Global Scientific JOURNALS

GSJ: Volume 11, Issue 5, May 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

SECURING HEALTHCARE CYBER-PHYSICAL SYSTEMS: AN ANALYSIS OF THE DANGERS AND MITIGATIONS.

[1]Omenka Ugochukwu E, [2]Luke-Odoemena Ijeoma V, [3] Emeagi Ijeoma (nee Agwamba),

[4] Saheed Oladimeji, [5]Iwuoha Obioha,[6] Nwoduh Udochukwu,

Abstract: This research examines the potential risks posed by cyber-physical systems (CPS) in a healthcare environment, focusing on the dangers of medical equipment and the potential for cyberattacks. The study aims to analyze the body of literature on healthcare cyber-physical systems (HCPS), industrial control systems (ICS), and supervisory control and data acquisition (SCADA), to better understand the underlying technologies. The research methodology involves conducting a literature review, experimentation, and simulation to carry out this analysis. Using Simul8, a simulation is created to model the operation of a smart medical device in the hospital environment, known as the Target Controlled Infusion (TCI) device. The study will explore the potential for cyber-physical attacks, such as man-in-the-middle attacks, distributed denial of service attacks, or ransomware attacks, on the hospital network that causes physical harm to the target medical device. The results of this study will identify potential vulnerabilities and suggest mitigations to enhance the security and safety of healthcare facilities.

Keywords: Healthcare, Cyberattack, Ransomware, Simulation

INTRODUCTION

This scenario will examine a healthcare setting, including cyber physical components like monitoring systems, sensors, actuators, and medical equipment. We will examine the dangers posed by these gadgets, analyse possible cyber physical attacks that might take place in such an environment, and suggest mitigations.

The need for constant interaction, management, and cooperation of efficient and effective systems ushered in a new phase in technology known as Industry 4.0. This phase features cyber physical systems, which are systems that connect the cyber and physical worlds. This is achieved by using sensors that operate as data collectors, gathering information for transmission to servers in the cloud for processing and analysis, and actuators that receive control signal from servers in the cloud. The System operates in a closed loop as seen below in Figure 1 (Verma, 2021)

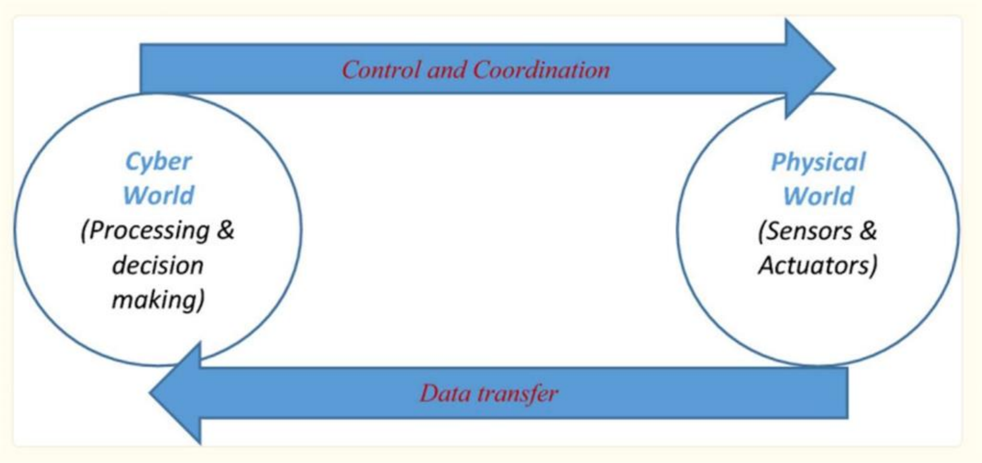

Control and Coordination
Cyber World (Processing & decision making)
Physical World (Sensors & Actuators)
Data transfer

Fig 1.Cyber physical Systems Overview (Verma, 2021)

Right now, the foundation of any smart city is a sound healthcare system. This system can be achieved by building a predictive mechanism that foresees healthcare emergencies. This system functions smartly by handling medical emergencies in real-time, making it possible to monitor patients effectively and efficiently, regularly supply them with medications, and treat them using medical devices.

METHODOLOGY

We must ask whether cyber physical attacks pose a significant risk to healthcare organisations, specifically intelligent hospital environments.

