Journal of Mechanical Science and Engineering 8(1) 1-4, 2021
ISSN 2354-9467

INDUSTRIAL CONTROL SYSTEM APPLIED AND PROBLEMS: A REVIEW AND EXPERIENCES

Yudianto[1], Mohruni A. S. [1*]

[1]Department of Mechanical Engineering, Faculty of Engineering, Universitas Sriwijaya, South Sumatera, Indonesia

ABSTRACT

This paper aims to explain examples of industrial control system applications that are applied in the industrial world today and the problems that arise in the Industrial Control System (ICS). The methodology used in this paper is to review several journals, books, and work experiences (experiment). SCADA in the highest position, the DCS at level 2, then the PLC at the very bottom. And there are two problems encountered, namely in terms of hardware and software. In case of hardware problem SCADA, DCS and PLC hit by lightning, exposed to droplets of water seepage, electrical fuse problem, the temperature of the hot room, high humidity, mainboard problem (due to lifetime), power supply (due to lifetime and bad electric power supply). In terms of the software, its software is corrupt, so it should be in the re-install. In general, a CD contains software for one PC (personal computer) because there is one CD software there is activation code where when you enter the activation code must be connected to the internet network that is detected automatically. The effect that causes the most loss was a broken fuse. So, dividing the same load each digital output or part is good architecture. The SCADA system had to be more concerned for cybersecurity compares with the DCS system due to its connection with the network. That was for maintaining availability and reliability.

Keywords: SCADA, DCS, PLC, activation code, encountered problem, software, hardware, cybersecurity.

1 INTRODUCTION

Industrial Control System is a general term that includes supervisory control and data acquisition system, distributed control system, and programmable logic control [1]. For more understanding, the design is shown in **Error! Reference source not found.**.

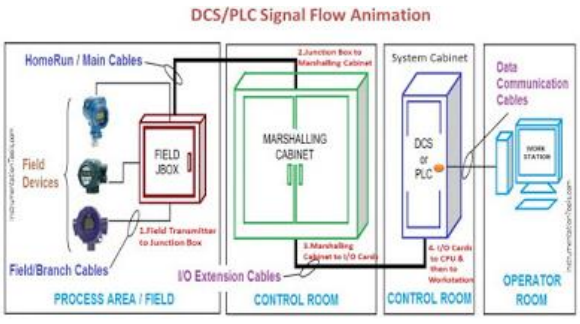

Figure 1 DCS/PLC Sinyal Flow Animation

The terms of an industrial control system, in this paper, are sensor, transmitter, junction box, surge arrester, actuator, marshaling cabinet, FSC (Fail-Safe Controller), C300 controller, console station (HMI), server, supervisory control network, NAS (Network Attached Storage), etc. A sensor is a device that converts a physical stimulus or variable of interest (such as temperature, force, pressure, or displacement) into a more convenient form (usually an electrical quantity such as voltage) to measure the stimulus [2]. The transmitter is an electrical instrument that interfaces a temperature sensor, flow sensor, level sensor, pressure sensor to a measurement or control device like a PLC, DCS, PC (Personal Computer), loop controller, data logger, display, recorder, etc. The junction box is an enclosure used for interconnection between field devices (outdoor) and indoor devices. A surge arrester is a device to protect electrical equipment from over-voltage transients caused by external (lightning) or internal (switching) events. The actuator is a hardware device that converts a controller command signal into a change in a physical

*Corresponding author's email: mohrunias@unsri.ac.id
https://doi.org/10.36706/jmse.v8i1.49

parameter (control valve, solenoid valve, limit switch, etc). The marshaling cabinet is between the junction box and the system cabinet functionally is to interface the incoming field cable (which is usually a multi-pair wire.) and the I/O (input/output) card connection. FSC is a Safety Integrity Level (SIL), certified integrated safety platform that supports a wide range of high integrity process control and safety function including high integrity process control, burner or boiler management systems, safeguarding process, and emergency shutdown, turbine and compressor safeguarding, fire and gas detection systems, pipeline monitoring.

The main purpose of this paper is to resolve the problems encountered so the equipment like SCADA, DCS, PLC, sensor (flow sensor, pressure sensor, temperature sensor, level sensor, etc), and the actuator can operate again and work together on the system in a major industry (maintenance of availability and reliability). SCADA and DCS can be integrated and developed as required by a large company [3]. and will be described where the position of the sensor, actuator, control valve, ESDV (Emergency Shutdown Valve). Because in general many people know about SCADA and DCS but not knowing the system architecture that exists in the field. then how does the transmitter for processing and transmitter for ESD (emergency shutdown system), where the type of actuator to process and actuators for ESD.

2 METHODOLOGY

This study was conducted by reviewing at least five International Journals, one book, experiences at a national oil and gas company. On an industrial control system that concentrates SCADA/DCS issues and describes more details on the SCADA/DCS architecture.

