JURNAL LOCUS: Penelitian & Pengabdian
Volume 5 No. 1 January 2026
E-ISSN 2829-7334| P-ISSN 2829-5439
Hompage: https://locus.rivierapublishing.id/index.php/jl

Study of SCADA System Implemented for Coal Fired Steam Power Plant IPP Kendari - 3 with Reliability Rate Comparison of Redundancy 2 Gateway Device and Stand Alone Gateway Device SCADA System

Indra Yuliarta I. E.[1], Harry Christanto Pinta Masiri[2]
PT DSSP Power Kendari, Indonesia[1,2]
Email: indra.yuliarta@dsspower.co.id, harry.christanto@dsspower.co.id

Abstract:
This paper aims to examine the influence of the Supervisory Control and Data Acquisition (SCADA) system on operational performance, reliability, and availability at the IPP Kendari–3 Coal-Fired Steam Power Plant (CFSPP) with a capacity of 2 × 50 MW, which serves as a critical backbone in the 150 kV Southeast Sulawesi interconnection system. The study focuses on the utilization and implementation of a SCADA architecture designed with a redundancy configuration employing two gateway devices—namely, a main gateway and a backup gateway. This redundancy scheme is intended to ensure continuous system operation, high reliability, and data integrity, particularly in the event of hardware malfunction or communication network failure. The research discusses the SCADA configuration design, communication topology, and redundancy logic that governs automatic failover between the primary and secondary gateways. Through continuous monitoring and real-time data acquisition, the SCADA system enables operators to detect disturbances promptly and respond effectively to abnormal operating conditions. The findings indicate that the implementation of gateway redundancy significantly enhances system availability by minimizing downtime and preventing data loss during failures. As a result, plant operational safety, efficiency, and stability are improved. Overall, the study demonstrates that a properly designed SCADA redundancy system plays a crucial role in supporting reliable power generation and strengthening the resilience of the regional transmission network.

Keywords: SCADA, redundancy, gateway device, steam power plant, reliability, system availability.

Corresponding: Indra Yuliarta I. E
E-mail: indra.yuliarta@dsspower.co.id

INTRODUCTION

Due to technological advancements and the spread of knowledge-based economies, information systems have played a significant role, mainly at the administrative level (Javier Maseda et al., 2021). Technological development has laid the foundation for an information society that operates through knowledge operations management to process, capture, and store information. Operators, feeders, and beneficiaries are responsible for knowledge operations management (Scranton, 2021).

Given their increasing importance, information technology systems—particularly SCADA—have been widely integrated into vital sectors such as electricity and oil by adopting open systems that interact with the environment to realize socioeconomic goals and establish future visions and general orientations (Zhang et al., 2019; Liu et al., 2021). Information technology systems are the pillar of success and development (Kaufman et al., 2020; Wang & Lin, 2021). They help improve behaviors, skills, and thought patterns (Sankaran et al., 2020; Palacios et al., 2019). The SCADA system has reduced dependency on the human element and provides critical information for senior management to perform their duties to the fullest (Nagaraj et al., 2021; Xu et al., 2020).

Furthermore, this system provides transparent, accurate, and rapid access to goals related to receiving, storing, transferring, and updating data and information in business organizations (Ahmed, 2025; Hosen et al., 2024). In addition, it secures internal controls and displays all warning cases (Nițulescu & Korodi, 2020). Steam power plants rely on continuous data acquisition and control systems to maintain stable operations. SCADA systems play a crucial role in monitoring plant performance, controlling critical parameters, and detecting faults in real time.

However, a single-point failure in communication or gateway hardware can lead to data loss or operational disruption. To mitigate these risks, implementing a redundancy system with two gateway devices is proposed. This configuration provides a backup secondary gateway when the primary one fails, ensuring uninterrupted communication between field devices and the control center.

Technology for technical improvements develops rapidly to meet the growing needs of power systems. Following technological advancements and the spread of knowledge-based economies, information systems have played a significant role (Javier Maseda et al., 2021). The SCADA system has reduced dependency on the human element and provides critical information for senior management to perform their duties to the fullest (Upadhyay & Sampalli, 2020).

