International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

From Component Reliability to Dynamic Predictive Reliability: A Multilayer Framework for Cyber-Physical Systems

Ass. Eng. Iliyan Vasilev, PhD
University of Chemical Technology and Metallurgy, Sofia, Bulgaria

ABSTRACT: The reliability of cyber-physical systems (CPS) cannot be reduced to the failure probability of individual hardware components. Modern industrial, urban, educational and energy CPS combine physical processes, sensors, communication networks, software services, control algorithms, cyber-security mechanisms, human operators and environmental conditions. This paper proposes an integral-predictive view of CPS reliability based on two complementary models: the multilayer integral reliability index of a cyber-physical system (MINKFS) and the dynamic cognitive-predictive reliability model (DKPN). The framework takes different types of signals, converts them into standardized layer indices, combines them using a weighted structure, and updates the current reliability estimate by adding the predicted chance of future failure. The empirical part uses a synthetic industrial CPS dataset of 336 hourly observations and demonstrates how layer statistics, scenario analysis, operational regimes and criticality rankings can support early warning and preventive decision-making. The model transforms diverse inputs to normalized layer indexes, integrates these using a weighted integrative model, and adds the forecast probability of future failure to the present measure of reliability. The empirical part studies a fabricated data set related to industrial CPS which consists of 336 hourly measurements and provides a demonstration of how layer, scenario, regime and criticality information is used for detection and prevention. It was observed that the cyber-resilience layer had the lowest average reliability as well as the highest critical contribution, whereas communications and environment-energy layers were characterized by high volatility. Cyber event scenario resulted in the lowest predictive reliability and highest likelihood of failure. These results confirm the thesis that reliability of a CPS is better analyzed as a time-dependent, interpretable, and scenario-dependent feature instead of being just another component coefficient.

KEYWORDS: cyber-physical systems, cyber-resilienc, reliability, predictive maintenance, MINKFS, DKPN.

INTRODUCTION

Cyber-physical systems have become a foundational infrastructure for Industry 4.0 and 5.0, smart cities, smart buildings, autonomous transport, energy management, healthcare and education. They are not merely collections of machines, controllers and sensors, but socio-technical configurations in which physical processes, digital models, communication networks, control algorithms and human decisions form a unified operational environment. For this reason, reliability cannot be interpreted only as the probability that a hardware component will continue to operate without failure. It is increasingly a systemic property that depends on the quality of data, the stability of communication, the correctness of software, the robustness of control and the ability of the organization to detect, respond to and recover from disturbances (Lee, 2008; Rajkumar et al., 2010; Griffor et al., 2017). The transition from classical technical systems to CPS changes the logic of failure assessment. A conventional technical system usually fails because of physical degradation, random component failure, fatigue or wear. A CPS may also fail because of delayed packets, inconsistent sensor data, corrupted digital models, software version conflicts, cyberattacks, inadequate human intervention or algorithmic decisions that are correct in a narrow computational sense but unsafe in a changing physical context. Therefore, the reliability model must combine probabilistic, structural, data-driven, cyber-risk and human-factor perspectives (Humayed et al., 2017; Ding et al., 2018; Giraldo et al., 2018). The objective of this paper is to formulate a multilayer integral-predictive framework for CPS reliability and to demonstrate its empirical use on a synthetic industrial CPS dataset. The paper is based on the thesis that classical reliability models remain necessary, but they are insufficient as global models for modern CPS. They should be used as local mathematical submodels inside a broader architecture that includes normalized layer indices, criticality weights, cascade-risk correction and predictive failure probability (Rausand & Hoyland, 2004; Birolini, 2017; Zio, 2016).

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Theoretical background: why classical reliability is not enough

Classical reliability theory defines reliability as the probability that a component or system performs its supposed function without failure during a specified time interval under determined operating conditions. This definition remains useful because it provides a rigorous quantitative basis for component design, testing and maintenance planning. Exponential, Weibull, Markov, fault-tree and Bayesian models all contribute valuable tools for modelling failure rates, degradation, state transitions, causal dependencies and uncertainty (Rausand & Hoyland, 2004; Birolini, 2017; Nikolov, 2025).

