Human-Centric Dev-X-Ops Process for Trustworthiness in AI-Based Systems

Antonello Calabrò[1][a], Said Daoudagh[1][b], Eda Marchetti[1][c], Oum-El-kheir Aktouf[2][d]
and Annabelle Mercier[2][e]

[1] *Institute of Information Science and Technologies "A. Faedo", National Research Council of Italy (CNR), Pisa, Italy*
[2] *Grenoble INP, LCIS - Université Grenoble Alpes, Valence, France*
{*name.surname*}*@isti.cnr.it*, {*name.surname*}*@grenoble-inp.fr*

Keywords: AI, Agile, Cybersecurity, DevOps, Holistic, Human-Centric, Lifecycle, Privacy, Trustworthiness.

Abstract: Ai's potential economic growth necessitates ethical and socially responsible AI systems. Increasing human awareness and the adoption of human-centric solutions that incorporate, combine, and assure by design the most critical properties (such as security, safety, trust, transparency, and privacy) during the development will be a challenge to mitigate and effectively prevent issues in the era of AI. In that view, this paper proposes a human-centric Dev-X-Ops process (DXO4AI) for trustworthiness in AI-based systems. DXO4AI leverages existing solutions, focusing on the AI development lifecycle with a by-design solution for multiple desired properties. It integrates multidisciplinary knowledge and stakeholder focus.

1 INTRODUCTION

Recent researchers estimate the value of AI for the global economy at around $13 trillion by 2030 (Institute, 2018) and predict that by 2035, AI could double the annual growth rates of gross value added in 12 developed countries (Thaci et al., 2024). With this enormous potential for economic growth and possible impact on humans and society, understanding and promoting AI ethical and social considerations is urgently needed for every business and management (B&M) domain. AI's ethical and social considerations include fairness, transparency, accountability, privacy, bias mitigation, job displacement, and the broader societal impacts of AI adoption.

As emphasized in the AI Act [1], this is especially critical for AI applications, where data poisoning (i.e., the manipulation of data used to train AI models) and adversarial attacks (i.e., deceiving AI systems by subtly manipulating inputs that are invisible to humans but highly influential to the algorithm) are the most common types of attacks. These threats present a serious risk to the security of AI applications, as they can compromise the integrity of the results and lead to harmful consequences, often with significant implications for ethics, privacy, security, and public trust. As the practice evidences (Song et al., 2017), to achieve this objective, it is necessary to consider the above properties to be jointly and by design satisfied since the early stages of the development lifecycle and aligned with social and human needs and abilities. Therefore, research should move in three parallel directions:

1. Jointly integrate target properties (like ethics, security, safety, trust, transparency, and privacy) as by-design properties of the development lifecycle.
2. Provide new or align existing models, methods, and tools to the industrial needs and their cost-saving program.
3. Focus on the needs of the final stakeholders (like ordinary people, companies, organizations, and governments).

One way to achieve this is by adopting an ethical and social by-design human-centric development process. The DevOps development process is one of the most widely adopted processes that can be easily tailored to address ethical and social aspects of AI.

A preliminary conceptualization of a DevOps-based lifecycle for trustable developing systems

[a] https://orcid.org/0000-0001-5502-303X
[b] https://orcid.org/0000-0002-3073-6217
[c] https://orcid.org/0000-0003-4223-8036
[d] https://orcid.org/0000-0002-0493-9096
[e] https://orcid.org/0000-0002-6729-5590
[1] AI Act can be found at: https://artificialintelligenceact.eu/

Calabrò, A., Daoudagh, S., Marchetti, E., Aktouf, O. and Mercier, A.
Human-Centric Dev-X-Ops Process for Trustworthiness in AI-Based Systems.
DOI: 10.5220/0012998700003825
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 20th International Conference on Web Information Systems and Technologies (WEBIST 2024)*, pages 288-295
ISBN: 978-989-758-718-4; ISSN: 2184-3252
Proceedings Copyright © 2024 by SCITEPRESS – Science and Technology Publications, Lda.

and ecosystems, called 2HCDL (Holistic Human-Centered Development Lifecycle), has already been presented in (Daoudagh et al., 2024). Inspired by this idea and by the shift-left development (Bjerke-Gulstuen et al., 2015), this paper develops DXO4AI as a human-centric Dev-X-Ops process for trustworthiness in AI-based systems, where X stands for desired properties (such as ethics, security, safety, trust, transparency, or privacy).

