Impact Assessment of Anomaly Propagation in a Naval Water Distribution Cyber-Physical System

Nicolas Pelissero, Pedro Merino Laso, John Puentes

Impact assessment of anomaly propagation in a naval water distribution cyber-physical system

Nicolas Pelissero
Chair of Naval Cyber Defense
Ecole navale
Brest, France
nicolas.pelissero@ecole-navale.fr

Pedro Merino Laso
French Maritime Academy (ENSM)
Nantes, France
pedro.merino-laso@supmaritime.fr

John Puentes
IMT Atlantique
Lab-STICC, UMR CNRS 6285
Brest, France
john.puentes@imt-atlantique.fr

***Abstract*—Cyber-Physical Systems (CPS) are composed by multiple subsystems that encompass numerous interdependencies. Although indispensable and highly performant from a functional perspective, complex interconnectivity constitutes paradoxically a significant vulnerability when an anomaly occurs. Anomalies could propagate and impact the entire CPS with irreversible consequences. This paper presents an approach to assess the anomaly propagation impact risk on a three layers oriented graph which represents the physical, digital, and system variables of a CPS components and interdependencies. Anomalies are detected applying information quality measures, while potential propagation paths are assessed computing the cumulated risk represented by weights assigned to the graph edges. To verify the cascading impact of different anomalies four cyber-attacks - denial of service, sensor offset alteration, false data injection, and replay attack - were implemented on a simulated naval water distribution CPS. The propagation impact of three anomalies was successfully assessed and the corresponding estimated propagation path, if applicable, confirmed.**

***Index Terms*—Cyber-physical system, cybersecurity, propagation assessment, multilayer graph model, risk estimation.**

I. Introduction

Cyber-physical systems (CPS), essential in the naval domain, rely on numerous interdependencies and interactions of heterogeneous physical, digital, and communication components [1]. Whereas such strong emergence of CPS is part of the current progress towards autonomous ships, it has also brought a major concern related to cybersecurity. Even if global guidelines of the International Maritime Organization have requested, among others, to address cybersecurity threats by 2021 [2], currently only partial assessments of some risks have been conceptualized in this domain. One of the reasons that explain this setback is the increasing complexity of data and information flow interdependencies, which hinder the identification, modeling, and analysis of interactions between connected components. Furthermore, conceptualizing the vessels' CPS as multilayer networks [3], it is evident that a cyber-attack or a system malfunction could cause cascading failures, engendering potential irreversible damage on board.

A crucial vessel system that could be the target of a cyber-attack or break down because of an anomaly is the water supply, which ensures a sustainable life condition level for crew members and passengers. The water distribution CPS is commonly composed of several tanks to stock water, pumps to fill up the tanks, valves to control water circulation, consumption nodes, and the particular global control system. Water quality and distribution alterations could generate infectious disease transmission [4] that may compromise a given mission. Other CPS like power generation, navigation, and propulsion will produce equivalent detrimental issues on board. Considering the consequences of cascading failures on naval CPS, the major aim of this work is to define a CPS-adapted model for the evaluation of how an altered subsystem could impact other subsystems it is connected to, when an anomaly occurs, to anticipate critical failures. This evaluation is based on a multilayer graph model and a specific propagation risk assessment. A naval water distribution study case is used to test the proposed approach. This paper is organized as follows. Section II introduces previous works on CPS modelling and anomaly propagation. Section III describes the proposed graph modeling and anomaly propagation approach. Section IV presents the experimental setup of a simulated naval water supply. The main results are presented in section V. Section VI comments the conclusions and perspectives of the study.

II. Related Works

One of the most challenging aspects of CPS modeling is cyber-physical duality. Physical components operate mostly in continuous time, while cyber components run in a discrete-time manner. Therefore, the connection between these two operations is essential to model any CPS behavior. Initiatives in the literature have reported about agent-based models to describe interactions between physical and cyber components within a CPS [5] and hybrid system behavior modeling of the communication infrastructure in a smart grid [6]. Another model [7], focused on CPS representation to enable combined safety and security analyses, using a multilayered structure to conceptualize subsystems and their interactions. Although, without specifying subsystem interdependencies and covering partially the cyber-physical duality, a recent work proposed to weight interdependencies value, computed according to their amount and a predefined protection level, to determine the risk of anomaly propagation in an information technology network [8].