Furthermore, this system provides transparent, accurate, and rapid access to goals related to receiving, storing, transferring, and updating data and information in business organizations. In addition, it secures internal controls and displays all warning cases (Nițulescu & Korodi, 2020). From these outcomes, the technology used in organizations has contributed to developing communication channels between various administrative levels, whether horizontal or vertical. Consequently, the SCADA system is not just about tools and devices but also about ideas for problem-solving and a technological means to improve performance efficiency (Budiman, Sunariyo, & Jupriyadi, 2021).

Supervisory control and data acquisition (SCADA) systems are widely used in conventional electrical grids for transferring sensor and control data among different systems. In , a reliability analysis is performed for a SCADA system in an electrical grid. The analysis focuses on power generation and transmission systems with centralized and distributed architectures. A model based on Monte Carlo simulation and the IEEE reliability test system (RTS) is applied. In addition, a damage cost function is defined to determine the annual cost of SCADA system reliability.

This cost arises if power is not supplied properly due to a lack of measurement information from SCADA failure. The analysis shows that the centralized architecture could cost 5.5 times more than a distributed one when failures occur. In, an information architecture is proposed for a power system, and a reliability analysis is performed for it. The proposed architecture uses a distributed hierarchical structure to achieve fault tolerance and scalability in an electrical grid. The layered model abstracts the control center, power plants, transmission, and distribution substations. In this way, communication and computation loads are relieved from higher layers (i.e., the control center) through data aggregation and processing. The reliability performance of the proposed architecture is derived, and evaluation results show that a fully redundant system (e.g., using backup control centers) can significantly improve system reliability.

This study introduces novelty through a comparative analysis of SCADA system reliability between a redundancy configuration of two gateway devices and a stand-alone single gateway configuration, applied directly to the Coal Fired Steam Power Plant IPP Kendari-3, using actual operational data. This provides empirical evidence rarely discussed in previous studies.

The purpose of this study is to analyze the implementation of the SCADA system and compare the performance, reliability, and availability between the two configurations in supporting plant operational continuity and the stability of the regional electricity interconnection system. The benefits of this research are expected to theoretically enrich scientific development in industrial control systems and electricity, particularly regarding SCADA redundancy design. Practically, it can serve as a reference for power plant operators, engineers, and policymakers in selecting more reliable, efficient, and safe SCADA configurations to enhance power plant operational reliability.

METHOD

Looking at application – protocol - independent redundancy, we focus on failover processes for remote control and monitoring systems in electrical distribution systems. Critical components in power system control systems are usually redundantly deployed. In case of component failures, defined failover processes ensure a reliable switch-over to a working unit within a given time constraint. The novelty of the proposed approach is the use of SDN for the detection of system failures and for performing the actual switch-over. Typically, remote control and monitoring in power distribution systems is deployed across two levels (according to the smart grid architecture model—SGAM): the station level and the operation level.

The operation level groups the infrastructure, which is necessary to enable the control of field facilities using central control systems. The operation level particularly includes communication networks and the SCADA system. The station level, in comparison, denotes the equipment within field stations, which is necessary for remote control and monitoring. Besides, a communication network, at station level; IEDs; and remote terminal units (RTUs) are deployed, implementing particular functions of the remote control and monitoring system. The gateway device is responsible for the interconnection of station level and operation level and thus is highly important for remote control and monitoring. This device is in the focus of the redundancy management in this use-case.

Stand-Alone Gateway

One gateway device is used for the connection of field controllers (RTUs or IEDs) to the central SCADA system. This leads to a situation in which a failure of the gateway renders the field station unavailable to monitoring and control applications (a typical single point of failure).

Redundance Gateway

The state-of-the-art approach (shown in the centre) uses redundancy and failover management of gateway devices using a special voter component. The voter selects one of the available gateways based on its configuration with regard to predefined performance indicators. Whenever the alternative gateway performs better under these parameters, the voter switches to the other device. An example for such a parameter would be the communication quality between gateway and SCADA.

The redundant gateway approach, however, suffers from an intersection of concerns, as the voter (which is basically a part of the SCADA system) needs to be aware of the internal states of gateways, which are mainly communication devices such as switches and routers. Thereby, artificial dependencies between the SCADA system, the communication network, the communication protocols and the failover operation are created.

