

Reliability Modeling for Virtualized PLC Architectures with Redundant Supervision and Stealth Attack Mitigation

Lucas Restivo de Oliveira

CTE - Space Sciences and Technologies, Aeronautics Institute of Technology (ITA)
Praça Marechal Eduardo Gomes, 50, Vila das Acácias, São José dos Campos - SP, 12228-900,
Brazil
`l.restivo93@gmail.com`

Moacyr Machado Cardoso Junior

CTE - Space Sciences and Technologies, Aeronautics Institute of Technology (ITA)
Praça Marechal Eduardo Gomes, 50, Vila das Acácias, São José dos Campos - SP, 12228-900,
Brazil
`moacyr@ita.br`

Nathan Assis Demoliner

Faculdade de Engenharia da Universidade do Porto
Rua Dr. Roberto Frias, s/n 4200-465 Porto, Portugal
`nathandemoliner@outlook.com`

ABSTRACT

The virtualization of industrial systems has enabled the consolidation of multiple PLCs into centralized environments, improving scalability and efficiency. However, this also increases exposure to simultaneous failures and stealth cyberattacks. This paper presents a hybrid reliability model combining physical failures - represented by Weibull and exponential distributions - with cyberattack dynamics and imperfect detection by a central supervisor. System logic is structured using Minimal Cut Sets (MCCs) to identify critical failure combinations. Monte Carlo simulations are used to estimate system reliability as a function of physical and cybernetic factors. Sensitivity, nonlinearity, and curvature analyses reveal how reliability varies with detection effectiveness and attack frequency. The findings highlight the existence of critical regions where reliability sharply declines, underscoring the need for robust detection strategies in virtualized industrial architectures.

KEYWORDS. Virtual PLCs, Reliability modeling, Cyber-physical resilience.

7. EN&OG - Operations Research in Energy, Oil and Gas

5. D&SP - OR in Defense and Security

1. Introduction

The progressive virtualization of industrial automation infrastructures has facilitated the consolidation of Programmable Logic Controllers (PLCs) into centralized execution environments, frequently hosted within container - based architectures and virtual machines. This paradigm shift is primarily driven by the pursuit of reduced hardware overhead, enhanced operational scalability, and streamlined deployment of updates and redundancy mechanisms. Nevertheless, such configurations introduce a new spectrum of reliability and cybersecurity challenges. Specifically, the co-location of multiple virtualized PLCs on a shared computational substrate increases susceptibility to correlated failures and coordinated stealth attacks, which may compromise critical control functionalities across multiple subsystems.

In the context of hydroelectric power plants, for instance, the dependable operation of systems such as gate control, excitation, and remote monitoring is vital for overall plant stability. Any undetected failure within these systems - whether caused by physical degradation or malicious interference - can degrade performance or precipitate systemic collapse. In virtualized settings, the propagation of such faults can be accelerated due to shared infrastructure, particularly when redundancy and supervision mechanisms are themselves centralized. Stealth cyberattacks, which exhibit low observability, persistence, and strategic timing, pose a particularly acute threat under these conditions, especially when detection relies on the continuous availability and correctness of a single supervisory agent.

Conventional reliability modeling approaches, including Fault Tree Analysis (FTA) and Markov processes, encounter notable limitations in this domain. These techniques often assume event independence and discrete failure transitions, offering limited expressiveness for systems in which functional correctness is conditioned on detection capabilities and cyber-physical interactions. In this context, there is a critical need for modeling strategies that can encapsulate Minimal Cut Sets structures while concurrently integrating failure propagation, detection probability, and coordinated attack behavior within a unified analytical framework.

To examine these vulnerabilities under realistic conditions, preliminary experiments were performed in a virtualized laboratory environment. The setup consisted of three independent Docker containers simulating PLC instances, along with a fourth container serving as a supervisory agent, all hosted on a single Ubuntu-based virtual machine. A separate Kali Linux virtual machine was configured to launch various cyberattacks - such as packet flooding (e.g., *hping3*), network filtering (e.g., *iptables*), and active reconnaissance probes (e.g., *nmap*, *nikto*) - against the control infrastructure. While the number and variety of attacks were constrained, the tests effectively demonstrated that even basic stealth interference can disrupt supervisory detection logic and hinder failover decision-making. These empirical findings motivated the formulation of formal reliability models capable of incorporating adversarial behavior and detection uncertainty.