In particular, the paper provides the following original contributions: (i) Definition of the Smart Objectives (SOs) for targeting the 3 research dimensions identified. (ii) Description of the conceived DXO4AI approach. (iii) Description of an architecture supporting DXO4AI. (iv) Preliminary implementation of the DXO4AI and preliminary results evaluation.

Outline. Section 2 reports on the state-of-the-art. Section 3 reports the 8 smart objectives we have identified. Section 4 describes the conceptualization of our proposal DXO4AI. Section 5 describes the supporting architecture of the DXO4AI development process and its preliminary implementation. Initial results and discussions are reported in Section 7 and 8.

2 BEYOND THE STATE-OF-THE ART

AI technology provides development for virtually endless applications. However, it is often neglected that ethical vulnerabilities can be exploited through psychological and social implications via interference with human behaviour (Scherr and Brunet, 2017). Even if scholars are becoming aware of the double-edged sword of technological progress (Winfield et al., 2019), the current practices only aim to protect humans by considering, for instance, malicious attacks on systems, without considering attacks that exploit human psychology, overlooking ethics inherent to AI systems.

The DXO4AI proposal develops solutions that leverage societal concerns to the digital evaluation of technical properties, such as ethics, security, accountability, privacy, etc., that enable self-adaptation of systems w.r.t. to ethical concerns. Hence, the DXO4AI goes beyond the current state of the art to respond to the digital disruption caused by societal and ethical vulnerabilities directed towards undermining the cohesion and functioning of European industries and societies. In the DXO4AI proposal, the emergent behavior from AI-based systems is evaluated in a dedicated Dev-X-Opslifecycle that enables continuous analysis, testing, and evaluation during the design phase and the gathering of runtime evidence, w.r.t. properties defining ethical features. This information can guide the development process toward continuously improving the system behavior at design time, preparing it for the runtime operation to support behavioral adaptation that accounts for the system's technical capabilities and social and ethical concerns.

Another aspect close to ethical and social concerns when using digital technologies, including AI-based systems, is sustainability. This is addressed by the European "Green Deal" (to the European Parliament, 2019) and will be considered in the DXO4AI proposal through the targeted use case, which is related to developing an intelligent decentralized system to model collaboration between human operators and drones in wildfire fighting. The chosen underlying intelligent model is a multi-agent system. Indeed, the multi-agent paradigm is particularly suited to deploying intelligent and autonomous systems (Calvaresi et al., 2017; Dorri et al., 2018). Such systems are found in many new applications based on intelligent nodes placed in natural environments or close to users to measure, optimize, and reduce resource usage. For example, optimizing the energy consumption in a building (Hafsi et al., 2021), or responding to climate issues (Bibri et al., 2024).

Also, DXO4AI will enhance past projects' innovative methods and tools with human-centricity. This assures trustworthiness in multiple directions, including technical and social directions, boosting the general level of trust in emergent new digital developments and boosting the technological adoption of innovative solutions.

3 ENVISIONED SMART OBJECTIVES

By focusing on the realization of the three parallel research directions identified in the previous section, the following Smart Objectives (SOs) should be considered.

Holistic Approach (SO1). The complexity of AI-based systems and applications and the diversity of the stakeholders involved in the conceiving, development, implementation, and use require holistic solutions to consider all the system dimensions: software, hardware, automation, electronics, and corresponding stakeholders' expertise and knowledge, in addition to social and ethical requirements (Thomas et al., 2019).

Human-Centered Approach (SO2). Supporting human-centered development in AI is essential for aligning with social and ethical values, sustainability, and trustworthiness. Enhancing multidisciplinary stakeholder involvement throughout the AI development lifecycle promotes public awareness, adoption of AI methods, and transparency. The Internet of People (IoP) (Miranda et al., 2015) is a recent data management paradigm that helps model and predict misbehavior or accidents.

Modeling the Behavior (SO3). Behavioral profiles of stakeholders in a target application domain should be considered throughout systems' modeling, implementation, validation, and prediction (Dobaj et al., 2022). AI, Digital Twins, crowdsourcing, and collaborative platforms can help create these profiles. These profiles should incorporate understanding relationships by combining various functional and non-functional aspects.

Integrated By-Design Approach (SO4). Promoting ”by-design” approaches, such as Privacy By Design (Cavoukian et al., 2009)), is increasingly becoming a legal obligation, exemplified by the GDPR's Data Protection By Design and By Default (Art. 25) (Commission, 2016). These principles should be integrated early in development to prevent flaws, vulnerabilities, and issues due to new devices and components.