978-1-7281-5684-2/20/$31.00 ©2021 IEEE

CPS's subsystem interdependencies encompass additional complexity and could have a tremendous impact on system performance, since a minor failure in a critical infrastructure could propagate through the entire system and trigger numerous other failures [9]. However, a given CPS subsystem interconnected to a failed one may not be immediately impacted by that failure, and subsystems that do not interact directly with the physical world could still be impacted by an attack propagation. Because of these reasons, several analyses of CPS interdependencies are based on graph abstraction, even if the proposed CPS mathematical models do not reflect the operational specifications of the subsystems interdependencies. Graph modeling has been applied to optimize the recovery ability of interdependent networks after cascading failures [10], as well as to evaluate the propagation consequences of attacks by comparing the dynamic behavior of physical processes through their sensor measurements and control command outputs, in normal conditions and under attack [11]. These modelling approaches integrate only to a certain degree part of the CPS specifications and application domains. Otherwise, graph theory abstraction was used to model anomaly propagation, matching critical infrastructures interactions and interdependencies, based on mixed holistic reductionism [12], which is not adapted to CPS. Our work intends to further unify the CPS cyber space and physical world, with the perspective of a generic and comprehensive methodology [13], to cover the design, development, verification, and real-time analysis of CPS. We focus on anomaly propagation assessment to anticipate critical failures.

III. Proposed method

A. CPS graph generation model

In our previous work a simplified generic CPS-adapted graph model was proposed [14]. This model focused on a preliminary anomaly detection and propagation analysis, based on data and information quality measures on a simplified CPS. According to CPS specificities, each CPS subsystem node belongs to the digital or physical layer of the multilayered generated graph. A third layer groups the variables associated to subsystem nodes. The three layers of the generated graph model are illustrated in Fig. 1. Components of the layers are assigned as follows:

- **Digital subsystems:** Integrate networking and/or computing capacities (e.g. in Fig. 1 PLCs and SCADA).
- **Physical subsystems:** Interact with a physical process, transmit measured data or receive control commands (e.g. in Fig. 1 PU10 and PU11 pumps, and T7 tank).
- **System variables:** Describe the CPS current state with measured and control variables (e.g. in Fig. 1 pump state s, flow f, and T7 tank level l_7).

The defined graph structure represents node dependencies for both CPS modeling and anomaly propagation assessment. These dependencies can be assembled in two major groups:

- Between subsystems of the digital and physical layers: Defined digital/physical communication dependencies, e.g sensor measurements transmission, PLC-to-actuator control command, pump activation and tank fill-up.
- Between system variables of the third layer: State-correlation model [15] of structural – a variable deviation can cause the variation of others –, or operational – subject to the activation of a specific value in other variables – dependencies.

B. Anomaly detection

After the previous graph generation, anomalies in the CPS are detected on the system variables layer. To this end, information quality measures and parameters of concerned digital and physical subsystems nodes are associated to each one of the resulting CPS variables. The pertinence of these information quality measures was validated previously in the case of a static anomaly detection scenario [16]. An information quality measure vector $\overrightarrow{IQV}$, composed by s dimensions of information quality metrics, is defined as follows:

$$\overrightarrow{IQV} \in \{i_1, ..., i_s\} \tag{1}$$

These information quality vectors are assigned as measure vectors $\overrightarrow{IQV}$ of the corresponding system variables (Fig. 1). Anomalies are detected when data flows of the CPS subsystem contradict expected agreement levels of the quality measures.

C. Impact assessment processes of an anomaly propagation

Two distinct anomaly propagation assessment processes are conducted on the proposed graph model. The first process is initiated once an anomaly has been detected at a time t_1. An evaluation of the propagation on system variables (PSV) starts to evaluate the potentially impacted variables. This propagation assessment process is conducted on the **third layer** of the graph model, based exclusively on the graph characteristics defined by the given system variables dependencies model. Whenever the same anomaly impacts another system variable at a time t_2, and if this variable was previously identified through the PSV evaluation at t_1, an impact time on the second system variable defined as $\Delta t = t_2 - t_1$, confirms the estimated propagation path.