This work proposes two complementary modeling frameworks to address the reliability assessment of virtualized control systems under cyber-physical adversities. The first framework models a specific container-based configuration inspired by the aforementioned laboratory experiments, capturing dual-path redundancy and imperfect detection using closed-form reliability expressions. The second, more general formulation, builds upon the Minimal Cut Sets paradigm to represent arbitrary architectures composed of multiple PLCs, supervisory agents, and auxiliary defense layers. This generalized structure allows system reliability to be expressed as a function of structural redundancy, attack frequency, and multi-layer detection effectiveness.

Both formulations are analytically constructed and critically contrasted. The specific model serves as a direct abstraction of experimental results, validating key behavioral trends observed in a minimal architecture. The generalized model, in turn, enables scalable evaluation across

a broader range of configurations and parameter regimes. By addressing both operational and adversarial dimensions, this dual - model approach provides a robust and extensible methodology for reliability analysis in industrial systems - particularly within critical infrastructure sectors undergoing digital transformation.

Recent studies support the integration of physical and cybernetic dimensions in reliability modeling. Works on small hydropower monitoring systems (Li et al. [2010]) and hardware-in-the-loop testing (Zaev et al. [2012]) confirm the operational sensitivity of critical control logic in hydro-electric settings. The vulnerability of Modbus-based supervisory architectures to stealth cyberattacks has been experimentally demonstrated (Radoglou-Grammatikis et al. [2020]), reinforcing the importance of incorporating detection effectiveness as a probabilistic parameter. The virtualization of PLCs via container-based or convergent architectures (Cruz et al. [2016]) introduces failure interdependencies, which have motivated high-availability solutions in real-time cloud environments (Kampa et al. [2023]). To mitigate such risks, protective strategies such as microprocessor relay schemes (Klyuev et al. [2021]) and intelligent centralized supervisory centers (Bo et al. [2015]) have been proposed. Additionally, recent reviews on virtualized power systems emphasize the role of layered detection mechanisms in preserving resilience under coordinated cyber threats (Rao et al. [2024]). These contributions frame the relevance of the dual-model strategy proposed in this work.

1.1. Virtualized System Reliability

The total system reliability, as defined by the architecture deployed in the experimental setup, is mathematically represented as:

$$R_{\text{sys}}(t) = R_1(t) \cdot R_3(t) \cdot R_s(t) \cdot [P_d + (1 - P_d)R_a(t)^2] \quad (1)$$

Where:

- $R_1(t)$: reliability of the primary PLC;
- $R_3(t)$: reliability of the backup PLC;
- $R_s(t)$: reliability of the Supervisor;
- P_d : probability that the Supervisor detects a stealth attack;
- $R_a(t) = e^{-\lambda_a t}$: probability that no stealth attack occurs up to time t ;
- $R_a(t)^2$: probability that neither PLC is compromised by an undetected stealth attack.

It is important to note that Equation 1 corresponds to a specific reliability expression for a system composed of two PLCs with sequential failover logic and a single supervisory module. This simplified formulation is useful for illustrating the fundamental interaction between physical failures, stealth attacks, and detection probability. However, to accommodate more general architectures with multiple components and diverse interdependencies, the following sections adopt a MCS-based reliability formulation that generalizes the system structure and failure logic.

In this expression, $R_a(t)^2$ represents the probability that two independent stealth attacks fail to compromise the system. This assumption reflects a dual-path fallback where both the primary PLC and the backup must remain uncompromised by undetected malicious behavior.

1.2. Modeling via Minimal Cut Sets

The critical events leading to system failure were modeled as Minimal Cut Sets:

- MCS_1 : simultaneous failure of PLC_1 , PLC_3 , and Supervisor;
- MCS_2 : stealth failure of PLC_1 and PLC_3 , combined with detection failure ($\neg D$);
- MCS_3 : physical failure of PLC_1 or PLC_3 , combined with Supervisor failure;
- MCS_4 : stealth failure of PLC_1 or PLC_3 , combined with detection failure ($\neg D$);
- MCS_5 : stealth failure of the Supervisor, leading to undetected loss of control logic.

1.3. Reliability Expansion Using Minimal Cut Sets

The general expression for system reliability, based on the exclusion of Minimal Cut Sets, is given by Breneman et al. [2022]:

$$R_{\text{sys}}(t) = 1 - P\left(\bigcup_{k=1}^5 MCS_k(t)\right) \quad (2)$$

Equation 2 can be expanded using the inclusion-exclusion principle to obtain an analytical approximation or to guide the structure of Monte Carlo simulations.