Limitations arise when using such models as a basis for adaptive and networked systems. The behaviour of a CPS is generally non-stationary since software may be updated, communications conditions may vary, there may be intervention by operators, cyber risks may grow, and environmental and energetic conditions may impact the physical process. Failure occurrences do not necessarily happen independently. Sensor drifts by any reason may distort a controller, network delays might destabilise a physical process, cyber events might mute alarms, and the actions of an operator might compensate or exacerbate technical issues. This type of frameworks with an approach to reliability keeps both mathematical elegance and takes account of dependencies, context, and dynamism (Leveson, 2012; ISO 31000, 2018; ISO/IEC 23894, 2023). System considerations become important. A reliable CPS is not just the sum of reliable components, but a system whereby the physical, cyber, communication, control, and human layers work harmoniously. This issue becomes especially critical for industrial CPS, smart buildings and smart city infrastructures wherein any failures at the local level can propagate through different layers, causing problems with regards to safety, service delivery, and resources management. Thus, the objective of reliability engineering lies in moving away from indicators based on components towards meaningful operational indices (Griffor et al., 2017; Marwedel, 2021; NIST, 2024).

MATERIALS AND METHODS

Proposed multilayer integral-predictive framework

Layered structure of CPS reliability

The proposed MINKFS model represents CPS reliability as a set of normalized layer indices. In the industrial configuration used for empirical verification, the following layers are included: hardware reliability Rh, sensor reliability Rs, communication reliability Rk, software/PLC reliability Rp, control reliability Ru, cyber-resilience Rc, human-operator reliability Rch and environmental/energy reliability Re. Each layer is calculated from one or more raw operational variables and transformed into the interval [0, 1], where higher values indicate a more reliable state.

The integral reliability estimate is based on weighted aggregation:

$$R_M INKFS(t) = \Sigma \alpha_i R_i(t), i \in h, s, k, p, u, c, ch, e$$

The α_i represent the importance of each individual layer functionally. The equation was carefully designed for its clarity: should the global number decline, the engineer would be able to pinpoint the cause and understand its numerical meaning in relation to real-world metrics like vibration, latency, packet loss, PLC scan time, intrusion detection system (IDS) triggers, human error, or power quality. This transparency is essential to engineering because an overall number alone is inadequate for management purposes.

Dynamic cognitive-predictive reliability

The DKPN concept incorporates the existing concept of integral reliability with a dynamic risk function and failure probability prediction. It implies that the system under consideration can possess sufficient integral reliability even though degradation indicators exist already. Hence, the probabilistic layer provides for calculating the failure probability at some horizon h ahead of time:

$$P_{fail}(t + h|t) = 1/\left[1 + exp\left(-z * (t)\right)\right]$$

The final predictive reliability can be expressed as a balance between the corrected current reliability R*(t) and the predicted future risk:

$$R_{DKPN}(t + h) = \gamma R * (t) + (1 - \gamma)\left[1 - P_{fail}(t + h|t)\right]$$

Such a system allows predicting critical failures. Should the probability of failure rise due to abnormalities, degradation, cyberspace incidents, human factors or environmental issues, R_DKPN will be reduced even prior to the apparent critical failure event. Thus, the approach shifts the analysis of reliability to predictive, rather than descriptive, terms.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Empirical verification

Data set and simulation methodology

For empirical test, we consider a synthetic data set composed of 336 hourly observations made during 1 January 2026 to 14 January 2026. The simulated object is the industrial production line where its reliability will depend on the integrated operation of hardware components, sensors, communication system, software, PLC/edge solutions, control systems, resilience to cybersecurity risks, and human and environmental variables. The data set under consideration is synthetic and used only for methodological purposes.

The raw variables include vibration, bearing temperature, electric motor current, hydraulic pressure deviation, sensor noise and drift, missing readings, communication latency, packet loss, jitter, OPC interruptions, PLC scan time, log errors, service restarts, CPU load, control error, robotic cycle time, actuator lag, alarms, vulnerabilities, operator interventions and power quality. These variables are grouped into the eight reliability layers of the MINKFS model. The simulation includes normal operation, communication degradation, cyber event, environmental-energy stress, planned maintenance and recovery.

Table 1. Layer weights used in the industrial MINKFS model

Layer	Meaning	α_i
Rh	Hardware layer	0.140
Rs	Sensor layer	0.120
Rk	Communication layer	0.160
Rp	Software/PLC layer	0.140
Ru	Control layer	0.160
Rc	Cyber-resilience layer	0.140
Rch	Human-operator layer	0.080
Re	Environmental/energy layer	0.060

Source: *adapted from the empirical simulation chapter.*

RESULTS

Empirical layer statistics

It is worth noting that the average corrected integral reliability R* = 0.923 is higher than the average value of predictive reliability R_DKPN = 0.891. Such discrepancy can be explained by the fact that DKPN takes into account the intervals where the value of risk factors is growing in spite of the presence of an adequate level of integral reliability. Average value of predicted probability of failure equals 0.147 and reaches its maximum at 0.954. This means that the risk is unevenly distributed in time and is related to certain scenarios of equipment degradation. The lowest values of average layer reliability R* belong to the cyberr-resilience layer Rc. Layers associated with communication Rk and energy Re are highly variable in time. This finding is of great importance since one can expect operational danger from the layer characterized by high value but high variations in time and low scenario reliability.

