2026 56th Annual IEEE International Conference on Dependable Systems and Networks Workshops (DSN-W) | 979-8-3195-3244-2/26/$31.00 ©2026 IEEE | DOI: 10.1109/DSN-W70714.2026.00026

Consequence-Driven Dependability Models for Cyber-Physical Systems (CPS)

Ronan Oostveen, Stefano Simonetto, Peter Bosch, Alessandro Chiumento, Maarten van Steen
Department of Computer Science, University of Twente, Enschede, The Netherlands
Email: {r.oostveen, s.simonetto, h.g.p.bosch, a.chiumento, m.r.vansteen}@utwente.nl

***Abstract*—Cyber-physical systems (CPS) are a cornerstone of modern industry, combining Operational Technology (OT) with Information Technology (IT) to enhance the monitoring and control of systems. While this improves efficiency, it also exposes critical OT systems to new threats, as seen by incidents like Stuxnet and the attack on Ukraine's energy grid. In both cases, attackers exploited vulnerabilities within the cyber layer to gain unauthorized access, allowing them to affect the physical operations and compromise the safety and dependability of the broader system. This highlights the growing need to better understand how failures might cascade across several dependability domains. Conventional security metrics, such as the Common Vulnerability Scoring System (CVSS) overlook aspects like operational context, limiting their relevance to CPS. While CVSS provides valuable insights into technical vulnerability severity, system operators must also evaluate operational risk across dependability dimensions, including availability, reliability, safety, integrity, and maintainability. This misalignment calls for a priority shift in CPS risk analysis, moving from data-driven approaches to consequence-driven models.**

By utilizing a Cyber Digital Twin (CDT), we can measure the impact of failures on operational risk. The CDT provides a high-fidelity replica of both the OT and IT domains within the CPS. In this environment, failures are generated and injected probabilistically, and their impact is analyzed across the dependability dimensions of the model. Through comprehensive sampling of failure scenarios, we develop quantifiable metrics that enable a consequence-driven risk assessment.

This position paper advocates for a unified CPS risk assessment framework that prioritizes operational consequences and probabilistic failure modeling, which is achieved using high-fidelity cyber-physical digital twins. We explore the implications and future research directions of our method, highlighting its potential to identify critical dependability weaknesses and assist security analysts in prioritizing threats according to operational risk.

***Index Terms*—Industrial Control Systems (ICS), Cyber Physical Systems (CPS), Security-Enhancing Digital Twins (SEDT), Cyber Digital Twins (CDT)**

I. Introduction

The convergence of Operational Technology (OT) and Information Technology (IT) has given rise to Cyber-Physical Systems (CPS), which serve as the foundation for modern industry ranging from power grids to advanced manufacturing. While these CPS can enhance performance and efficiency compared to the original OT-systems, they also expose these systems to the threats associated with IT-infrastructure. Well-known CPS incidents (such as Stuxnet [11] and the Ukrainian power grid [5]) have shown that a cyber layer threat can directly affect system operations, jeopardizing dependability (availability, reliability, safety, integrity, and maintainability).

A fundamental gap remains in our ability to understand the impact these threats can have on the operations of a CPS. Current risk triage often focuses on data-driven metrics, such as the Common Vulnerability Scoring System (CVSS), which quantifies the technical severity but does not consider the asset's operational context. This approach is insufficient for CPS, where the primary concern is not the vulnerability itself, but its impact on system dependability. Furthermore, as highlighted by [13], current models for understanding the impact of complex cyber attacks remain largely limited and rely on oversimplified assumptions (i.e., standard probability distributions). Validating such models remains a challenge, as experimenting on live CPS is too risky, leaving operators unable to assess the true operational impact of a failure.

Because of the complex and interdependent nature of a CPS, evaluating the impact of a specific failure is complicated. A single failure in the cyber layer can spread throughout the network to the physical layers, jeopardizing system control and dependability. Since failures cannot be precisely predicted in timing or nature, understanding their full cascading impact requires characterizing them as probabilistic rather than deterministic events. This highlights the need for high-fidelity models capable of evaluating operational impacts across a broad range of failure scenarios. While previous research has used Digital Twins (DTs) and Cyber Ranges to model these complex systems, these tools struggle to balance scalability with the fidelity required to capture cascading effects across both the IT and OT domains. We argue that consequence-driven dependability models, require the creation of high fidelity models capable of injecting failures probabilistically and measuring their operational impact across the system.