Inclusion-exclusion expansion (up to second-order terms):

$$P\left(\bigcup_{i=1}^5 MCS_i(t)\right) \approx \sum_{i=1}^5 P(MCS_i(t)) - \sum_{1 \leq i < j \leq 5} P(MCS_i(t) \cap MCS_j(t)) + \dots \quad (3)$$

Substituting into Equation (2), we obtain:

$$R_{\text{sys}}(t) = 1 - \left[\sum_{i=1}^5 P(MCS_i(t)) - \sum_{1 \leq i < j \leq 5} P(MCS_i(t) \cap MCS_j(t)) + \dots \right] \quad (4)$$

Practical approximation with five MCSs:

$$R_{\text{sys}}(t) \approx 1 - [P(MCS_1) + P(MCS_2) + P(MCS_3) + P(MCS_4) + P(MCS_5)] + [P(MCS_1 \cap MCS_2) + P(MCS_1 \cap MCS_3) + \dots] \quad (5)$$

As the number of MCSs increases, higher-order intersections become increasingly complex, and joint probabilities may not be independent. For this reason, the system reliability was numerically estimated through Monte Carlo Simulation using the following configuration.

2. Simulation Setup and Results

The reliability of PLC_1 was modeled with a Weibull distribution using shape parameter $\beta_1 = 1.5$ and scale parameter $\eta_1 = 2000$, while PLC_3 used $\beta_3 = 1.7$ and $\eta_3 = 2500$. The Supervisor was modeled with an exponential distribution with constant failure rate $\lambda_s = 1/5000$. The stealth attack rate λ_a was varied between $1/5000$ and $1/1000$, while the probability of attack detection by the Supervisor, P_d , was evaluated across the range from 0.5 to 0.99.

The simulations were implemented in Python using the NumPy and SciPy libraries. A total of $N = 10^6$ iterations were conducted for each parameter set. Simulations were executed on a system equipped with an Intel Core i7 processor and 16 GB of RAM, ensuring adequate computational resources for statistical convergence. The reliability evaluation was performed over a fixed time horizon of 2000 hours, representative of mid-term operational windows in industrial environments.

The reliability estimate was computed by:

$$\hat{R}_{\text{sys}}(t) = \frac{1}{N} \sum_{i=1}^N I_{\text{operational}}^{(i)} \quad (6)$$

where $I_{\text{operational}}^{(i)} = 1$ if the system did not fail in experiment i , and 0 otherwise.

Table 1 presents the estimated system reliability $\hat{R}_{\text{sys}}(t = 2000 \text{ h})$ as a function of the stealth attack rate λ_a and the probability of attack detection P_d . These values were obtained via Monte Carlo simulation using the MCS-based failure model described previously.

As expected, the results show that higher detection probabilities consistently increase system reliability. Conversely, increasing the stealth attack rate leads to a progressive decrease in $\hat{R}_{\text{sys}}$, particularly at lower P_d values where the Supervisor is less effective in identifying compromised controllers.

Table 1: Estimated Reliability $\hat{R}_{\text{sys}}(t = 2000 \text{ h})$ for varying P_d and λ_a

$P_d \backslash \lambda_a$	0.00020	0.00033	0.00050	0.00100
0.50	0.47807	0.41567	0.38501	0.36626
0.70	0.58068	0.54211	0.52311	0.51249
0.90	0.68123	0.66802	0.66361	0.65804
0.99	0.72613	0.72490	0.72277	0.72522

Figure 1 visualizes these results, highlighting how the impact of increasing λ_a is more pronounced for low values of P_d . At higher detection probabilities, the system becomes more resilient, and the reliability curves flatten, indicating reduced sensitivity to variations in the stealth attack rate. This behavior is consistent with the analytical model and will be further examined in the sensitivity analysis.

2.1. Sensitivity with Respect to P_d and λ_a

To understand how minor variations in the system's security parameters influence reliability, we begin by analyzing the partial derivatives of the reliability function with respect to (P_d) and (λ_a) . This step is critical to identify which variables most strongly affect system performance and to what extent. By quantifying the sensitivity gradient, we obtain a first-order diagnostic that highlights potential vulnerabilities in supervisory design.