Table 2. Descriptive statistics of CPS layer reliability indices

Layer	Component	Mean	Min.	Max.	Std.	P05	P50	P95
Rh	Hardware	0.994	0.902	1.000	0.018	0.946	1.000	1.000
Rs	Sensor	0.986	0.900	1.000	0.016	0.959	0.990	1.000
Rk	Communication	0.948	0.471	1.000	0.133	0.544	0.994	1.000
Rp	Software/PLC	0.985	0.751	1.000	0.043	0.900	1.000	1.000
Ru	Control	0.990	0.881	1.000	0.023	0.933	1.000	1.000

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Layer	Component	Mean	Min.	Max.	Std.	P05	P50	P95
Rc	Cyber-resilience	0.854	0.389	0.988	0.099	0.537	0.867	0.951
Rch	Human-operator	0.946	0.724	1.000	0.038	0.872	0.953	0.989
Re	Environmental/energy	0.947	0.418	1.000	0.144	0.519	1.000	1.000

Source: *adapted from the empirical simulation chapter.*

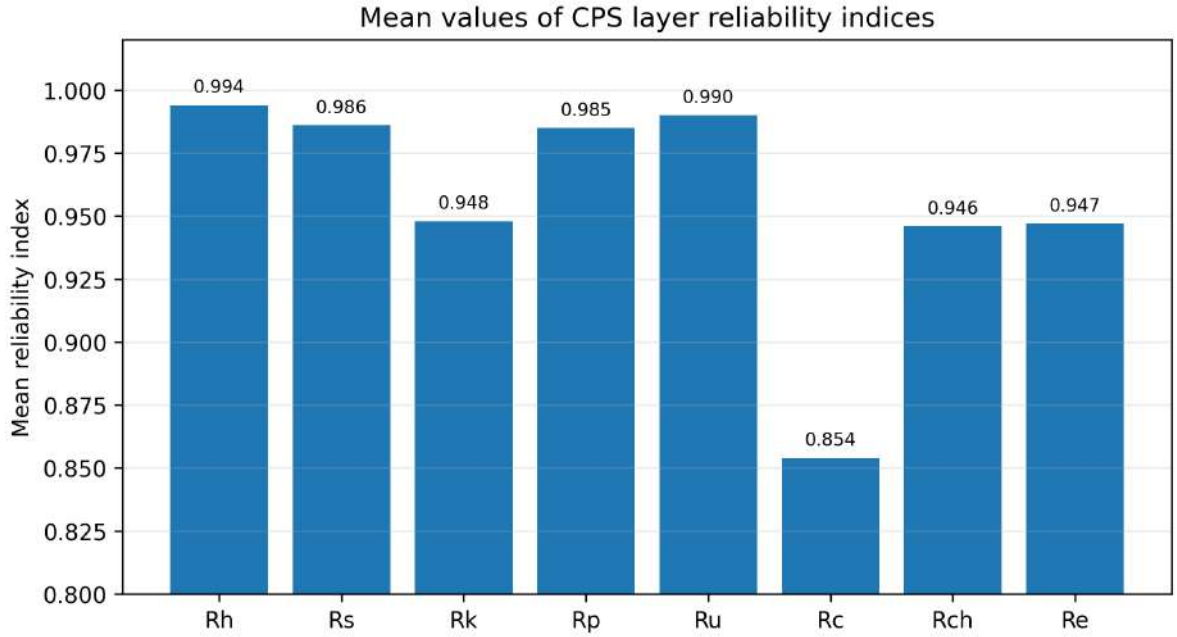

Figure 1. Mean values of the CPS layer reliability indices.