To answer this question, we will use a literature review, experimentation, and simulation to carry out this analysis. Having learned what Cyber physical Systems are, we need to understand the concept of Healthcare Cyber physical Systems and note the related dangers and hazards. We will analyse the body of literature on HCPS, ICS, and SCADA to better grasp the underlying technologies. Then, utilising the operation and connections of medical equipment that we have identified as a test target, we will create and simulate an attack scenario, such as a man-in-the-middle attack, distributed denial of service, or ransomware attack on the hospital network that will cause a physical assault on this target gadget.

We will use the Simul8 simulation software to model this smart medical device in the hospital environment, including the various actors and their interconnections. We will establish the 100% operational level of the medical device and then introduce cyber physical risks by simulating an attack that alters the configurations on the medical device, noting the parameters and data at each stage.

LITERATURE REVIEW:

Healthcare Cyber physical Systems (HCPS) are cutting-edge cyber and medical technologies that can help the medical community manage existing health issues more effectively. These technologies increase Medicare quality by delivering efficient and intelligent services, which allow medical practitioners to monitor and control a diverse range of situations without being limited by geographical location. Leveraging on the operation of typical cyber physical systems, HCPS focuses on the complex physical dynamics of the patient's body and emphasises executable clinical workflows, validated patient models for sensed data, and an adaptive patient-specific algorithm to control actuators (Lee & Sokolsky, 2010). HCPSs are generally classified as Industrial Control Systems (ICS). ICS is a broad term for describing

Supervisory Control and Data Acquisition (SCADA) and Distributed Control System (DCS) (Kostadinov, 2020), both of which are components of Operation Technology (OT). ICS are cyber physical systems, which means that a process or activity in cyberspace can result in physical action or change (Pekarova, 2021).

A SCADA system refers to a mixture of hardware and software that automates industrial processes by gathering real-time data from Operation Technology. Organisations can use a SCADA system to control operations locally or remotely, acquire real-time data from sensors, analyse and visualise the data, interact with industrial equipment, and record and save occurrences for report generation or reference (Wangsness, 2022). A typical SCADA system is made up of sensors and actuators in charge of gathering physical parametric data. Field controllers (Remote Terminal Units and Programme Logic Controllers) convert these analogue signals to digital data and vice versa. Supervisory computers and human machine interfaces are responsible for process control and presentation of data to the operator in a human-readable form and a communication infrastructure that allows a link between industrial systems and the outside world (Loshin, 2021). SCADA protocols were designed to be very compact; an example is the traditional Modbus RTU. Several equipment vendors recognise and standardise this protocol, as well as many others. More recently, many of these protocols now have extensions allowing them to operate over the internet, leveraging the protocol suite TCP/IP. SCADA systems architecture has evolved through four generations: monolithic, distributed, networked, and web-based. In all, it is essential to note that the legacy protocols and system architectures were designed with the availability of resources in mind; security was an afterthought. However, the standardisation of protocols and the evolution of architecture has left SCADA systems more open and vulnerable to security threats common with systems that have moved from legacy to modern technologies (SCADA, 2023).

Cyber-attacks on Cyber Physical Systems are becoming increasingly prevalent as physical systems grow in number and become more interconnected. CPS, especially HCPS, are targets of several attacks classified mainly as internal and external threats. While external threats will require exploitation of vulnerabilities identified on target devices, systems, or networks from outside the environment and then coordinated attacks from experienced cybercriminals, internal threats usually deal with compromising the systems from within the infrastructure by resentful employees/former employees (Nair et al., 2019).

Common CPS attacks include Distributed Denial of Service, Ransomware, Replay/Man-in-the-Middle attacks, Zero Day attacks, and Data breaches. The most prevalent type of assault is ransomware, but when environments that provide Medicare are hacked, the consequences may be far-reaching, posing a direct threat to human life (Sarka & Levalle, 2021).

Case Study:

We will simulate a scenario in a surgical room of an intelligent hospital, where an Automated ///Target Controlled Infusion Device is deployed. This SCADA system is used to administer, control, and monitor anaesthetics. Target Controlled Infusion is an anaesthetic method used chiefly for intravenous anaesthesia. It relies on two key components: drug models to simulate the drug/body behaviour and a control algorithm to control infusion rate and drive infusion devices. The anaesthesiologist determines a desirable target concentration intending to create a specific effect. The drug model estimates the quantity of drug required to attain the concentration, and an infusion rate control algorithm decides how to provide the medication dosage. The effect depends on what needs to be achieved, which is seen in three phases: induction, maintenance, and emergence. Like every other SCADA system, the automated TCI device is made up of the following components, as shown in Figure 2:

Sensors – to read specific parameters and build a validated model.