The partial derivatives of Equation (1) are:

$$\frac{\partial R_{\text{sys}}}{\partial P_d} = R_1 R_3 R_s (1 - R_a^2) \quad (7)$$

$$\frac{\partial R_{\text{sys}}}{\partial \lambda_a} = -2t R_1 R_3 R_s (1 - P_d) R_a^2 \quad (8)$$

The magnitude of the sensitivity gradient is given by:

$$\|\nabla R_{\text{sys}}\| = \sqrt{\left(\frac{\partial R_{\text{sys}}}{\partial P_d}\right)^2 + \left(\frac{\partial R_{\text{sys}}}{\partial \lambda_a}\right)^2} \quad (9)$$

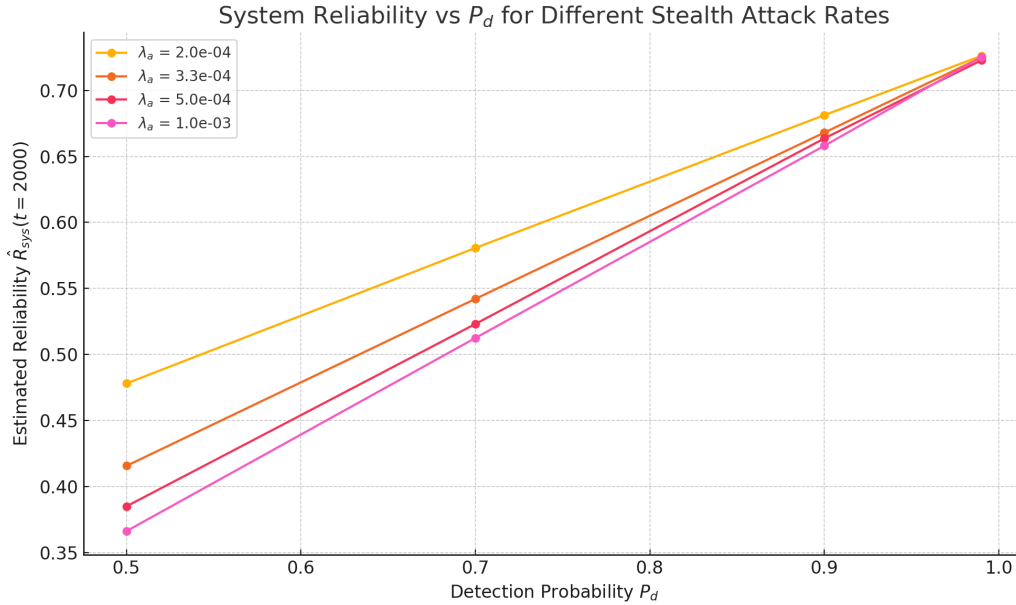


Figure 1: Estimated system reliability $\hat{R}_{sys}(t = 2000 \text{ h})$ for varying λ_a and fixed values of P_d .

2.2. Nonlinear Behavior of Reliability

The nonlinear behavior arises from the combination of exponential and linear components. The curve $R_{sys}(t)$ exhibits abrupt changes within specific ranges of P_d and λ_a , as illustrated below.

From an engineering perspective, increasing P_d represents improvements in the detection capabilities of the supervisory system, such as deploying more accurate anomaly detection algorithms, adding redundant supervision paths, or enhancing system logging and diagnostics. Similarly, variations in λ_a reflect changes in the intensity or frequency of stealth attacks targeting the system.

Figure 2 presents the heatmap of the sensitivity gradient magnitude for system reliability, calculated as the Euclidean norm of partial derivatives of $R_{sys}(t)$ with respect to parameters P_d and λ_a . This metric represents the degree to which reliability is sensitive to simultaneous small variations in these security parameters.

It can be observed that the highest sensitivity region is concentrated at low values of P_d , combined with low attack rates. At these points, small variations in either P_d or λ_a lead to abrupt changes in overall reliability, characterizing a critical transition zone between robust and vulnerable operational regimes.

At the extremes of the map - that is, when P_d approaches 1 or when λ_a is very high - the sensitivity decreases significantly. In the first case, the system becomes highly resilient even under attack conditions, and further improvements in detection capability have only marginal effects on $R_{sys}(t)$. In the second case, the system is already compromised due to the high frequency of stealth attacks, and additional variations in P_d have little influence on reliability, as the response capability is severely impaired.