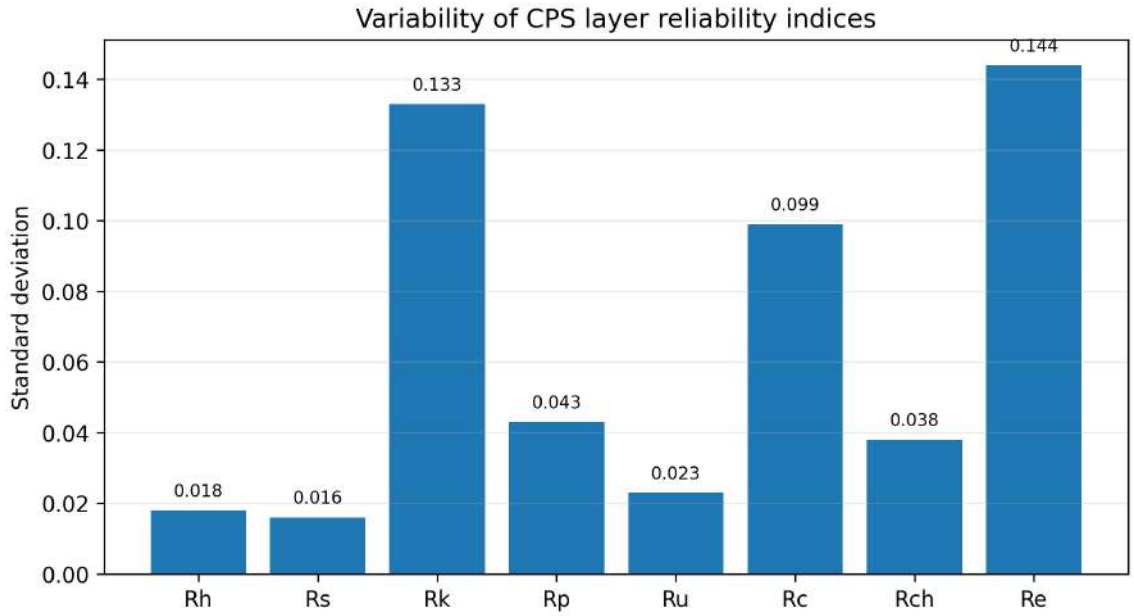

Figure 2. Variability of the CPS layer reliability indices.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Figures 1 and 2 reveal two complementary patterns. Hardware, sensor, software/PLC and control layers remain close to the upper reliability boundary in the simulated period. The cyber-resilience layer, however, has a lower mean value, while the communication and environmental-energy layers show the highest standard deviations. This confirms the methodological need to evaluate both mean state and variability. Average reliability alone may hide short but critical intervals of degradation.

Scenario-based reliability and predictive risk

Scenario analysis is crucial because worldwide data cannot reflect the degradation process. Scenarios of normalcy and recovery continue to operate within the high reliability and low risk regime. The scenario of cyber event, on the other hand, stands out for its lowest average value of R_DKPN and highest value of P_fail. Degradation in communication and energy degradation from the environment constitute intermediate risks (Table 3.).

Table 3. Scenario comparison of reliability and predictive risk

Scenario	Obs.	Mean R*	Mean R_DKPN	Mean P_fail	Min. R_DKPN	Max. P_fail
Recovery	30	0.985	0.980	0.027	0.964	0.043
Cyber event	19	0.729	0.581	0.599	0.456	0.954
Communication degradation	36	0.786	0.748	0.299	0.580	0.747
Normal operation	199	0.974	0.962	0.052	0.938	0.090
Planned maintenance	16	0.953	0.934	0.089	0.772	0.386
Environmental/energy stress	36	0.815	0.715	0.408	0.614	0.704

