The DYNABIC approach to resilience of critical infrastructures

Erkuden Rios, Eider Iturbe, Angel Rego, Nicolas Ferry, Jean-Yves Tigli, Stéphane Lavirotte, Gérald Rocher, Phu Nguyen, Hui Song, Rustem Dautov, et al.

The DYNABIC approach to resilience of critical infrastructures

Erkuden Rios
TECNALIA Research Innovation, Basque Research and Technology Alliance (BRTA)
Derio, Spain
erkuden.rios@tecnalia.com

Eider Iturbe
TECNALIA Research Innovation, Basque Research and Technology Alliance (BRTA)
Derio, Spain
Faculty of Engineering, University of the Basque Country
Bilbao, Spain
eider.iturbe@tecnalia.com

Angel Rego
TECNALIA Research Innovation, Basque Research and Technology Alliance (BRTA)
Derio, Spain
angel.rego@tecnalia.com

Nicolas Ferry, Jean-Yves Tigli, Stéphane Lavirotte, Gérald Rocher
Université Côte d'Azur, I3S
Sophia Antipolis, France
name.surname@univ-cotedazur.fr

Phu Nguyen, Hui Song, Rustem Dautov
SINTEF
Oslo, Norway
name.surname@sintef.no

Wissam Mallouli, Ana Rosa Cavalli
Montimage EURL
Paris, France
name.surname@montimage.com

ABSTRACT

With increasing interdependencies and evolving threats, maintaining operational continuity in critical systems has become a significant challenge. This paper presents the DYNABIC (Dynamic business continuity of critical infrastructures on top of adaptive multi-level cybersecurity) approach as a comprehensive framework to enhance the resilience of critical infrastructures. The DYNABIC approach provides the resilience enhancement through dynamic adaptation, automated response, collaboration, risk assessment, and continuous improvement. By fostering a proactive and collaborative approach to resilience, the DYNABIC framework empowers critical infrastructure sectors to effectively mitigate disruptions and recover from incidents. The paper explores the key components and architecture of the DYNABIC approach and highlights its potential to strengthen the resilience of critical infrastructures using the concept of Digital Twins in the face of evolving threats and complex operating environments involving cascading effects.

KEYWORDS

Cybersecurity, Critical Infrastructure Protection, Digital Twin, SecDevOps

ACM Reference Format:
Erkuden Rios, Eider Iturbe, Angel Rego, Nicolas Ferry, Jean-Yves Tigli, Stéphane Lavirotte, Gérald Rocher, Phu Nguyen, Hui Song, Rustem Dautov, and Wissam Mallouli, Ana Rosa Cavalli. 2023. The DYNABIC approach to resilience of critical infrastructures. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation email (STAM '23).* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

STAM '23, September, 2023, Benevento, Italy

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Most of essential services in modern societies rely on Critical Infrastructures (CIs), which are large-scale complex cyber-physical systems (CPS). Due to their criticality, CIs must show a high level of resilience, i.e., they need to be *"able to withstand, adapt and quickly recover from all hazards whether natural or man-made"* [15]. These infrastructures are becoming more and more natural targets for attacks, and the new EU CER Directive [8] is born to be the definitive stimulus for European critical entities to be conscious of the need of protecting such infrastructures and pushing the hard work to protect them. In joint efforts with NIS 2 Directive [7], the CER Directive aims at reducing vulnerabilities in CIs and enhance their resilience. The directive requires that Member States identify the critical entities in Europe and that these entities ensure adequate technical, security and organisational measures are taken to protect their infrastructures and prevent incidents.

Today, CIs are largely leveraging software systems and the growing adoption of Internet of Things, Cloud, and Artificial Intelligence (AI) as integral part of the systems has opened the door to new cyber-physical attack vectors whose sophistication requires new approaches to CI resilience. Moreover, CIs do not work in isolation, but their services are interleaved with services of other CIs. A CI may depend on a third-party service provider or have hybrid capability. Therefore, it is of utmost importance to empower the operators of CIs (named *critical entities* in CER Directive) with means to predict the extent and ways business disruptions and cyber-physical damages can propagate between the critical infrastructure systems and from one CI to another. Improving the CI capacities at preparedness, detection and response phases requires attention to the human factor as well as the collaboration of heterogeneous organisations involved in the CI development and operation (e.g., using security orchestration platforms), ensuring a continuum of

care, just as it is done for other ICT systems with the adoption of SecDevOps approaches.

This paper first presents the DYNABIC research roadmap, identifying the key challenges in critical infrastructures to effectively prevent and mitigate disruptions and recover from incidents. We introduce an extension of the SecDevOps paradigm and discuss the related DYNABIC contributions to address these challenges, which will be realized into the DYNABIC Framework. This framework will be explored and further developed in the newly founded DYNABIC H2020 project that started in December 2022.

The remainder of the paper is organized as follows. Section 2 presents the research roadmap in terms of technical challenges and state-of-the-art. Section 3 details the overall DYNABIC approach, illustrates how it will help addressing these research challenges and describes the set of enablers that forms the core of the DYNABIC Framework. Finally, Section 4 concludes.