Self-Adaptation and Prediction (SO5). Self-adaptive methodologies that ensure components and devices are trustable, validated, and verified before integration into complex environments help reduce development costs in case of problems (Casimiro et al., 2021). Frameworks for measurable, risk-based trust to develop, deploy, and operate complex, interconnected ICT systems are important for smart failure predictions (Calabrò et al., 2024).

Multidisciplinary Approach (SO6). Different sources of knowledge and requirements, such as the Law (e.g., regulation and directives), standards, technical specifications, and domain-specific best practices, should be taken into account from the beginning to derive a set of technical requirements that can be used for developing the intended digital solutions that will consider social and ethical properties (Thomas et al., 2019).

Quantitative and Qualitative Proposal and Solutions (SO7). Effective and efficient development necessitates quantitative and qualitative data collection and analysis methods]. Proposals should incorporate risk management and prevention; capabilities for modeling, testing, monitoring, and analyzing cybersecurity risks, attacks, and violations; and stakeholder-driven, domain-specific requirements (Van Looy, 2021). They should adopt standards, metrics, guidelines, and approaches to ensure functional properties such as security, safety, trust, transparency, and privacy throughout the entire lifecycle. Integrating these standards and metrics is essential for maintaining these properties over the system's lifetime.

Combining Different Xs (SO8). Non-functional requirements, known as Xs properties (such as accountability, trust, privacy, security, safety, and transparency), have traditionally been studied separately (Giraldo et al., 2017). However, in many contexts, these properties can interact deeply or conflict. Integrated approaches are needed to combine and analyze the Xs properties during system execution to achieve the required quality. According to the literature, the relationships between these properties can be classified into (Kriaa et al., 2015): (1) Independence, where Xs are defined independently; (2) Enforcement, where Xs impact each other through conditional relationships, mutual reinforcement, or mutual overlap; and (3) Conflicts, where antagonisms or oppositions exist between two or more Xs.

4 IMPLEMENTATION GUIDELINES

The implementation of the SOs mentioned above will be performed considering the following guidelines:

Multidisciplinary. This dimension is found in two main aspects: (1) exploiting and integrating different sources of information and knowledge and (2) promoting collaboration with experts in the requirements, analysis, design, deployment, and runtime phases (as suggested by SO2 and SO3).

To Be Holistic. The DXO4AI proposal applies to the development of the system, the ecosystem, and their hardware-software (HW-SW) components, considering all system dimensions (software, hardware, automation, electronics) (as suggested by SO1). It also targets vulnerabilities, erroneous state detection, and satisfaction of different application domains' needs, requirements, and properties (see SO7).

To Be Human-Centric. As suggested by SO2, it provides easy-to-use facilities focusing on the commonly adopted technologies that put humans, social interaction, and ethical concerns at the core of digital and AI services. It adopts the “Internet of People (IoP)” paradigm. Additionally, as suggested by SO7, stakeholders will continuously have a clear view of what is going on, be able to verify properties or express needs, get certification and assurance of the process and the applied methodology, get the continuous enforcement of the required properties; and, be able to exercise their rights.

To Be Focused on X-Aware Properties (-X-). As suggested by SO8, it provides the possibil-

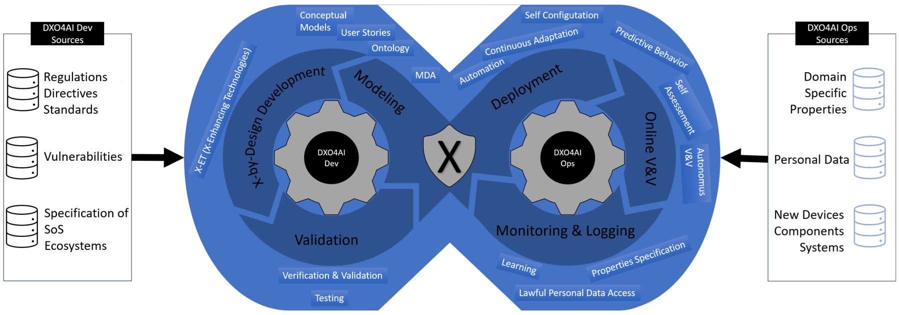


Figure 1: Human-centric Dev-X-Ops Process for Trustworthiness in AI-based Systems (DXO4AI).

ity to combine and assures Security (X=Sec), Privacy (X=Pri), Transparency (X=Tra), Lawfulness (X=Law), Accountability (X=Acc), as well as Auditability (X=Aud) and Certification (X=Cer). Additionally, as suggested by SO2 and SO7, it provides a means for sharing responsibilities throughout the entire system and ecosystem lifecycle, assuring the -X- properties for leveraging consciousness, learning, shared knowledge, and overall Quality.