The anomaly detection at t_1 also initiates another anomaly propagation assessment process on the **first and second layers** of the graph model. It is based on weighting of dependencies through propagation risk assessment of CPS subsystems. To this end, four major metrics E_n –that enhance anomaly propagation risks– and R_n –that reduce these risks– are adapted to naval CPS features, taking into account subsystems interactions, functional specifications, and the possible impact on the whole system. Each E and R metric is subdivided in two submetrics, e_n or r_n, defined with a level value from 1 to 4, organized in pairs:

$$E_n = \left\{e_{n,1}, e_{n,2}\right\}, R_n = \left\{r_{n,1}, r_{n,2}\right\}, n = [1, 2] \;\; and \; n \in \mathbb{N} \tag{2}$$

These metrics and associated submetrics, are defined as:

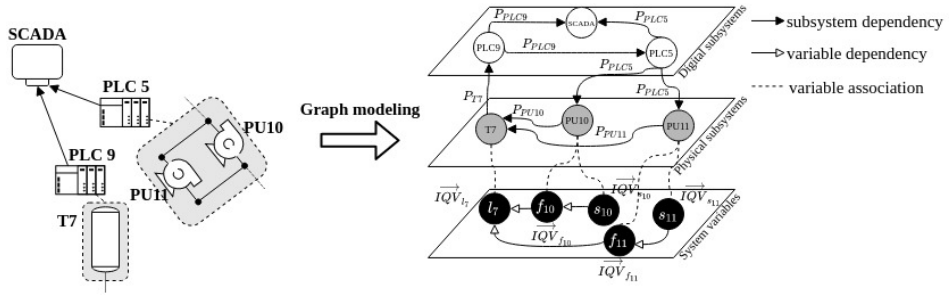

Fig. 1. Graph modeling of a simplified water distribution CPS

- **Connectivity** (E_1**:** Defines the subsystem **type of connection** ($e_{1,1}$) and the associated **privileges** ($e_{1,2}$).
- **Knowledge** (E_2**:** Denotes the **operational ignorance degree** ($e_{2,1}$) about the studied subsystem and its **operational impact** ($e_{2,2}$) in case of failure.
- **Oversight** (R_1**:** Describes the subsystem **communication control** ($r_{1,1}$) and **management** ($r_{1,2}$).
- **Control** (R_2)**:** Highlights the **cyber-approval level** ($r_{2,1}$) of the given subsystem and its **resiliency** ($r_{2,2}$) in case of failure.

It is assumed that applying prior expert knowledge, from manufacturing to operational features, users estimate the risk of each CPS subsystem. To feed the model, initially each proposed submetric level must be associated to the given subsystem specifications. The submetrics $e_{n,1}$ and $r_{n,2}$ are paired in 4 counterbalance associations. From these associations, four propagation risk levels, L_i, are deduced as:

$$L_1 = \frac{e_{1,1}}{r_{1,1}} \qquad L_2 = \frac{e_{1,2}}{r_{1,2}} \qquad L_3 = \frac{e_{2,1}}{r_{2,1}} \qquad L_4 = \frac{e_{2,2}}{r_{2,2}} \tag{3}$$

The sum of these four levels provides a weight P that reflects the subsystem disposition to propagate an anomaly. This estimation is repeated for each subsystem of the first and second layers of the graph model and defined as nodes' edges weights:

$$P = \sum_{i=1}^{4} L_i \;\; as \;\; L_i = [0,25;4] \; ; \;\; then \;\; P = [1;16] \tag{4}$$

For a given CPS, the propagation risk assessment is estimated for each one of its subsystems. As shown in Fig. 1, the values of P are dependency weights assigned to the corresponding subsystems. A propagation impact score PIS is calculated for each subsystem interconnection path in the physical and digital layers, starting with the subsystem node associated to the node variable where the anomaly was initially detected. This score is a sum of the traveled P node weights and depicts the possible anomaly impact of one graph path.

$$PIS = \sum_{i=1}^{d} P_i \; ; \;\; d > 0 \tag{5}$$

IV. Experimentation

A. Naval water distribution CPS

The main purpose of a water distribution system is to satisfy consumers demand and ensure a proper quality of the delivered water. Various CPS components are needed to guarantee this purpose. On the other hand, a ship water supply network (Fig. 2) is designed as for a small village. For this reason, the C-town water distribution network was adapted to our study case. It is composed by 388 nodes, 429 pipes, 7 tanks, 11 pumps, 4 valves (1 actionable), 9 PLC and 1 SCADA. Water storage and distribution depends on the water levels of 7 tanks that control when the 11 pumps should be activated. Each actuator, i.e. pumps and valves, and each sensor, are connected to one of 9 PLCs that control or monitor each of them. A SCADA system collects the PLCs readings and coordinates the process. PLCs that are controlling actuators, in accordance with sensor readings, mostly receive this information from other PLCs. To assess the anomaly propagation impact on physical and digital systems, an entire simulation of the adapted water distribution network physical and digital dimensions must be conducted.

