International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Mathematical Reliability Modeling of Cyber-Physical Systems: From Classical Failure Theory to Multilayer Predictive Indices

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

ABSTRACT: Cyber-physical systems (CPS) require a reliability theory that is broader than the classical probability of failure-free operation of a technical component. In CPSs, failure can be caused by deterioration, sensor error, delay in communication, software malfunction, control problems, cyber vulnerabilities, human interaction, and stress due to environment. This paper offers a mathematical approach to CPS reliability that brings together classical theories of reliability with multilayer, state-dependent, logical, Bayesian, and predictive approaches. The result is an integrated model in which the exponential and Weibull life distributions, structural reliability approaches, Markov models of state transitions, fault trees, Bayesian inference, normalization, and multilayer integral approach to reliability are combined into one coherent methodology. The paper presents some extended concepts of reliability, such as availability, maintainability, resilience, recoverability, data integrity, and CPS safety. The proposed approach makes possible theoretical work and practical decisions, since it connects layer-by-layer indicators with layer indices, layer indices with system reliability, and system reliability with failure probability prediction.

KEYWORDS: cyber-physical systems; reliability; Weibull model; Markov model; fault tree analysis; Bayesian updating; availability; predictive maintenance; MINKFS; DKPN.

INTRODUCTION

The reliability of a cyber-physical system cannot be reduced to the operational status of a single machine, controller, or sensor. CPS combines physical processes, embedded computation, communication networks, control algorithms, data flows, human decisions, and organizational procedures. As a result, a failure can be produced by mechanical wear, sensor noise, delayed communication, unstable software, a cyber incident, or an inappropriate operator action. The idea on which this article is based explicitly treats CPS reliability as a multidimensional and time-dependent characteristic rather than as a purely hardware property (Lee, 2008; Rajkumar et al., 2010; Griffor et al., 2017; Marwedel, 2021).

The purpose of this second article is different from the empirical article. Instead of focusing mainly on the simulation dataset, it develops the mathematical side of the research problem. It answers the following question: how can the classical mathematical theory of reliability be extended so that it remains useful for intelligent, connected, adaptive, and cyber-exposed systems? The answer is to preserve the rigor of classical models but to embed them into a multilayer predictive framework. The proposed method is grounded on four assumptions. Firstly, reliability of a CPS depends on time and on the conditions in which it operates. As a second rule, CPS's condition is multistage, with critical and recovery states lying between normal functioning and failure. Thirdly, reliability metrics should be normalized prior to being combined within different layers. Fourthly, the obtained reliability index should imply action on part of the maintainer, including maintenance, reconfiguration, patching, isolation, training, or fallback mode.

Reliability Concepts for CPS

Reliability in general terms can be defined as a probability of successful functioning of a certain system at a time interval [0,t]. In the case of CPS reliability, however, this statement needs further elaboration, and the system is expected to operate properly in terms of functionality, data quality, communications, cyber security, stability, and recovery (Rausand & Høyland, 2004; Birolini, 2017; Zio, 2016).

$$F(t) = P(T \leq t), R(t) = P(T > t) = 1 - F(t)$$
$$f(t) = dF(t)/dt, \lambda(t) = f(t)/R(t)$$
$$R(t) = exp\left[-\int_0^t \lambda(u)du\right]$$

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Here T is the random time to failure, F(t) is the cumulative distribution function, f(t) is the density of failure time, R(t) is the reliability function, and λ(t) is the hazard rate. The hazard rate is particularly important because it distinguishes early failures, random failures, and aging-related degradation.

Table 1. Core reliability and dependability indicators for CPS.

Indicator	Mathematical form	Meaning in CPS
Reliability	$R(t) = P(T > t)$	Probability of failure-free operation during mission time t.
Failure probability	$F(t) = 1 - R(t)$	Probability that failure occurs by time t.
Hazard rate	$\lambda(t) = f(t)/R(t)$	Conditional instantaneous failure tendency.
MTTF	$MTTF = \int_0^\infty R(t)dt$	Expected time to failure for non-repairable elements.
MTBF	Mean operating time between failures	Used for repairable systems and service cycles.
MTTR	Mean time to repair/recover	Includes physical repair, restart, patching, recalibration, or safe-mode recovery.
Availability	$A = MTBF/(MTBF + MTTR)$	Probability that the system is operational at an arbitrary time.
Maintainability	$M(t) = P(repairtime \leq t)$	Probability that restoration is completed within a specified time.
Resilience	Function of degradation, absorption, adaptation, and recovery	Ability to preserve or restore function after disturbance.