Developing consequence-driven dependability models requires us to look beyond isolated security metrics and return to the fundamental principle of system engineering: ensuring dependability. Security must be seen as an attribute within the larger dependability framework, deeply interconnected to other dependability attributes. Rather than asking "how severe is this vulnerability?", a consequence-driven approach asks "what is the resulting operational risk when this failure propagates across dependability dimensions?".

We propose extending Cyber Digital Twins (CDTs) beyond traditional security scenarios to measure operational risk across all dependability dimensions. As high-fidelity replicas of

2325-6664/26/$31.00 ©2026 IEEE
DOI 10.1109/DSN-W70714.2026.00026

both the IT and OT domains, CDTs enable probabilistic fault injection and the quantification of distinct dependability attributes.

To summarize, this position paper makes the following contributions:

1) We propose using consequence-driven framing for CPS risk triage, rather than data-driven approaches based on vulnerability metrics.
2) We propose modeling failures (i.e. cyber exploits, misconfigurations, software flaws, and hardware failures) as probabilistic events that can propagate through the CPS and may impact dependability.
3) We propose leveraging CDTs as a simulation environment integrating the cyber, cyber-physical, and physical layers, enabling probabilistic fault injection and quantification of distinct dependability attributes.
4) We define a research agenda identifying key open challenges: model fidelity, deriving meaningful probabilities, modeling cascading effects, and validation.

II. An Overview of CPS Risk

Cyber-Physical Systems (CPS) integrate both digital and physical processes, where embedded devices and networks monitor and control physical processes across multiple layers. We adopt the hierarchical layered structure from Guzman et al. [4], shown in Figure 1, dividing the CPS into three layers: the Cyber layer (IT), the Cyber-Physical layer (IT/OT), and the Physical layer (OT). Each layer carries an associated set of risks ranging from digital to electrical to kinetic. Within the lower layers, electronic and mechanical components directly influence the physical control loop, making them most critical for system dependability.

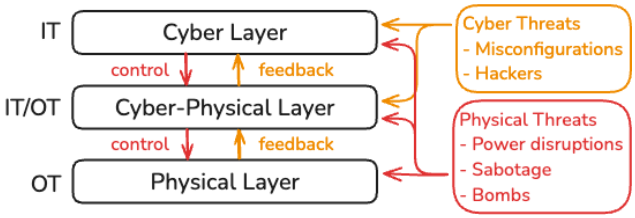

Fig. 1. The multi-layered representation of the CPS, including the flows and threats

Although IT integration increases efficiency, it exposes OT environments to cascading cross-layer failures. For example, during a 2019 U.S.A. grid incident, attackers exploited a firewall vulnerability (CVE-2018-0296) [17]. Tracing the cascade: the cyber-layer exploit caused intermittent reboots over a 10-hour window, which disrupted the cyber-physical layer by severing communication between generation assets and the Energy Management System (EMS).

Table I contrasts a data-centric assessment of this incident against our consequence-driven model. Notably, an investigation in 2019 showed that grid sites utilizing High-Availability (HA) redundant firewalls experienced zero downtime despite running the identical vulnerable firmware [12]. CVSS blindly assigns a critical 8.6 score to both setups, risking misaligned patching efforts. Conversely, our model quantifies operational consequences (e.g., EMS downtime), accurately reflecting the near-zero operational risk of the HA configuration.

TABLE I
2019 Firewall Incident: Data-Centric vs. Consequence-Driven

Metric	Data-Centric (CVSS)	Consequence-Driven
Focus	Vulnerability severity	Dependability impact
Single Firewall	**8.6 (High):** Based on vulnerability.	**High Operation Risk:** 10-hr loss of EMS.
HA Redundant	**8.6 (High):** Based on vulnerability.	**No Operation Risk:** 0 minutes downtime.

Furthermore, capturing these operational consequences highlights the limitations of traditional deterministic modeling. Deterministic approaches typically assume worst-case attack paths, ignoring dynamic interdependencies like redundancies or physical safeguards. To overcome this, our model probabilistically injects failures (e.g., exploits, misconfigurations) as stochastic events. By continuously sampling interdependent system states rather than single predefined paths, this probabilistic approach provides a comprehensive and realistic overview of the system's true dependability landscape.