B. Simulation of the water distribution network

The hydraulic simulation of the naval water distribution network was implemented on *EPANET*. This application allows performing extended-period simulations of a water distribution network and offers a large range of CPS components models like pumps, valves, storage tanks, reservoirs, pipes, and junctions. Required functions to design, run, and modify simulations by the effect of external parameters are also available. An external toolbox, *EpanetCPA*, broadens *EPANET* features to the cyber-physical domain, enabling to specify different kinds of attacks on both physical and digital dimensions of a water supply network [17].

C. Graph of the naval water distribution CPS

Each system and subsystem variable of the naval water distribution network are defined by a node, with interdependencies between two nodes being represented by edges. The structural and operational variable dependencies, determined as part of the system design process, are built from the subsystems interdependencies described in a study that characterized cyber-physical attacks on water distribution systems [17]. A

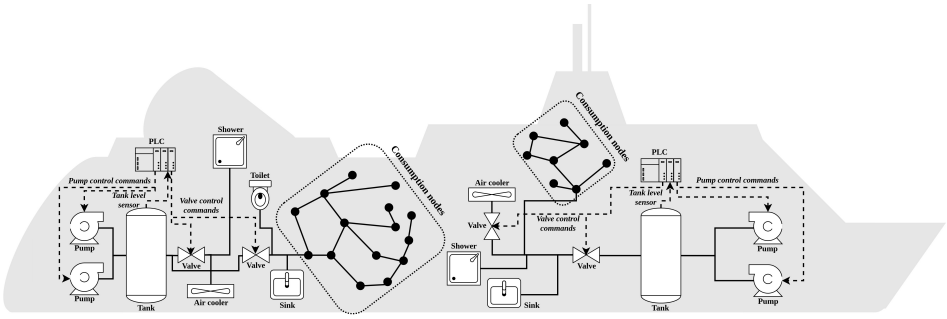

Fig. 2. Representation of a simplified ship water distribution system

simplified illustration of the resulting generated graph model is shown in Fig. 1. The modeled part of the water supply network is in charge of T7, the tank-level controlled when pumps PU10 and PU11 are activated by PLC 5, and transmitted from PLC 9 to PLC 5 for process control. All variable values of actuators and sensors are communicated through the PLCs-to-SCADA connections for process monitoring.

D. Quality analysis

Quality evaluation can be measured by using multiple dimensions depending on the studied CPS configuration [16]. For the study case, contextual information quality is evaluated according to the presence of erroneous information (cd_{err}). This metric denotes if information is different from the expected one. Extrinsic information quality is estimated according to coherence (ed_{coh}) to signify if information appears to be logic compared to other information.

An information quality vector $\overrightarrow{IQV}$ is defined for each network's subsystem and its associated variables. Information quality of the pumps is evaluated through cd_{err}, to identify if pump state s and flow f values match, and ed_{coh} to describe if the pump state value is coherent with the associated tank level. The tank information quality is calculated by using cd_{err} to measure if the given tank level is a viable value, bounded by the *min* and *max* tank-level thresholds. To follow any possible anomaly propagation in the network, each quality metric is associated as a parameter of the corresponding system variable node.

E. Anomaly propagation assessment

To perform an anomaly propagation assessment on the naval water distribution network, each subsystem of the generated graph is weighed according to several metrics based on propagation risk, which are weighted graph dependencies, as defined in III-C. The weighting approach for edges is illustrated hereof with the example of defining weights for PLC9 (Fig3). Each e_n and r_n submetric values are determined by the expert providing the prior propagation assessment knowledge. These values allow to calculate the 4 propagation risk levels L_i (equation 3) and to define P_{PLC9}:

$$P_{PLC9} = \sum_{i=1}^{4} L_i = \frac{3}{1} + \frac{4}{1} + \frac{3}{1} + \frac{4}{1} = 14 \tag{6}$$