Further details on reliability need to be taken into account as CPS are socio-technical systems. Availability can sometimes be easier to achieve as opposed to reliability as the service could be interrupted for a short time and restored without human intervention. Maintainability refers to the ease of restoration. Resilience pertains to the capability to withstand the shock, adapt, and recover. Safety and security of the cyber-physical aspect should also be considered since a problem with the cyber component can result in a physical one, and vice versa (Humayed et al., 2017; Leveson, 2012; NIST, 2024). Exemplary pattern is given in ***Figure 1.***

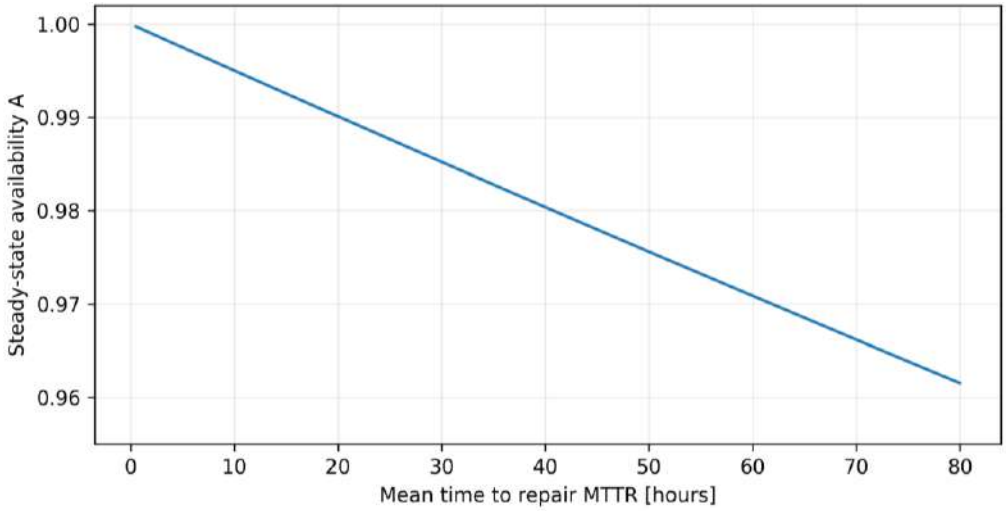

Figure 1. Availability sensitivity for MTBF = 2000h for a repairable CPS component.

Classical Lifetime Models

The Exponential Model is the most basic lifetime model as it uses constant hazard rate and thus, is appropriate for random failure during a certain stable operation period. It is also mathematically simple and hence, can be considered as the first approach where there is lack of historical data.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

$$\lambda(t) = \lambda = const, \qquad R(t) = exp(-\lambda t), \qquad F(t) = 1 - exp(-\lambda t), \qquad MTTF = 1/\lambda$$

For λ = 0.0005 failures per hour, MTTF will be 2000 hours and R100 = exp -0.05 ~0.951. It is applicable to communication modules and electronic components during stable periods, but not enough for those which undergo aging, drifting, patching, attacks, or environmental stresses.

The Weibull distribution can be seen as an extension to the exponential distribution, whereby the risk function varies with time. The model makes use of the two parameters namely, η the scale parameter and β the shape parameter. Depending on the value of β, we get three regimes of failure.

$$R(t) = exp\left[-(t/\eta)^{\beta}\right], F(t) = 1 - exp\left[-(t/\eta)^{\beta}\right]$$
$$\lambda(t) = (\beta/\eta)(t/\eta)^{(\beta-1)}$$
$$t_crit = \eta[-ln(R_min)]^{(1/\beta)}$$

The critical time t_crit gives the moment at which reliability reaches the minimum admissible value R_min. This formula is useful for planning preventive maintenance before the system enters a high-risk degradation zone. Summary in ***Figure 2***. and ***Figure 3***. as well ***Table 2***.

