

Grey-Box Models for Cyber-Physical Systems Reliability, Safety and Resilience Assessment

Juan-Pablo Futalef

Energy Department, Politecnico di Milano, Italia. E-mail: juanpablo.futalef@polimi.it

Francesco Di Maio

Energy Department, Politecnico di Milano, Italia. E-mail: francesco.dimaio@polimi.it

Enrico Zio

Energy Department, Politecnico di Milano, Italia; Centre de Recherche sur les Risques et les Crises (CRC), MINES Paris PSL, France. E-mail: enrico.zio@polimi.it

Cyber-Physical Systems (CPSs) integrate physical components with cybernetic elements. Modeling the complex interactions that arise among these is necessary to realistically represent the physical processes, the interconnections among physical components and cybernetic elements, and the data transmission within the cyber network. The computational effort needed for the solution of such a model challenges the CPSs reliability, safety and resilience assessment, which implies simulating a large number of scenarios. Grey-Box Models (GMB), which combine physics-based and data-driven models, offer a way to tackle the problem, while keeping model accuracy and preserving interpretability. In this work, we elaborate on a hierarchy-based architecture of literature to develop a systematic methodology in support of the development of GBMs for CPSs. The methodology is exemplified by developing the GBM of an Integrated Power-Telecommunication (IP&TLC) CPS infrastructure.

Keywords: Cyber-physical systems reliability, safety and resilience; grey-box modeling; physics-guided machine learning; smart power grids.

1. Introduction

Systems that integrate Cyber Elements (CEs) of a Cyber Network (CN) and Physical Elements (PEs) of a Physical Network (PN), such as shown in Figure 1, are known as Cyber-Physical Systems (CPSs) (Derler et al., 2012). Many benefits are expected to arise from this integration, like a wide reliance on Integrated Power-Telecommunication (IP&TLC) and Internet of Things (IoT) for the control of important lifelines and smart assets.

Nonetheless, the integration may expose PNs, such as electric power grids and transportation systems, to unknown threats that must be identified for the sake of their reliability, safety and resilience (Zio, 2018), whose assessment requires modeling the entire system and identifying the uncertainties affecting its behavior (Zio, 2013). Modeling is not only challenging but also computationally demanding. Assumptions can be made to lower the computational burden, but most of them lead to oversimplifying the CPS model, which in turn may cause wrong decision-

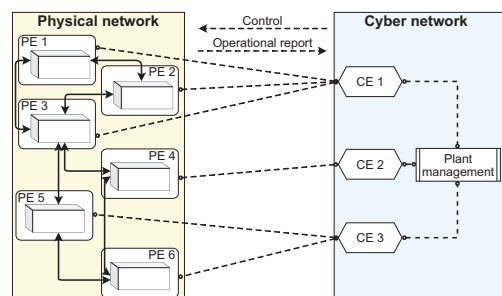


Fig. 1. Elements in a CPS

making and severe consequences during operation (Yohanandhan et al., 2020).

A CPS model must, in principle, mimic the actual process not only in normal conditions, but also under scenarios of failure of PEs and CEs, which can be stochastic or intentionally induced (Wang et al., 2019). Epistemic uncertainty arises due to noise and imperfect behavior of internal components, whereas aleatory uncertainty may come from sudden shock events, disconnections

or attacks.

For this, the use of *White-box Models* (WBM), based on first principles (An et al., 2015), can be difficult to build, given the complexity of CPSs and of the interdependent processes therein, so that the necessary level of realism may not be reached (Ljung, 2010). *Black-box Models* (BBMs), on the other hand, are purely based on data, making them appealing as they can learn the response of the system from field data (An et al., 2015). However, representative data sets can be difficult to obtain due to technical and economical reasons, and even if the data were representative, BBMs would provide little prediction capabilities outside the data domain and little interpretability (Larose and Larose, 2014). *Grey-box Models* (GBMs) combine WBMs and BBMs, aiming to exploit their benefits in an integrated manner (Bohlin, 2006; Karpatne et al., 2017), for example, by a virtuous loop that uses data for WBM calibration and its outcomes for BBM training (Rai and Sahu, 2020; Arias Chao et al., 2022).