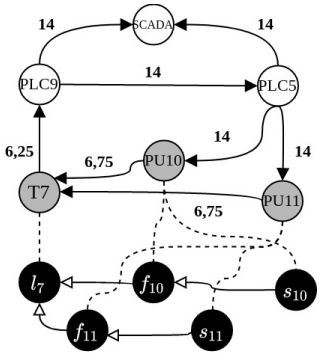

Fig. 3. Impact assessment of the anomaly propagation initiated by l_7

The assessment process is initiated by the anomaly detection on a node of a subsystem variable. Next, a list of associated subsystem variables that could be impacted by the identified anomaly is obtained from the graph analysis. As shown in Tab. II, the resulting PSV is calculated for each anomaly detection. Then, the propagation evaluation starts on the subsystem node associated to the node variable where the anomaly was detected applying a quality metric. The anomaly propagation is assessed for all paths of the given graph. A propagation impact rate is calculated for each edge of the first and second layers of the graph. This rate highlights the possible anomaly impact on a subsystem and its propagation likelihood.

Fig. 3 depicts an application example of the described approach for the simplified study case. An anomaly is detected on the level node (l_7) of tank 7:

- On the system variables layer: no other variable is impacted.
- On the digital and physical subsystem layers: the anomaly propagation is initiated from T7, the subsystem node associated with l_7. Therefore, each propagation path impact score PIS needs to be calculated as defined in equation (5).

V. Results and discussion

Four functional scenarios –denial of service (DoS), sensor offset alteration, false data injection, and replay attack– on which the water storage and distribution network is altered by

TABLE I
SCENARIO DESCRIPTIONS

Scenario	Anomaly triggering			Anomaly description		
	Condition	Begin	End	Type	Target	Impacted security criteria
1	Time	50h	144h	DoS	**Digital layer**: communication between PLC1 and PLC2 (l_1 tank-level exchange)	Availability
2	Time	30h	144h	Offset	**Physical layer**: l_7 tank level	Integrity
3	Tank 3 level	$l_3 \leq 3$	144h	False data injection	**Physical layer**: PU4 and PU5 pump stopping	Integrity
4	Time	50h	144h	Replay attack	**Digital layer**: communication between PLC4 and SCADA	Integrity

an attacker, like overflow or low-level of a tank, were designed to evaluate the proposed anomaly propagation impact assessment model (Table I). Each scenario extends during 144 hours and corresponds to a specific type of cyber-attack initiated on the digital or physical layer. Anomaly triggering conditions are time-based (scenarios 1, 2, and 4) or depending on a particular value reading (scenario 3). Changes in the quality metrics at a given time t, associated to system variable nodes detect anomalies. The main results of these four experiments are summarized in Table II.

In the first scenario, an adversary floods the PLC2-to-PLC1 communication link, until unavailability, with a **denial of service (DoS)** attack and impedes PLC1 to receive the T1 tank-level value (l_1) from PLC2. It causes an altered state change of PU1 and PU2 pumps, detected by the information coherence evaluation ed_{coh}=$true$ (anomaly propagation step 1, and step 2) at $t = 57h$ and $t = 79h$ of PU1 and PU2. This initial anomaly detection on the system variable layer, points towards a possible impact on T1 tank level (l_1). A T1 overflow is detected later (propagation step 3) with T1 cd_{err}=$true$, when T1 reaches its maximum level at $t = 79,9h$. The ensuing anomaly verification impact time Δt is calculated as: $\Delta t = t_2 - t_1 = 79,6 - 57 = 22,6h$. In this case, the proposed model estimation of the T1 tank overflow is confirmed **22,6 hours** later. Table III shows the most critical propagation impact scores for each step of scenario 1.

In the second scenario, an attacker impacts the l_7 tank-level integrity by adding a constant **offset**. As shown in Fig. 3, the l_7 value is transmitted from PLC9 to PLC5 for T7 level control through the PU10 and PU11 pumps. This integrity alteration generates a wrong pump state switch and has a critical impact on the T7 tank level. As a consequence, T7 overflow is detected through its associated erroneous information evaluation cd_{err} at $t = 30h$. This anomaly has no impact on any other subsystems.