The behavior identified in the sensitivity map reflects the nonlinear and threshold-dependent nature of the proposed system. The analysis demonstrates that it is insufficient to optimize security parameters individually; it is essential to simultaneously maintain both - a high P_d and a low λ_a - within a coherent range to ensure robustness. This result has direct implications for sizing supervisory components in virtualized architectures, as it delineates parameter-space regions where

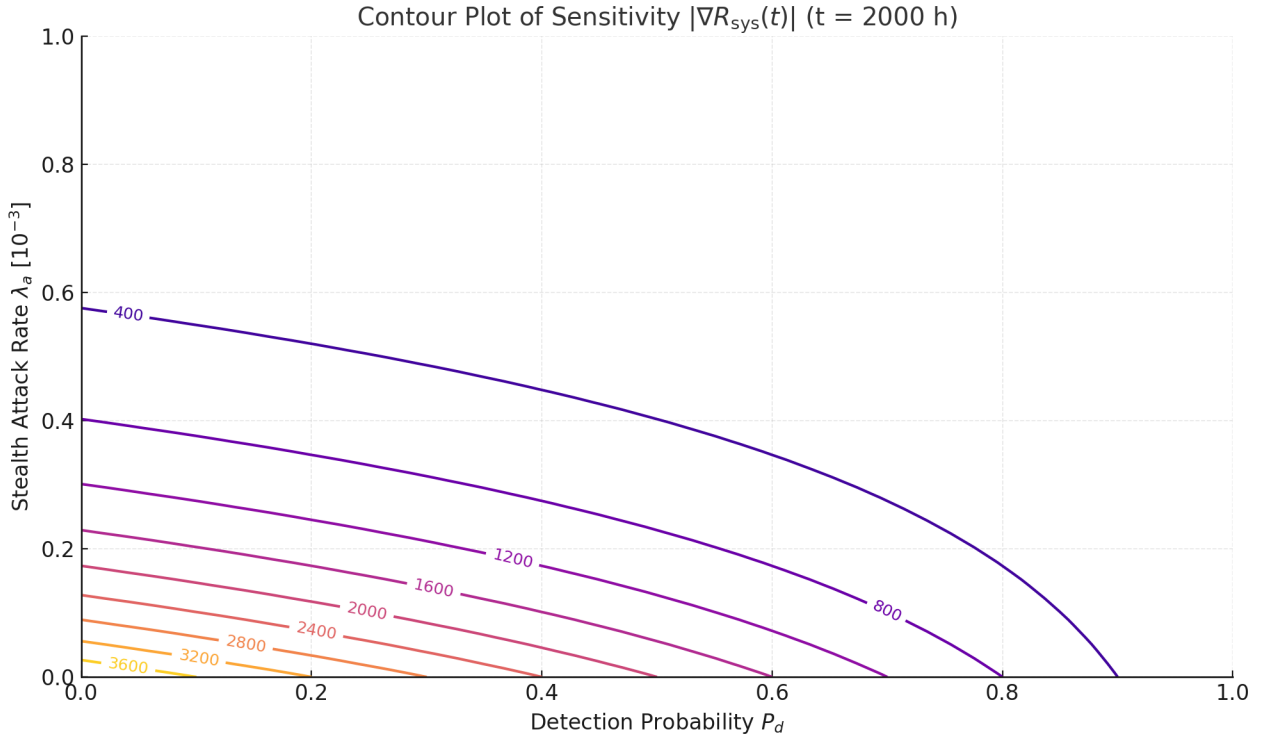


Figure 2: Sensitivity heatmap $\|\nabla R_{\text{sys}}(t = 2000 \text{ h})\|$ as a function of P_d and $m\lambda$.

technical interventions yield the greatest reliability improvements.

To further interpret the trends identified in the sensitivity heatmap, we examine how system reliability behaves as a direct function of the stealth attack rate for fixed detection probabilities. The analytical structure of the model allows us to isolate the cybernetic component of the reliability function through the reformulated security expression:

$$f(P_d, \lambda_a) = P_d + (1 - P_d)e^{-2\lambda_a t} \quad (10)$$

This equation captures the probability that both controllers remain uncompromised by undetected stealth attacks. It reveals how even small increases in λ_a can significantly reduce $R_{\text{sys}}(t)$ when P_d is low, while improvements in P_d yield diminishing returns once λ_a becomes small. Figure 3 illustrates this behavior across different detection probabilities. The curves confirm the earlier sensitivity analysis: the system exhibits a nonlinear transition from robustness to collapse, and optimal configurations require joint tuning of both parameters.