2 THE DYNABIC RESEARCH ROADMAP AND RELATED WORK

The strategic objective of DYNABIC is to increase the resilience and business continuity capabilities of European critical services in the face of advanced cyber-physical threats. This objective will be pursued by delivering new socio-technical methods, models, and tools to support resilience through holistic business continuity risk management and control in operation, and dynamic adaptation of responses at system, human and organization planes. More precisely, this objective is underpinned by the following research sub-objectives.

Research Objective 1: Methods and tools for disaster preparedness and the prevention of business continuity risks in cross-organisation and cross-domain incidents and attacks.

Context: Complex cyber-physical systems such as critical infrastructures are typically cross-organisations and involve stakeholders, services, and infrastructures from multiple domains. In order to prevent business continuity risks and prepare for disasters, it is important not only to monitor the system but also being able to simulate and analyse multiple types of potential attacks and disruptions. Virtual models of the physical systems, the so called Digital Twins (DTs), are thereby a perfect fit as a solution that, on the one side can reflect the status of the running system together with situational-awareness, and, on the other side, provides means to simulate the system and its interconnections. By recording history and actual values of cyber-physical system variables and status, DTs have the potential to allow predicting the possible propagation and impact of incidents across domains, organisations, and CIs.

State-of-the-art: As a new and fast developing technology, Digital Twins start to gain attention on the use for business continuity. A modern DT combines the simulation of the physical twin and the continuous collection of real-time data from it. The DT provides interfaces to both human operators and automatic analysis tools for real-time monitoring of the systems, timely analysis of data, and the scheduling of preventive maintenance to reduce or prevent downtimes [20]. The main advantage of DTs is that they allow the simulation of the system states ahead of the time based on the current system state, and they enable to predict potential problems [29] and to test the effectiveness of different interventions to the systems [17]. The state-of-the-art research include the so-called digital supply chain twin for the monitoring and prediction of supply chain risks[16] and their integration into the management decision systems. Some companies provide loosely coupled tool chains to facilitate DT development. For example, the Azure Digital Twins[1] platform combines a set of Azure services for IoT, data analytics and AI, under a standard Digital Twin Definition Language (DTDL). Despite the existence of plentiful use cases, there is a lack of systematic research on what a DT should contain and provide to fully support business continuity, beyond the classical monitoring and failure prediction operations.

Research Objective 2: Enable operators of CIs to predict, quantitatively assess, and mitigate in real-time business continuity risks and cascading effects in interconnected CIs.

Context: Business Continuity Management refers to the capability of organizations to keep their critical business processes working in the event of disruptive events [37]. As part of business continuity management, organizations must systematically implement procedures for business impact analysis and risk assessment. In the context of CIs, this must be done considering cascading effects across interconnected CIs.

State-of-the-art: There are multiple risks management methodologies and tools, such as CORAS [19] and OWASP RRM [26]. However, none of these tackles the challenge of managing risks dynamically nor do they leverage risks records [2]. On risk analysis itself, several approaches have been proposed such as Failure Mode and Effects Analysis (FMEA) [36], cause and effect (Ishikawa) charts, enhanced attack-defence trees (ADTs) [33] and Bayesian approaches. The last have been proved effective in risk analysis of industrial control systems (ICS) [30]. Bow-tie analysis [6] is becoming popular particularly in high-hazard industries. The approach proposes the combination of fault-tree and event-tree analysis to identify incident triggering events. However, the focus is on system layer analysis rather than on the analysis of the business process execution in real time. Regarding the evaluation of CIs' performance, few works consider consequence-based criteria (i.e., cross-cutting effects and interdependencies). For instance, in [38], the performance of an energy system is evaluated against hospital beds availability and mortality. There exists a number of gaps on monitoring CIs. First, resilience focuses on the consequences of disruptions rather than on their possibilities [18]. However, the majority of CI performance indicators proposed are built on specific reliability criteria that measure CIs performance against potential low impact/highly probable events, and therefore, their use to measure resilience is not recommended [32]. Second, most performance indicators do not take into account the time-dependency and context influence in the expected behaviour/outcome of CIs. Third, no unified framework exists of CI performance indicators which hinders comparison and aggregation. This is of particular importance considering that different stakeholders usually view performance from different perspectives, concerns [21] at different abstraction levels. Multiple approaches have been proposed for assessing cascading effects in

[1] https://azure.microsoft.com/en-us/services/digital-twins/#features

critical systems, which leverage Markov chains[31], interdependency graphs [35], etc. However, most models, besides suffering from indicators limitations explained above, fail to address the intrinsic uncertainty of cyber-physical incidents and they focus on propagation within systems, rather than between interconnected systems. In DYNABIC the goal is to design and develop DT that enable business disruption risks analysis and their real-time assessment on top of quantitative indicators as much as possible. The risk assessment shall include the propagation of the risks to other CIs interconnected to the CI under study.

Research Objective 3: Dynamic autonomous adaptation of critical infrastructures to meet resilience goals with personalized assistance in human tasks.

