Intelligent Human Systems Integration (IHSI 2025), Vol. 160, 2025, 416–430
https://doi.org/10.54941/ahfe1005846

Human Factors-Centric Validation of a Security Management System in a Linked Critical Infrastructures Environment

Florian Piekert[1], Tim H. Stelkens-Kobsch[1], Hilke Boumann[2], Meilin Schaper[1], and Nils Carstengerdes[1]

[1]Institute of Flight Guidance, German Aerospace Center DLR, 38108 Braunschweig, Germany
[2]Formerly Institute of Flight Guidance, German Aerospace Center DLR, 38108 Braunschweig, Germany

ABSTRACT

This work reports the human factors-related validation results of a security system for the protection of linked critical infrastructures (CIs) against combined cyber-physical attacks. Attacks of any kind on CIs have increased in number and complexity. In order to prevent or mitigate interruption of services to the public, the protection of CIs is of high importance. As an evolution of recent security research on single and linked CIs, the EU H2020 project PRAETORIAN adopted a holistic security management approach that addressed linked CIs with one overarching toolset. The PRAETORIAN toolset is specifically designed to support security managers of CIs in their decision-making processes. It enables them to anticipate, manage, and withstand potential cyber, physical, or combined security threats that could target their own infrastructures, as well as other interconnected CIs. These threats could have a substantial impact on the operational performance or service provision of these infrastructures and potentially compromise the safety and security of the population residing in their vicinities. The toolset consists of four primary systems: The Physical Situation Awareness (PSA) system, the Cyber Situation Awareness (CSA) system, the Hybrid Situation Awareness (HAS) system, and the Coordinated Response (CR) system. Central to the toolset is the Interoperability Platform (IOP), which interconnects all the modules within the PRAETORIAN toolset. This interconnection facilitates seamless information exchange across all systems and modules, ensures efficient data storage, prevents the duplication of data between modules, replicates any changes made, and avoids potential inconsistencies. This integration is crucial for providing unified data accessibility across the entire platform and to obtain a clear nomenclature for events and situations across the different infrastructure domains. Each system is composed of multiple modules. This document offers only a brief overview of each system, comprehensive and detailed explanation of the toolset's architecture can be obtained from the corresponding cited documents within the full paper. The focus of the system validation was put on the assessment of operators' feedback about the PRAETORIAN system (the toolset). In four exercises, potential attack scenarios were presented to groups of selected operators along with demonstrations of the PRAETORIAN tools. Feedback was collected using questionnaires, debriefing questions and open questions throughout the presented scenario. The key validation results show that the system could offer benefits for cross-infrastructure security management, but that improvements relating to systems and HMIs, procedures and responsibilities are required.

Keywords: Validation, Human factors, Security management, Linked critical infrastructures

INTRODUCTION

In recent years, society was repeatedly struck by diverse security incidents which need to be anticipated, detected and managed. While such events happen and after suffering from them, it is of utmost importance that vital services for society are kept operational and secured. The bomb attacks in Brussels (2016) directed at the airport and a metro station (BBC, 2023) are just one example for interconnected, coordinated, and increasingly more complex acts of terrorism. Adding up to this, there is a threat that is largely unrecognized by the general public despite its risk potential. The risk posed by a cyber and/or physical attack on a Critical Infrastructure (CI) that extends beyond the owners and operators of the targeted assets. It also encompasses their suppliers, customers, businesses, and individuals in close proximity of the infrastructure. Moreover, CIs that are linked due to nowadays increasing connectivity can be negatively impacted by such an attack. The consequences of an attack on a single CI can be extensive and have far-reaching effects on multiple sectors of the economy. In this paper, the term 'linked CIs' will be used to describe all instances in which events at one CI could affect another CI in any way.