Source: *adapted from the empirical simulation chapter.*

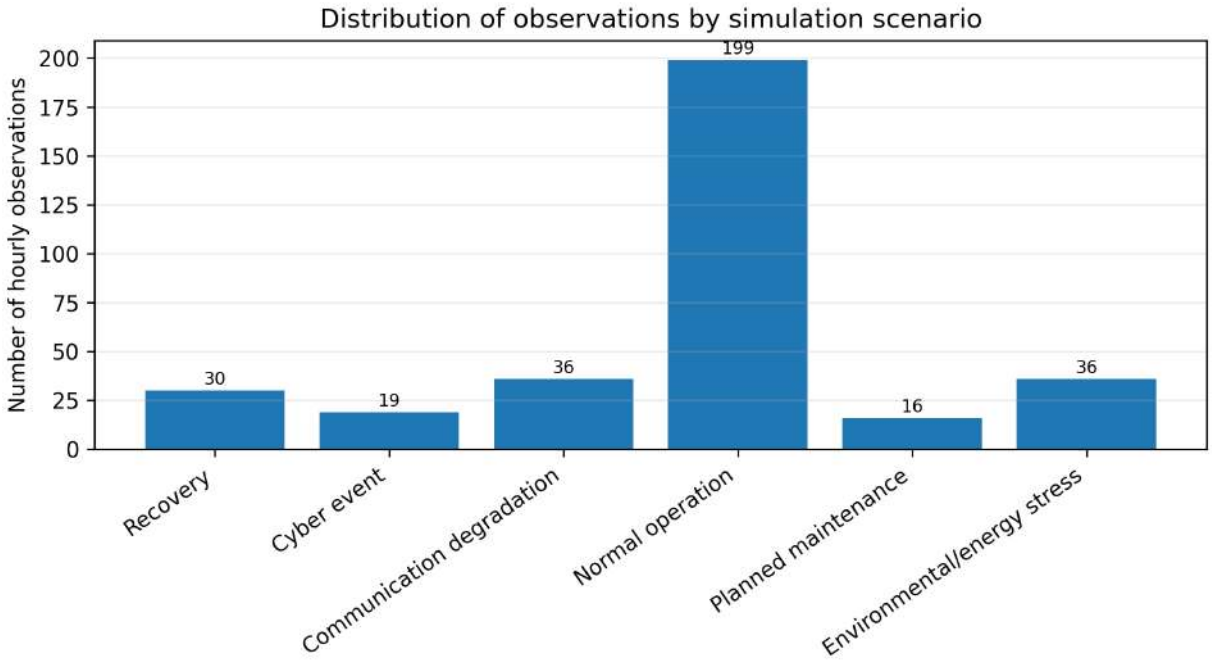

Figure 3. Distribution of observations by simulation scenario.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

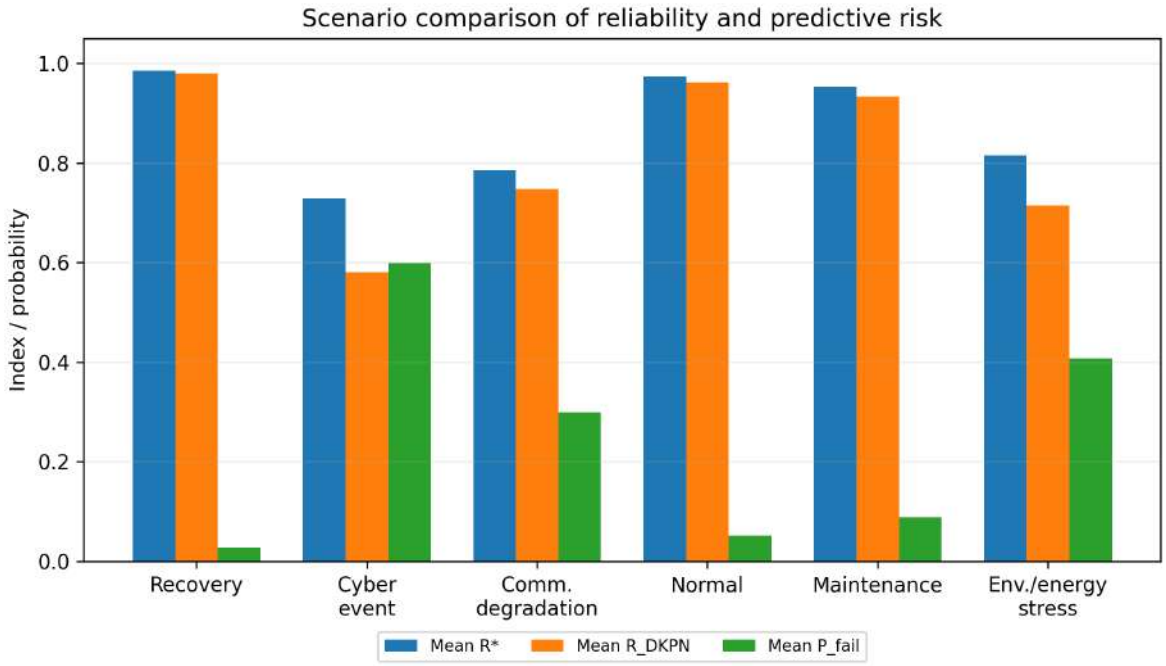

Figure 4. Scenario comparison of R*, R_DKPN and P_fail.

The cyber-event scenario has mean R* = 0.729, mean R_DKPN = 0.581 and mean P_fail = 0.599. It is therefore the most risky scenario in the simulated dataset. The main degradation is concentrated in Rc: IDS alerts, unsuccessful access attempts, vulnerability exposure and delayed patching reduce the cyber-resilience layer and increase the latent risk function. Importantly, cyber risk may increase without immediate communication failure; monitoring latency and packet loss alone is not sufficient for CPS reliability assessment.