Regardless of the modeling approach adopted, the CPS model should comprehensively describe all PEs and CEs, and their interdependencies. Drawing from automatic control theory, what is sought is *coordination* (Bemporad and Morari, 1999; Scattolini, 2009), typically achieved via hierarchical structures in which systems at different levels can operate with different dynamics. Such hierarchical structures are, indeed, appealing also for CPS modeling, as CE dynamics are discrete and slower than the continuous and faster dynamics of PEs.

Along this line, this work presents a methodology for the development of CPS GBMs that consists in mapping the CPS into a hierarchical structure, in which each layer contains PEs or CEs. This methodology provides guidelines on how WBMs and BBMs should be integrated into GBMs for modeling the CPS with the required accuracy, while preserving interpretability. Such architecture can be used to benchmark the effects on the safety, reliability and resilience assessment of the CPS when substituting some of the WBMs with BBMs in the GBM. An IP&TLC CPS infrastructure (Di Maio et al., 2022) is used to illustrate the method, in which some WBMs of the electrical components (i.e., PEs) and the control units (i.e., CEs) are replaced by BBMs. Then, the

benefits of GBMs are discussed.

The paper is organized as follows. Section 2 presents a short review on challenges and methods currently used for CPS modeling. Section 3 develops the hierarchical CPS structure which supports the construction of the CPS GBM. Section 4 provides the application. Finally, Section 5 concludes about the work and lists future research tasks.

2. Modeling Cyber-Physical Systems

Modeling the dynamics of internal elements in the CPSs and their coupling is challenging. A CPS is a hybrid system that combines continuous and discrete dynamics, where non-linearities and uncertainty sources should be considered due to the integration of a PN of interconnected PEs, and a CN of CEs that communicate among each other (Bemporad and Morari, 1999; Derler et al., 2012).

2.1. The Physical Network

A PN is a collection of PEs that interact between each other by exchanging energy or mass by means of some physical coupling. A PN can be modeled as a network of objects $G_P = (P_E, E_P)$, where $P_E = \{1, \dots, n_{P_E}\}$ is the set of network nodes and E_P is the set of network links. A node is characterized by its own dynamic model $\mathcal{S}_{[i]}$, containing a set of n_i^x state variables, grouped in a state vector $\mathbf{x}_{[i]} \in \mathbb{R}^{n_i^x}$, in which the explicit time dependence is dropped to simplify notation. A set of nonlinear differential equations can be therefore used to describe the dynamics of $\mathcal{S}_{[i]}$ (Lygeros et al., 1996; Ding et al., 2019):

$$\mathcal{S}_{[i]} \begin{cases} \dot{\mathbf{x}}_{[i]} = \mathbf{f}_{[i]}(\mathbf{x}_{[i]}, \mathbf{u}_{[i]}, \boldsymbol{\xi}_{[i]}, \boldsymbol{\omega}_{[i]}) \\ \mathbf{y}_{[i]} = \mathbf{g}_{[i]}(\mathbf{x}_{[i]}, \mathbf{u}_{[i]}, \boldsymbol{\rho}_{[i]}), \end{cases} \quad (1)$$

where $\mathbf{f}_{[i]}(\cdot)$ is the vector-wise state transition function, $\mathbf{u}_{[i]} \in \mathbb{R}^{n_u}$ is the input, $\boldsymbol{\xi}_{[i]} \in \mathbb{R}^{n_\xi}$ is the coupling input, $\boldsymbol{\omega}_{[i]}$ is the process noise, $\mathbf{y}_{[i]}$ is the subsystem output, $\mathbf{g}_{[i]}(\cdot)$ extracts the output from the internal state vector, and $\boldsymbol{\rho}_{[i]}$ is the output noise. Functions $\mathbf{f}_{[i]}(\cdot)$ and $\mathbf{g}_{[i]}(\cdot)$ should include the laws and effects of controllers, such as PI-PID, on the PEs (Ding et al., 2019). Advanced techniques, such as Model Predictive Control (MPC) (Scattolini, 2009; Prodan and Zio, 2014) or game theory (Lygeros et al., 1996; Fang and Zio, 2019; Wang et al., 2019), can be considered, although they increase the model complexity.