2.3. Curvature-Based Analysis of Reliability Behavior

While first-order sensitivities reveal the most volatile regions of system reliability with respect to stealth attack parameters, a second-order analysis is required to characterize how rapidly this volatility changes. For this purpose, we examine the second derivative of the reliability function with respect to the stealth attack rate λ_a .

The curvature of $R_{\text{sys}}(t)$, derived from Equation (1), is expressed as:

$$\frac{\partial^2 R_{\text{sys}}}{\partial \lambda_a^2} = 4t^2 R_1 R_3 R_s (1 - P_d) e^{-2\lambda_a t} \quad (11)$$

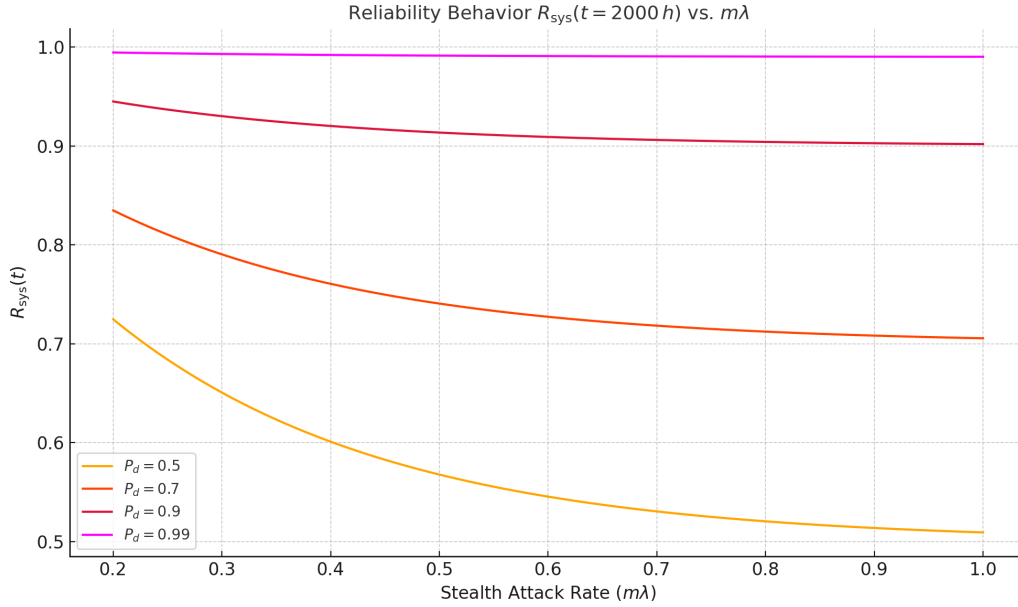


Figure 3: Curves of $R_{\text{sys}}(t = 2000 h)$ for different values of P_d vs. $m\lambda_a$.

This expression is always positive for any $P_d < 1$, indicating that the reliability function is strictly convex in λ_a throughout the entire domain. In practical terms, this implies that while system reliability decreases with increasing attack frequency, the rate of degradation slows down progressively. As the system enters degraded regimes, further increases in λ_a have a diminishing impact on $R_{\text{sys}}(t)$.

This behavior is particularly critical near operational thresholds, where the system transitions from stable to unstable regimes. The steepest gradient - corresponding to maximum sensitivity - occurs in these intermediate zones, where small variations in λ_a or P_d lead to substantial drops in reliability. Conversely, when $\lambda_a \rightarrow 0$ (rare attack scenario) or $P_d \rightarrow 1$ (near-perfect detection), the curvature magnitude decreases due to the exponential damping and the vanishing influence of $(1 - P_d)$.

To visualize this effect, Figure 4 presents the contour curves of $R_{\text{sys}}(t)$ over a continuous range of λ_a and P_d . These level curves confirm the convexity of the function and highlight how reliability varies nonlinearly across the parameter space. The spacing and curvature of the contours reveal that the system exhibits pronounced sensitivity in intermediate regions, reinforcing the results obtained in the sensitivity and gradient analyses.

2.4. Generalized Modeling for N PLCs and M Supervisors

To extend the applicability of the proposed model beyond the specific architecture of three PLCs and one supervisor, we present a generalized formulation capable of representing systems with arbitrary numbers of controllers, supervisory modules, and security mechanisms.

Let the system consist of N virtualized PLCs denoted as $\{PLC_1, PLC_2, \dots, PLC_N\}$, M supervisory agents $\{S_1, S_2, \dots, S_M\}$, and K auxiliary security mechanisms $\{Sg_1, Sg_2, \dots, Sg_K\}$ such as firewalls or intrusion detection modules. Each component may fail independently, either due to physical degradation or stealth attack interference.

