones for the relevant service in the firewall.
- Layer 3, on the other hand, is accepted as the control center level and includes Site-Wide Supervisory devices to collect, monitor and control data from all testbed units, as well as open source HIDS and NIDS (Network Intrusion Detection) components to manage the cyber security operations of the control center. Devices in Tier 3 are considered in three separate categories. In the first category, Zenon SCADA and OPC servers and computers are used to collect, monitor, and control data from substations and distribution centers. Log Server, Wazuh HIDS, and ELK servers in the second category are located to monitor cyber security events within the control center. The third category includes Domain Controller and Time server. A domain has been created in the control center; all end systems are included in the domain. Depending on different security assumptions, end systems in substations can be included in the domain with the necessary configuration over the Firewall. A multi-user working system with different authorizations has been created. The time server used in the control center is hardware-based. Configurations were made so that the signal received from the GPS (Global Positioning System) could be transmitted to the control center and to the devices in the substations and distribution centers by writing special rules to the IP address over the firewall.
- In addition, one DMZ zone have been defined to manage remote operations of control center servers in Layer 3. In this zone, the remote terminal PC is defined in a network accessed by SSL (Secure Socket Layer) VPN (Virtual Private Network) for remote access to the testbed. This remote terminal PC has access to service PCs in other DMZ zones. According to the Defense in Depth concept, the remote terminal PC is configured as a Jumping Host.
- The zones created on the firewall are terminated with the connection made through the own switch of each relevant network. Each zone that terminates on the firewall has its VLANs (Virtual Local Area Network). Future configuration updates have been planned to create different VLANs under the zones.

4.2. SOC Activities on Secure Testbed

The concept of SOC, which we frequently hear in the IT security world, is also critical in OT security. The awareness of this security process, which includes people, processes, and technology, is less in the OT infrastructure. Security operation centers are an integrated structure that includes more than one security process. These processes are asset management, cyber threat intelligence, incident

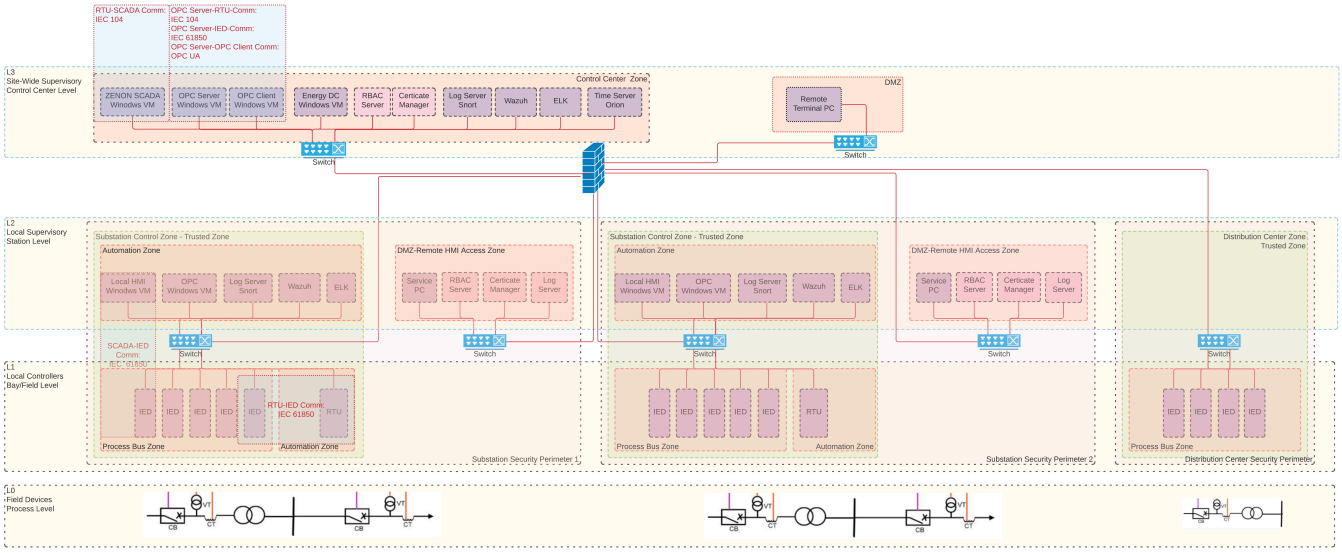


Figure 3. Network Architecture of The Electric Energy Management Testbed Center.

detection/prevention system, risk management, etc. SOC activities created in establishing the critical infrastructures national testbed center to provide infrastructure for cyber security studies are included in this section. SOC applications have been applied for the electrical energy infrastructure process.