For instance, there was an attack in 2016 that resulted in destruction of computers across six Saudi Arabian organizations, including energy, manufacturing and aviation sectors (Pagliery, 2016). Additionally, the WannaCry Ransomware attack, which occurred in 2017, impacted over 100,000 organizations in 150 countries (DPR, 2017). Ukraine experienced vast power outages in both 2015 and 2017 (Zetter, 2016) and not to forget the attack on the New York Dam in 2013 (Connor, Winter and Gosk, 2015). Malware attacks like NotPetya in 2017 cause damages in the order of billions (Greenburg, 2018) while the largest Distributed Denial of Service (DDoS) attack in the world targeted GitHub in 2018 (Ranger, 2018).

Combined cyber and physical attacks on linked CIs will likely continue to rise. Several reasons contribute to this trend, as for example the five mentioned in Gooch (2020): (i) they already happened, (ii) there is a proliferation of industrial control system malware, (iii) there is an increased reliance of industry and CIs on Information and Communications Technology (ICT) systems, (iv) industrial control system networks are notoriously difficult to secure, (v) cyber criminals have a proven business model. Adding to this, the availability of generative Artificial Intelligence (AI) opens up a completely new area of application for adversaries. Furthermore, attackers are eager to take advantage of situations that leave a country weak and defenceless, e.g., during an already on-going attack, natural disasters or pandemic events. Some recent examples are the series of attacks during the pandemic situation caused by COVID-19, e.g., the Ripple20 vulnerabilities impacting the communications of millions of Internet of Things (IoT) medical devices (Davis, 2020), cyber-attacks to vaccine test centres (Winder, 2020), or ransom demands to hospitals (Gallagher and Bloomberg, 2020).

In order to support successful handling of such critical situations, several projects have been funded by the European Commission during the last decades. First these were focused on securing specific domains and CIs.

E.g., the project GAMMA (Asgari, Stelkens-Kobsch et al., 2017) addressed security management in the domain of Air Traffic Management (ATM), and SATIE (Stelkens-Kobsch, Carstengerdes et al., 2017) was focused on airports. Later on, a more holistic approach that considers CIs as linked systems was taken. Among the latter kind of projects is PRAETORIAN Protection of Critical Infrastructures from advanced combined cyber and physical threats (Papadopoulos, Demestrichas et al., 2023), which was designed to enhance the security and resilience of European CIs by aiding the coordinated protection of linked CIs against combined physical and cyber threats. The project provides a toolset of: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system; (iii) a Hybrid Situation Awareness system, which includes digital twins of the infrastructure under protection; and (iv) a Coordinated Response system. The PRAETORIAN toolset aims to assist security managers of CIs by providing decision-making support and enabling to anticipate and withstand potential security threats, whether they are cyber, physical, or a combination. It is intended to support operators to protect their own as well as linked CIs, as any disruption may have a significant impact on operational efficiency and overall safety of the surrounding population.

The project specifically handles manmade cyber and physical attacks affecting linked CIs by fostering prevention, detection and – in case of an ongoing attack – mitigation of the attack. PRAETORIAN also addresses cascading effects on normal operations in linked CIs, by aiming to increase the resilience of these connected CIs. To this end, the system predicts cascading effects, proposes a unified response among CIs and assists First Responder (FR) teams.

In order to evaluate the operational feasibility of the overall toolset and the underlying operational concept, validation exercises were conducted to obtain expert feedback. The validation exercises were conducted based on the European Operational Concept Validation Methodology (E-OCVM; EUROCONTROL, 2010) a framework originating from ATM research. This paper presents selected results from the PRAETORIAN validation exercises.

Four validation scenarios that contain a wide range of attacks and CIs were developed within the project. There was one validation exercise per scenario in which the respective scenario was presented to a selected group of participants. Based on the maturity level of the system, the validation approach combined presentations and elements of a cognitive walkthrough with selective hands-on-phases. Since PRAETORIAN is aimed to be generalizable to different settings and not tailored to one specific scenario, the results of the four validation exercises will be reported in an aggregated manner covering the entirety of attacks and CIs in this paper. Further, only results regarding the overall system will be regarded, i.e., results concerning individual tools will not be included.