In the communication degradation scenario, the reliability reduction has a different causal structure. The lower values are driven primarily by Rk through delay, jitter, packet loss and OPC interruptions. Such degradation should not be treated as an isolated IT problem because delayed or incomplete data can directly affect synchronization between sensors, PLCs, edge devices, SCADA components and robotic cells. The environmental-energy stress scenario has a third mechanism: it does not represent a cyberattack or a network failure, but it can generate systemic risk through temperature, humidity, dust, power quality and their cascade effects on hardware and control.

Operational regimes and decision interpretation

The DKPN model can therefore be put into practical regimes. It is significant to note that apart from providing descriptive information, a reliability model needs to provide useful basis for making decisions. The simulation dataset consists of 243 hours of normal regime operation, 56 hours of preventative maintenance regime operation, 32 hours of critical regime operation and 5 hours of surveillance regime operation.. The distribution is presented in Table 4 and Figure 5.

Table 4. Operational regimes derived from the DKPN interpretation

Regime	Hours	Share
Normal operation	243	0.723
Critical mode	32	0.095
Monitoring	5	0.015
Preventive intervention	56	0.167

Source: *adapted from the empirical simulation chapter.*

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

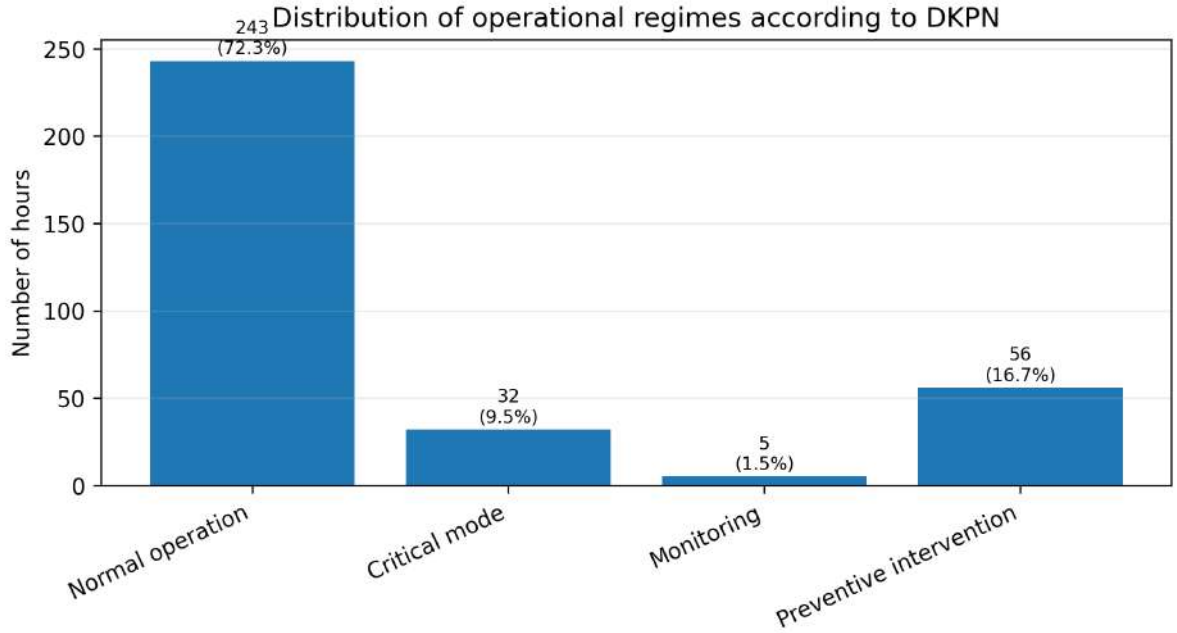

Figure 5. Distribution of operational regimes according to DKPN.

The regime distribution shows that most hours remain in normal operation, but the number of preventive and critical intervals is non-negligible. This supports the practical value of the model: it can trigger different levels of response, such as routine monitoring, intensified observation, preventive maintenance, network diagnostics, cyber-response, or temporary transition to a safe operating mode.

Criticality contribution of CPS layers

A key advantage of the multilayer framework is that it ranks not only the global reliability state but also the contribution of each layer to systemic risk. The critical contribution K_i combines the importance of a layer, its unreliability and its degradation behaviour. Table 5 and Figure 6 show that cyber-resilience is ranked first by mean critical contribution, followed by communication reliability. This confirms that the digital and networked aspects of CPS are not external additions to reliability engineering; they are internal reliability determinants.