4.2.1 Asset Management

Asset management is the essential and first step of almost all SOC processes. This case applies to both IT and OT infrastructures. When the assets in the system are managed wholly and correctly, other processes will be carried out indirectly and correctly. We used the Integrity Asset Management [23] tool for asset management in the electrical energy critical infrastructure SOC installation. Although this tool offers an open-source solution, there is also an enterprise version. With this tool, we obtained datas about the detection and information of the devices in the testbed center. Thus, we obtained a helpful structure in establishing a physical and logical relationship in the system.

4.2.2 System and Network Monitoring for Intrusion Detection

Early detection of a cyberattack is essential in both IT and OT infrastructures. In the testbed center, we have established, we have positioned the event detection system on two main structures: Host-based IDS and Network-based IDS. The Wazuh HIDS [24] tool for endpoint monitoring is integrated with agent-server communication. Wazuh HIDS offers an open-source solution. Apart from the rules that come with its installation, external rules can also be written according to the security policies applied in the system. Agents have been installed on all machines that make up the control and monitoring systems of the process, such as Active Directory, Engineering workstations, SCADA servers, OPC servers in our testbed center. Agent installed machines are computers with Windows operating system at L2 and L3 levels of the Purdue reference

model. The system, application, and security logs are produced by default in the Windows operating system. However, essential logs such as WMI Events, DNS Query, File Create/Delete, Process Create/Delete are not produced. The Sysmon tool is installed on all machines to ensure that logs of 24 such essential events are produced. In order to evaluate the generated logs within the framework of a standard, the Sysmon tool is configured according to MITRE ATT&CK techniques and tactics. The Figure 4 indicates that Windows logs and Sysmon logs produced in endpoint systems are transmitted to the Wazuh analysis engine via ossec-agent. It operates matching the Sysmon and Windows logs on the Wazuh analysis engine with the alarm rules. By default, alarms below alarm Level 3 are ignored in Wazuh rules. Alarms at levels 3-16 are generated as alarms. Since the alarms in JSON format require a very intensive review process, visualization is required to analyze the alarms more conveniently and effectively. In addition to the visualization, a database is also required to review historical alarms. To solve these problems, Elasticsearch for database and Kibana for visualization tools, which are frequently used from opensource solutions, are integrated. Wazuh HIDS has ease of integration with many tools. Kibana also has a template for visualizing alarms and the Kibana Applicaion. After the related installation and configurations are completed, alarms from Wazuh analysis engine can be read and reacted quickly thanks to dashboard screens created with various chars.

Tap devices were used to receive the traffic flowing from the transformer centers and load distribution centers in our testbed center. Thus, we had the opportunity to monitor the network communication of all centers. For example, monitoring is carried out for four different points in substation 1. The first of these communication points; According to the Purdue reference model, between SICAM SCC with local HMI SCADA in L2 and IEDs controlling the process directly, second between Siemens RTU and IEDs, third between Zenon SCADA server and RTU in Control Center in L3 and last one between two IEDs configured to capture packets such as GOOSE between devices. Thus, network traffic can be monitored both horizontally and vertically. The entire network structure in the testbed center can be monitored from 32 different points. Thus, we made the monitoring system open to configuration by configuring all necessary physical connections and configurations from the desired center with the desired devices. The monitoring structure of the network traffic provided by Tap devices is valid for all centers. Industrial protocols are used to process and transfer process information. There are industrial protocols IEC 61850 and IEC 104 at the points where the traffic is monitored in the testbed center. It was integrated with Snort, an open-source NIDS using these protocol rules. In order to examine the alarms of the Snort tool and increase readability, dashboards with various graphics were created in the Kibana interface [25].

4.2.3 Vulnerability Management System

Vulnerability management is one of the crucial processes in the center of cyber security operations. We used the “Vuln Detector” tool in the Wazuh HIDS tool to meet this need at the testbed center. Thus, all machines with ossec-agent installed are periodically scanned from the NIST database. As a result of scanning, findings are generated as an alarm in the system with CVE (Common Vulnerabilities and Exposures) codes. The findings show in vulnerability dashboard (Fig. 5) provided by the Wazuh HIDS.