Also, addressing non-continuous behaviors and stochasticity challenges the reliance on WBM (Rai and Sahu, 2020). Linearization may reduce the model complexity, but, at the same time, it may oversimplify the model, making WBMs not suitable for reliability, safety and resilience assessment of CPSs.

2.2. The Cyber Network

A Cyber Network (CN) is a collection of Cyber Elements (CE), where each CE is a digital device running an algorithm. These algorithms aim at processing collected information from the PEs via a cyber-physical link (see Section 2.3) for the sake of decision-making on the control of the PN.

Similar to a PN, a CN can be described as a fully-connected network object $G_C = (C_E, E_C)$, in which the set of nodes C_E are digital devices, and the arcs E_C represent channels of communication among them. These channels of communications form the Telecommunication Network (TLCN), defined as a weighted undirected graph $G_T = (V_T, A_T)$, where V_T is the set of nodes and E_T is the set of arcs. V_T contains all TLC devices in the TLCN and the CEs in the CN. The connection through an arc implies the ability of two (or more) devices linked through that arc to communicate.

As CEs are connected to TLC devices, a path can be developed so that the information flows between CEs. The Open Shortest Path First (OSPF) protocol is commonly used to define paths from origin to destination (Pióro et al., 2002). This method can be complimented with Shortest Path Problem (SPP) solvers, like Dijkstra's method, to optimize the path creation (Pióro et al., 2002). In some occasions, some TLC devices may become unavailable or time delays may increase (or decrease) due to information packages traffic (Paxson and Floyd, 1995).

Typical WBMs used to model CE dynamics are, to name a few, Finite State Machines (FSM) (Clarke et al., 1986), statecharts (Harel, 1987), and Petri Nets (PN) (Murata, 1989). FSM and statecharts aim to characterize the internal transition of the CE states, although statecharts generalize FSM by embedding models into models.

2.3. The Cyber-Physical Link

The cyber-physical link provides a bidirectional interaction between the PN and the CN. CEs

can collect measurements from the PN, whereas controlled PEs get their corresponding set points (Derler et al., 2012; Yohanandhan et al., 2020).

The *physical-to-cyber* link is achieved via a transducer and circuitry that turns physical quantities into digital signals. The key device is an analog-to-digital converter (ADC) that turns analog voltages from the transducer into bytes. This information is, then, sent to the corresponding CEs for measurement collection and processing. Both the transducer and ADC impact the quality of measurements by introducing noise, limiting the range and resolution of measurements, and fixing a sampling time.

On the other hand, the *cyber-to-physical* link is possible thanks to a digital-to-analog converter (DAC) and an actuator. Designated CEs calculate suitable set points for those PEs that can be controlled. Then, these set points are sent to the target PEs using the TLCN. Finally, the DAC turns the corresponding signal into the desired analog value. Similarly to an ADC, a DAC provides a limited resolution, operating range and sampling time. Besides, imperfect circuitry may introduce input noise into the system.

An Intelligent Electronic Device (IED) embeds both link types and connects them to the TLCN, as shown in Figure 2. On the left-hand side, the PE $\mathcal{S}_{[i]}$ follows the continuous dynamics from Eq. (1), in which the IED provides an input $u_{[i]}(t)$ and samples the output $y_{[i]}(t)$. On the right-hand side, $\bar{u}_{[i]}(k)$ and $\bar{y}_{[i]}(k)$ are their discrete-time representations, which are shared via the TLCN with CE $\mathcal{C}_{[j]}$, where $i \neq j$. Therefore, the IED acts as another TLC agent that can send and receive information from other CEs. It is reasonable to assume that all PEs in the PN are equipped with an IED so that measurements from all PEs can be obtained, although an IED only provides a DAC interface on those elements that can be controlled.