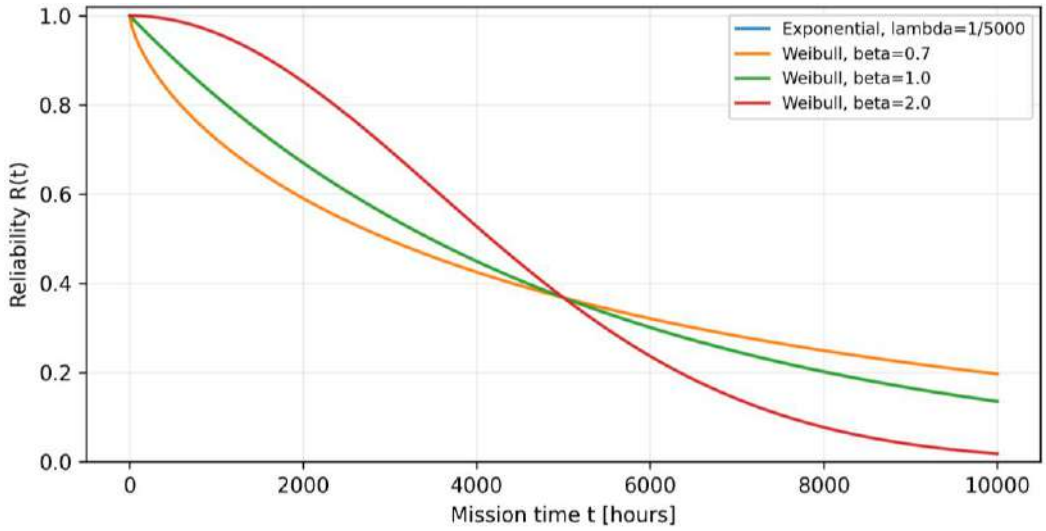

Figure 2. Reliability curves under exponential and Weibull assumptions.

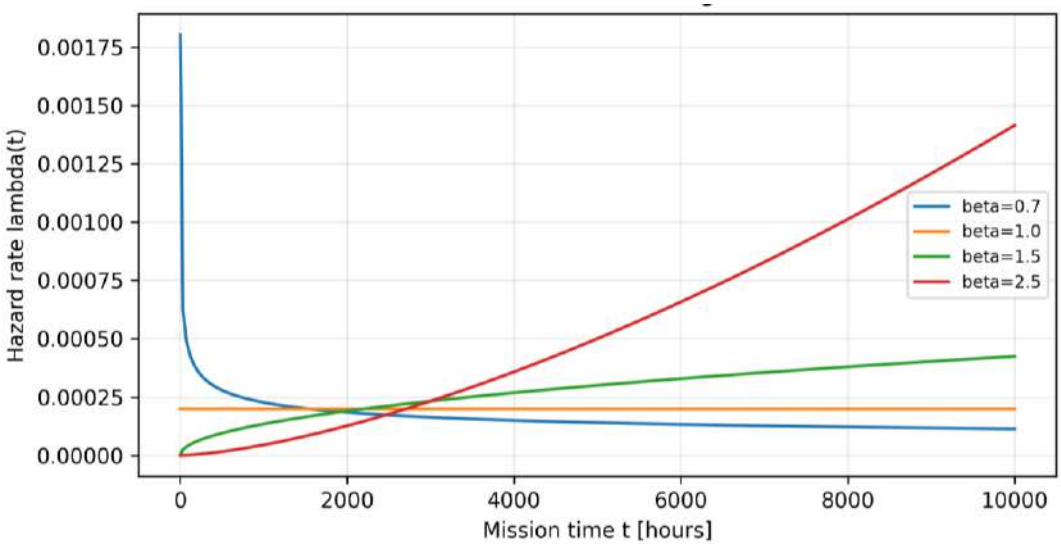

Figure 3. Weibull hazard-rate regimes and their reliability interpretation.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Table 2. Lifetime models and CPS interpretation.

Model	Reliability function	Hazard behavior	Typical CPS use
Exponential	$R(t) = e^{(-\lambda t)}$	Constant	Random failures; first approximation for stable electronic components.
Weibull, β<1	$R(t) = e^{[-(t/\eta)^{\beta}]}$	Decreasing	Early defects, installation/configuration problems, burn-in period.
Weibull, β=1	Equivalent to exponential	Constant	Stable useful-life period.
Weibull, β>1	$R(t) = e^{[-(t/\eta)^{\beta}]}$	Increasing	Aging, wear, sensor drift, thermal fatigue, actuator degradation.
Lognormal	T follows lognormal law	Non-monotonic possible	Degradation driven by multiplicative effects.