The chosen validation approach and parts of the results were already described and discussed in the Stelkens-Kobsch et al. work (2023). This includes, e.g., a discussion of the suitability of the chosen validation approach, lessons learned from the validation exercises and an overall assessment of all validation objectives.

METHODS

Objectives and Acceptance Criteria

The data was analysed in regard to pre-defined objectives and Acceptance Criteria (AC). Table 1 lists the three objectives and their corresponding AC that were chosen for this work. The AC were evaluated using questionnaires and debriefing feedback (see section C).

Table 1. Selected objectives and acceptance criteria.

Objective	AC	The Praetorian solution…
A. Better Understanding of Attacks and Consequences	A1	… enhances situation awareness.
	A2	… enables a faster detection of cyber and physical threats.
	A3	… does not induce operator overload.
	A4	… provides the relevant information.
	A5	… provides helpful decision support.
B. Better Resilience and Improved Coordinated Response	B1	… enables a faster coordinated response to cyber and physical threats.
	B2	… improves the resilience of CIs.
	B3	… enhances teamwork between the parties involved, e. g. operators and first responders.
C. Usability and Acceptance of Solution	C1	… is accepted.
	C2	… is trustworthy.
	C3	… is usable.
	C4	… is intuitive to use.
	C5	… conforms to operators' mental models.

Sample

There was one group of participants per validation exercise. There were five participants in exercise #1, eight participants in exercise #2, six participants in exercise #3 and five participants in exercise #4. The overall number of participants was 24. Due to the small sample size and data protection concerns, no information about age and gender were collected. The participants were staff members from organizations included in the validation scenarios, but they were naïve about the contents of the scenarios. Among these were three FR organizations, a laboratory, two hospitals, two ports, two airports, a power plant and a hydro power plant. Since each participant took on one or several defined roles in the validation scenarios, their work-related responsibilities were considered during the recruitment phase in order to create a match with their scenario role to the possible extent.

Material

1) *Validation Scenarios:* Four validation scenarios demonstrated the PRAETORIAN solution's functionalities in different situations. Each validation scenario contained cyber-, physical or combined cyber-physical attacks affecting multiple CIs, either directly or indirectly due to cascading effects.

- Scenario #1 is a cyber-physical attack on a hydro power plant causing blackout and flooding, cascading to a hospital.
- Scenario #2 is about cyber-physical attacks on a power plant and a port.
- In Scenario #3, a cyber-physical attack on a port has cascading effects on a hospital and an airport.
- Scenario #4 involves a cyber-physical attack on a laboratory proceeding cross-border to an airport.

The validation scenarios were presented using presentation slides supported by narrations, pictures or videos. An initial overview of the scenario was provided, followed by a four-step approach:

- First, each scenario step was narrated in more detail.
- Second, participants were asked about their current procedures and operations, e.g., which systems and procedures would currently be used in such situations.
- Third, the relevant PRAETORIAN tools for the scenario step were demonstrated by showing the human-machine interfaces (HMIs) via screen-sharing. Alerts were simulated in the background. Since participants had received role-dependent credentials for the different tools, they were able to click along on their own screens. Some participants were asked to share their own screens and then instructed on using the HMIs, while in most other cases, developers demonstrated the tools by sharing their own screens. It became apparent that an interactive approach is advisable to obtain more valid feedback.
- Fourth, participants' feedback on the demonstrated tools was gathered.

The described four-step approach was utilized for most scenario steps, but deviations were possible depending on the course of the scenario. It should generally be noted that the presentation slides, including the tools shown and the questions asked, were tailored specifically for each of the four validation scenarios. Further, Scenario #2 deviated in the third step as some scenario steps were executed live on the digital twin.