Based on the system analysis carried out, the system is determined according to the needs of Sriwijaya University. The stages of the website design that will be built are shown in the research flow diagram Figure 2.

3 RESULTS AND DISCUSSIONS

Direct into the chapter such as:

3.1 SCADA/DCS Architecture

The architecture is shown in **Error! Reference source not found.** in a single plant like SPG A (Stasiun Pengumpul Gas A: Gas Collecting Station A).

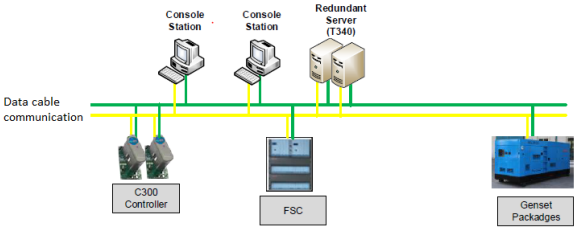

Figure 2 Architecture DCS at PT Pertamina EP Asset 2

For the DCS architecture (C300 controller) as the sensor emitter position (TT: temperature transmitter, PT: pressure transmitter, LT: level transmitter), Control Valve is the actuator (pressure control valve, level control valve, temperature control valve, flow control valve), cmd start (command start is a command order to start a pump, air fan cooler, air compressor, hydrant pump, etc), cmd stop (command stop is a command order to stop a pump, air fan cooler, air compressor, hydrant pump, etc). And for FSC (Fail-Safe Controller is like PLC especially for safety system) such as TT (temperature transmitter, THH: temperature high-high and TLL; temperature low, etc as the input). The output is ESDV (Emergency Shutdown Valve which operates full open or full closed when signal LL, HH, Gas Detector, Fire Detector, etc). And then the output of signal LL, HH, Gas Detector, Fire Detector are for cmd stop, sirene, alarm, etc. Special for UPS (Uninterruptible Power Supply), Genset Packages are communicated with data cable communication so it can be just monitored at console station (same as HMI: Human Machine Interface) [4]. If plants are would be monitored and controlled they can be connected under the C300 controller. All are shown in **Error! Reference source not found.**.

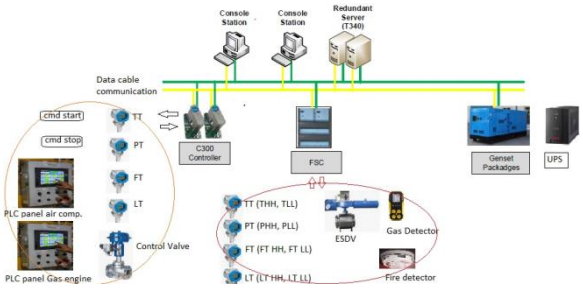

Figure 3 Architecture DCS (input and output)

More advance for upgrading DCS for more advanced monitoring, control, and data acquisition as shown in **Error! Reference source not found.**. Network-attached storage (NAS) is a file-level (as opposed to block-level storage) computer data storage server connected to a

computer network providing data access to a heterogeneous group of clients [5]. NAS is specialized for serving files either by its hardware, software, or configuration [6]. It is often manufactured as a computer appliance – a purpose-built specialized computer. NAS systems are networked appliances that contain one or more storage drives, often arranged into logical, redundant storage containers or RAID [7]. Network-attached storage removes the responsibility of file serving from other servers on the network. They typically provide access to files using network file sharing protocols such as NFS, SMB, or AFP [8]. From the mid-1990s, NAS devices began gaining popularity as a convenient method of sharing files among multiple computers [9]. Potential benefits of dedicated network-attached storage, compared to general-purpose servers also serving files, include faster data access, easier administration, and simple configuration [10].

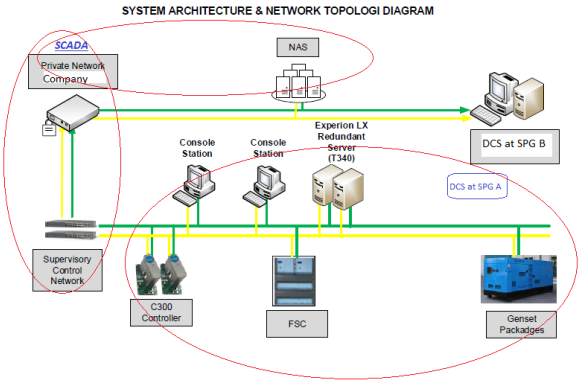

Figure 4 System Architecture & Network Topology Diagram

3.2 Problems Encountered and Problem Solving

The problems encountered in the Gas Collecting Station are;