To Support Continuous and Incremental Delivery. As suggested by SO4, the DXO4AI proposal interrelates two main phases, development, and operation, for continuous delivery and mutual feedback. As indicated by SO7, the DXO4AI also promotes the incremental adoption of and compliance with standards, metrics, and guidelines throughout the lifetime.

To Be Based on By-Design Principles. As suggested by SO4, it includes the X-by-design principles (such as Security-by-Design and Privacy-by-Design) in all the development and operational stages. The possibility of customizing the life cycle depending on the combination of Xs (as suggested by So8), the application domain environment, and the stakeholders' behavioral profiles (as indicated by SO3) are pivotal elements of the novelty of the DXO4AI proposal.

To Support Self-Adaptation and Timely Prediction. According to SO5, monitoring and logging enhanced with X-based technologies can be essential in assuring self-management and assessment of systems and ecosystems. Continuous and incremental delivery (as suggested by SO4) and using behavioral profiles (as indicated by S03) can provide a clear understanding of Xs violations and threats.

5 DEVELOPMENT PROCESS

By leveraging the preliminary proposal of 2HCDL (Daoudagh et al., 2024), the DXO4AI conceptual process, depicted in Figure 1, includes two phases: the Holistic Human-Centric Development phase (*DXO4AI Dev*) and the Holistic Human-Centric Operation phase (*DXO4AI Ops)*. Therefore, the process is transformed into "Dev-X-Ops methodology," where the X represents the X (or combination of) desired nonfunctional property for each target system, ecosystem, or constituent HW/SW component. The realization of the *DXO4AI Dev* phase will be guided by analyzing sources of knowledge (e.g., specification of vulnerabilities, law and EU directives, system, and ecosystem specification) and include three steps: Modeling, X-by-Design Development, and Validation. In particular, different proposals and methodologies will be considered when realizing each step. For instance, the Modelling step could use Model-Driven Architecture (MDA) or Semantic Web-based solutions (such as Ontologies) (Daoudagh et al., 2023). During the realization of the *DXO4AI Ops* phase, different sources of information will be considered to define its three steps: Deployment, Monitoring and Logging, and Reports & Recommendations.

6 PRELIMINARY IMPLEMENTATION

Figure 2 and Figure 3 present the supporting architecture of the DXO4AI development process explained in the previous section. They realize the *DXO4AI Dev* and *DXO4AI Ops* phases described in Figure 1, respectively. In figures, the human in the center can play different roles, e.g., tester, developer, legal expert, user, cybersecurity expert, or data protection officer. The preliminary implementation of the DXO4AI architecture relies on several existing artifacts that collaborate through a supporting framework that accommodates the *DXO4AI Dev* and *DXO4AI Ops* phases (Daoudagh et al., 2024).

6.1 DXO4AI Dev Implementation

The main components described for the *DXO4AI Dev* are realized by leveraging and composing the following existing artifacts.

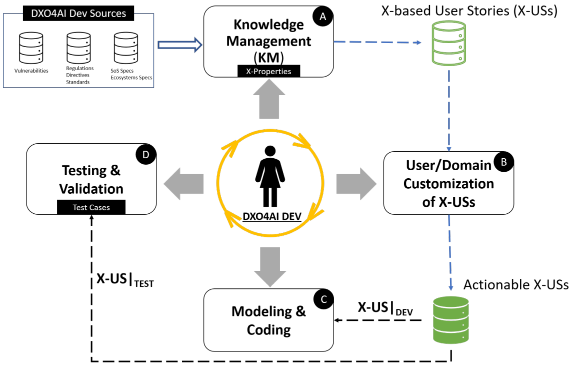

DXO4AI Dev Sources
Vulnerabilities
Regulations Directives Standards
SoS Specs Ecosystems Specs
Knowledge Management (KM)
A
X-Properties
X-based User Stories (X-USs)
Testing & Validation
D
Test Cases
DXO4AI DEV
User/Domain Customization of X-USs
B
X-US|TEST
Actionable X-USs
Modeling & Coding
C
X-US|DEV

Figure 2: DXO4AI: Proposed Architecture Supporting Dev Phase.

Knowledge Management encompasses the management of different sources of information, e.g., industrial standards, specific databases like the CVE and CWE databases for security analysis, etc. Leveraging machine-readable representations, such as ontologies, DXO4AI allows an automated adaptation of mitigation solutions related to a particular X or a combination of X properties in the presence of identified threats. The implementation of this component relies on the domain-based ontology DAEMON (Daoudagh et al., 2023) and supports relationships among SoS, IoT (Calabrò A., 2021).