The reliability of each PLC is modeled by a Weibull distribution Breneman et al. [2022]:

$$R_i(t) = \exp \left(- \left(\frac{t}{\beta_i} \right)^{\alpha_i} \right) \quad (12)$$

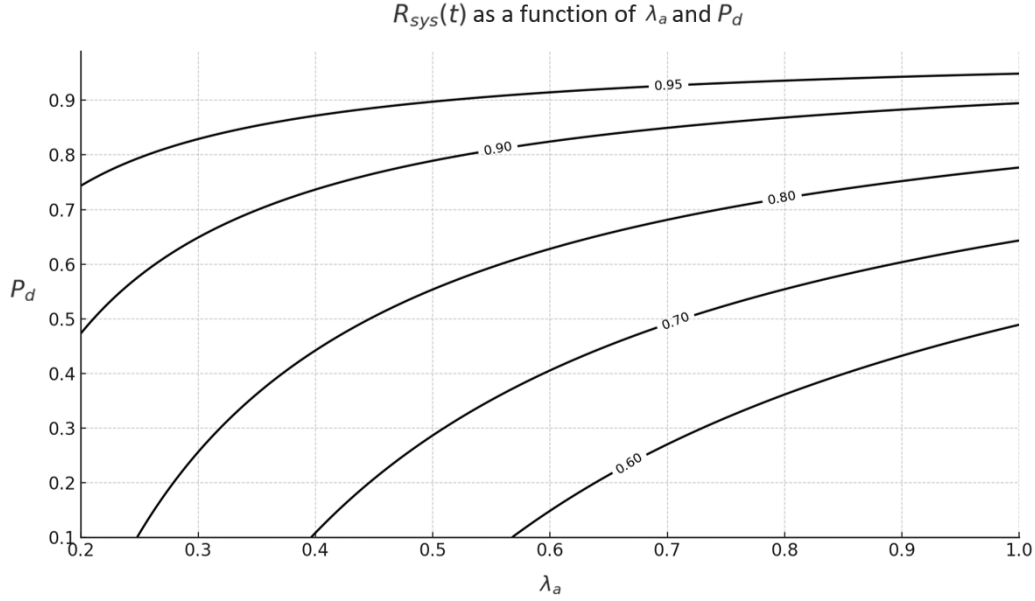


Figure 4: Contour plot of $R_{sys}(t)$ as a function of λ_a and P_d . Curves indicate level sets of constant reliability.

while the supervisory agents and auxiliary security components follow exponential models:

$$R_{S_j}(t) = \exp(-\lambda_{S_j} \cdot t), \quad R_{S_{gk}}(t) = \exp(-\lambda_{S_{gk}} \cdot t) \quad (13)$$

Stealth attacks arrive as a Poisson process with rate λ_a , and detection attempts are modeled as Bernoulli trials with probabilities P_{d_j} for each supervisor and P_{sgk} for each security mechanism.

System failure occurs when a Minimal Cut Sets arises, defined as the simultaneous failure of at least one PLC and the complete failure to detect or mitigate the corresponding attack. The probability of a critical failure set at time t is thus approximated by:

$$P_{MCC}(t) = \sum_{i=1}^N [1 - R_i(t)] \cdot \left(1 - \prod_{j=1}^M P_{d_j} R_{S_j}(t) \right) \cdot \Gamma(t) \quad (14)$$

where

$$\Gamma(t) = \begin{cases} 1, & \text{if } K = 0 \\ \left(1 - \prod_{k=1}^K P_{sgk} R_{S_{gk}}(t) \right), & \text{if } K > 0 \end{cases}$$

This formulation ensures consistency with the original model when no auxiliary security components are present ($K = 0$). In such cases, the security term is omitted entirely, rather than treated as a neutral multiplicative factor, to preserve the original failure semantics and maintain numerical accuracy. This correction avoids underestimating failure probability in simplified configurations.

This generalized expression enables the representation of various architectures, including multiple redundant PLCs, distributed detection logic, and layered security strategies. It preserves

the original model's ability to incorporate logical combinations of physical failure and imperfect detection, and extends it to complex topologies with arbitrary interdependencies.

The general model naturally extends the initial formulation by incorporating security layers and scalable redundancy in supervision and detection. It maintains compatibility with the specific case represented by Equation (1) when configured with $N = 2$, $M = 1$, and $K = 0$, thus preserving the original logic while allowing broader applicability.