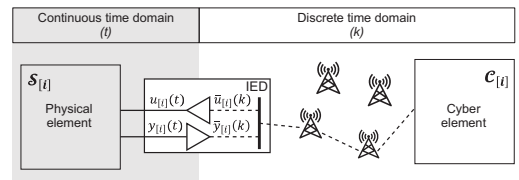


Fig. 2. An IED embeds all necessary components to implement the cyber-physical link

3. The Hierarchical Architecture to Model the CPS

Hierarchical structures are useful to organize the information flow and coordinate the agents in distributed systems (Scattolini, 2009; Ding et al., 2019): elements at some level of the hierarchy aim at giving (receiving) inputs to (from) the elements at the immediate closer level of the hierarchy. At the top of the CPS hierarchy is placed the plant management device that controls the entire operation of the system, whereas at the bottom of the hierarchy, multiple elements operate based on the inputs provided by the intermediate CEs, as shown in Figure 3. Among the CEs, we mention the Control Units (CUs), that gather measurements from a set of PEs and provide suitable inputs to those PEs that can be controlled. The structure allows clusters of PEs to be directly connected to specific CEs.

More levels can be added to the structure: the rule is to properly categorize the time response of systems and controllers. At the bottom layers, controllers tend to be simpler and faster, i.e. PI-PID. On the other hand, controllers at higher levels are slower as they aim at optimizing the overall operation, i.e. MPC or intelligent control techniques. For the case in Figure 3, the bottom layer contains the PEs of the CPS, which typically embed continuous-time controllers. At the second layer, the CUs operate in discrete time and aim to provide the desired set points to PEs or controllers in the PEs. The set points come from simple calculations according to instructions given by the plant management device. This device at the top level also operates in discrete time, performing high burden calculations. As a result, its time response is slower to those devices in the second layer.

As shown in Figure 3, by using the architecture, the information flow between elements is clearly defined: if WBM are available for each element of the hierarchy, one can develop the higher level models based on the constraints imposed by lower level models, i.e., *bottom-up*. This procedure yields an explicit IO characterization of the elements in the hierarchy, enabling its simulation.

As mentioned earlier, linearization should be avoided to lower the complexity of CPS. Then, the hierarchical structure can be used to guide the GBM development, in which some elements (either cyber or physical) are replaced by BBMs.

Appropriate criteria should be used to pick which elements are replaced. For example, typical system identification methods (Ljung, 2010) may be applied when access to sufficient data is confirmed, such that replacing a WBM by a BBM is justified. In general terms, different alternative ways to build a GBM can be envisaged, as we shall discuss along with the case study in Section 4. The unifying rationale among the alternatives is that each one of these must:

- account for the sources of uncertainty that impact the normal and abnormal system operation (Di Maio et al., 2020);
- allow the operational performance to be characterized by Key Performance Indicators (KPIs) that provide an insight of the operational quality for a given operational scenario (Wang et al., 2022);
- be capable of integrating Uncertainty Quantification (UQ) techniques to estimate the Probability Density Functions (PDFs) necessary to calculate the KPIs for reliability, safety and resilience assessment (Zio, 2007).

In all cases, the differences among the CPS element failure modes are to be modeled properly (Wang et al., 2018, 2020; Yaacoub et al., 2020):

Physical Network. Poorly implemented protections, sudden natural events, wrong human operation and vandalism may accelerate degradation of PEs and increase their probability of failure. As PEs are tightly connected, the failure of a single PE may trigger cascading effects on the entire CPS.

Cyber-physical link An IED may fail due to anomalous conditions of the sensors, actuators and the TLCN. IEDs are also exposed to cyber attacks that can either alter or remove the original signals between sensors and actuators, potentially disrupting the entire CPS. Also, the TLCN may fail due to transmission delays and package losses.

Cyber Network. CEs are exposed to cyber threats, in which attackers can modify the settings of controllers and the hyper-parameters of internal procedures, leading to Denial of Service (DoS) (Khan and Salah, 2018).

Such a variety of failure modes requires sophisticated coordinated techniques, making the hierarchy approach from Section 3 handy.