Structural Reliability: Series, Parallel and k-out-of-n Architectures

System reliability model defines how the failures of the components can lead to the system's failure. The series system represents the most stringent system, where failure of any one critical component leads to the failure of the system. On the other hand, parallel systems represent tolerant systems in which all the redundant components have to fail before the system fails (***Table 3.***, ***Figure 4.***)

Series: $R_S(t) = \prod_{i=1}^{n} R_i(t)$

Parallel: $RP(t) = 1 - \prod_{i=1}^{n}[1 - R_i(t)]$

k-out-of-n: $\boldsymbol{R_{k|n}(t) = \sum_{j=k}^{n} C(n,j) R(t)^j [1 - R(t)]^{(n-j)}}$

Table 3. Structural reliability models for CPS architecture.

Structure	Operating condition	Example	Comment
Series	All components must work	Critical PLC, power supply chain, unique controller path	Often pessimistic but realistic for non-redundant functions.
Parallel	At least one component must work	Redundant networks, backup controllers, duplicated power supply	Improves availability but creates dependency and voting issues.
k-out-of-n	At least k of n components must work	Sensor networks, replicated measurement nodes	Useful when not all sensors are required for a reliable estimate.
Hybrid	Combination of series, parallel and voting blocks	Smart factory cell, building automation system, energy microgrid	More realistic for complex CPS architectures.

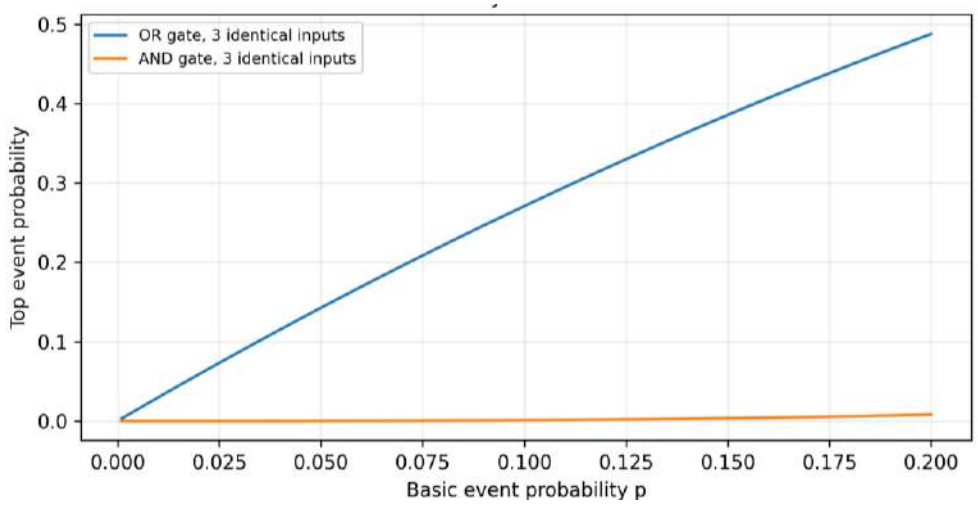

Figure 4. Sensitivity of top-event probability in OR and AND fault-tree structures.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Markov State Models for Degraded and Recoverable CPS

Binary classification of working and failed systems does not apply to CPS because the system passes through phases like normal functioning, degraded functioning, critical degradation, failure, and recovery. Transitions between different phases can be modeled using continuous-time Markov chains via a generator matrix Q. Let pi(t) be the probability vector of the states..

$$d\pi(t)/dt = \pi(t)Q, \pi(0) = \pi_0$$
$$A(t) = \sum_{s\in U}\pi_s(t),$$

U = set of operational states

For a four-state CPS model, S0 is normal operation, S1 is degraded operation, S2 is critical degradation, and S3 is failure. The transition intensities λ01, λ12, and λ23 describe degradation, while mu10, mu21, and mu32 describe recovery. These intensities can be constant or data-dependent.

$$\lambda_{01}(t) = \lambda_{01}^{0} + a1Lat(t) + a2Loss(t) + a3Cyber(t) + a4Load(t)$$

This formula links Markov modeling with actual CPS monitoring (***Figure 5***.), where latency, packet loss, cybersecurity metrics, and load can influence transitions' intensity from the good to bad state. Therefore, the Markov modeling itself is no longer static but dynamic (Trivedi, 2002; Zio, 2016).