Context: CIs are typically exposing a large surface attack and their integration of Internet of Things, Cloud, and Artificial Intelligence services is opening for novel attack vectors. Manual handling and response to these attacks is an overwhelming task that cannot effectively be handled by SecDevOps teams. Thereby, automation and self-healing mechanisms are key to improve efficiency, accuracy and speed of response. Digital Twins are an essential ingredient for such mechanisms as they provide abstractions and models of the running system and offer means to understand and simulate the possible impact of a threat or attack and to explore possible responses.

State-of-the-art: Recently, frameworks based on Digital Twins have been proposed for building smarter, resilient and trustworthy CPS that can self-monitor, self-diagnose and ultimately self-heal. The conceptual framework proposed by Flammini[13] leverages DT run-time models that focus on data-driven evaluation and prediction of critical dependability attributes such as safety. Parriet al. [28] propose using a DT-based reflective architecture to represent and control system structural aspects with reliability requirements, which can be automatically derived from SysML Block Definition Diagrams. Their DT-empowered framework aims to equip remote actuation capabilities, enabling both recoverability and adaptability in a proactive way. There are also domain-specific infrastructure layer self-healing approaches, such as the one dedicated to smart grids by Colson et al. [3], which utilizes smart microgrid control agents that cooperate during normal and emergency situations to improve power system resiliency. Online reinforcement learning (RL) [1] enables to create self-adaptive systems able to adapt to a dynamically changing environment to maintain the system's security and quality requirements[1]. Since design time uncertainty hinders the efficiency of the runtime adaptation logic [39], online RL is employed to make the system learn the self-adaptation logic automatically at runtime [34]. After a predefined adaptation reward function is defined, distributed RL agents continuously interact with the environment applying actions and sensing their effects on system status. The goal is to obtain the optimal policy, i.e., the function that maximizes the cumulative reward of an action sequence. Deep RL uses Neural Networks (NN) to represent the learned policy. For instance, Deep Q-Network (DQN) algorithm enhances the RL Q-learning algorithm with DNN. However, there are two major drawbacks. First, online RL agents need to be trained before they are used at runtime to avoid them to take arbitrary actions, which is very risky, particularly when controlling Cyber-Physical Systems. Second, Deep RL requires large amounts of training data [22]. Initial attempts to overcome agents training and solution space scalability in security orchestration problem have been proposed [22].

Research Objective 4: Facilitate the coordinated vulnerability and threat information disclosure across the EU.

Context: Vulnerability and threat information sharing and disclosure is key to strengthen cybersecurity in EU as finders of vulnerabilities and threats should work and share information with the relevant stakeholders. This is particularly relevant in the context of critical infrastructures, which can be interconnected and are typically cyber-physical systems with entities from multiple stakeholders. The Proposal of NIS Directive 2.0 establishes the policies for both coordinated vulnerability disclosure between entities, and a two-stage reporting of incidents to competent authorities. Therefore, CI operators face a double challenge: voluntary information sharing and timely incident reporting.

State-of-the-art: Today, collaborative CTI is being built on top of both internal data (e.g., netflow data, vulnerability assessments), and external data sources (e.g., public news and reports, hacker forums, etc.). This enables enhanced identification and understanding of emerging threat vectors and agents. There is a variety of commercial and open-source CTI platforms and tools for sharing and collating CTI indicators and feeds[27], for example, OpenCTI [12], MISP [24], GOSINT [4], etc. However, in order to fully extract knowledge from multiple heterogeneous sources, it remains a challenge to appropriately collect, rationalize, correlate and evaluate diverse CTI data types. The main challenge remains to decide what type of information should and can be shared across multiple networks to help ML-based threat detection and responses adapt to new coordinated attacks [25]. A critical issue in information sharing is the separation of user's sensitive data to avoid privacy and security concerns [14]. Furthermore, CTI platforms have the potential to support automatic incident reporting. Therefore, there is an important need for a comprehensive and European platform that offers the possibility of easily sharing, managing privacy and offering end-to-end capabilities from data collection to visualisation and incident response.

3 THE DYNABIC APPROACH

The DYNABIC Framework relies on the adoption of defensive AI and novel approaches to continuous business risk management. It is based on enhanced SecDevOps which could drastically improve critical services resilience. DYNABIC proposes the extension of the typical SecDevOps loop to include an Adapt phase as the operations can flexibly accommodate to the evolution of threats and to the changing conditions in which a CI operates. This extension results in the so-called SecDevOpsAdapt loop that is detailed in the following subsection.

3.1 SecDevOpsAdapt cycle

DYNABIC will provide means to facilitate business continuity planning and dynamic control at runtime. The solution builds innovation on top of SecDevOps best practices and results (e.g., from

H2020 ENACT project's delivered solution [9–11]) to continuously enhance the preparedness towards business disruption.

DevOps is becoming the mainstream system development practice, which pursues frequent agile updates of system design be deployed directly to the production in order to continuously keep runtime system upgraded. SecDevOps encompasses processes and tools that integrate security considerations and testing across all the DevOps stages, to build security from the ground up, and to reduce system's vulnerabilities. We will combine the continuous enhancement practice with measures for cyber physical resilience, and the result, as shown in Figure 1, will be an extended SecDevOps cycle with an additional Adapt loop running at system operation phase, as proposed by Metzger [23]. At the Adapt loop, autonomous adaptability (self-modification) of the system occurs according to self-observation and context sensing, while the final decision making requires human supervision all along the whole SecDevOpsAdapt cycle to respond promptly and correctly to potential threats and disruptions.