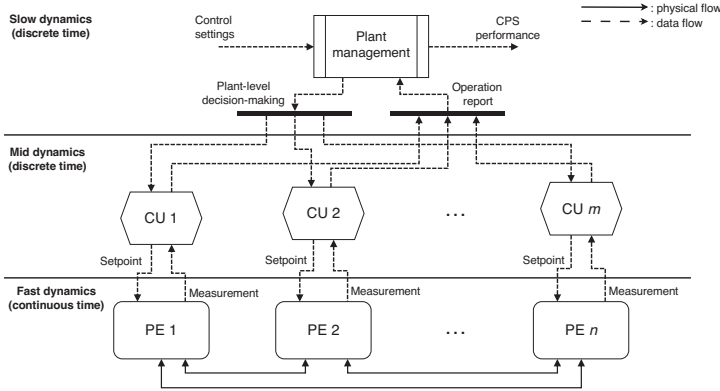


Fig. 3. Graphical representation of a hierarchical CPS infrastructure

4. Case Study

4.1. The Integrated-Power Telecommunication Grid

The hierarchical structure that guides the GBM construction for a CPS is exemplified using a IP&TLC infrastructure of literature (Di Maio et al., 2022). It consists of the IEEE14^a power grid equipped with sensors and cyber elements that collect measurements for monitoring and control. The electrical diagram of the power grid is displayed in Figure 4a and consists of two power generators, twelve loads, three transformers, and three synchronous condensers for proper grid operation. From a CPS perspective, this diagram represents the PN of the CPS.

The physical-to-cyber link is provided by Phasor Measurement Units (PMU) installed on all buses. The cyber-to-physical link exists via the actuators in the power generators at buses one and two. The grid is divided into six zones as shown in Figure 4a. Each zone is assigned to a Phasor Data Concentrator (PDC) that collects the measurements from the PMUs and provides control inputs to the power generators, as depicted in Figure 4b. The PDCs send the measurements via the TLCN to a Control Center (CC) in charge of monitoring and controlling the entire power grid.

The hierarchical Integrated-Power Telecommunication (IP&TLC) infrastructure is created by providing all necessary elements mentioned

above. CUs are the PDCs, whereas the plant-level management device is the CC. Figure 4c exemplifies the flow of information through the levels of the hierarchy. First, the PMUs measure voltage, phase and power consumption of the bus they are connected to. In this step, the continuous-time outputs $y_1(t)$ and $y_2(t)$ of buses 1 and 2, respectively, are represented as discrete time measurements $z_1(k)$ and $z_2(k)$. Then, these values go up in the hierarchy and reach PDC 1, which puts them into the measurements vector \mathcal{Z}_1 . This vector is, then, sent to the CC, which processes it and solves the Optimal Power Flow (OPF) problem to obtain optimal control inputs for the generators.

4.2. Grey-box Models: alternatives

Figure 5a shows the most direct approach, in which the original WBM of two PEs are replaced by BBMs. In Figure 5b, PEs have been grouped into clusters according to their assigned CU. Then, a BBM is constructed for each PE cluster. Figure 5c integrates a multi-layer BBM, which embeds CEs and PEs that are interconnected. Figure 5d turns WBMs of either physical or cyber elements on different levels into BBMs.

In the scope of risk assessment, the interest is in extreme or low-probability scenarios so that some topologies may fit the scope better than others. Nevertheless, in all cases we keep a balance between WBMs and BBMs to limit, on one hand, the lack of extrapolation capabilities of BBMs (that are compensated by the WBMs in input domains of interest where BBMs cannot) and, on the other hand, the computational demand of WBMs (that is lowered by the adoption of BBMs). In any case, a

^aIEEE14 power grid, with full description at http://labs.ece.uw.edu/pstca/pf14/pg_tcal4bus.htm.