Table 5. Critical contribution of layers to CPS risk

Layer	Component	α_i	Mean R_i	Mean K_i	Max. K_i	Rank
Rc	Cyber-resilience	0.140	0.854	0.021	0.090	1
Rk	Communication	0.160	0.948	0.008	0.088	2
Rch	Human-operator	0.080	0.946	0.004	0.026	3
Re	Environmental/energy	0.060	0.947	0.003	0.036	4
Rp	Software/PLC	0.140	0.985	0.002	0.038	5
Rs	Sensor	0.120	0.986	0.002	0.013	6
Ru	Control	0.160	0.990	0.002	0.020	7
Rh	Hardware	0.140	0.994	0.001	0.014	8

Source: *adapted from the empirical simulation chapter.*

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

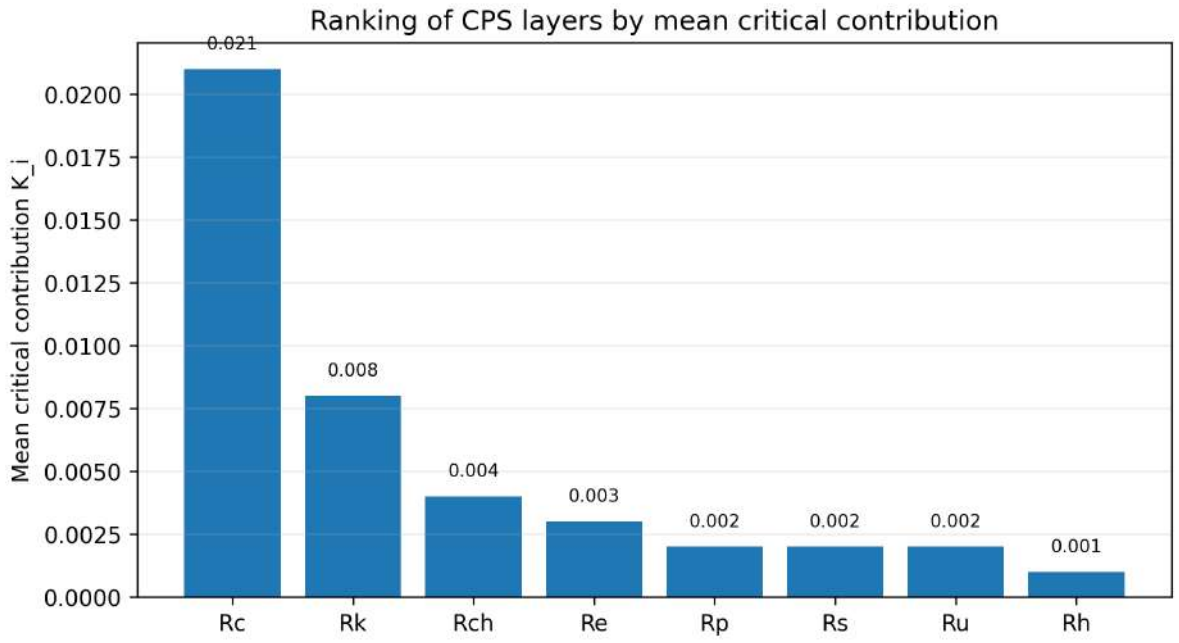

Figure 6. Ranking of CPS layers by mean critical contribution.

The ranking has a direct management interpretation. Rc requires systematic cyber-hygiene, vulnerability management, access monitoring, patch control and incident response. Rk requires network diagnostics, redundancy, latency monitoring and protocol stability. Rch requires operator training and better human-machine interfaces. Re requires environmental and power-quality monitoring. The ranking therefore turns the reliability model into a prioritization tool for operational risk management.