2) *Debriefing Questions:* After each validation scenario, a debriefing was conducted with all present participants. The debriefing questions were identical for all validation exercises. Participants were asked what benefits they see in PRAETORIAN's concept and technology and how this concept and technology could be improved. It was subsequently pointed out to the participants that PRAETORIAN can share all information received during the previously presented attacks with other CIs on a European scale. The participants were asked what benefits and what obstacles they see in this kind of cooperation. Lastly, they were asked for final comments.
3) *Bespoke Validation Questionnaire:* A bespoke validation questionnaire was created on LimeSurvey (LimeSurvey, 2024) which participants received after the validation exercise. It contained questions and statements about the validation scenario, the overall PRAETORIAN solution and its individual tools. Each solution-related item was mapped

to an AC. This paper will present results from items related to the selected objectives and AC in Table 1 that focus on the overall PRAETORIAN solution. This comprises 28 five-level Likert items rated from 1 (strongly disagree) to 5 (strongly agree). Means (M) and standard deviations (SD) were calculated for each item. The neutral rating of 3 (neither agree nor disagree) served as a cut-off criterion, i.e., to fulfil an AC, related statements had to be rated with a mean rating of 3 at the minimum. In the case of inverse statements, mean ratings had to be below 3. Free text answers to open questions (independent or follow-up questions based on participants' agreement or disagreement with specific statements) will not be reported in detail, but may serve to further elaborate on quantitative results in the discussion if relevant. Results from items focusing on individual tools, the validation scenarios or one of the objectives not listed in Table 1 are not reported in this paper.

4) *System Usability Scale:* The System Usability Scale (SUS; Brooke, 1996) was administered after each validation exercise along with the bespoke validation questionnaire. The SUS was used for the evaluation of the PRAETORIAN solution's usability in the context of AC C3 "The PRAETORIAN solution is usable". It comprises ten five-level Likert items ranging from 1 (strongly disagree) to 5 (strongly agree), from which a SUS score between 0 and 100 is calculated. M and SD were calculated from the SUS scores and interpreted following (Bangor, Kortum and Miller, 2009; Brooke, 2013).

Procedure

The validation exercises were performed remotely using web-conference tools. Each validation scenario was run once, so four validation exercises were conducted in total. Because the validation scenarios were specific to the involved CIs and FR organizations, each validation exercise was attended by only one group of participants. In the sense of an iterative process, insights from conducted validation exercises were used to improve the following validation exercises, e.g., regarding the selection of participants, procedure or implementation of tools.

Each validation exercise lasted one day. In the morning, informed consent was collected, and participants received project information and an introduction to the PRAETORIAN tools. The morning ended with questions-and-answers and participants were encouraged to ask questions as needed during the exercise. Participants received specific credentials for their roles and logged in to the PRAETORIAN tools. In the afternoon, the validation scenario was presented. During this, participants were asked for their feedback, and afterwards, the debriefing was conducted with all participants of the exercise. Online questionnaires were completed either immediately or later, depending on time constraints.

The validation exercise of scenario #2 deviated partially, as not all participants could join live. Therefore, this exercise was recorded for the absent participants and they sent written feedback afterwards.

Data Analysis

Quantitative data from the questionnaires were analysed descriptively using IBM SPSS Statistics 26 (IBM Corp., 2019) M and SD for the selected bespoke questionnaire items and SUS scores were calculated over all scenarios for the 24 participants.

Free text answers to open questions from the bespoke questionnaire were categorized, but these will not be reported in this work in detail. However, they will be used to elaborate on certain discussion points in the next chapter These results were analysed with regards to their assigned AC. Debriefing feedback was analysed in an aggregated manner over all scenarios and categorized by AC or, if there was no fitting AC, identified as additional feedback. Feedback from the validation scenario playouts was used to gather lessons learned for future research.