Virtualised Gateway Redundancy

By contrast, the application-protocol-independent redundancy approach depicted on the right side enables a separation of concerns by use of SDN. Here, SDN is employed to monitor the communication behaviour between the Gateway devices and the SCADA systems. Thereby, gateway failures (non-operational or non-responding gateways) can be detected and an immediate switch to another available gateway can be performed without notifying the SCADA application.

However, after switching to another gateway, the application layer communication (e.g., IEC 60870-5-104) needs to be re-established, as the state of the particular application layer connection between gateway and SCADA cannot be monitored using SDN. An evaluation of this approach showed that the SDN approachis able to complete the failover procedure within five seconds of failure occurrence (software and hardware failures of the gateway). This is considered sufficiently fast for most applications in field.

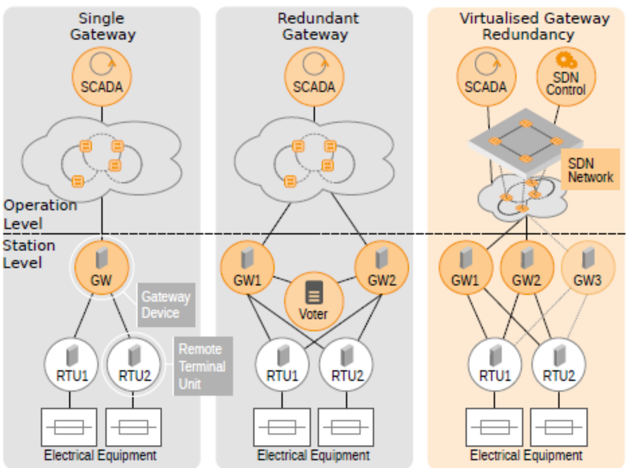

Fig 1. The virtualised gateway redundancy

For the implementation of the gateway-failure and switch-over operation, we had a look at two different technologies, the SDN reference implementation Open Flow (Switch

Specification, Version 1.5.1) and the network programming language P4. First, we conducted a theoretical comparison of both technologies. While both technologies allow a fast detection of broken physical network connections of the gateway (broken link), things become more complex when detecting non-responsive gateways.

With Open Flow, switch port metrics (byte and packet counts) are available to analyze the communication activity between a gateway and the SCADA system. Hence, to detect an unresponsive gateway, the 104 requests and replies sent between the main component and the gateway are analyzed by observing the relation of the associated traffic, and as soon as SCADA requests are not answered by the gateway, a switch-over is performed.

During the last years, several approaches have been proposed to supplement and replace MPLS and VLANs with software-defined networking (SDN) in Smart Grids, in particular due to its promises to increase flexibility and to simplify network management and due to its network monitoring capabilities. SDN achieves this by basically separating the networks' control plane from its data plane by moving the networks' intelligence to a centralized SDN controller. Using the standardized south-bound-interface, SDN switches (the data plane) communicate to SDN controllers (the control plane) in order to exchange monitoring data and control data.

The centralized control plane, for its part, offers a standardized north-bound-interface, providing the possibility for a network owner to tailor network behavior to specific needs. Standardized open interfaces and centralization of control allows for faster implementation of new network functionalities for the Smart Grid than in traditional networks, where new functionalities are based on standards that are required to be implemented (and rolled out) on each particular network device (Rinaldi et al., 2015). Examples for fast implementation include the deployment of new routing algorithms implemented at controller level, particularly suitable for power grid communication. Besides this, SDN has been shown to be particularly useful when dependable communication is required like in real-time production machinery networks (Herlich et al., 2016).

In the context of power grid dependability, SDN has been applied---particularly in three fields related to dependability: Ensuring Quality of Service (QoS), mitigation of cyber-attacks, and mitigation of failures. The heterogeneity of applications in Smart Grids is ranging from energy trading to machine-to-machine (M2M) communication for control of grid devices. All these particular applications open up a diverse and potentially mutually exclusive set of QoS requirements. In general, SDN provides flexible QoS to prioritize critical traffic (Zhao et al., 2016). With a particular focus on critical traffic flows, for instance switching commands, a behavior similar to DiffServ has been implemented based on SDN.

This has been realized by enabling an SDN controller to configure different queues of ports at an SDN Soft switch (Open Switch). DiffServ-like, the different queues are reflecting different traffic classes and thus priorities. In evaluation, it has been shown that this approach allows for reliably guaranteed data rates and latencies for a set of selected traffic classes common in power grid environments (IEC 61850 MMS, real-time control, common data transfers). A similar DiffServ inspired approach utilizing queuing capabilities of Open Switch, which is controlled by an SDN controller, is applied for enforcing critical IEC 61850 traffic in presence of link flood attacks.