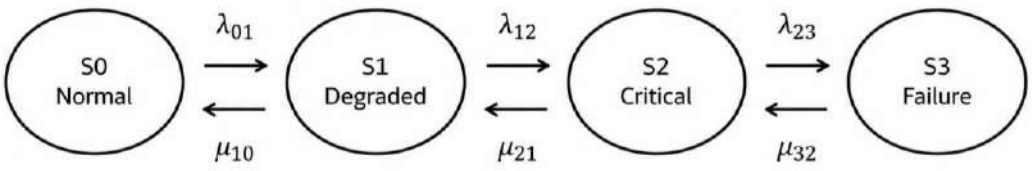

Figure 5. Four-state Markov model for CPS reliability and recovery.

Logical and Bayesian Reliability Models

Fault tree analysis describes the logical combination of basic events that lead to an undesirable top event. It is useful when the analyst must identify how physical faults, communication losses, software errors, cyber events, and human actions combine. The two basic gates are OR and AND.

OR gate: $P(T) = 1 - \prod_{i=1}^{n}[1 - P(E_i)]$

AND gate: $P(T) = \prod_{i=1}^{n}P(E_i)$

The OR structure is one where all events accumulate risks, meaning that a single basic event can cause the top event to occur. In the AND structure, all basic events must happen simultaneously in order for the top event to take place. Both structures are found in CPS failures. For instance, loss of HVAC control might be caused by failure of the controller OR a breach in communication OR intentional manipulation (Kabir, 2017; Ruijters & Stoelinga, 2015).

Bayesian networks add probabilistic causality and updating. They are especially appropriate when the failure is not directly observed but can be inferred from evidence: missing sensor values, increased latency, abnormal commands, CPU load, IDS alerts, or operator overrides.

$$P(X_1, X_2, \ldots, X_n) = \prod_i P\left(X_i | Pa(X_i)\right)$$
$$P(F|E) = P(E|F)P(F)/P(E)$$

Naive Bayes: $P(F|E_1, \ldots, E_m) \propto P(F)\prod_j P(E_j|F)$

Bayesian updating forms an appropriate connection between Bayesian analysis and predictability reliability. Prior information about failure causes can be updated as new data comes up. This aspect is crucial for CPS since the risk situation is affected whenever software versions, cybersecurity, environment conditions, or operational behavior change (Weber et al., 2012).

From Diverse Indicators to Multivariate Reliability Indices

Metrics for CPS include various values such as vibrations expressed in mm/s, temperature of bearings expressed in degrees, packet loss rates expressed in percentages, jitter expressed in milliseconds, cyber security risk ratings, override rates, and power sags. It is clear that the heterogeneity indicates the need to convert these metrics into dimensionless local reliability indexes between [0,1].

Positive normalization: $r_{ij}(t) = [x_{ij}(t) - x_m in]/[x_m ax - x_m in]$

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Negative normalization: $r_{ij}(t) = [x_max - x_{ij}(t)]/[x_max - x_min]$
Deviation-based reliability: $r_{ij}(t) = exp(-|x_{ij}(t) - x*_{ij}(t)|/\tau_{ij})$
Layerindex: $R_i(t) = \sum_j \beta_{ij} r_{ij}(t), \sum_j \beta_{ij} = 1$
In case a larger number indicates a good status, positive normalization applies. For negative normalization, it should be employed when the indicator value is high because of the occurrence of poor state, like latency, packet loss, errors, intrusion detection system (IDS) warnings, vulnerabilities, or operator deviation. Deviation-based reliability would be appropriate when there is a normal profile of x*.

Table 4. CPS layers and representative indicators.