In the third scenario, the PU4 and PU5 pumps are forced to an improper state with a **false data injection**. Their integrity is impacted with a constrained state that differs from the process control needs, based on T3 tank level (l_3). A first anomaly detection at PU4 ed_{coh}=$true$ enables the propagation assessment on the system variables layer, leading to a potential impact on the T3 tank level (l_3). Another anomaly is detected at PU5 ed_{coh}=$true$. A low condition level is later detected with T3 cd_{err}=$true$. As a result the estimated propagation path is confirmed $\Delta t = \mathbf{9,8}$ **hours** later.

In the fourth scenario, the attacker snoops the communication link between PLC4-to-SCADA, then analyzes the data, and stores the T3 tank level (l_3) during the first five hours. Next, the attacker channels again these readings with a random added value until the end of the simulation. This **replay attack** is too complex to be identified with the applied information quality analysis. To detect this kind of attack, a more elaborated quality metric should be implemented.

Obtained results show similar weights for various subsystems of the studied CPS because of several factors. On the one hand, an equivalent security criterion is applied homogeneously on the whole CPS system. On the other hand, given the simulated experimentation conditions and the ensuing lack of operational knowledge about the tested subsystems, several assumptions were adopted to define the risk assessment. Finally, although the approach was globally defined for the whole water supply network, it could have been specifically defined for each subsystem of the network, in accordance with the respective operational constraints. It is important to note that a comparison of the results with other approaches is far from evident, since the examined components, dependencies, and metrics differ considerably. For instance besides system variables, our approach considers both the digital and physical system layers, as well as all the concerned CPS subsystems and interdependencies, instead of focusing only on the well-known CPS physical behavior [11]. For the same reason, the applied propagation risk assessment metrics differ with respect to recently published works [8].

VI. CONCLUSION AND FUTURE DIRECTIONS

Modern ships are defined as highly interconnected complex systems and due to domain specificities, modelling of these interconnections to evaluate anomaly propagation through the multiple CPS components is very demanding. Yet, automatic anomaly propagation impact assessment in CPS is fundamental to identify evaluate, and anticipate the possible impact of an anomalous event in a highly interconnected multilayer network. In the case of a naval water distribution CPS, in some cases such propagation can affect the entire system with irreversible consequences.

TABLE II
RESULTS OF SCENARIOS CORRESPONDING TO THE FIRST ANOMALY PROPAGATION IMPACT ASSESSMENT PROCESS

Scenario	Anomaly propagation step 1		Anomaly propagation step 2		Anomaly propagation step 3		AVIT
	Detection	PSV	Detection	PSV	Detection	PSV	Δt
1	ed_{coh} = true t = 57 h	$s_2 \rightarrow f_2 \rightarrow l_1$	ed_{coh} = true t = 79 h	$s_1 \rightarrow f_1 \rightarrow l_1$	cd_{err} = true t = 79,6 h	l_1	**22,6 h**
2	cd_{err} = true t = 30 h	l_7	n/a n/a	n/a	n/a n/a	n/a	n/a
3	ed_{coh} = true t = 3,9 h	$s_4 \rightarrow f_4 \rightarrow l_3$	ed_{coh} = true t = 11,3 h	$s_5 \rightarrow f_5 \rightarrow l_3$	cd_{err} = true t = 13,7 h	l_3	**9,8 h**

PSV: Propagation on system variables; AVIT: Anomaly verification impact time

TABLE III
SCENARIO 1: MOST CRITICAL PROPAGATION PATHS AND SPECIFIC STEP PIS

Step	Propagation path	PIS
1	PU2-T1-PLC2-PLC1-PU1-T1	47,75
2	PU1-T1-PLC2-PLC1-PU2-T1	47,75
3	T1-PLC2-PLC1-PU1-T1 T1-PLC2-PLC1-PU2-T1	41 41

The proposed approach evaluates anomaly propagation risk according to naval water distribution CPS specificities, namely the abstraction of physical and digital components, related to the corresponding system variables, modeled in a three layers directed graph. Whereas anomalies are detected by means of information quality evaluations, the propagation risk assessment is achieved applying the prior knowledge-based weights that represent the likelihood of different components interdependencies to propagate an anomaly.