User/Domain Customization of X-USs focuses on managing user interaction and providing actionable User Stories (X-USs). X-USs are machine-readable representations of the desired non-functional properties (Xs) that users can select and customize. This allows developers to incorporate user needs and domain-specific considerations into the development process—the implementation. DXO4AI relies on GDPR-based User Stories defined in (Bartolini et al., 2019) and organized in specific Data Protection backlogs, which are lists of User Stories about GDPR provisions told as technical requirements.

Modeling & Coding component integrates various modeling approaches, such as UML diagrams and Domain-Specific-Languages (DSLs), to provide valuable support for the coding phase. By leveraging behavioral models, the dev and ops phases will mutually enrich each other. In implementing this component, two open-source tools for behavioral modeling are under evaluation: Xtext [2] and ANTLR [3]. Xtext empowers developers to design DSLs specifically tailored to a specific domain. These DSLs enable the creation of concise and readable models that effectively capture the system's behavior. This focus on clarity within a particular domain makes Xtext valuable for DXO4AI. ANTLR (ANother Tool for Language Recognition) has a different but complementary strength. While not directly generating code, ANTLR allows building parsers and interpreters for the custom DSLs created with Xtext. This unique combination unlocks the potential to create highly readable, executable models.

Testing & Validation focuses on specific Xs under evaluation and allows the integration of different tools and approaches for continuously assessing the system's properties during development. In the current implementation, a broader security and privacy testing Toolbox is specifically designed for access control systems, considering GDPR compliance that includes: (1) XACMET (XACML Modeling & Testing) tackles two essential tasks: generating XACML requests (used in access control) and acting as an automated oracle to measure test coverage (Daoudagh et al., 2020); (2) XACMUT (XACml MUTation) focuses on generating variations (mutants) of XACML policies (Bertolino et al., 2013); and (3) GROOT provides a unique methodology for combinatorial testing and helps evaluate compliance with the GDPR and its contextualization within a target system (Daoudagh and Marchetti, 2021).

6.2 DXO4AI Ops Implementation

The main components of the *DXO4AI Ops* phase are described in the following and are realized by leveraging and composing existing artifacts as follows.

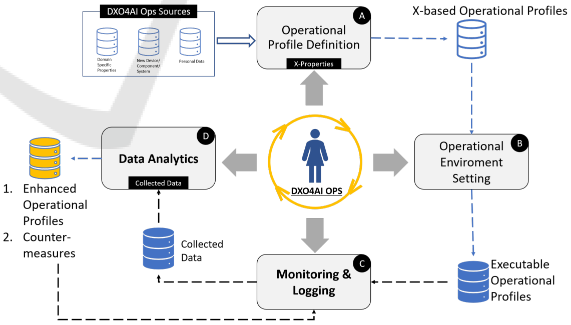

DXO4AI Ops Sources
Domain Specific Properties
New Device/ Component/ System
Personal Data
Operational Profile Definition
A
X-Properties
X-based Operational Profiles
Data Analytics
D
Collected Data
1. Enhanced Operational Profiles
2. Counter-measures
DXO4AI OPS
Operational Enviroment Setting
B
Collected Data
Monitoring & Logging
C
Executable Operational Profiles

Figure 3: DXO4AI: Proposed Architecture Supporting Ops Phase.

Operational Environment Setting aims at selecting X-based behavioral models useful for self-assessment or predicting possible violations and threats during the operation phase. This is also in charge of defining the operational test data if necessary. The component relies on **FIISS** (Priyadarshini et al., 2023), which analyses a target system's architectural and behavioral specifications to identify safety and security interactions. These implementa-

[2] https://projects.eclipse.org/projects/modeling.tmf.xtext
[3] https://www.antlr.org/

tions contribute to realizing the methodology by integrating and extending them to cover other Xs properties. The DXO4AI project will allow more in-depth research on social and ethical issues regarding this methodology and the underlying preliminary.

Operational Profile Definition aims at selecting X-based behavioral models useful for self-assessment or predicting possible violations and threats during the operation phase. This is also in charge of defining the operational test data if necessary.

Operational Environment Setting sets up the operational environment and specifies the required instrumentation for monitoring and reporting activities.