Actuators – the infusion device.

Programme Logic Unit – transmits signals to control the actuator.

Supervisory Computers – Control unit (Computing resource).

Human Machine Interface – Human readable user interface.

Communication – a link between all components and the network.

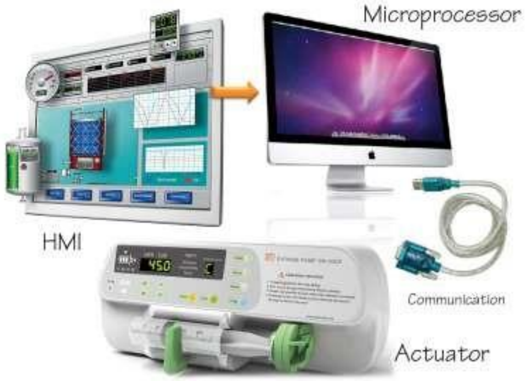


Fig 2. TCI System Components (Bressan,2011)

When combined with patient biodata, the sensor data provide the critical information that controls the anaesthesia delivery through the surgery period, monitoring vital life signs and determining the drug infusion rate, as shown in Figure 3. Standard sensors readings include:

Cardiovascular Monitoring (Electrocardiography, Blood Pressure), Respiratory Monitoring (Pulse Oxymetry, Ventilation), Nervous System Monitoring (Electroencephalogram, Cerebral Oxymetry), Neuromuscular Transmission, and Temperature (Bressan, 2011).

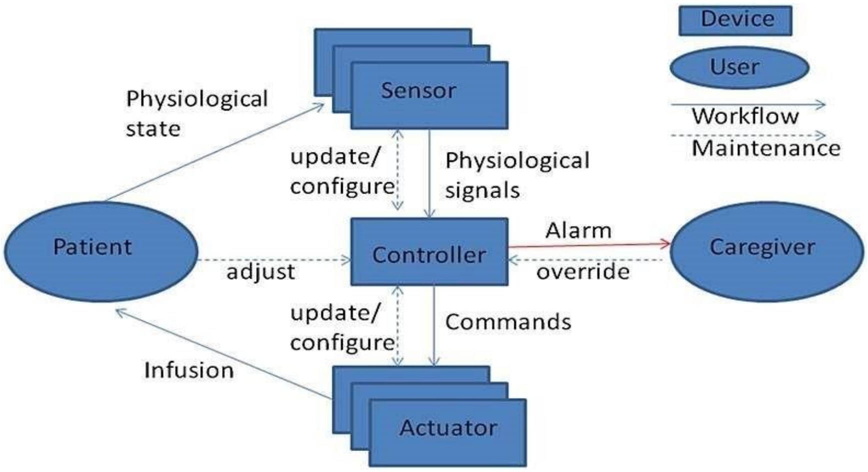


Fig 3. TCI Block Diagram. (Kanjee & Liu, 2016)
Attack Scenario

The Drug infusion pump directly injects drug concentrations into the human body. When an attacker modifies, the data exchanged between the infusion pump and the controller, a wrong dose is administered. Manipulating the drug infusion pump can be done remotely by modifying the configuration on the supervisory computers. A remote attacker can use port scanning tools to identify open and unsecured ports and exploit web server vulnerabilities to launch a ransomware attack that hijacks the supervisory and control system. Once the system is shut down, locked, or encrypted, there is no communication between the pump and its controller, which makes the TCI system malfunction, dispensing an overdose or underdose of the anaesthesia.