Log Collection and Management is a very impor-

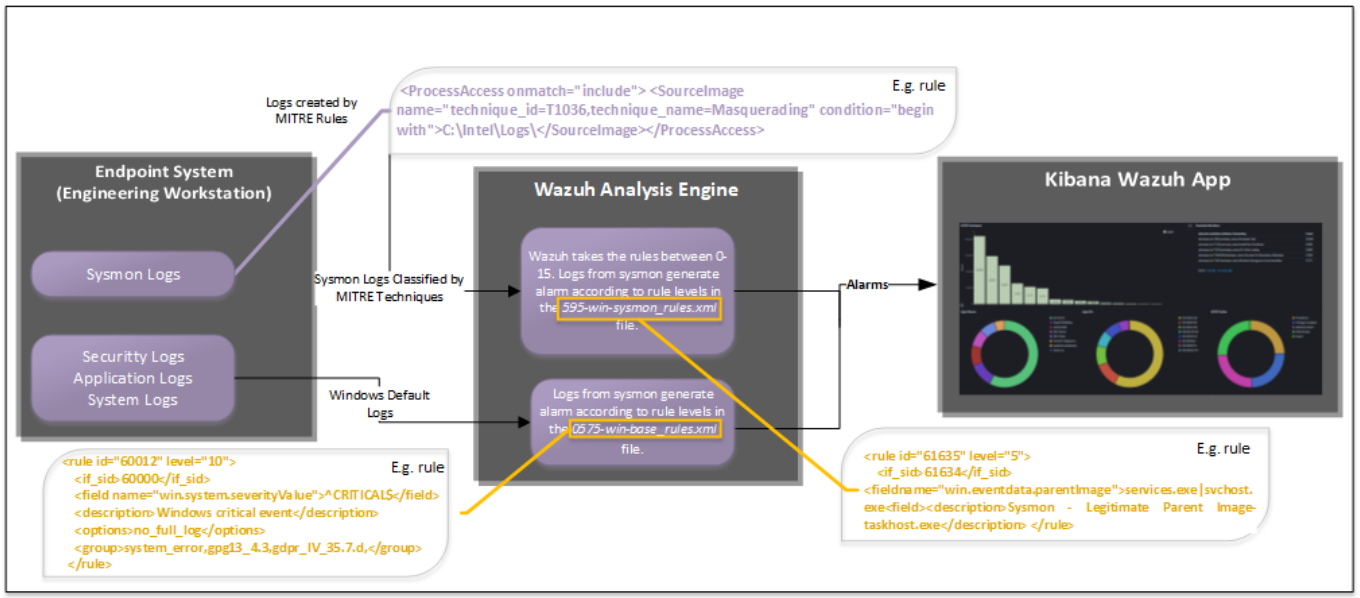


Figure 4. Wazuh HIDS Workflow for CENTER Energy.



Figure 5. Log Gathering Framework for CENTER Energy.

tant process within the scope of SOC. For log management, a process-based log framework structure was created by considering NIST ”Log Management” standard. In the Center Energy infrastructure, a Another critical process within the scope of SOC is Log Collection and Management. While creating our log management framework, a process-based structure was created by taking the NIST ”Log

Management" standard into account. We developed a framework with multi-tier architecture and multi-threading at the testbed center. The RestClient class is created to collect process, SNMP (Simple Network Management Protocol), diagnostic, and Syslog data defined on OPC servers. Data in OPC IoT tags are read with OPC UA (Unified Architecture) architecture for secure communication during data collection.

4.2.4 Penetration Tests

The CALDERA adversary simulation tool performed penetration tests in the CENTER Energy critical infrastructure. CALDERA is an attack simulation tool that enables attack scenarios according to the tactics and techniques found in the targeted MITRE Enterprise Matrix. Process hollowing was done via Powershell on the captured OPC Server machine in the Fig. 6.

Wazuh HIDS has created an alarm to the Kibana interface, where this attack process and Powershell commands are monitored. The image of the relevant alarm is in the Fig. 7.

The equivalents of the security solutions applied in both departments related to Center Energy in Defense in Depth models are given in Table 3.