III. Related Research

Since the start of Industry 4.0, Digital Twins (DTs) have been a popular modeling paradigm for CPS. We adopt the definition in [7], which defines DTs as *virtual replicas of the network and the logic layer of physical devices, closely matching the behavior of physical devices' in these layers*. This definition is particularly relevant for CPS, as many cascading effects arise directly from interactions between the network, logic, and physical layers.

While manufacturing and predictive maintenance are the most popular DT use-cases, Security-Enhancing Digital Twins (SEDT) [9] and Cyber Digital Twins (CDT) [14], have gained traction for cybersecurity purposes, including risk assessment [16] and training personnel [15]. These works position DTs as safe environment to explore attack scenarios, predominantly focus on IT-security metrics rather than measuring the downstream consequences on OT operations. Our work diverges by shifting from *simulating* attacks to *quantifying* their operational impact on dependability attributes.

The practicality of DTs for security is hindered by the inherent trade-off between budget and fidelity [8]. Cost-effective DTs have been proposed for security analyses [3], but their fidelity is limited. This trade-off is especially critical for consequence-driven modeling. Frameworks like MiniCPS [1] and ICSSIM [6] partially address this through combinations of simulation, emulation, and hardware-in-the-loop setups. Additionally, it has been shown that using topological abstractions can be sufficient to identify critical attack paths [10]. However, these topological abstractions strip away the physical dynamics necessary to measure actual consequences. Existing testbeds are typically used for deterministic, single-scenario testing. Our approach leverages high-fidelity CDT environments for probabilistic failure sampling, generating statistical risk distributions across

dependability attributes, rather than single-dimension data-driven outcomes.

Previous CDT research has shown the importance of DTs as a platform for security. However, to the best of our knowledge, no previous work has explicitly used DTs as a tool for probabilistic, consequence-driven dependability research. This gap supports our position that CDTs must be extended beyond traditional IT security, to assessing the likelihood and operational severity of failures across the full CPS.

IV. Position: A Unified CPS Dependability Framework

Current industrial security practices are based on data-centric metrics. These practices are a poor fit for CPS, where the dominant concern is not data loss, but the continuous operation of industrial processes. Frameworks such as CVSS quantify risk to data and software, but not to system dependability. As shown in Figure 2 [2], security encompasses a subset of dependability attributes while also introducing confidentiality as an additional concern. We propose addressing the full dependability risks in CPS, through utilizing CDTs that capture how different failure scenarios affect the various dependability attributes. In the remainder of this section, we outline how consequence-driven analysis, probabilistic sampling, and CDTs together enable this perspective.

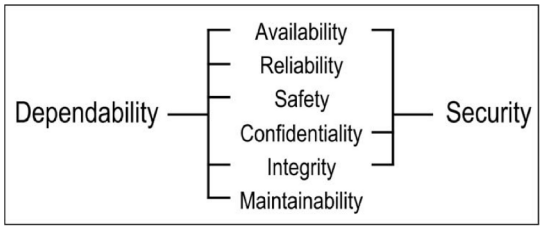

Fig. 2. Dependability and security attributes. (2004, Avižienis et al. [2])

A. Prioritizing Consequences over Vulnerabilities

Securing a CPS encompasses IT security, protecting information and infrastructure, but extends beyond it to maintaining system dependability across the cyber-physical and physical layers. We therefore define a consequence not as a incident or attack-path, but as a measurable deviation on the dependability attributes (e.g., minutes of lost availability, number of safety violations).

Metrics like CVSS often result in misleading risk assessments, as they do not consider the operational context. We argue that CPS risk assessment must focus on the consequences, assessing risk in terms of its impact on system rather than focusing on the vulnerabilities themselves. This shifts the question from *How exploitable is this flaw?* to *What are the operational consequences of this flaw on the system?*.

To illustrate this we return to the 2019 U.S.A. grid example: a data-driven approach demands immediate patching of the firewall due to its 8.6 score, potentially requiring an emergency maintenance that itself could be an operational disruption. In contrast, a consequence-driven model recognizes that if only one firewall in a High-Availability pair carries this vulnerability, the operational risk would be significantly reduced. Security analysts can thus safely choose to patch this in a scheduled maintenance window, instead of an emergency patch.

Our first position is thus: *CPS risk assessment must prioritize operational consequences, measured as physical or operational deviations, over static data-driven metrics*. This requires a shift from static risk assessment to developing consequence-driven models that can account for the topological context and states of the CPS.