3. Conclusions

This study presented an analytical and experimental framework for evaluating the reliability of virtualized control systems, with emphasis on architectures involving multiple PLCs running in containerized environments and the effects of undetected stealth failures. The proposed model integrates classical physical failure mechanisms with cybernetic threats - such as stealth attacks and imperfect detection - into a composite reliability function that is sensitive to operational security parameters.

By employing Minimal Cut Sets logic, the system was modeled through critical combinations of component failures and detection lapses. This enabled a compact yet expressive formulation of overall reliability as a function of individual component reliabilities and security variables, specifically the stealth attack rate λ_a and the detection probability P_d . Monte Carlo simulations validated the non-trivial interactions among these parameters, revealing critical zones of high sensitivity and abrupt functional degradation.

The analytical results - particularly the sensitivity heatmaps, the reliability response curves under varying P_d , and the curvature profile of $R_{\text{sys}}(t)$ - highlighted the system's nonlinear behavior. Reliability tends to decline more sharply in intermediate regions of the parameter space, where detection and attack rates are not yet stabilized. This trend was formally confirmed through first- and second-order derivatives of the reliability function.

From a practical standpoint, the findings show that the reliability of virtualized industrial systems cannot be assessed solely through physical failure rates. Cybersecurity parameters, especially the effectiveness of detecting stealth attacks, play a decisive role in functional robustness. The study provides quantitative design recommendations for configuring redundancy and supervision layers in virtualized control architectures. Specifically, maintaining $P_d > 0.9$ and preemptively mitigating threats before λ_a exceeds critical thresholds are key strategies for enhancing system resilience.

Future work should explore the inclusion of correlated failures, degraded operational states, and larger-scale configurations with multiple supervisors or distributed detection logic. Additionally, the integration of confidence intervals, risk profiles, and assessments under diverse cyberattack types (e.g., DoS, data injection, or variable manipulation) could further improve the applicability and generalization of the proposed methodology.

4. Acknowledgement

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001

References

- Bo, Z., Wang, Q., Zhao, Y., Wang, L., Chen, L., and Wei, F. (2015). A new concept intelligent integrated protection system for distribution network. In *Proceedings of the 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*, p. 1–6, Changsha, China. IEEE.

- Breneman, J. E., Sahay, C., and Lewis, E. E. (2022). *Introduction to Reliability Engineering*. John Wiley & Sons, Hoboken, NJ, 3 edition.
- Cruz, T., Simoes, P., and Monteiro, E. (2016). Virtualizing programmable logic controllers: Towards a convergent approach. *IEEE Embedded Systems Letters*. Early Access.
- Kampa, T., El-Ankah, A., and Grossmann, D. (2023). High availability for virtualized programmable logic controllers with hard real-time requirements on cloud infrastructures. In *Proceedings of the 2023 IEEE International Conference on Industrial Informatics (INDIN)*, p. 1–8. IEEE.
- Klyuev, R., Madaeva, A., and Dzhamalueva, A. (2021). Increasing the reliability of hydro power plants due to the application of microprocessor relay protection devices. In *Proceedings of the 2021 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, p. 1–6. IEEE.
- Li, Y.-p., Chang, J.-y., and Li, X. (2010). Small hydropower station monitoring system communication. In *Proceedings of the 2010 International Conference on Electrical and Control Engineering (iCECE)*, p. 1962–1964. IEEE.
- Radoglou-Grammatikis, P., Siniosoglou, I., Liatifis, T., Kourouniadis, A., Rompolos, K., and Sari-giannidis, P. (2020). Implementation and detection of modbus cyberattacks. In *Proceedings of the IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, p. 1–6. IEEE.
- Rao, S. P., Tiruvalluru, R. S., Balaji, S. R. A., Tomomewo, O. S., and Prakash, R. (2024). Virtual power plants: Security challenges, solutions, and emerging trends-a review. In *Proceedings of the 2024 IEEE Cyber Awareness and Research Symposium (CARS)*, p. 1–8. IEEE.
- Zaev, E., Tuneski, A., Babunski, D., Trajkovski, L., Nospal, A., and Rath, G. (2012). Hydro power plant governor testing using hardware-in-the-loop simulation. In *Proceedings of the Mediter-ranean Conference on Embedded Computing (MECO)*, p. 1–6, Bar, Montenegro. IEEE.