5. Conclusion

To date, many cyber-attacks have been made against critical infrastructures. The results of these attacks have caused economic and reputational loss and vital losses. These attacks and their results show us that the threats against critical infrastructures continue, and we need to take precautions. The literature researchers in this area are the optimum solution for security standards and security approaches to ensure the security of critical infrastructures. However, different applications are made in different standards and security approaches configurations. Therefore, the security awareness of the personnel using cyber security products is as important as the cyber security solutions in the system. For this purpose, testbed centers are ideal environments to develop new products in the field of cyber security, to develop detection and prevention systems against attacks, to test the efficiency of products in this field, to increase users' cybersecurity awareness, and to provide an environment for the development of new solutions. Thus, academic and sectoral cyber security initiatives will safely carry out test processes without worrying about vital, economic, or reputational loss. In line with these purposes, the electricity-energy network, one of the essential critical infrastructure components, has been established with a physical simulation environment and a secure architectural approach. The testbed center models electricity generation, transmission, distribution, and consumption processes. The electricity-energy network testbed center we have created consists of two substations (Sub-1 and Sub-2), a distribution center (MV), and a consumption center (LV). The system and network architecture are based on the Purdue model. We also tried to provide Defense in Depth requirements for cyber security solutions by developing solutions based on asset management, vulnerability management, log framework, HIDS, and NIDS. In the testbed center, training activities, CTF (Capture the Flag), internships, and camp studies continue to increase the awareness of cyber security in critical infrastructures and increase the sharing of technical knowledge and experience. Cyber security studies continue under NIST and IEC 62443 standards in our electricity-energy critical infrastructure center. In addition, it is among the objectives to create a comprehensive SOC environment with the integration of artificial intelligence-based studies, cyber threat intelligence,

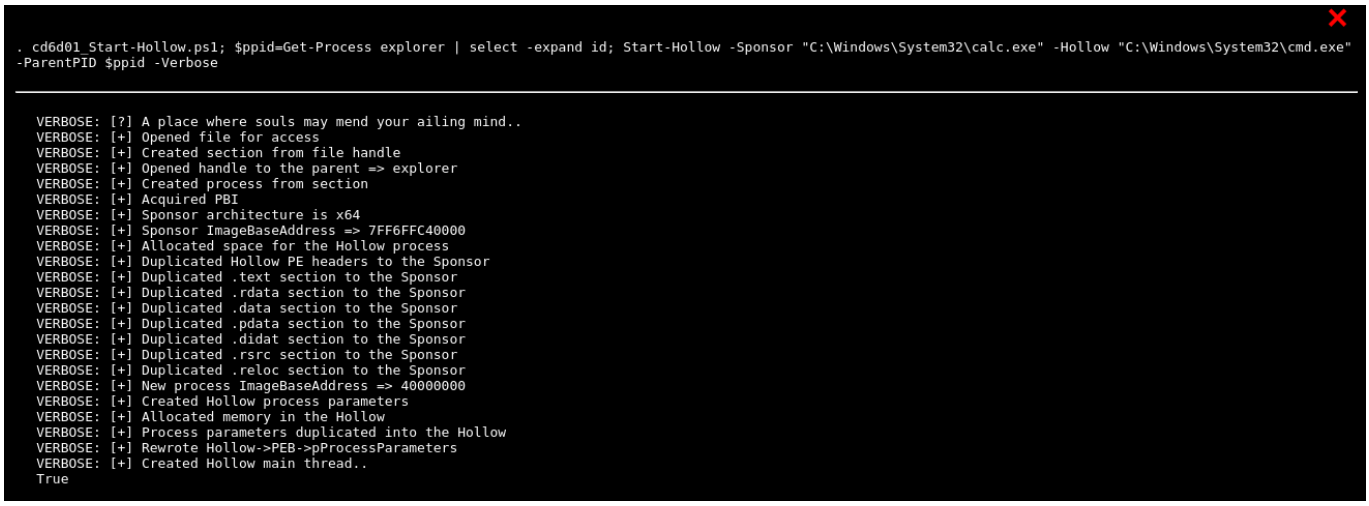


Figure 6. Penetration Screen-1.