RESULTS

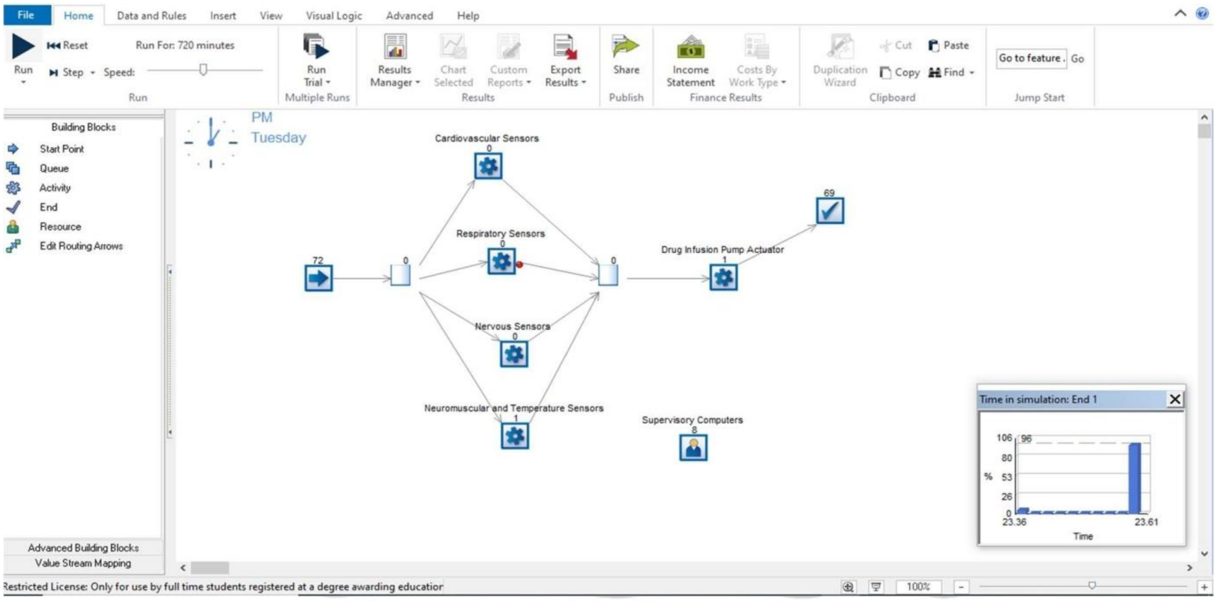
The system operates in a closed loop, this means that our start and end points are the body of the patient. The flow of the system is stated below:

Start Point (Patient) □ Queue (Communication Lines) □ Activities (4 Sensors)

Resource (10 Supervisory Computer and HMI) □ Activity (Actuator) □ End point(Patient). The resource is connected to the sensor and actuator, receiving input from one and sending output to the other. This simulation models a ransomware attack that hijacks the supervisory computers and then reduces the performances of the sensors and the actuator. This is achieved by reducing the availability of the supervisory computers, ten systems were deployed for this purpose. The following values and settings remained fixed for the system throughout the simulation, since the system deals with certainty:

1. Distribution: Fixed
2. Fixed Value: 10
3. Capacity for the Queues: Infinite

Figure 4 shows the first simulation where the operational level was 100%, where there were no threats to the system.



Run For: 720 minutes

Restricted License: Only for use by full time students registered at a degree awarding education

Fig.4 100% Operational Level Diagram

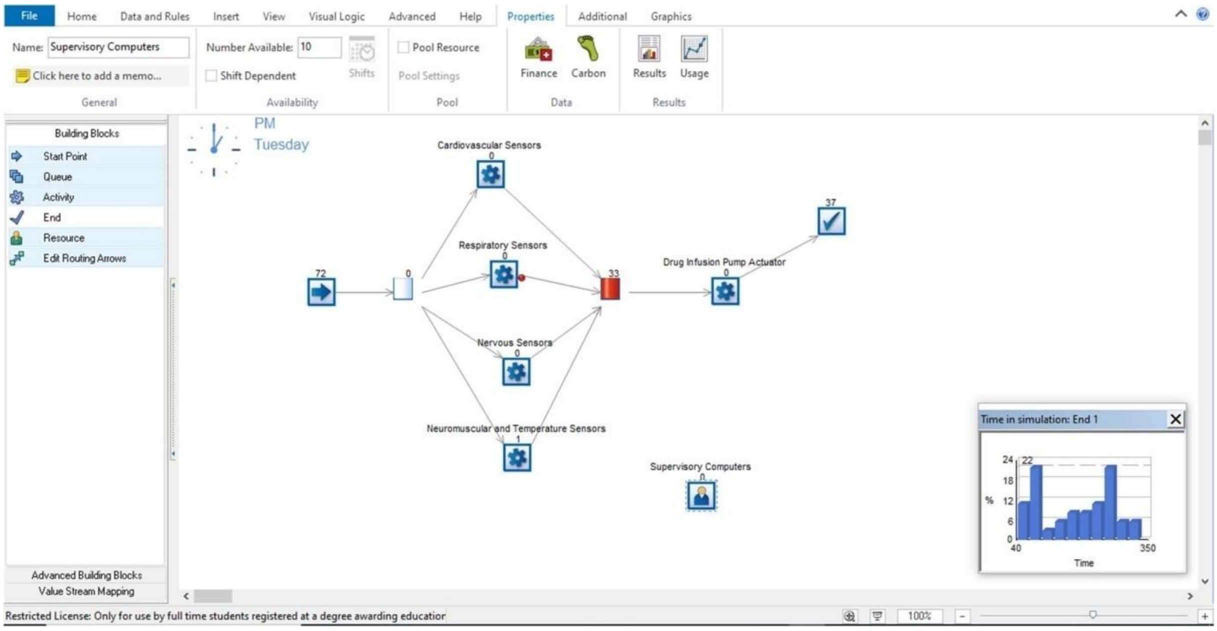
Table 1 shows the operational and financial parameters of the system at this level.