3.2 The DYNABIC Framework

Figure 2 shows the high-level architecture of the DYNABIC solution to ensure critical infrastructure resilience. The main components are the continuous management of business continuity risks (at the top center of the figure) in the adapt loop. DYNABIC will offer incident detection situational awareness (on the left of the figure) and autonomous adaptability capabilities (on the right of the figure) to support CI operators mastering response to completely new threats. All these services will be combined into the DYNABIC Framework that will enhance business level decision making and enable automatic dynamic execution of disruption recovery and business continuity processes under the best possible conditions at the time.

3.2.1 Multi-Aspect Digital Twins for Business Continuity Management. The DYNABIC solution pivots on a novel Multi-Aspect Digital Twins for Business Continuity Management (MADT4BC) concept. The MADT4BC component is the key enabler to achieve research objective 1. **MADT4BC** is devised as an evolution of traditional Digital Twins with a triple objective:

(1) To allow full situational awareness of the CI performance through continuous monitoring and inspection of different views of the system [5], as MADT4BC represents the real CI system and it is a "live" model synchronized to the running real system;
(2) To enable simulations of disruptions and threats at design and testing phases, as the user can play with MADT4BC and inject multiple types of threats and incidents, and test and predict their consequences in the system and effects on other dependent systems, as well as assess different options and combinations of response measures strategies to deploy in the system;
(3) To enable continuous assessment and management of the business disruption and CI performance degradation risks during the whole SecDevOpsAdapt cycle.

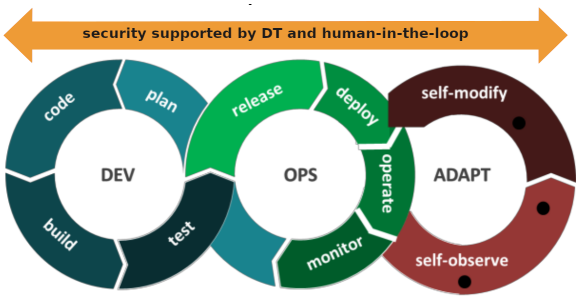

Figure 1: DYNABIC SecDevOpsAdapt cycle for Resilient systems

DYNABIC MADT4BC enables live models of critical systems capturing: i) infrastructure layer information (network, IT and OT assets, communication protocols, etc.), ii) human actors' permissions layer, iii) system event and finite state layer, and iv) finally, risk-enriched business process layer, where human actions and system functions are described in form of process activity diagrams showing the flows of data and outcomes. The core of MADT4BC is a knowledge graph representing the key assets of the CI, the live attributes of the assets, and the key relationships among them. The knowledge graph is constituted by multiple models representing the behaviour of the CI from different aspects, such as state machines, access permissions, business processes, etc. The knowledge graph maintains an entry point to access the behaviour models of the relevant assets, as well as the prediction and simulation modules based on these models. In this way, MADT4BC supports multiple types of reasoning and prognosis of disruptions and performance degradation at the business service level because it is connected to the real system. Predictions on top of MADT4BC benefit not only from historical data but also from resilience parameters collected in real time both from the system and the surrounding context. Furthermore, MADT4BC will be prepared to inject simulated inputs and data (e.g., attack vectors) into the real system so as the effects can be analysed as realistically as possible.

Figure 3 illustrates the position of MADT4BC within the DYNABIC approach. As its core element, MADT4BC maintains a live model of the underlying sub-systems, which simulates the main system (the IT and OT infrastructure of use case CI system), the business processes around the main system, and its external environment. The live model is synchronised with the real CI system via a systematic management of software components running on the whole IoT-Edge-Cloud continuum, to collect states and live data from the underlying systems, using a scalable data streaming platform. This solution is specific to the domain and the CI system (i.e., the case), since every system has its unique operational business data, data format, and possible ways of obtaining and maintaining these data.

The MADT4BC solution provides APIs for higher-level analysis of the system to support business continuity management. This includes:

- Real-time monitoring: timely detection and notification of already happened failures, early identification of about-to-happen failures, etc.