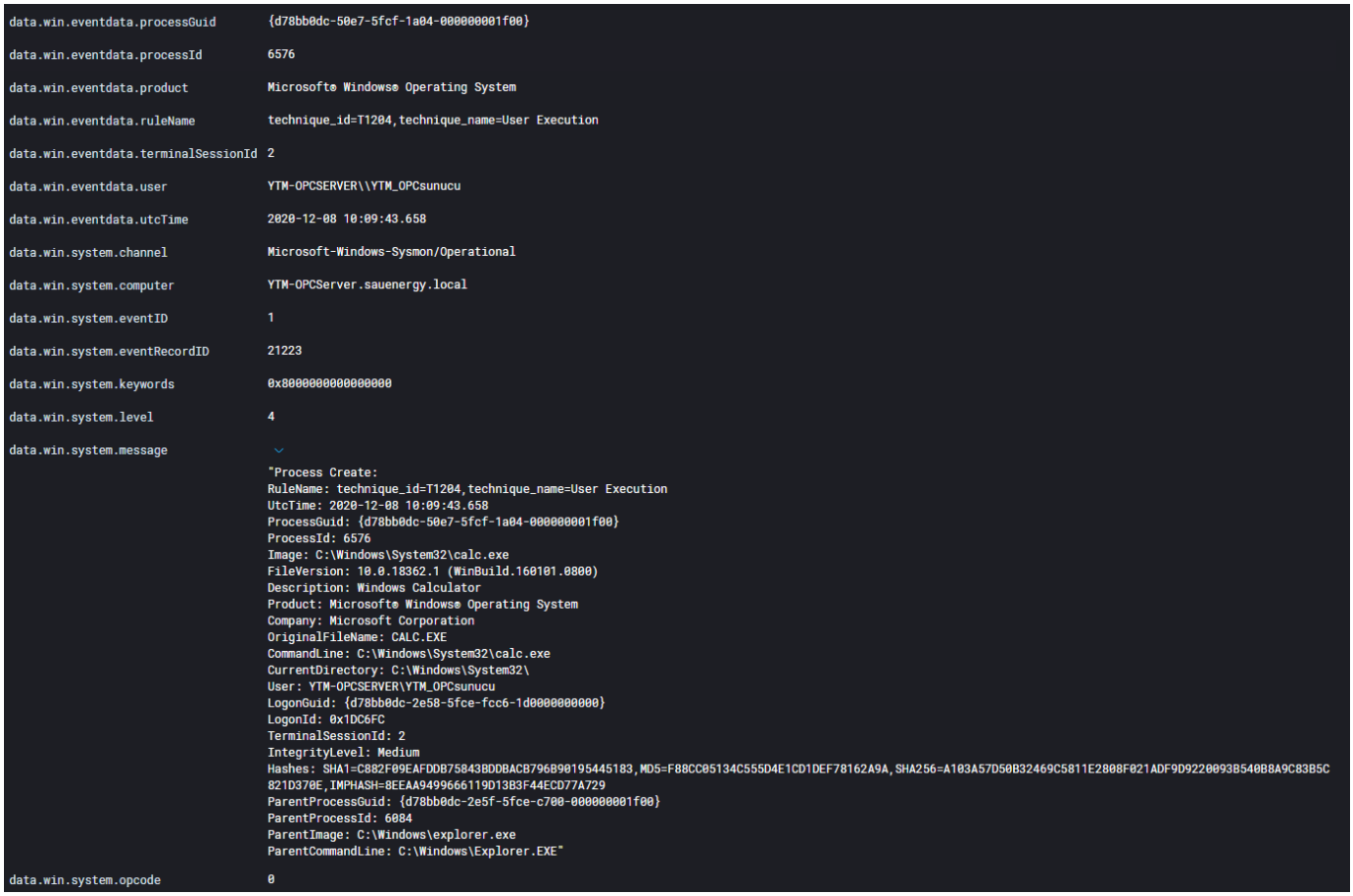


Figure 7. Detection Alarm Screen.

Table 3.
A sample table including some styles.

Defence in Depth (DiD)	Scope of DiD	CENTER Energy
Risk Management Program	Identify Threats	no
	Characterize Risk	no
	Maintain Asset Inventory	yes
Cybersecurity Architecture	Standards/Recommendations	yes
	Policy	yes
	Procedures	yes
Physical Security	Field Electronics Locked Down	yes
	Remote Site Video, Access Controls, Barriers	no
	Control Center Access Controls	yes
ICS Network Architecture	DMZ	yes
	Common Architectural Zones	yes
	Virtual LANs	yes
ICS Network Perimeter Security	Firewalls/One-Way Diodes	yes
	Remote Access and Authentications	yes
	Jump Servers/Hosts	yes
Host Security	Patch and Vulnerability Management	yes
	Field Devices	no
	Virtual Machines	yes
Security Monitoring	IDS	yes
	Security Audit Logging	no
	SIEM	yes
Vendor Management	Supply Chain Management	no
	Managed Services/Outsourcing	no
	Leveraging Cloud Services	no
The Human Element	Policies	yes
	Procedures	yes
	Training and Awareness	yes

and SOAR (Security Orchestration, Automation and Response) solutions to detect both process and cyber security anomalies.

Acknowledgment

Critical Infrastructures National Testbed Center (Center Water and Center Energy) is the output of a project supported in cooperation with STM-SAU under the auspices of the Defense Industry Presidency.