Table 1: 100% Availability Operational and Financial implications

Parameter:	Value:
Availability	100%
Resources left:	8
Work Started	72
Work in Queues and Activities	3
Work Completed	69

Cost	£1,799.83
Revenue	£6,900.00
Profit	£5,100.17

The values here show the system operates at the most optimal level. The values were reduced at every 20% interval, that is 100%, 80%, 60%, 40%, 20% and 0% The first significant changes to flow of control were noticed when resource availability reduced to 20% as shown in Figure 5 and Table 2.



Name: Supervisory Computers
Number Available: 10
☐ Shift Dependent
☐ Pool Resource
Restricted License: Only for use by full time students registered at a degree awarding educatior

Fig 5: 20% Operational Level Diagram

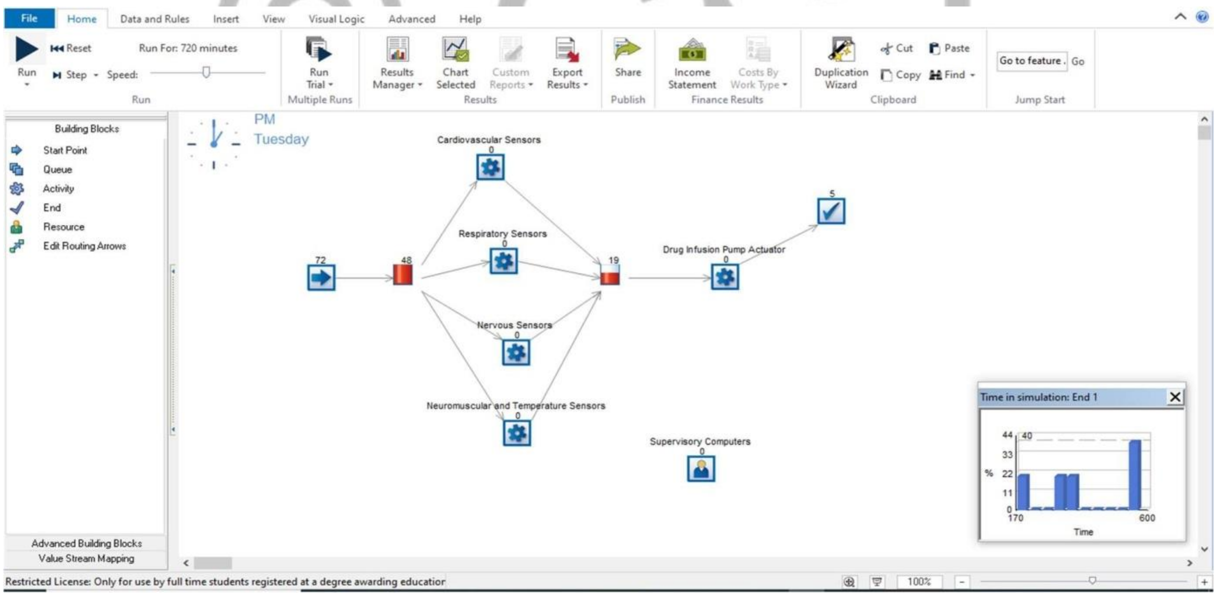
Table 2: 20% Availability Operational and Financial implications

Parameter:	Value:
Availability	20%
Resources left:	0
Work Started	72

Work in Queues and Activities	35
Work Completed	37
Cost	£15,424.15
Revenue	£4,300.00
Profit	-£11,124.15

A significant loss is noticed, and the system queues up a lot of work, also the resources become depleted.