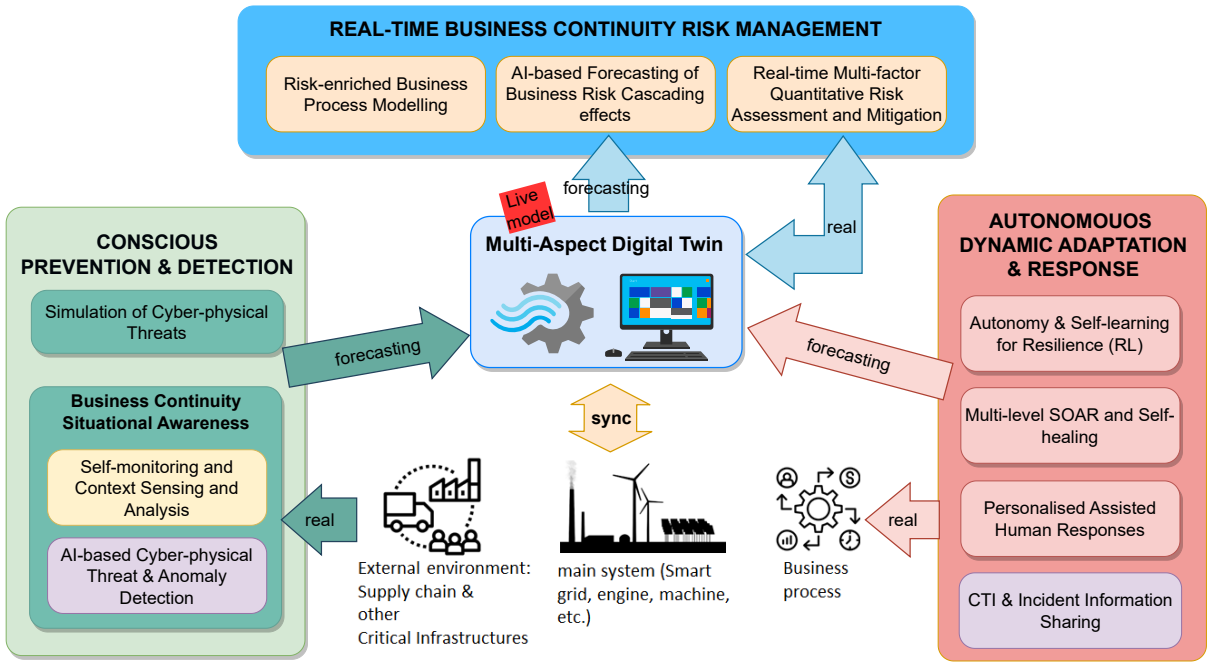

Figure 2: DYNABIC Framework components

- Forward-looking prediction and testing: using the current data/status to run the simulation ahead, to predict potential failures; run the adaptation plans using simulation to test the effectiveness.
- Backward-looking history analysis: learning from the previous failures to plan for system changes, tracing back to event history to understand the root cause of the current vulnerability, etc.

3.2.2 Business disruption risk management. First, the **RISKM4BC** component is a dynamic business risk management framework including both design and operation support to cascading impact assessment and real time risk quantification (both likelihood and impact) in the overall chain of Critical Infrastructures. RISKM4BC is the key enabler to achieve research objective 2. This module enables the accurate prospecting of business disruption risks, and it performs the quantitative risks assessment considering also threat impact cascading propagation to other CIs and conditional probability distribution models. To this aim, coordinated incidents and cyber attacks from multiple external sources using a variety of attacking tools and methods will be launched to simulate business degradation and failures and evaluate how disruption risks may propagate. This will be achieved through SIM4BC, an advanced threat simulation tool to test and prepare the whole supply-chain against cascading threats and incidents and ensure minimum self-healing capabilities.

RISKM4BC will continuously adjust the initial risk estimations through the feedback of multiple parameters (from AWARE4BC below) on the status of the system and deployed protections, which may require to further adjust cascading predictions too. For risk assessment in RISKM4BC, CI performance and business continuity parametrization and KPIs will be required for interconnected systems (including IoT-Cloud-Edge continuum), going beyond traditional resilience KPIs and metrics (e.g., Recovery Point Objective (RPO), Recovery Time Objective (RTO), minimum security service levels, etc.), including maximum allowed degradation of system security and safety, required balance between security and performance.

3.2.3 Business continuity situational awareness. The **AWARE4BC** component supports continuous self-observability and monitoring of the critical infrastructure, its environment, and its resilience, as well as advanced detection of hybrid and sophisticated threats and their symptoms. To do so, AWARE4BC will ingest and combine heterogeneous data sources from different infrastructure layers (network, system, applications), and different actors in the value chain and in the cyber threat intelligence communities. AWARE4BC will be the key enabler to achieve research objective 1.

AWARE4BC evaluates the situation by monitoring the internal of the application at multiple layers and applying deep learning and data analytics to perform advanced correlations of system status metrics, context sensors, network traffic traces, together with external CTI sources. The aim is to improve threat intelligence on suffered incidents and attack tactic symptoms, and gain intelligence of indicators of compromise (IOC) from attack information sharing within the value chain community and beyond. This way, AWARE4BC will distinguish weak symptoms of zero-day attacks and issues, and it will carry out the root-cause analysis of detected anomalies and incidents.