3.2.1 Broken fuse

It occurred a few times the fuse failure, never in 1 week 8 times mostly in the rainy season in which place the fuse broke was the same that caused the ESDV plant's inlet to closed, some AFCs closed so the plant was shut down [11]. Solve the problem first, look for the wiring schematic, then check by item, is there a charge of the fuse is there that connects to the ground, found a grounded ESDV (Emergency Shutdown System) cable solenoid, insulated the wires, wire disconnected from ESDV to JB (Junction Box), megger test by giving 50 VDC (the result was always correct), then solenoid was bypassed so that the operation of ESDV was not disrupted (ok). Then finding the terminal at the junction box, its condition was wet (water inserted into junction box). It dried, replaced the terminal with JB, then the JB's cover was sealed by silicon red resisting water or rainwater insert to JB as shown in Figure 6. The result was a fuse last only 25 days, then broke up again. A load of fuse no.7 was shown in Figure 5.

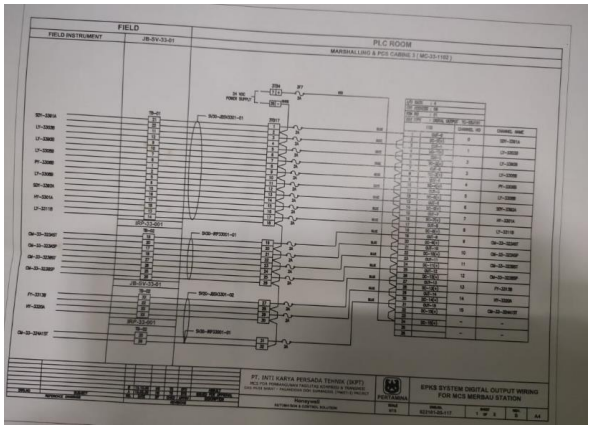

Figure 5 Wiring diagram for fuse no.7

Figure 6 All Junction Box was additionally isolated by red silicon after replacing cable's terminal

Secondly, try to replaced Digital Output as shown in Figure 7. Because of analysis that the digital output might be broken (the function). But one day later, the Fuse no.7 broke off again several times.

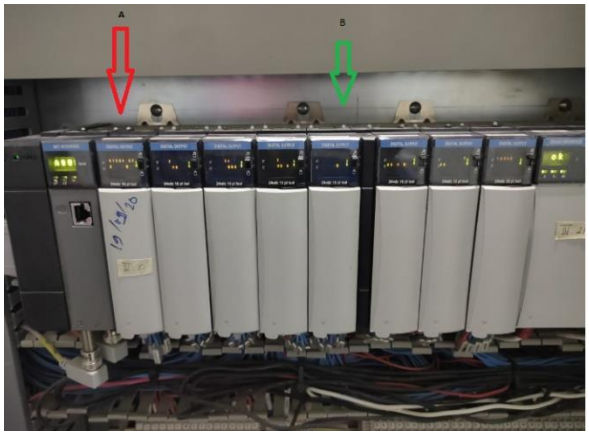

Figure 7 Digital Output red marked was replaced by a new one, that indicated crowded load

Third, tried to last option such as removing the cable's terminal to another block terminal as shown in Figure 8. So, the Digital Output load moved to other Digital Output green marked (that had a single load). The Digital Output red marked indicated the most crowded load as shown in Figure 7. The result was good (the same problem has been done).

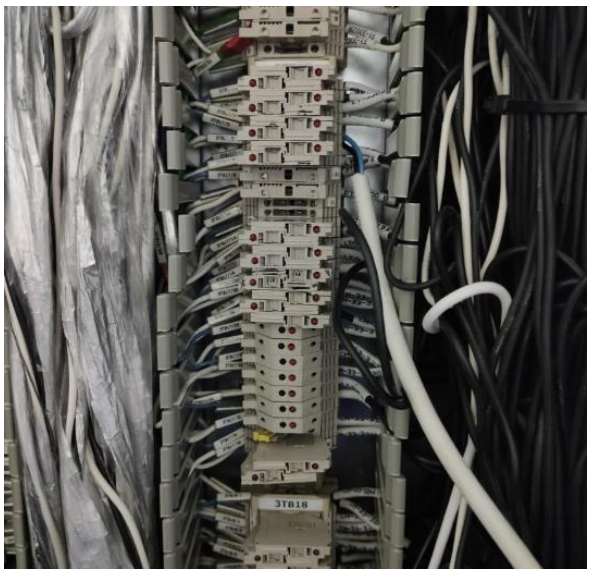

Figure 8 Terminal cable connected field JB to Digital Output (Relocated the most crowded load terminal to single load terminal)

3.2.2 Server Problem

The function of the redundant server was to operate server B directly in case of failure of server A. The problem was that server B wasn't synchronized. Thus, the Console Station (HMI) did not show all field process values (although the field processing plant was still working, this was not a safe operation). Try to clone the program to a different PC, but it did not work. The latter option was to use only one server. When trying to use a dual server, the B server always appears on a display such that a B server was not synchronized. It can be caused by a shattered life and fan on the rear PC. As a result, it generated a high temperature on the server PC (personal computer), which shortened the lifespan. The position server is shown in **Error! Reference source not found.**.