To test our hypothesis, we will now take the system down entirely by simulating 0% availability. This is what it would look like when a ransomware attack encrypts or locks computer in the environment. Figure 6 and Table 3 shows us the parameters.



Run For: 720 minutes

Restricted License: Only for use by full time students registered at a degree awarding education

Fig. 6: 0% Operational Level Diagram

Table 3: 0% Availability Operational and Financial implications

Parameter:	Value:

Availability	0%
Resources left:	0
Work Started	72
Work in Queues and Activities	67
Work Completed	5
Cost	£31,200.49
Revenue	£500
Profit	-£30,700.49

Here the resources in the systems have been totally depleted.

DISCUSSION

Our simulations revealed that the ransomware attack hampered the operation of infusion pumps and patient monitor via HMI. The assault significantly reduced the operation of the Cyber Physical System being modelled and the operating level of the smart healthcare environment. This can be seen as the profit has a negative value, meaning that the cost of maintaining the system is above what it generates. When the cyber attacker demands a ransom is paid before the system is restored to normal operations, this adds extra negative cost implications to the system.

As mentioned earlier, ransomware is one of the most prevalent cyber-attacks within the healthcare sector. This is because it easy to create, it spreads quickly, and its effect can be very devastating on health IT systems, let alone when it affects health OT systems. Our simulation has been able to prove how fatal a ransomware attack on a Healthcare Cyber Physical System can be. Our findings emphasise the importance of improved security mechanisms and procedures in the design, deployment, and usage of Healthcare Cyber Physical Systems, making sure security updates are issued on a regular basis, backups of system data are consistent, as well as proper network segmentation to protect vital systems CPS from the internet.

CONCLUSION

To summarise, the incorporation of Cyber Physical Systems in healthcare poses significant security risks that must be addressed by a combination of technical, governmental, and operational safeguards. This analysis emphasises the need of protecting connected medical equipment and healthcare systems, as well as the importance of ongoing research and development in this field.

REFERENCES

Bressan, N. M. (2011). Integrated Anaesthesia Software: Data Acquisition, Controlled Infusion Schemes, and Intelligent Alarms. Doctoral Thesis, University of Porto. Retrieved from https://repositorio aberto.up.pt/bitstream/10216/61305/1/000149414.pdf

Kanjee, M. R., and Liu, H. (2016) Authentication and key relay in medical cyberphysical systems. Security Comm. Networks, 9: 874– 885. doi: 10.1002/sec.1009.

Kostadinov, D. (2020) ICS Components | Infosec Resources.Retrieved from https://resources.infosecinstitute.com/topic/ics-components/ Lee, I., & Sokolsky, O. (2010). Medical Cyber Physical Systems. 47th Design Automation Conference (pp. 743–748). Pennsylvania: http://dx.doi.org/10.1145/1837274.1837463.

Loshin, P. (2021, December). SCADA (supervisory control and data acquisition). Retrieved from Target Tech https://www.techtarget.com/whatis/definition/SCADAsupervisory-control-and-data-acquisition

Nair, M. M., Tyagi, A., & Goyal, R. (2019). Medical Cyber Physical Systems and Its Issues. Procedia Computer Science, 165:647-655.

Pekarova, S. (2021, May 10). Industrial Control Systems in Healthcare Environments. Retrieved from Dreamlab Technologies AG: https://dreamlab.net/en/blog/scada-ics/post/industrial-control-systems-in-healthcare-environments/

Sarka, P., & Levalle, Y. (2021, March 02). Ransomware Attacks and Protections in Industrial Control Systems. Retrieved from Dreamlab Technologies AG: https://dreamlab.net/en/blog/scada-ics/post/ransomware-attacks-and-protections-in-industrial control-systems/ SCADA. (2023, Feb 23). Supervisory control and data acquisition (SCADA). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/SCADA

Verma R. Smart City Healthcare Cyber Physical System: Characteristics, Technologies and Challenges. Wirel Pers Commun. 2022;122(2):1413-1433. doi: 10.1007/s11277- 02108955-6. Epub 2021 Aug 26. PMID: 34462622; PMCID: PMC8387555.

Wangsness, C. (2022, September 20). What is a SCADA System, and How Does It Work? Retrieved from Onlogic Blog: https://www.onlogic.com/company/io-hub/what-is-ascada-system-and-how-does-it-work/