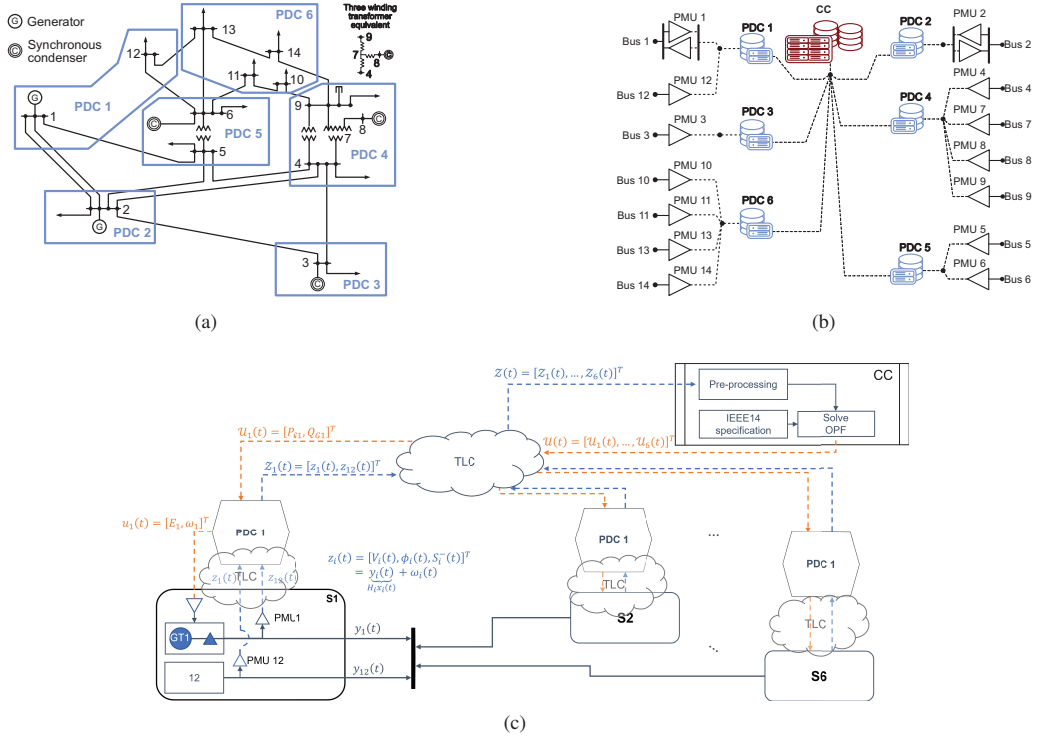


Fig. 4. IEEE14 CPS description. In (a), description of the PN considering the IEEE14 components. In (b), scheme of the CEs interconnection according to the zones shown in (a) and an example of data transfer over the TLCN. Finally, in (c), example of the flow of information from bottom-up and top-down

validation-verification procedure that enables the selection of the model is essential to properly place BBMs according to the model requirements.

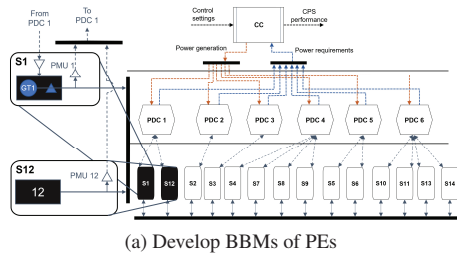
Until now, no comparison metrics are being agreed on among the scientific community. For example, Mean Absolute Error (MAE) or Root Mean Square Error (RMSE) can be used, although these metrics may be too much dependent on the quality of the available data; Bayesian measures, like the Bayes factor (Berger and Pericchi, 1996), account for both data and model belief, making them more appealing for GBM quality assessment (Rai and Sahu, 2020). Value of Information (VoI), a Bayesian-based method to evaluate the improvements of a priori knowledge via new information (Hoseyni et al., 2021), may also result useful for discerning whether the reliance on additional BBMs or WBMs may be beneficial for GBM developments.

From a qualitative point of view, we expect that the structure in Figure 5d will provide the

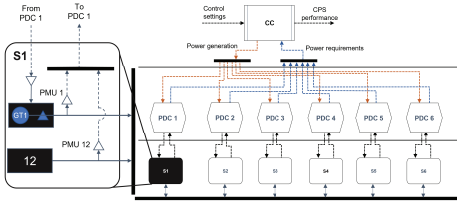
best trade-off between computational burden and quality of Input-Output (IO) response estimations. This reasoning is supported by the hypothesis that a sparse assignment of WBMs and BBMs (avoiding preferential bias towards one or the other type of model for specific components) can provide sufficiently accurate and computationally viable solutions, without losing interpretability in case the whole GBM is not satisfactory. To verify this, the IO response must be compared to that obtained from detailed WBMs, aiming to observe a reduction of simulation times, while maintaining model accuracy. Still, this approach is also the most difficult to implement due to the great number of models and combinations to be considered, which promotes the idea of studying the other CPS GBM alternatives.