In complement to the internal monitoring of the system aforementioned, the resiliency of the system (or the efficiency of the

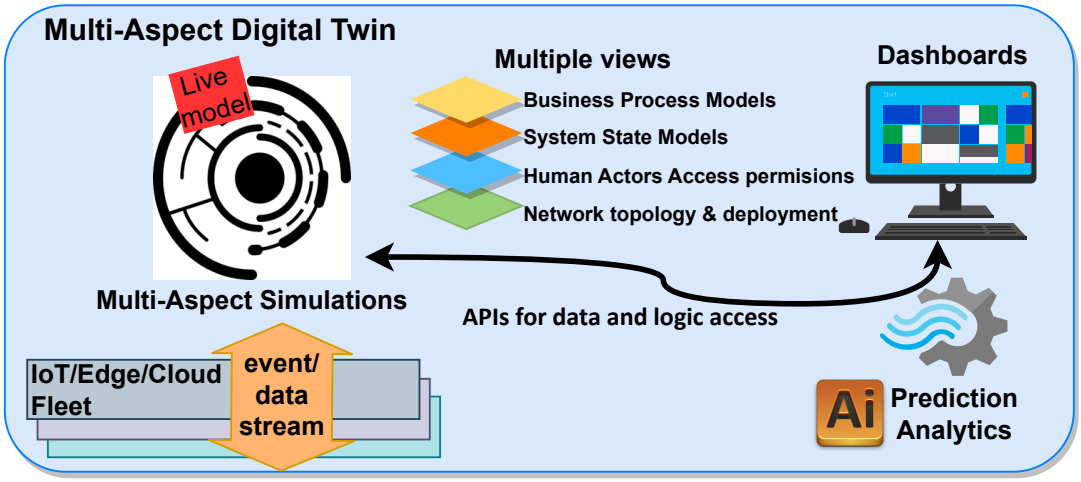

Figure 3: DYNABIC Multi-Aspect Digital Twin concept

resilience mechanisms within the system) will be monitored from a systemic approach with the objective to help decision-makers assessing the relevance of the actions taken to absorb and recover from disruptions. A multi-view approach will be adopted, enabling the evaluation of the performance of the CIs with regards to different perspectives and concerns, from high-level ones (e.g., safety and environmental properties imposed by institutional standards, certifications and norms) to low-level ones (e.g., functional properties of specific parts of the CIs), as well as supporting different levels of sensor availability and tolerances towards uncertainties. This solution will rely, as much as possible, on a dedicated infrastructure, isolated from the CIs internals. This infrastructural and computational isolation, enabled by the use of Internet of Things (IoT) technologies (e.g., self-powered sensors and edge computers) and communication protocols (e.g., Low Power Wide Area Network, LPWAN), aim at ensuring the independence of the proposed tools and methods from potentially disrupted CIs.

3.2.4 Security response orchestration. Upon the novel anomaly is detected, the **SOAR4BC** (Security Orchestration Automation and Response) service, enhanced with RL-based adaptation intelligence, autonomously orchestrates the necessary combination of automatic and human responses that jointly can minimise assessed business continuity risks in real time. AI-based response adaptation and actionable security in SOAR4BC enriches the decision and orchestration of which security mechanisms shall be deployed for real-time reactions (immediate) and recovery (longer term) in each of the assets of interconnected critical infrastructures so as to prevent and minimise risk propagation. SOAR4BC allows optimization of required security strategies and tactics, as well as improved decision support. It enables considering assessed risk levels and the protections deployed at real time in the interconnected CIs to be protected.

The SOAR4BC orchestrator's goal is the fast delivery, continuous building, deployment and decommissioning of security mechanisms and system reconfigurations to face escalation and de-escalation of defences and damage retaining walls. The module automatises the synchronization of multi-layer (multi-organisation, multi-cloud, multi-infrastructure) security workflows according to decided response strategies. The SOAR4BC's self-healing mechanisms for Energy operators of essential services include, for instance, isolating damages through the SDN capabilities, to prevent cascading failures such as a wide-area blackout or a blackout in an area supplying power to another critical infrastructure. While security mechanisms automation will have a major role in short-term reaction, human operators will enter in the long-term recovery loop, who will be assisted through digital avatars providing personalized guidance on actions to do and measures to adopt (AVATAR4BC). SOAR4BC and AVATAR4BC will be the key enablers to achieve research objective 3.

3.2.5 Information sharing. Finally, **CTI4BC** is the DYNABIC Incident Information Sharing component, which will automatically generate the incident and IOCs information tailored to the different stakeholders it will be shared with. CTI4BC will be the key enabler to achieve research objective 4. CTI4BC will communicate with AWARE4BC, SOAR4BC and MADT4BC, and it will dynamically extract and share digital evidences (traces) among different actors, as prescribed by NIS Directive 2.0. The component will integrate with existing open CTI platforms such as MISP to provide add-on intelligence for automation of both CTI sharing and incident notification. For voluntary sharing, CTI4BC will act as a common channel or CTI Community Feed of rationalized data on advanced threats, potential defences, etc. to serve third parties to enhance the CTI for more efficient detection. The information endorsed will first undergo anonymization processes so as to keep secrecy of sharing organisation identity, as well as privacy of any personally identifiable information that may be contained in the digital evidences. For incident reporting, it will offer notifications to relevant stakeholders, including CSIRTs, with the purpose to facilitate incident handling. CTI4BC will enable the incident report including insights of disruption risk level and potential cascading effects to other organisations and CIs, so CSIRTs can early react and inform them.