RESULTH AND DISCUSSION

Designs and implementations of supervisory control and data acquisition systems for improving the use of industrial machinery have been increasing in recent years, with an evolution towards novel objectives, such as standardization, complex data analysis and robustness against failure.

Complexity of Architecture Design

Architecture design within include the Comparison of performance between Two identical industrial-grade gateways (Gateway A and Gateway B) were connected to the same network switch and SCADA server compare with Standalone industrial-class of gateways. Following the technology development, cost also linear with the complexity of the system. It is caused by more complex a system will be affect to the cost expanding during the project and also implementation, besides the cost that may appears and affected also for operating, maintaining and sparepart managing.

Table. 1. Result of Ranking Complexity Level – Total Cost Implication

Gateway Type	Complexity Level	Total Cost Implication
Single Gateway	1	1
Redundant Gateway	2	2
Virtualised Redundant Gateway	3	3

Comparison of Complexity of Architecture design SCADA System following the Table 1, show that Single Gateway has the 1st Rank with level of complexity and total cost the simple ones. After that Redundant Gateway placed the 2nd position which is the complexity increase following the installation of 2nd gateway means that multiply two times also the network configuration. And the last rank placed with Virtualized Gateway Redundancy with the most complex and costly architecture design.

Availability of SCADA System Faulty

Performance metrics such as failover time, data loss percentage, and abnormal control for HV Apparatus rate.

Table. 2. Result of Failover System – Data Loss Percentage

Gateway Type	Failover System Percentage (1)	Data Loss Percentage (2)
Single Gateway	3	3
Redundant Gateway	2	2
Virtualised Redundant Gateway	1	1

Table. 3. Result of Ranking Abnormal HV Apparatus – Malfunction SCADA Device

Gateway Type	Reliability to Control HV Apparatus (3)	Availability SCADA Device (4)
Single Gateway	3	3
Redundant Gateway	2	2
Virtualised Redundant Gateway	1	1

From Table. 2. and Table. 3. we can summarize rank from availability of SCADA system faulty or malfunction following Table. 4. With node 1 for Failover System Percentage, 2 for Data Loss Percentage, 3 for Reliability to Control HV Apparatus Percentage and 4 for Availability SCADA Device Percentage.

Table. 4 Summarize for Availability of SCADA system

Gateway Type	1	2	3	4
Single Gateway	3	3	3	3
Redundant Gateway	2	2	2	2
Virtualized Redundant Gateway	1	1	1	1

From Table. 4. Author can take big result that more complexity of the SCADA System will reduce the potential of malfunction whole system event partially. It is shown how easily malfunction single gateway to do all tasks. But system with redundant and also virtualized redundant gateway still have chance can able to execute and pass the task event partially SCADA device event 1 gateway malfunction.

Potential of Data Collision and Disruption

Data were collected from the indication of HV Apparatus and also measurement electrical parameter including the relay protection status.

Table. 5. Rank of Related Data Acquisition Collision and Mismatch Potential

Gateway Type	Data Collision Percentage	Data Mismatch Percentage
Single Gateway	2	2
Redundant Gateway	3	3
Virtualised Redundant Gateway	1	1

After do summarize we can see that the 3rd aspect comparison of SCADA, virtualized redundant gateway takes the 1st rank with smallest potential data collision and disruption. It is caused by Software Define Network capable separate between data with control and also supervisory. It means that each task can execute in separate subsystem or “room”.

CONCLUSION

The comparison of three SCADA system types—Virtualized Redundant Gateway, Redundant Gateway, and Single Gateway—across major aspects ranked Virtualized Redundant Gateway first, Redundant Gateway second, and Single Gateway last, though the former's weakness lies in its high complexity and total cost implications. SDN has proven particularly effective for dependable communication in real-time networks like production machinery and power grids, addressing dependability through QoS assurance, cyber-attack mitigation, and failure recovery; this study introduces a novel SDN-based redundancy approach for power plants and complex transmission lines, confidently enhancing SCADA efficiency, reliability, and resilience against abnormal conditions, with broader applicability beyond power systems. For future research, exploring cost-optimization strategies for Virtualized Redundant Gateway systems, such as hybrid SDN implementations or AI-driven complexity reduction, could make them more viable for widespread adoption in resource-constrained environments like Indonesian steam power plants.