3.2.3 False Signal Problem

This problem is usually not coming in DCS compared with SCADA. But this problem had happened in this plant (it is rare). Lean Amine pump was suddenly shut down with indications was an Emergency Stop signal, although did not push the emergency shutdown button. So the solution was tightening the wires. It has been done.

3.2.4 Future Problem

The next project will use the SCADA system to accommodate some gas collecting stations, so from the office center at Prabumulih could monitoring the DCS process at station A and station B at Muara Enim. The scoping project is replacing all software and hardware (server, console station PC, all parts in marshaling cabinet (PLC, digital input, digital output, arrester, fuse, terminal block, and tagging, new software). Due to software and hardware will be new. It will sure that the DCS will be more reliable. Our future problem will more generate from the SCADA system especially for telecommunication and cybersecurity [12][13][14][15].

4 CONCLUSIONS

1. The effect that causes the most loss was a broken fuse. So dividing the same load each digital output or part is good architecture.
2. The SCADA system had to be more concerned for cybersecurity compares with the DCS system due to it is connected with the network.

REFERENCES

[1] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for Industrial Control Systems : A Survey," *Computers & Security*, p. 101677, 2019, doi: 10.1016/j.cose.2019.101677.

[2] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial Attacks on Machine Learning Cybersecurity Defences in Industrial Control Systems," *arXiv*, vol.

58, no. February, p. 102717, 2020, doi: 10.1016/j.jisa.2020.102717.

[3] G. Li *et al.*, "Detecting Cyberattacks in Industrial Control Systems Using Online Learning Algorithms," *Neurocomputing*, vol. 364, pp. 338–348, 2019, doi: 10.1016/j.neucom.2019.07.031.

[4] T. Alladi, V. Chamola, and S. Zeadally, "Industrial Control Systems: Cyberattack Trends and Countermeasures," *Computer Communications*, vol. 155, no. February, pp. 1–8, 2020, doi: 10.1016/j.comcom.2020.03.007.

[5] S. Zhanwei and L. Zenghui, "Abnormal Detection Method of Industrial Control System Based on Behavior Model," *Computers and Security*, vol. 84, pp. 166–178, 2019, doi: 10.1016/j.cose.2019.03.009.

[6] T. K. Das, S. Adepu, and J. Zhou, "Anomaly Detection in Industrial Control Systems Using Logical Analysis of Data," *Computers and Security*, vol. 96, p. 101935, 2020, doi: 10.1016/j.cose.2020.101935.

[7] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A Survey on Attack Detection, Estimation and Control of Industrial Cyber-Physical Systems," *ISA Transactions*, 2021, doi: 10.1016/j.isatra.2021.01.036.

[8] S. A. Qasim, J. M. Smith, and I. Ahmed, "Control Logic Forensics Framework Using Built-in Decompiler of Engineering Software in Industrial Control Systems," *Forensic Science International: Digital Investigation*, vol. 33, p. 301013, 2020, doi: 10.1016/j.fsidi.2020.301013.

[9] L. Rosa *et al.*, "Intrusion and Anomaly Detection for the Next-Generation of Industrial Automation and Control Systems," *Future Generation Computer Systems*, vol. 119, pp. 50–67, 2021, doi: 10.1016/j.future.2021.01.033.

[10] E. Edelson, "Security in Network Attached Storage (NAS) for Workgroups."

[11] H. X. Zhang, "Design of Industrial Computer Control System in Grease Production," *Procedia Computer Science*, vol. 166, pp. 376–380, 2020, doi: 10.1016/j.procs.2020.02.081.

[12] X. Liu, J. Zhang, P. Zhu, Q. Tan, and W. Yin, "Quantitative Cyber-Physical Security Analysis Methodology for Industrial Control Systems Based on Incomplete Information Bayesian Game," *Computers and Security*, vol. 102, p. 102138, 2021, doi: 10.1016/j.cose.2020.102138.

[13] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System," *IEEE Access*, vol. 8, pp. 83965–83973, 2020, doi: 10.1109/ACCESS.2020.2992249.

[14] T. Kiravuo, M. Sarela, and J. Manner, "A Survey of Ethernet LAN Security," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1477–1491, 2013, doi: 10.1109/SURV.2012.121112.00190.

[15] C. W. Lin and H. Yu, "Invited - Cooperation or Competition?: Coexistence of Safety and Security in next-Generation Ethernet-Based Automotive Networks," *Proceedings - Design Automation Conference*, vol. 05-09-June, 2016, doi: 10.1145/2897937.2905006.