DISCUSSION

The empirical results support three main scientific arguments. First, CPS reliability is an emergent characteristic of the layered interactions and cannot be derived simply by adding the reliability of the components involved. The simulation reveals that a CPS may possess extremely reliable hardware and sensors but still become risky due to cyber exposure or degradation of communications/ambient conditions. Second, reliability needs to be considered from a dynamic perspective. While R* offers a real-time correct integral value, R_DKPN is better suited for an early warning since it measures risk accumulation. Finally, reliability analysis should be interpretable for engineers or managers to understand from which layer risk comes. the results also reveal why cyber-resilience of a CPS should be seen as another reliability layer, not an additional security function. Manipulations with the digital environment lead to observable physical consequences through manipulated signals, command injections, failure to send alarms, late software patches, etc. This finding fits well with general developments in the field of CPS science, according to which security, safety and reliability are viewed as interrelated concepts (Humayed et al., 2017; Ding et al., 2018; Giraldo et al., 2018; NIST, 2024).At the same time, the empirical dataset is synthetic. The numerical results should therefore be interpreted as a methodological validation of the MINKFS and DKPN apparatus rather than as evidence about a specific enterprise. Future research should test the model on real industrial data, compare alternative weighting strategies, calibrate the logistic risk function, validate thresholds with expert judgement and investigate the portability of the approach across smart campuses, smart buildings, transport platforms, energy microgrids and smart-city infrastructures.

CONCLUSION

The purpose of the present work was to design a multi-layered integrative-predictive approach to CPS reliability using MINKFS and DKPN. The primary conclusion drawn from this study was that the reliability of cyber-physical systems is inherently a time-dependent, hierarchical and contextual phenomenon. Traditional approaches to modeling reliability need to be expanded through normalized layer indexing, cascade-risk adjustment, anomaly detection, degradation patterns and failure probability prediction.. The

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 09 September 2026
DOI: 10.47191/ijcsrr/V9-i9-11, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

long part on empirical studies demonstrated how the proposed framework could be applied with the help of data tables, parameters of layers, scenarios for comparison, operational zones, and critical layers. In particular, it became clear that the cyber resilience is the least stable and most important layer in terms of an industrial CPS. Furthermore, the communication reliability is among those factors that generate high variability risk. What is more, the framework made it possible to determine that environmental energy stress becomes an important contextual factor that impacts degradation.

REFERENCES

1. Alur, R. (2015). Principles of cyber-physical systems. MIT Press. https://doi.org/10.5555/2774947
2. Birolini, A. (2017). Reliability engineering: Theory and practice (8th ed.). Springer. https://doi.org/10.1007/978-3-662-54209-5
3. Ding, D., Han, Q.-L., Xiang, Y., Ge, X., & Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 275, 1674–1683. https://doi.org/10.1016/j.neucom.2017.10.009
4. Giraldo, J., Urbina, D. I., Cárdenas, A. A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N. O., Sandberg, H., & Candell, R. (2018). A survey of physics-based attack detection in cyber-physical systems. ACM Computing Surveys, 51(4), Article 76. https://doi.org/10.1145/3203245
5. Griffor, E. R., Greer, C., Wollman, D. A., & Burns, M. J. (2017). Framework for cyber-physical systems: Volume 1, overview (NIST Special Publication 1500-201). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1500-201
6. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172
7. International Organization for Standardization. (2018). Risk management—Guidelines (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html
8. International Organization for Standardization, & International Electrotechnical Commission. (2023). Information technology—Artificial intelligence—Guidance on risk management (ISO/IEC Standard No. 23894:2023). https://www.iso.org/standard/77304.html
9. Lee, E. A. (2008). Cyber physical systems: Design challenges. In 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC) (pp. 363–369). IEEE. https://doi.org/10.1109/ISORC.2008.25
10. Leveson, N. G. (2012). Engineering a safer world: Systems thinking applied to safety. MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001
11. Marwedel, P. (2021). Embedded system design: Embedded systems foundations of cyber-physical systems, and the Internet of Things (4th ed.). Springer. https://doi.org/10.1007/978-3-030-60910-8
12. Nikolov, N. (2025). Intelligent urban systems and Industry 5.0: Creating adaptive ecosystems for sustainable energy and resource management. *International Journal of Current Science Research and Review,* *8*(1), 103–115. https://doi.org/10.47191/ijcsrr/V8-i1-11
13. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
14. Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. In Proceedings of the 47th Design Automation Conference (pp. 731–736). Association for Computing Machinery. https://doi.org/10.1145/1837274.1837461
15. Rausand, M., & Høyland, A. (2004). System reliability theory: Models, statistical methods, and applications (2nd ed.). Wiley. https://doi.org/10.1002/9780470316900
16. Zio, E. (2016). Some challenges and opportunities in reliability engineering. IEEE Transactions on Reliability, 65(4), 1769–1782. https://doi.org/10.1109/TR.2016.2591504

Cite this Article: Vasilev, I. (2026). From Component Reliability to Dynamic Predictive Reliability: A Multilayer Framework for Cyber-Physical Systems. International Journal of Current Science Research and Review, 9(9), pp. 4958-4966. DOI: https://doi.org/10.47191/ijcsrr/V9-i9-11