REFERENCES

Ahmed, S. (2025). Enhancing data security and transparency: The role of blockchain in decentralized systems. *International Journal of Advanced Engineering, Management and Science*, *11*(1), 593258.

Budiman, Sunariyo, & Jupriyadi. (2021). SCADA system implementation in power plants. *Proceedings of the IEEE*. IEEE.

Herlich, M., Du, J. L., Schorghofer, F., & Dorfinger, P. (2016). Proof-of-concept for a software-defined real-time ethernet. In *Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1–4). IEEE.

Hosen, M. S., Islam, R., Naeem, Z., Folorunso, E. O., Chu, T. S., Al Mamun, M. A., & Orunbon, N. O. (2024). Data-driven decision making: Advanced database systems for business intelligence. *Nanotechnology Perceptions*, *20*(3), 687–704.

Javier Maseda, F., López, I., Martija, I., Alkorta, P., Garrido, A. J., & Garrido, I. (2021). Sensors data analysis in supervisory control and data acquisition (SCADA) systems to foresee failures with an undetermined origin. *Sensors*, *21*(8), 2762. https://doi.org/10.3390/s21082762

Kaufman, L., Green, P., & Teixeira, T. (2020). The role of information technology in organizational success: A comprehensive framework. *Journal of Information Technology Management*, *39*(2), 144–159. https://doi.org/10.1080/10383642.2020.1741830

Liu, J., Zhang, X., & Yu, L. (2021). SCADA systems and their integration with IoT for smart grids: A review. *IEEE Access*, *9*, 113454–113463. https://doi.org/10.1109/ACCESS.2021.3058786

Nagaraj, K., Suresh, S., & Jha, A. (2021). SCADA systems in industrial automation: Achievements and future perspectives. *Industrial Engineering Journal*, *37*(2), 52–67. https://doi.org/10.1016/j.iej.2020.11.010

Nițulescu, M., & Korodi, A. (2020). SCADA systems architecture based on OPC and web services. *Applied Sciences*, *10*(8), 2639. https://doi.org/10.3390/app10082639

Palacios, A., Romero, R., & Smith, P. (2019). Information systems as the foundation of organizational behavior and decision-making processes. *Journal of Organizational Studies*, *34*(3), 134–148. https://doi.org/10.1016/j.jos.2019.07.004

Rinaldi, S., Ferrari, P., Brandao, D., & Sulis, S. (2015). Software defined networking applied to the heterogeneous infrastructure of smart grid. In *Proceedings of the IEEE International Workshop on Factory Communication Systems* (pp. 1–4). IEEE.

Sankaran, K., Kumar, P., & Dey, S. (2020). Transforming organizational behavior through information technology integration: The case of SCADA systems. *Journal of Business Research*, *121*, 320–331. https://doi.org/10.1016/j.jbusres.2020.06.021

Scranton, P. (2021). *Technology, science and the uses of history*. Routledge.

Upadhyay, D., & Sampalli, S. (2020). SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, 101666. https://doi.org/10.1016/j.cose.2019.101666

Wang, Y., & Lin, B. (2021). Strategic impact of information systems in critical infrastructure sectors. *Journal of Strategic Information Systems*, *30*(1), 52–64. https://doi.org/10.1016/j.jsis.2020.101597

Xu, J., Li, Z., & Zhang, Y. (2020). SCADA in the energy sector: Automation and optimization for future energy systems. *Energy Reports*, *6*, 426–439. https://doi.org/10.1016/j.egyr.2020.02.039

Zhang, H., Li, Y., & Chen, F. (2019). SCADA systems in energy management: Enhancing decision-making with real-time data. *Energy Management Journal*, *27*(3), 132–141. https://doi.org/10.1016/j.emj.2019.01.013

Zhao, J., Hammad, E., Farraj, A., & Kundur, D. (2016). Network-aware QoS routing for smart grids using software defined networks. In A. Leon-Garcia et al. (Eds.), *Smart City 360* (Vol. 166, pp. 384–394). Springer International Publishing.