Monitoring & Logging collects data during the operation, assesses the Xs properties, and launches necessary countermeasures in case of detected violations or misbehavior. The component is implemented through the Concern Monitoring Infrastructure [4]. It is an open-source, customizable, and generic monitoring proposal that has already been evaluated as appropriate in several specific contexts and application domains (such as (Calabrò and Marchetti, 2024; Calabrò et al., 2016)) for evaluating functional and non-functional properties. Additionally, to allow loosely coupled communication and to manage vast amounts of data, the Concern communication backbone implementation is message-based and ready for integration through REST interfaces.

Data analytics performs post-analysis of the data collected during the operation execution, suggests countermeasures in case of Xs violations, and improves for successive development iterations.

7 PRELIMINARY RESULTS

The multi-agent system paradigm has gained interest with the widespread adoption of IoT and AI-based systems and their need for intelligence (reactiveness and proactiveness). The embedded multi-agent system model combines hardware and software components, supporting various applications such as autonomous vehicles and smart grids. However, this model increases the need for trust among agents, as some could be malicious and intend to harm the entire system's operation. Trust is a property that can primarily benefit from the DXO4AI methodology. Considering the peculiarity of the trust management systems, DXO4AI methodology focuses on the following actions: (1) Information gathering for trust evaluation using evidence from past interactions, contexts, and other agents; (2) Trust modeling and evaluation to represent trust in an agent. It describes how trust-related values are defined and calculated from evidence; and (3) Decision-making to evaluate the effect of decisions made on trust values.

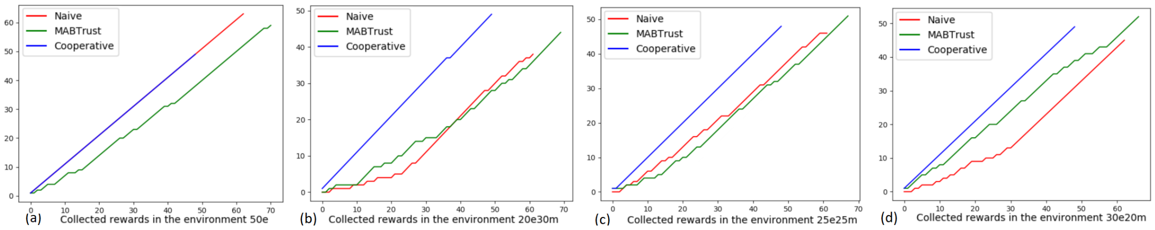
DXO4AI methodology has been applied to a trust management proof-of-concept system (PoC) representing traditional applications for explorers and harvester agents (Darroux et al., 2019). Specifically, a group of light and rapid agents are explorers and investigate targeted resources disseminated in a given field. Once explorer agents find resources, harvester agents are informed of the resources' locations to bring them back to a base. An issue may arise from malicious explorer agents, which can indicate incorrect locations, causing harvester agents to run out of energy. By applying the DXO4AI methodology and instantiating it to trust (X=trust), the evolution of trust among a group of explorer and harvester agents is evaluated by considering some malicious explorer agents. This PoC focuses on three different potential behaviors of harvester agents concerning their interactions with explorer agents:

- naive behavior: the agent only uses experience to adapt its trust level. This behavior is more straightforward when most explorers are trustworthy because the likelihood of getting reliable information is high. But if the harvester agent selects a malicious explorer agent, it loses part of its energy needed to go to the resource location and return without any resources.
- cooperative behavior: in his behavior, the harvester agent will select the explorer agent using his own experience and ask for recommendations from other agents.
- basic learning behavior: in this behavior, the harvester agent can choose between the naive behavior and the cooperative behavior based on available trust information. The learning process is based on the *multi-arm bandit* model (Xia et al., 2017)

For harvester agents, simulations are deployed using three agents' behaviors (naive, cooperative, and MABTrust). They operate in four different environments where the number of malicious agents differs to see how trust influences the overall result. The simulations were done with 80 agents with:

1. *no malicious agents:* 50 reliable explorer agents and 30 harvesters (50e);
2. *40% of malicious explorer agents:* 30 reliable explorer agents, 20 malicious explorer agents, and 30 harvesters (30e20m);
3. *50% of malicious explorer agents:* 25 reliable explorer agents, 25 malicious explorer agents, and

[4] https://github.com/ISTI-LABSEDC/Concern



(a) Collected rewards in the environment 50e (b) Collected rewards in the environment 20e30m (c) Collected rewards in the environment 25e25m (d) Collected rewards in the environment 30e20m

Figure 4: Results with different configurations: (a) no malicious (b) 40% malicious(c) 50% malicious (d) 60% malicious.