Layer	Name	Typical indicators	Reliability meaning
R_h	Hardware	vibration, temperature, current, pressure deviation	wear, fatigue, overheating, mechanical degradation
R_s	Sensor	noise, drift, missing data, calibration state	wrong or incomplete perception of the physical process
R_k	Communication	latency, jitter, packet loss, OPC interruptions	delayed or inconsistent data/control exchange
R_p	Software/PLC	scan time, log errors, service restarts, CPU load	software instability and control-platform faults
R_u	Control	control error, actuator lag, robot cycle deviation	unstable or delayed control action
R_c	Cyber-resilience	IDS alerts, failed logins, vulnerability score, patch age	security-driven reliability degradation
R_{ch}	Human-operator	manual overrides, response time, procedural deviations	human reliability and operational discipline
R_e	Environmental/energy	temperature, humidity, dust, voltage sags	external stress and power-quality degradation

Mathematical Formulation of the Multilayer Integral CPS Reliability Index
Let L={h,s,k,p,u,c,ch,e} be the set of layers and α_i be the functional weight of layer i. A basic additive multilayer reliability index can be written as:

$$R_A(t) = \sum_{i \in L} \alpha_i R_i(t), \sum_i \alpha_i = 1, \alpha_i \geq 0$$

Additive model interpretation is easy and straightforward, though it might compensate overly much, where one layer with low strength value could get lost in the midst of highly valued layers. Multiplication/Geometric model would "punish" lower-strength layers severely.:

$$R_G(t) = \prod_{i \in L} R_i(t)^{\alpha_i}$$

Hybrid Risk Index is formulated for combining both interpretability and increased sensitivity to poor layers:

$$R_H(t) = \nu R_A(t) + (1 - \nu) R_G(t), 0 \leq \nu \leq 1$$

Malfunctions of cyber-physical systems have interdependencies. Impairment of communication could affect the control process; cyber attack could cause tampering of sensor signals; environmental threat could result in physical system failure. From this respect:

$$C(t) = \sum_{i<j} \gamma_{ij} [1 - R_i(t)][1 - R_j(t)]$$
$$R*(t) = R_H(t) exp[-C(t)]$$

The reliability function R*(t) reduces if there is simultaneous deterioration in more than one layer. It is critical for CPS that a slight deterioration in a few dependent layers is far more hazardous than a heavy local error. All summarized in ***Figure 5***. and ***Tables 5.***

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Table 5. Example layer weights for a multilayer CPS reliability model.

Layer	α_i	Role
R_h	0.140	Functional weight used for illustrative multilayer aggregation
R_s	0.120	Functional weight used for illustrative multilayer aggregation
R_k	0.160	Functional weight used for illustrative multilayer aggregation
R_p	0.140	Functional weight used for illustrative multilayer aggregation
R_u	0.160	Functional weight used for illustrative multilayer aggregation
R_c	0.140	Functional weight used for illustrative multilayer aggregation
R_{ch}	0.080	Functional weight used for illustrative multilayer aggregation
R_e	0.060	Functional weight used for illustrative multilayer aggregation