5. Conclusions and Future Work

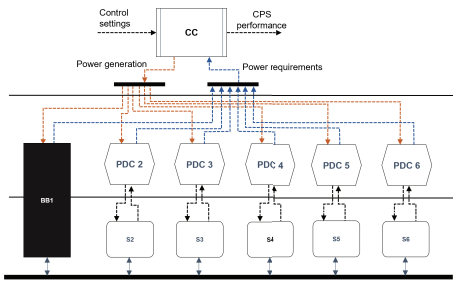
This work introduces a generalized methodology to construct Cyber-Physical System (CPS) Grey-



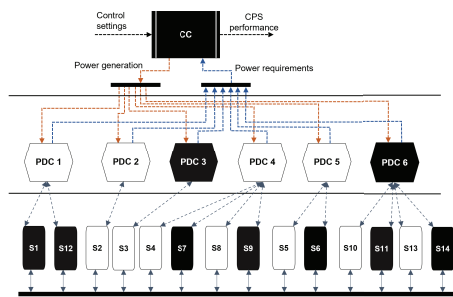
(a) Develop BBMs of PEs



(b) Group PEs into zone-based clusters and construct BBMs of those clusters



(c) Consider multi-layer BBMs that embed PEs and CEs into a single model



(d) Consider BBMs of single elements at different levels

Fig. 5. Multiple alternatives to develop a CPS GBM with applications to the IEEE14 bus system

box Models (GBM) for enabling the Reliability, Safety and Resilience assessment of CPSs. First, the CPS is represented by a hierarchical architecture, in which devices at a level of the hierarchy control devices in the level immediately below

them. This representation organizes the flow of information enabling to coordinate the elements in the CPS. Then, elements in the hierarchy may be replaced by BBMs, depending on the benefits they provide or the costs incurred in replacing them. The methodology is exemplified via a IP&TLC infrastructure. Future work tasks involve addressing proper GBM selection metrics, creation of ground-truth data sets, and benchmarking comparison of the different GBM alternatives.

Acknowledgement

The work presented in this paper has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 955393.

References

- An, D., N. H. Kim, and J. H. Choi (2015). Practical options for selecting data-driven or physics-based prognostics algorithms with reviews. *Reliab. Eng. Syst. Saf.* 133, 223–236.
- Arias Chao, M., C. Kulkarni, K. Goebel, and O. Fink (2022). Fusing physics-based and deep learning models for prognostics. *Reliab. Eng. Syst. Saf.* 217.
- Bemporad, A. and M. Morari (1999). Control of systems integrating logic, dynamics, and constraints. *Automatica* 35(3), 407–427.
- Berger, J. O. and L. R. Pericchi (1996, mar). The Intrinsic Bayes Factor for Model Selection and Prediction. *J. Am. Stat. Assoc.* 91(433), 109–122.
- Bohlin, T. (2006). *Practical Grey-box Process Identification: Theory and Applications*, Volume 1.
- Clarke, E. M., E. A. Emerson, and A. P. Sistla (1986, apr). Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications. *ACM Trans. Program. Lang. Syst.* 8(2), 244–263.
- Derler, P., E. A. Lee, and A. Sangiovanni Vincenzelli (2012). Modeling cyber-physical systems. *Proc. IEEE* 100(1), 13–28.
- Di Maio, F., R. Mascherona, and E. Zio (2020). Risk Analysis of Cyber-Physical Systems by GTST-MLD. *IEEE Syst. J.* 14(1), 1333–1340.
- Di Maio, F., A. Stincardini, and E. Zio (2022). Identification of Vulnerabilities in Integrated Power-Telecommunication Infrastructures: A