30 harvesters (25e25m);

4. *Most malicious explorer agents (60%):* 20 reliable explorers, 30 malicious explorers, and 30 harvesters (20e30m).

Figure 4 shows the resources the harvester agents collected before running out of energy. In an environment without malicious explorer agents (a), the MAB algorithm does not perform as well as the naive or cooperative behavior. This is because, in this environment, agents ought to use most of their energy to collect resources and not as much for the Trust Management System (TMS) because it will reduce their performance. Within environments *30e20m* and *25e25m*, the MAB algorithm performs better than the others. In the last configuration (d), with the most trustworthy harvester agents, the cooperative behavior performs better than the two others, with the MAB being a close second. Using the DXO4AI methodology, we analyzed the trust property within an intelligent system under development. This process allows for the trust model to be adjusted for future design cycles.

8 EXPECTED OUTCOMES AND DISCUSSION

Even if in the proposal stage, the presented smart objectives, the DXO4AI methodology, and its preliminary supporting architecture envision different impacts and outcomes for the research and industrial environment. Indeed, they can stimulate the research in the design and development of specific models and methods and underlying platforms and tools for enforcing the by-design and combined implementation of Xs properties during the development and operation phases. Leveraging the DevOps principles, the proposed solution will be an industrial, practical, and effective approach for continuously assessing and enhancing the considered properties throughout the entire lifecycle. Finally, the developed processes, models, and tools could lead to the proposal of patents or licensed platforms, increasing economic/industrial impact. Considering the human aspects, the DXO4AI could contribute to leveraging the Xs awareness and education in general for any possible stakeholder (both professionals and ordinary users) with a substantial societal impact. DXO4AI can close the current literature and technological gap in combining security and privacy by design (Abu-Nimeh and Mead, 2012). We expect our approach to be generic enough to consider other processes and properties. The novel Integrated framework will allow the industrial context to integrate processes such as threat analysis, risk analysis, testing, formal verification, effective audit procedures for cybersecurity testing, validation, and consideration of certification aspects. It also promotes the behavioral model as an effective means of modeling and testing Xs properties and analyzing HW/SW components to discover their potential vulnerabilities.

ACKNOWLEDGEMENTS

This work was partially supported by the project RESTART (PE00000001), the project SERICS (PE00000014), and the project THE (CUP B83C22003930001) under the NRRP MUR program funded by the EU - NextGenerationEU.

REFERENCES

Abu-Nimeh, S. and Mead, N. R. (2012). Combining security and privacy in requirements engineering. In *Information Assurance and Security Technologies for Risk Assessment and Threat Management: Advances*, pages 273–290. IGI Global.

Bartolini, C., Daoudagh, S., Lenzini, G., and Marchetti, E. (2019). Gdpr-based user stories in the access control perspective. In *QUATIC 2019, Ciudad Real, Spain, September 11-13, 2019, Proceedings*, pages 3–17.

Bertolino, A., Daoudagh, S., Lonetti, F., and Marchetti, E. (2013). XACMUT: XACML 2.0 mutants generator. In *ICST 2013 Workshops Proceedings, Luxembourg, Luxembourg, March 18-22, 2013*, pages 28–33. IEEE Computer Society.

Bibri, S. E., Krogstie, J., Kaboli, A., and Alahi, A. (2024). Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. *Environmental Science and Ecotechnology*, 19:100330.

Bjerke-Gulstuen, K., Larsen, E. W., Stålhane, T., and Dingsøyr, T. (2015). High level test driven development–shift left. In *XP 2005 Conference*, pages 239–247. Springer.

Calabrò, A. and Marchetti, E. (2024). MOTEF: A testing framework for runtime monitoring infrastructures. *IEEE Access*, 12:38005–38016.

Calabrò A., Daoudagh S., M. E. (2021). Mentors: Monitoring environment for system of systems. In *WEBIST 2021, pp. 291–298, 26-28/10/2021*.

Calabrò, A., Daoudagh, S., and Marchetti, E. (2024). Towards enhanced monitoring framework with smart predictions. *Log. J. IGPL*, 32(2):321–333.

Calabrò, A., Lonetti, F., Marchetti, E., and Spagnolo, G. O. (2016). Enhancing business process performance analysis through coverage-based monitoring. In *QUATIC 2016, Lisbon, Portugal, September 6-9, 2016*, pages 35–43. IEEE Computer Society.

Calvaresi, D., Marinoni, M., Sturm, A., Schumacher, M., and Buttazzo, G. (2017). The challenge of real-time multi-agent systems for enabling iot and cps. In *Proceedings of the international conference on web intelligence*, pages 356–364.