Three out of four anomalies propagation were assessed, with the confirmation of estimated propagation path when applicable. Even though the proposed representation model facilitates the implementation of diverse anomaly propagation scenarios, it is somewhat limited by the demanding task of verifying the exhaustiveness of CPS dependencies, particularly when those dependencies are not explicitly provided by the CPS manufacturer. Otherwise, risk assessment depends on expert knowledge, implying that anomaly propagation assessment results may differ from one expert to another. Nevertheless, the weighting process could be improved by the definition of complementary dynamic intrinsic information quality metrics depending on the trust granted to a given subsystem and its interdependencies. Also a unified knowledge base of risk assessment will reduce the possible variability of results.

REFERENCES

[1] O. Jacq, X. Boudvin, D. Brosset, Y. Kermarrec, and J. Simonin, "Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre," in *2018 2nd Cyber Security in Networking Conference (CSNet)*. IEEE, 2018, pp. 1–8.

[2] International Maritime Organization (IMO), "Guidelines on maritime cyber risk management," MSC-FAL.1/Circ.3. International Maritime Organization., 2017.

[3] S. Boccaletti, G. Bianconi, R. Criado, C. I. Del Genio, J. Gómez-Gardenes, M. Romance, I. Sendina-Nadal, Z. Wang, and M. Zanin, "The structure and dynamics of multilayer networks," *Physics Reports*, vol. 544, no. 1, pp. 1–122, 2014.

[4] R. M. Rooney, E. H. Cramer, S. Mantha, G. Nichols, J. K. Bartram, J. M. Farber, and P. K. Benembarek, "A review of outbreaks of foodborne disease associated with passenger ships: evidence for risk management," *Public health reports*, vol. 119, no. 4, pp. 427–434, 2004.

[5] Q. Zhu, L. Bushnell, and T. Başar, *Resilient Distributed Control of Multi-agent Cyber-Physical Systems*. Heidelberg: Springer International Publishing, 2013, pp. 301–316.

[6] H. Li, A. Dimitrovski, J. B. Song, Z. Han, and L. Qian, "Communication infrastructure design in cyber physical systems with applications in smart grids: A hybrid system framework," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1689–1708, 2014.

[7] 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*, vol. 23, no. 2, pp. 189–210, 2020.

[8] A. A. Malik and D. K. Tosh, "Quantitative risk modeling and analysis for large-scale cyber-physical systems," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, 2020, pp. 1–6.

[9] E. Pournaras, R. Taormina, M. Thapa, S. Galelli, V. Palleti, and R. Kooij, "Cascading failures in interconnected power-to-water networks," *SIGMETRICS Perform. Eval. Rev.*, vol. 47, no. 4, p. 16–20, Apr. 2020.

[10] Z. Yang, Y. Chen, and J. Marti, "Modelling cascading failure of a cps for topological resilience enhancement," *IET Smart Grid*, vol. 3, no. 2, pp. 207–215, 2020.

[11] H. Orojloo and M. A. Azgomi, "A method for evaluating the consequence propagation of security attacks in cyber–physical systems," *Future Generation Computer Systems*, vol. 67, pp. 57 – 71, 2017.

[12] C. Foglietta, D. Masucci, C. Palazzo, R. Santini, S. Panzieri, L. Rosa, T. Cruz, and L. Lev, "From detecting cyber-attacks to mitigating risk within a hybrid environment," *IEEE Systems Journal*, vol. 13, no. 1, pp. 424–435, 2019.

[13] X. Guan, B. Yang, C. Chen, W. Dai, and Y. Wang, "A comprehensive overview of cyber-physical systems: from perspective of feedback system," *IEEE/CAA Journal of Automatica Sinica*, vol. 3, no. 1, pp. 1–14, 2016.

[14] N. Pelissero, P. Merino Laso, and J. Puentes, "Naval cyber-physical anomaly propagation analysis based on a quality assessed graph," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2020, pp. 1–8.

[15] Y. Wang, Z. Xu, J. Zhang, L. Xu, H. Wang, and G. Gu, "Srid: State relation based intrusion detection for false data injection attacks in scada," in *Computer Security - ESORICS 2014*, M. Kutyłowski and J. Vaidya, Eds. Springer, 2014, pp. 401–418.

[16] P. Merino Laso, D. Brosset, and J. Puentes, "Monitoring approach of cyber-physical systems by quality measures," in *International Conference on Sensor Systems and Software*. Springer, 2016, pp. 105–117.

[17] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems," *Journal of Water Resources Planning and Management*, vol. 143, no. 5, p. 04017009, 2017.