4 CONCLUSIONS

This paper has presented the architecture and the key components of the so-called DYNABIC approach for dynamic business continuity of critical infrastructures on top of adaptive multi-level cybersecurity. DYNABIC aims for the adoption of defensive AI and novel approaches to continuous business risk management based on enhanced SecDevOps that can drastically improve the resilience of critical services in the face of advanced cyber-physical threats. The proposed DYNABIC Framework aims to empower critical infrastructures the ability to predict, quantitatively evaluate, and promptly mitigate business continuity risks along with their potential cascading consequences. Moreover, the framework will facilitate dynamic autonomous adaptation of critical infrastructures, ensuring they align with Resilience goals through automatic optimisation and orchestration of response strategies. As the next steps, all the key components of the DYNABIC framework are being developed and they will undergo a validation process through two types of demonstrations. The first demonstration will focus on Smart Preparedness, Prevention, and Response to Business Disruption risks in four critical infrastructures and their corresponding supply chains: Electric vehicle charging stations, Critical transport services, Telecommunication infrastructures, and Hospital services. The second demonstration will emphasise Smart Preparedness and Response to Cascading Business Disruption risks within interconnected critical infrastructures, i.e, risks causing cross-domain cascading effects.

ACKNOWLEDGMENTS

This work has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101070455 (DYNABIC).

REFERENCES

[1] Mehdi Amoui, Mazeiar Salehie, Siavash Mirarab, and Ladan Tahvildari. 2008. Adaptive action selection in autonomic software using reinforcement learning. In *Fourth International Conference on Autonomic and Autonomous Systems (ICAS'08)*. IEEE, 175–181.

[2] Richard Baskerville, Paolo Spagnoletti, and Jongwoo Kim. 2014. Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management* 51, 1 (2014), 138–151.

[3] CM Colson, MH Nehrir, and RW Gunderson. 2011. Distributed multi-agent microgrids: a decentralized approach to resilient power system self-healing. In *2011 4th International Symposium on Resilient Control Systems*. IEEE, 83–88.

[4] Cisco Csirt. [n. d.]. Welcome to GOSINT's documentation! — gosint 0.0.1 documentation. https://gosint.readthedocs.io/en/latest/. Accessed: 2023-5-24.

[5] Rustem Dautov and Hui Song. 2023. Context-Aware Digital Twins to Support Software Management at the Edge. In *Research Challenges in Information Science: Information Science and the Connected World*, Selmin Nurcan, Andreas L. Opdahl, Haralambos Mouratidis, and Aggeliki Tsohou (Eds.). Springer Nature Switzerland, Cham, 239–255.

[6] Alex de Ruijter and Frank Guldenmund. 2016. The bowtie method: A review. *Safety science* 88 (2016), 211–218.

[7] European Commission. 2022. EUR-Lex - 32022L2555 - EN - EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2555. Accessed: 2023-5-24.

[8] European Commission. 2022. EUR-Lex - 32022L2557 - EN - EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557. Accessed: 2023-5-19.

[9] Nicolas Ferry, Jacek Dominiak, Anne Gallon, Elena González, Eider Iturbe, Stéphane Lavirotte, Saturnino Martinez, Andreas Metzger, Victor Muntés-Mulero, Phu H. Nguyen, Alexander Palm, Angel Rego, Erkuden Rios, Diego Riviera, Arnor Solberg, Hui Song, Jean-Yves Tigli, and Thierry Winter. 2020. Development and Operation of Trustworthy Smart IoT Systems: The ENACT Framework. In *Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment*, Jean-Michel Bruel, Manuel Mazzara, and Bertrand Meyer (Eds.). Springer International Publishing, Cham, 121–138.

[10] Nicolas Ferry, Phu Nguyen, Hui Song, Pierre-Emmanuel Novac, Stéphane Lavirotte, Jean-Yves Tigli, and Arnor Solberg. 2019. GeneSIS: Continuous Orchestration and Deployment of Smart IoT Systems. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 1. 870–875. https://doi.org/10.1109/COMPSAC.2019.00127

[11] Nicolas Ferry, Phu H. Nguyen, Hui Song, Erkuden Rios, Eider Iturbe, Satur Martinez, and Angel Rego. 2020. Continuous Deployment of Trustworthy Smart IoT Systems. *Journal of Object Technology* 19, 2 (July 2020), 16:1–23. https://doi.org/10.5381/jot.2020.19.2.a16 The 16th European Conference on Modelling Foundations and Applications (ECMFA 2020).

[12] Filigran. 2022. Filigran - OpenCTI - Open platform for cyber threat intelligence. https://www.filigran.io/en/solutions/products/opencti/. Accessed: 2023-5-24.

[13] Francesco Flammini. 2021. Digital twins as run-time predictive models for the resilience of cyber-physical systems: a conceptual framework. *Philosophical Transactions of the Royal Society A* 379, 2207 (2021), 20200369.

[14] Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott. 2017. Security and privacy in device-to-device (D2D) communication: A review. *IEEE Communications Surveys & Tutorials* 19, 2 (2017), 1054–1079.

[15] Seyedmohsen Hosseini, Kash Barker, and Jose E Ramirez-Marquez. 2016. A review of definitions and measures of system resilience. *Reliability Engineering & System Safety* 145 (2016), 47–61.

[16] Dmitry Ivanov and Alexandre Dolgui. 2021. A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control* 32, 9 (2021), 775–788.