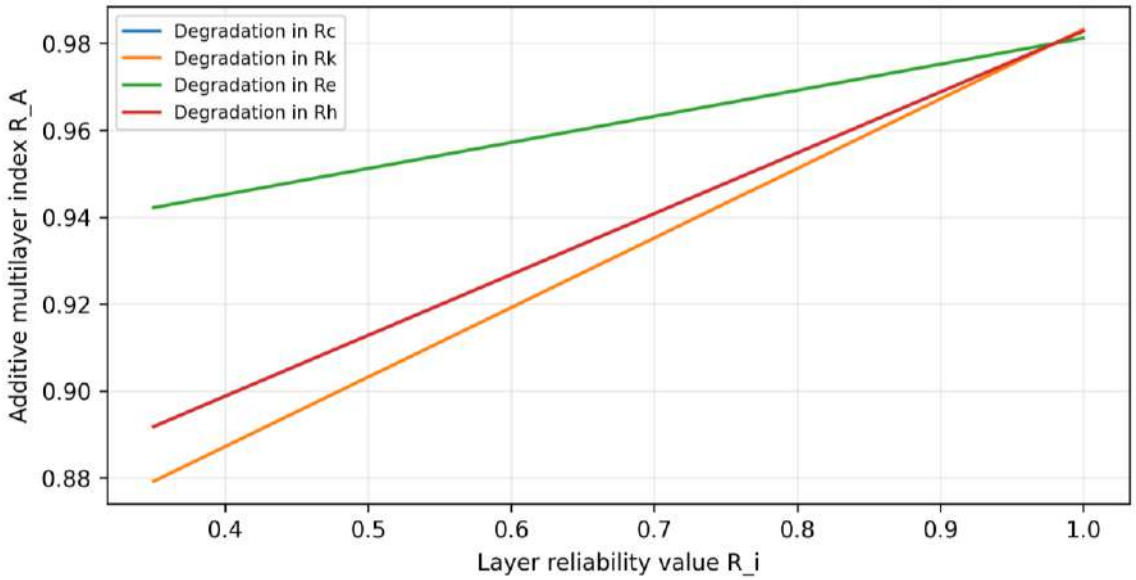

Figure 6. Sensitivity of the additive multilayer reliability index to layer degradation.

Dynamic Predictive Reliability and Failure Probability

The current reliability value is not enough for decision-making. Two CPS states may have the same R*(t), but different trends. One may be stable, while the other may be moving toward degradation. Therefore, the reliability model must include predictive risk. A logistic failure probability can be defined in advance for time horizon h as:

$$P_f ail(t+h|t) = 1/\left[1 + exp[-z(t)]\right]$$

Where $z(t) = \theta_0 + \theta_1[1 - R*(t)] + \theta_2 D(t) + \theta_3 A_n(t) + \theta_4 C_\gamma(t) + \theta_5 H_u(t) + \theta_6 E_n(t)$.

In the above formula, D(t) could indicate degradation rate, $A_n(t)$ - anomaly severity, $C_\gamma(t)$ - cybersecurity risks, $H_u(t)$ - human factor risk, and $E_n(t)$ - environmental or energy stresses. The resulting dynamic predictive reliability index can be expressed as follows:

$$R_D KPN(t) = R*(t)\left[1 - P_f ail(t+h|t)\right]^\rho, \rho > 0$$

Parameter ρ determines the impact weight of future failure probability on the current reliability index. The constructed measure can be decreased.

Critical contribution: $K_i(t) = \alpha_i[1 - R_i(t)] + \sum_{j \neq i} \gamma_{ij}[1 - R_i(t)][1 - R_j(t)]$

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

The critical contribution $K_i(t)$ ranks layers according to their contribution to total risk. This is important because a reliability model should not merely state that the system is risky; it should indicate whether the dominant risk is cyber, communication, hardware, sensor, control, human, or environmental.

Illustrative Numerical Reliability Calculations

Calculations easily prove how both classical and multilayer reliability measures may be combined effectively. These are just examples and cannot take the place of empirical verification (***Table 6.***, ***Table 7***.)

Table 6. Exponential reliability example.

t [h]	λ [1/h]	R(t)	F(t)
100	0.0005	0.9512	0.0488
500	0.0005	0.7788	0.2212
1000	0.0005	0.6065	0.3935
2000	0.0005	0.3679	0.6321
5000	0.0005	0.0821	0.9179

Table 7. Availability example for MTBF = 2000 h.

MTBF [h]	MTTR [h]	Availability A	Unavailability
2000	1	0.99950	0.050%
2000	4	0.99800	0.200%
2000	8	0.99602	0.398%
2000	24	0.98814	1.186%
2000	48	0.97656	2.344%
2000	72	0.96525	3.475%

DISCUSSION: What Additional Reliability Means in CPS

The extra reliability dimension of CPS is thus not just about adding new indicators. What counts as a failure needs a new interpretation here: a component may technically operate normally but be considered unreliable because of the delay, corruption, poor synchronization, or compromise of its data in terms of the prevailing cyber environment. Conversely, a temporary failure of some components may be compensated by redundancy and fail-over mechanisms and lead to no system-level failure. Consequently, six desirable attributes of a CPS reliability index can be listed. First of all, the index should be probabilistic, due to the nature of uncertainty. Second, it should be structural since the structure of CPS influences propagation of failures. Third, it should be dynamic since risk evolves. Fourth, it should be based on data, owing to the ever-increasing number of data streams in modern systems. Fifth, it should be interpretable, as engineers need to understand what is happening at any point. Finally, the reliability index should be actionable as well. The above framework allows retaining the benefits of classic approaches to CPS reliability modeling while expanding their applicability significantly. Exponential and Weibull models account for the local lifetime distribution. Structural models cover the impact of architecture on system operation. Markov processes describe degrading and recoverable states. Both fault trees and Bayesian nets include logical and probabilistic associations between faults. Normalization provides homogeneous measures based on varied measurements, while the multi-level indicator integrates all these different types of measurements. Failure probability makes reliability a sophisticated alert system. This study could be integrated as an optimization task on intelligent systems, sustainable urban management, and KPI-based decision support (*Nikolov, 2024, 2025, 2026*).