B. From Incidents to Probabilities

Identifying consequences is insufficient without understanding their likelihood. However, predicting the exact timing of a cyber attack is impossible. CPS risk assessment must therefore move away from approaching threats as unpredictable deterministic events, and instead attempt to predict the likelihood of occurrence probabilistically, similar to the approach used in reliability engineering.

CPS risk assessment must attempt to convert abstract vulnerabilities and misconfigurations into probabilistic variables, similar to how predictive maintenance depends on failure rate distributions rather than forecasting exact component failures. By holistically sampling these failures as scenarios, we eliminate the need to find all deterministic attack paths. Instead, it transforms the qualitative question *Are we secure?* into a quantitative one: *What is the probability that the current system state will move outside acceptable dependability bounds?*

Our second position is thus: *CPS dependability must be modeled probabilistically, treating cyber threats and other faults as probability distributions that can impact the CPS dependability attributes.*

C. Quantifying Dependability using Cyber Digital Twins

While consequence-driven modeling and probabilistic representations combined give a more complete picture of CPS risk, using static analysis alone is challenging. Static analysis suffers from a significant trade-off between precision and scalability. To accurately model and measure the probabilities of the cascading failures described in Section II, we require an environment capable of simulating the dynamic interactions between digital and physical components.

We propose the Cyber Digital Twin (CDT) as the tool that enables the quantification of dependability attributes. A CDT provides a high–fidelity replica containing both the IT domain (e.g., networks, authentication) and the OT domain (e.g., control logic, physics). This environment treats cyber attacks not as isolated events, but as probability distributions similar to component failures.

By running iterative simulations within the CDT we can comprehensively sample failure scenarios, integrating vulnerabilities and physical tolerances probabilistically to observe fault propagation. This allows analysts to directly measure the risk to specific dependability attributes resulting from a given failure, converting the abstract concepts of a *risk* into a measurable, quantifiable metric.

V. Research Agenda

Realizing the vision outlined in this position paper requires a multi-disciplinary research approach, combining the fields of dependability engineering, stochastic modeling, cybersecurity, and digital twin technology. We propose a research agenda structured around the following core questions:

1) **System Modeling:** How can the complex, multi-layered dependencies within the CPS hierarchy (cyber/cyber-physical/physical), and operational processes in a CPS be formally modeled with sufficient fidelity for a dependability risk assessment?
2) **Probabilities:** How can discrete system states, such as cyber threats, network misconfigurations, and potential hardware/software failures, be abstracted into meaningful probabilistic failure rates for individual components within the model?
3) **Cascading Effects:** What is the appropriate framework to model how risks propagate through the system model and can result in cascading failures?
4) **Model Validation:** How can the output of the consequence-driven dependability model be validated for accuracy, relevance, and utility in a real-world operational context?

VI. Conclusion

This paper examines the challenges of assessing risk in CPS and proposes a consequence-driven dependability framework as a solution. Current methods, such as CVSS, measure the technical severity but do not consider the impact. In CPS, the primary concern is not the severity of the vulnerability, but that impact. We propose a shift from data-driven to consequence-driven methods, with an emphasis on context-aware dependability metrics that quantify the operational impact.

Rather than identifying discrete attack paths, we propose sampling failure scenarios to directly evaluate the affect of failures on the system's operation. By utilizing a Cyber Digital Twin (CDT) as the modeling environment a high fidelity replica is made, taking into account both the IT and OT domains. This approach allows for failure scenarios to be probabilistically introduced into the model and their impact to be measured across various dependability attributes. This enables analysts to evaluate system risk not only from a cybersecurity perspective, but also on dependability dimensions including safety and reliability. We believe this multidisciplinary approach will considerably improve the understanding of the CPS risk landscape and provide operators with practical, operationally grounded insights needed to prioritize threats effectively.

References

[1] D. Antonioli and N. O. Tippenhauer. MiniCPS: A Toolkit for Security Research on CPS Networks. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, CPS-SPC '15, pages 91–100, New York, NY, USA, Oct. 2015. Association for Computing Machinery. Read_Status: Read Read_Status_Date: 2025-05-09T12:13:05.903Z.

[2] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, Jan. 2004. Read_Status: New Read_Status_Date: 2025-12-17T15:25:43.838Z.