[17] Adnan Khan, Martin Dahl, Petter Falkman, and Martin Fabian. 2018. Digital twin for legacy systems: Simulation model testing and validation. In *2018 IEEE 14th International Conference on Automation Science and Engineering (CASE)*. IEEE, 421–426.

[18] Zhiyi Li, Mohammad Shahidehpour, Farrokh Aminifar, Ahmed Alabdulwahab, and Yusuf Al-Turki. 2017. Networked microgrids for enhancing the power system resilience. *Proc. IEEE* 105, 7 (2017), 1289–1310.

[19] Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen. 2010. *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media.

[20] Azad M Madni, Carla C Madni, and Scott D Lucero. 2019. Leveraging digital twin technology in model-based systems engineering. *Systems* 7, 1 (2019), 7.

[21] Quan Mao and Nan Li. 2018. Assessment of the impact of interdependencies on the resilience of networked critical infrastructure systems. *Natural hazards* 93 (2018), 315–337.

[22] John Mern, Kyle Hatch, Ryan Silva, Jeff Brush, and Mykel J Kochenderfer. 2021. Reinforcement learning for industrial control network cyber security orchestration. *arXiv preprint arXiv:2106.05332* (2021).

[23] Andreas Metzger. 2022. Data quality issues in online reinforcement learning for self-adaptive systems (keynote). In *Proceedings of the 2nd International Workshop on Software Engineering and AI for Data Quality in Cyber-Physical Systems/Internet of Things*. 1–1.

[24] MISP. [n. d.]. MISP open source Threat Intelligence platform & open standards for threat information sharing. https://www.misp-project.org/. Accessed: 2023-5-24.

[25] Talha Ongun, Simona Boboila, Alina Oprea, Tina Eliassi-Rad, Alastair Nottingham, Jason Hiser, and Jack Davidson. 2021. Collaborative information sharing for ml-based threat detection. *arXiv preprint arXiv:2104.11636* (2021).

[26] OWASP. [n. d.]. OWASP Risk Rating Methodology. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology. Accessed: 2023-5-24.

[27] Ali Pala and Jun Zhuang. 2019. Information sharing in cybersecurity: A review. *Decision Analysis* 16, 3 (2019), 172–196.

[28] Jacopo Parri, Fulvio Patara, Samuele Sampietro, and Enrico Vicario. 2021. A framework for model-driven engineering of resilient software-controlled systems. *Computing* 103, 4 (2021), 589–612.

[29] Qianzhe Qiao, Jinjiang Wang, Lunkuan Ye, and Robert X Gao. 2019. Digital twin for machining tool condition prediction. *Procedia CIRP* 81 (2019), 1388–1393.

[30] Yuanqing Qin, Qi Zhang, Chunjie Zhou, and Naixue Xiong. 2018. A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50, 10 (2018), 3863–3870.

[31] Mahshid Rahnamay-Naeini and Majeed M Hayat. 2016. Cascading failures in interdependent infrastructures: An interdependent Markov-chain approach. *IEEE Transactions on Smart Grid* 7, 4 (2016), 1997–2006.

[32] Habibollah Raoufi, Vahid Vahidinasab, and Kamyar Mehran. 2020. Power systems resilience metrics: A comprehensive review of challenges and outlook. *Sustainability* 12, 22 (2020), 9698.

[33] Erkuden Rios, Angel Rego, Eider Iturbe, Marivi Higuero, and Xabier Larrucea. 2020. Continuous quantitative risk management in smart grids using attack defense trees. *Sensors* 20, 16 (2020), 4404.

[34] Mazeiar Salehie and Ladan Tahvildari. 2009. Self-adaptive software: Landscape and research challenges. *ACM transactions on autonomous and adaptive systems (TAAS)* 4, 2 (2009), 1–42.

[35] Stefan Schauer, Thomas Grafenauer, Sandra König, Manuel Warum, and Stefan Rass. 2020. Estimating cascading effects in cyber-physical critical infrastructures. In *Critical Information Infrastructures Security: 14th International Conference,*

CRITIS 2019, Linköping, Sweden, September 23–25, 2019, Revised Selected Papers 14. Springer, 43–56.

[36] Diomidis H Stamatis. 2003. *Failure mode and effect analysis: FMEA from theory to execution*. Quality Press.

[37] Nallan C Suresh, G Lawrence Sanders, and Michael J Braunscheidel. 2020. Business continuity management for supply chains facing catastrophic events. *IEEE Engineering Management Review* 48, 3 (2020), 129–138.

[38] Jean-Paul Watson, Ross Guttromson, Cesar Silva-Monroy, Robert Jeffers, Katherine Jones, James Ellison, Charles Rath, Jared Gearhart, Dean Jones, Tom Corbet, et al. 2014. Conceptual framework for developing resilience metrics for the electricity oil and gas sectors in the United States. *Sandia national laboratories, albuquerque, nm (united states), tech. rep* (2014).

[39] Tianqi Zhao, Wei Zhang, Haiyan Zhao, and Zhi Jin. 2017. A reinforcement learning-based framework for the generation and evolution of adaptation rules. In *2017 IEEE International Conference on Autonomic Computing (ICAC)*. IEEE, 103–112.