References

[1] U. ve Altyapi Bakanligi. Ulusal siber guvenlik stratejisi ve eylem stratejisi. https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf. Accessed: 07.06.2021.

[2] O. o. t. P. S. The White House. Presidential policy directive 21 (ppd-21): Critical infrastructure security and resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Accessed: 07.06.2021.

[3] H. Holm, M. Karresand, A. Vidström, and E. Westring, "A survey of industrial control system testbeds," in *Secure IT Systems*, S. Buchegger and M. Dam, Eds. Cham: Springer International Publishing, 2015, pp. 11–26.

[4] H. Gao, Y. Peng, Z. Dai, T. Wang, X. Han, and H. Li, "An

industrial control system testbed based on emulation, physical devices and simulation," vol. 441, 03 2014, pp. 79–91.

[5] U. P. D. Ani, J. M. Watson, B. Green, B. Craggs, and J. R. C. Nurse, "Design considerations for building credible security testbeds: Perspectives from industrial control system use cases," *Journal of Cyber Security Technology*, vol. 5, no. 2, pp. 71–119, 2021. [Online]. Available: https://doi.org/10.1080/23742917.2020.1843822

[6] Y. Geng, Y. Wang, W. Liu, Q. Wei, K. Liu, and H. Wu, "A survey of industrial control system testbeds," *IOP Conference Series: Materials Science and Engineering*, vol. 569, no. 4, p. 042030, jul 2019. [Online]. Available: https://doi.org/10.1088/1757-899x/569/4/042030

[7] Z. O'Toole, C. Moya, C. Rubin, A. Schnabel, and J. Wang, "A cyber-physical testbed design for the electric power grid," in *2019 North American Power Symposium (NAPS)*, 2019, pp. 1–5.

[8] I. OzcelİK, M. Iskefiyeli, M. Balta, K. O. Akpinar, and F. S. Toker, "Center water: A secure testbed infrastructure proposal for waste and potable water management," in *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, 2021, pp. 1–7.

[9] I. Ozcelik, M. Iskefiyeli, M. Balta, K. Ovaz Akpinar, and F. S. Toker, "Center energy: A secure testbed infrastructure proposal for electricity power grid," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, 2021, pp. 149–154.

[10] National scada testbed. https://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed. Accessed: 07.06.2021.

[11] Idaho national laboratory. https://inl.gov/national-security/testing/. Accessed: 07.06.2021.

[12] Sandia national laboratory. Accessed: 07.06.2021. [Online]. Available: http://www.sandia.gov/

[13] Argonne national laboratory. http://www.anl.gov/. Accessed: 07.06.2021.

[14] Los alamos national laboratory. http://www.lanl.gov/. Accessed: 07.06.2021.

[15] Lawrence berkeley national laboratory. http://www.lbl.gov/. Accessed: 07.06.2021.

[16] S. University. itrust centre for research in cyber security. https://itrust.sutd.edu.sg/. Accessed: 07.06.2021.

[17] J. Hieb, J. Graham, and S. Patel, "Security enhancements for distributed control systems," in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi, Eds. Boston, MA: Springer US, 2008, pp. 133–146.

[18] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, and R. Reddi, "A control system testbed to validate critical infrastructure protection concepts," *International Journal of Critical Infrastructure Protection*, vol. 4, pp. 88–103, 08 2011.

[19] A. Almalawi, Z. Tari, I. Khalil, and A. Fahad, "Scadavt-a framework for scada security testbed based on virtualization technology," in *38th Annual IEEE Conference on Local Computer Networks*, 2013, pp. 639–646.

[20] M. Haney and M. Papa, "A framework for the design and deployment of a scada honeynet," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, ser. CISR '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 121–124. [Online]. Available: https://doi.org/10.1145/2602087.2602110

[21] T. J. Williams, "The purdue enterprise reference architecture," *Computers in Industry*, vol. 24, no. 2, pp. 141–158, 1994. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0166361594900175

[22] C. Smith, "Understanding concepts in the defence in depth strategy," in *IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology, 2003. Proceedings.*, 2003, pp. 8–16.

[23] Dragos asset visibility. https://www.dragos.com/platform/asset-visibility/. Accessed: 07.06.2021.

[24] Wazuh systems. https://documentation.wazuh.com/current/index.html. Accessed: 01.06.2021.

[25] Elk stack. https://www.elastic.co/what-is/elk-stack. Accessed: 02.06.2021.