Casimiro, M., Romano, P., Garlan, D., Moreno, G. A., Kang, E., and Klein, M. (2021). Self-adaptation for machine learning based systems. In *ECSA (Companion)*.

Cavoukian, A. et al. (2009). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, 5:2009.

Commission, E. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*, L119:1–88.

Daoudagh, S., Lonetti, F., and Marchetti, E. (2020). XACMET: XACML testing & modeling. *Softw. Qual. J.*, 28(1):249–282.

Daoudagh, S. and Marchetti, E. (2021). Groot: A gdpr-based combinatorial testing approach. In *ICTSS 2021, London, UK, November 10–12, 2021, Proceedings*, page 210–217, Berlin, Heidelberg. Springer-Verlag.

Daoudagh, S., Marchetti, E., and Aktouf, O.-E.-K. (2024). 2hcdl: Holistic human-centered development lifecycle.

Daoudagh, S., Marchetti, E., Calabrò, A., Ferrada, F., Oliveira, A., Barata, J., Peres, R. S., and Marques, F. (2023). DAEMON: A domain-based monitoring ontology for iot systems. *SN Comput. Sci.*, 4(5):632.

Darroux, A., Jamont, J.-P., Aktouf, O.-E.-K., and Mercier, A. (2019). An energy aware approach to trust management systems for embedded multi-agent systems. In *Software Engineering for Resilient Systems - Serene 2019 workshop*, pages 121–137.

Dobaj, J., Riel, A., Krug, T., Seidl, M., Macher, G., and Egretzberger, M. (2022). Towards digital twin-enabled devops for cps providing architecture-based service adaptation & verification at runtime. In *SEAMS*, SEAMS '22, page 132–143, New York, NY, USA. Association for Computing Machinery.

Dorri, A., Kanhere, S. S., and Jurdak, R. (2018). Multi-agent systems: A survey. *IEEE Access*, 6:28573–28593.

Giraldo, J., Sarkar, E., Cardenas, A. A., Maniatakos, M., and Kantarcioglu, M. (2017). Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Design & Test*, 34(4):7–17.

Hafsi, K., Genon-Catalot, D., Thiriet, J.-M., and Lefevre, O. (2021). Dc building management system with ieee 802.3 bt standard. In *2021 High Performance Switching and Routing (HPSR)*, pages 1–8. IEEE.

Institute, M. G. (2018). Notes from the ai frontier: Modeling the impact of ai on the world economy.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., and Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, 139:156–178.

Miranda, J., Mäkitalo, N., Garcia-Alonso, J., Berrocal, J., Mikkonen, T., Canal, C., and Murillo, J. M. (2015). From the internet of things to the internet of people. *IEEE Internet Computing*, 19(2):40–47.

Priyadarshini, Greiner, S., Massierer, M., and Aktouf, O. (2023). Feature-based software architecture analysis to identify safety and security interactions. In *ICSA 2023, March 13-17, 2023*, pages 12–22. IEEE.

Scherr, S. and Brunet, A. (2017). Differential influences of depression and personality traits on the use of facebook. *Social Media + Society*, 3(1):2056305117698495.

Song, H., Fink, G. A., and Jeschke, S. (2017). *Security and privacy in cyber-physical systems: foundations, principles, and applications*. John Wiley & Sons.

Thaci, A., Thaci, S., Zylbeari, A. K., and Baftijari, A. Y. (2024). Economic impact of artificial intelligence. *KNOWLEDGE-International Journal*, 62(1):21–25.

Thomas, D., Hristo, A., Patrick, M., Göbel, J. C., and Sven, F. (2019). A holistic system lifecycle engineering approach – closing the loop between system architecture and digital twins. *Procedia CIRP*, 84:538–544. CIRP Design Conference 2019, Portgal.

to the European Parliament, C. (2019). Communication from the commission to the european parliament, the european council, the council the european economic and social committee and the committee of the regions, pp. 24, 2019 (climate change mitigation.

Van Looy, A. (2021). A quantitative and qualitative study of the link between business process management and digital innovation. *Information & Management*, 58(2):103413.

Winfield, A., Michael, K., Pitt, J., and Evers, V. (2019). Machine ethics: The design and governance of ethical ai and autonomous systems. *Proceedings of the IEEE*, 107:509–517.

Xia, Y., Qin, T., Ding, W., Li, H., Zhang, X., Yu, N., and Liu, T.-Y. (2017). Finite budget analysis of multi-armed bandit problems. *Neurocomputing*, 258:13–29.