[3] R. Bitton, T. Gluck, O. Stan, M. Inokuchi, Y. Ohta, Y. Yamada, T. Yagyu, Y. Elovici, and A. Shabtai. Deriving a Cost-Effective Digital Twin of an ICS to Facilitate Security Evaluation. In J. Lopez, J. Zhou, and M. Soriano, editors, *Computer Security*, pages 533–554, Cham, 2018. Springer International Publishing. Read_Status: In Progress Read_Status_Date: 2025-07-10T10:19:36.393Z.

[4] N. H. Carreras Guzman, M. Wied, I. Kozine, and M. A. Lundteigen. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Systems Engineering*, 23(2):189–210, Mar. 2020. Read_Status: New Read_Status_Date: 2026-01-12T10:51:23.499Z.

[5] D. U. Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity information sharing and analysis center (E-ISAC)*, 388(1-29):3, 2016.

[6] A. Dehlaghi-Ghadim, A. Balador, M. H. Moghadam, H. Hansson, and M. Conti. ICSSIM — A framework for building industrial control systems security testbeds. *Computers in Industry*, 148:103906, June 2023. Read_Status: In Progress Read_Status_Date: 2025-05-14T10:07:42.744Z.

[7] M. Eckhart and A. Ekelhart. A Specification-based State Replication Approach for Digital Twins. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, CPS-SPC '18, pages 36–47, New York, NY, USA, Jan. 2018. Association for Computing Machinery. Read_Status: Not Reading Read_Status_Date: 2025-05-14T08:04:13.533Z.

[8] M. Eckhart and A. Ekelhart. Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook. In S. Biffl, M. Eckhart, A. Lüder, and E. Weippl, editors, *Security and Quality in Cyber-Physical Systems Engineering: With Forewords by Robert M. Lee and Tom Gilb*, pages 383–412. Springer International Publishing, Cham, 2019. Read_Status: In Progress Read_Status_Date: 2025-05-13T06:40:33.289Z.

[9] M. Eckhart, A. Ekelhart, D. Allison, M. Almgren, K. Ceesay-Seitz, H. Janicke, S. Nadjm-Tehrani, A. Rashid, and M. Yampolskiy. Security-Enhancing Digital Twins: Characteristics, Indicators, and Future Perspectives. *IEEE Security & Privacy*, 21(6):64–75, Nov. 2023. Read_Status: New Read_Status_Date: 2026-01-05T13:03:57.863Z.

[10] M. Eckhart, A. Ekelhart, and E. Weippl. Automated Security Risk Identification Using AutomationML-Based Engineering Data. *IEEE Transactions on Dependable and Secure Computing*, 19(3):1655–1672, May 2022. Read_Status: New Read_Status_Date: 2026-03-11T14:22:45.054Z.

[11] R. Langner. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, 9(3):49–51, May 2011. Read_Status: New Read_Status_Date: 2025-06-30T14:19:09.037Z.

[12] L. Learned. Risks posed by firewall firmware vulnerabilities. *North American Electric Reliability Corporation: Atlanta, GA, USA*, 2019.

[13] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap. Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. *ACM computing surveys*, 55(10):1–36, 2023.

[14] A. R. Qureshi, A. Asensio, M. Imran, J. Garcia, and X. Masip-Bruin. A survey on security enhancing Digital Twins: Models, applications and tools. *Computer Communications*, 238:108158, June 2025. Read_Status: In Progress Read_Status_Date: 2025-07-11T12:17:52.455Z.

[15] M. Vielberth, M. Glas, M. Dietz, S. Karagiannis, E. Magkos, and G. Pernul. A Digital Twin-Based Cyber Range for SOC Analysts. In K. Barker and K. Ghazinour, editors, *Data and Applications Security and Privacy XXXV*, volume 12840, pages 293–311. Springer International Publishing, Cham, 2021. Series Title: Lecture Notes in Computer Science Read_Status: Read Read_Status_Date: 2025-05-08T11:22:15.614Z.

[16] H. Xu, J. Wu, Q. Pan, X. Guan, and M. Guizani. A Survey on Digital Twin for Industrial Internet of Things: Applications, Technologies and Tools. *IEEE Communications Surveys & Tutorials*, 25(4):2569–2598, 2023. Read_Status: In Progress Read_Status_Date: 2025-07-10T14:34:30.130Z.

[17] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access*, 9:29775–29818, 2021. Read_Status: New Read_Status_Date: 2025-10-02T13:22:32.586Z.