- Simulation-based Approach. In *32nd Eur. Saf. Reliab. Conf.*
- Ding, D., Q. L. Han, Z. Wang, and X. Ge (2019). A Survey on Model-Based Distributed Control and Filtering for Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Informatics* 15(5), 2483–2499.
- Fang, Y. and E. Zio (2019). Game-Theoretic Decision Making for the Resilience of Interdependent Infrastructures Exposed to Disruptions BT - Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies. pp. 97–114. Cham: Springer International Publishing.
- Harel, D. (1987). Statecharts: a visual formalism for complex systems. *Sci. Comput. Program.* 8(3), 231–274.
- Hoseyni, S. M., F. D. Maio, and E. Zio (2021, jan). Optimal sensor positioning on pressurized equipment based on Value of Information. *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.* 235(4), 533–544.
- Karpatne, A., G. Atluri, J. H. Faghmous, M. Steinbach, A. Banerjee, A. Ganguly, S. Shekhar, N. Samatova, and V. Kumar (2017). Theory-guided data science: A new paradigm for scientific discovery from data. *IEEE Trans. Knowl. Data Eng.* 29(10), 2318–2331.
- Khan, M. A. and K. Salah (2018). IoT security: Review, blockchain solutions, and open challenges. *Futur. Gener. Comput. Syst.* 82, 395–411.
- Larose, D. T. and C. D. Larose (2014). Multivariate Statistics. In *Discov. Knowl. Data* (2nd ed.), Chapter 5, pp. 109–137. John Wiley & Sons, Inc.
- Ljung, L. (2010). Perspectives on system identification. *Annu. Rev. Control* 34(1), 1–12.
- Lygeros, J., D. N. Godbole, and S. Sastry (1996). A game-theoretic approach to hybrid system design BT - Hybrid Systems III. Berlin, Heidelberg, pp. 1–12. Springer Berlin Heidelberg.
- Murata, T. (1989). Petri nets: Properties, analysis and applications. *Proc. IEEE* 77(4), 541–580.
- Paxson, V. and S. Floyd (1995). Wide area traffic: the failure of Poisson modeling. *IEEE/ACM Trans. Netw.* 3(3), 226–244.
- Pióro, M., Á. Szentesi, J. Harmatos, A. Jüttner, P. Gajowniczek, and S. Kozdrowski (2002). On open shortest path first related network optimisation problems. *Perform. Eval.* 48, 201–223.
- Prodan, I. and E. Zio (2014). A model predictive control framework for reliable microgrid energy management. *Int. J. Electr. Power Energy Syst.* 61, 399–409.
- Rai, R. and C. K. Sahu (2020). Driven by Data or Derived through Physics? A Review of Hybrid Physics Guided Machine Learning Techniques with Cyber-Physical System (CPS) Focus. *IEEE Access* 8, 71050–71073.
- Scattolini, R. (2009). Architectures for distributed and hierarchical Model Predictive Control - A review. *J. Process Control* 19(5), 723–731.
- Wang, W., A. Cammi, F. Di Maio, S. Lorenzi, and E. Zio (2018). A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. *Reliab. Eng. Syst. Saf.* 175, 24–37.
- Wang, W., G. Cova, and E. Zio (2022). A clustering-based framework for searching vulnerabilities in the operation dynamics of Cyber-Physical Energy Systems. *Reliab. Eng. Syst. Saf.* 222, 108400.
- Wang, W., F. Di Maio, and E. Zio (2019). Adversarial Risk Analysis to Allocate Optimal Defense Resources for Protecting Cyber-Physical Systems from Cyber Attacks. *Risk Anal.* 39(12), 2766–2785.
- Wang, W., F. Di Maio, and E. Zio (2020). Considering the human operator cognitive process for the interpretation of diagnostic outcomes related to component failures and cyber security attacks. *Reliab. Eng. Syst. Saf.* 202.
- Yaacoub, J.-P. A., O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli (2020, sep). Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsystems.* 77, 103201.
- Yohanandhan, R. V., R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa (2020). Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications. *IEEE Access* 8, 151019–151064.
- Zio, E. (2007). *An Introduction to the Basics of Reliability and Risk Analysis* (1st ed.), Volume 13. World Scientific Publishing Company.
- Zio, E. (2013). *The Monte Carlo Simulation Method for System Reliability and Risk Analysis* (1st ed.). Springer-Verlag London.
- Zio, E. (2018). The future of risk assessment. *Reliab. Eng. Syst. Saf.* 177, 176–190.