CONCLUSION

Main contribution of this paper is a framework for modeling CPS reliability as a dynamic multilayer metric, which includes the reliability of its components, their transition and interdependencies, Bayesian information, normalization methods, cascades, and probability of failure prediction. The approach is suitable for use with any type of industrial CPS and various smart-building projects including those in education, transport, energy, and cities. The above-mentioned mathematical chain can be formulated

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

succinctly as follows: raw indicators are normalized to local reliability measures; local reliability measures are combined into layer indices; layer indices form the overall system reliability, either through multiplication or addition or both; interactions within and between layers account for cascade effects; logistic regression is used for failure probability prediction; and a dynamic predictive index emerges. Consequently, reliability becomes not just an abstract probability but also a governance tool.

REFERENCES

1. Alur, R. (2015). Principles of cyber-physical systems. MIT Press. https://doi.org/10.5555/2774947
2. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023
3. Birolini, A. (2017). Reliability engineering: Theory and practice (8th ed.). Springer. https://doi.org/10.1007/978-3-662-54209-5
4. Flammini, F. (Ed.). (2019). Resilience of cyber-physical systems: From risk modelling to threat counteraction. Springer. https://doi.org/10.1007/978-3-319-95597-1
5. Friederich, J., & Lazarova-Molnar, S. (2021). Towards data-driven reliability modeling for cyber-physical production systems. Procedia Computer Science, 184, 589–596. https://doi.org/10.1016/j.procs.2021.03.073
6. 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
7. Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. Ashgate. https://doi.org/10.1201/9781315607511
8. 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
9. Kabir, S. (2017). An overview of fault tree analysis and its application in model-based dependability analysis. Expert Systems with Applications, 77, 114–135. https://doi.org/10.1016/j.eswa.2017.01.058
10. 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
11. Lee, E. A., & Seshia, S. A. (2017). Introduction to embedded systems: A cyber-physical systems approach (2nd ed.). MIT Press. https://doi.org/10.5555/3086978
12. Leveson, N. G. (2012). Engineering a safer world: Systems thinking applied to safety. MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001
13. 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
14. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
15. Nikolov, N. (2026). A KPI-based model for smart management of urban green infrastructure and ecosystem services. *Forestry Ideas, 32*(1), 209–222.
16. Nikolov, N. (2025). Intelligent Urban Systems and Industry 5.0: Creating Adaptive Ecosystems for SustainableEnergyand Resource Management. International Journal of Current Science Research and Review, 8(1), 103-115,DOI:https://doi.org/10.47191/ijcsrr/V8-i1-11
17. Nikolov, N. (2024). Development of an Intelligent System for Managing Energy Consumption in the Home. ComputerScience and Technologies (Technical University of Varna), ISSN 1312-3335, pp. 11-20.
18. 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
19. Rausand, M., & Høyland, A. (2004). System reliability theory: Models, statistical methods, and applications (2nd ed.). Wiley. https://doi.org/10.1002/9780470316900

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 06 June 2026
DOI: 10.47191/ijcsrr/V9-i6-27, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

20. Ruijters, E., & Stoelinga, M. (2015). Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer Science Review, 15–16, 29–62. https://doi.org/10.1016/j.cosrev.2015.03.001
21. Trivedi, K. S. (2016). Probability and statistics with reliability, queuing, and computer science applications. Wiley. https://doi.org/10.1002/9781119285441
22. Weber, P., Medina-Oliva, G., Simon, C., & Iung, B. (2012). Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence, 25(4), 671–682. https://doi.org/10.1016/j.engappai.2010.06.002
23. 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). Mathematical Reliability Modeling of Cyber-Physical Systems: From Classical Failure Theory to Multilayer Predictive Indices. International Journal of Current Science Research and Review, 9(6), pp. 3212-3221. DOI: https://doi.org/10.47191/ijcsrr/V9-i6-27