RESULTS

Results from the bespoke validation questionnaire and the SUS are reported in the context of their corresponding objectives and AC. Table 2 provides means (M) and standard deviations (SD) for the 28 bespoke questionnaire items. The final column shows if the cut-off criterion was reached, i.e., if the mean was at least equal to or higher than 3, which is the neutral threshold. For inversely phrased statements, the cut-off criterion is reversed.

Table 2. Results of the bespoke questionnaire items (all N = 24).

Acceptance Criterion	Item	*M*	*SD*	✓/✗[a]
Objective A: Better Understanding of Attacks and Consequences				
A1. Situation Awareness	1. Compared to the current situation, I think the PRAETORIAN system will enhance my situation awareness.	4.13	0.45	✓
	2. The PRAETORIAN system helps to obtain a complete picture of the situation.	4.25	0.61	✓
A2. Faster detection of threats	3. Compared to the current situation, I think the PRAETORIAN system will enable a faster detection of cyber and/or physical threats.	3.92	0.83	✓
A3. No operator overload	4. The PRAETORIAN system displays too much information.[b]	3.13	0.95	✗[b]
A4. Relevant information	5. The PRAETORIAN system provides the information that I need.	3.58	1.02	✓
	6. The interfaces used to share data with external sources and organizations provide the right information.	3.54	0.83	✓
A5. Helpful decision support	7. The PRAETORIAN system provides helpful decision support.	4.04	0.62	✓
Objective B: Better Resilience and Improved Coordinated Response				
B1. Faster coordinated response	8. Compared to the current situation, I think the PRAETORIAN system will enable a faster coordinated response to **physical** threats.	3.71	1.00	✓
	9. Compared to the current situation, I think the PRAETORIAN system will enable a faster coordinated response to **cyber** threats.	3.92	0.72	✓

(Continued)

Table 2. Continued

Acceptance Criterion	Item	*M*	*SD*	✓/✗[a]
	10. Compared to the current situation, I think the PRAETORIAN system will enable a faster coordinated response to **combined** physical and cyber threats.	4.04	0.91	✓
B2. Improved resilience	11. Compared to the current situation, I think the PRAETORIAN system will improve the resilience of Critical Infrastructures.	3.83	0.70	✓
B3. Enhanced teamwork	12. Compared to the current situation, I think the PRAETORIAN system will enhance **communication** between the parties involved, e. g. operators and first responders.	3.88	0.80	✓
	13. Compared to the current situation, I think the PRAETORIAN system will enhance **coordination** between the parties involved, e. g. operators and first responders.	3.83	0.70	✓
Objective C: Usability and Acceptance of Solution				
C1. Acceptance	14. The PRAETORIAN system is compatible with procedures and systems currently used in operations.	3.04	0.95	✓
	15. I would like to use the PRAETORIAN system in real operations.	3.88	0.85	✓
	16. Compared to my current systems, the PRAETORIAN system provides advantages.	4.00	0.51	✓
	17. The PRAETORIAN system needs improvement.[b]	4.13	0.68	✗[b]
	18. Compared to my current systems, the PRAETORIAN system provides innovations.	4.17	0.70	✓
C2. Trust	19. I think I would trust the information provided by the PRAETORIAN system.	3.96	0.46	✓
C3. Usability	20. The PRAETORIAN system is user-friendly.	3.00	1.18	✓
	21. The interfaces used to share data with external sources and organizations were easy to use.	2.79	1.02	✗
C4. Intuition	22. The PRAETORIAN system is intuitive to use.	2.83	1.05	✗
C5. Conformance with mental models	23. The PRAETORIAN system could be easiliy integrated in my current workflow.	2.71	0.95	✗
	24. The PRAETORIAN system is scalable, modular and flexible.	3.58	0.88	✓
	25. The PRAETORIAN system should raise warnings when sensors, critical process or any related modules are not available.	4.46	0.51	✓
	26. The PRAETORIAN system should offer a possibility to consult status and historical data.	4.13	0.85	✓
	27. The PRAETORIAN system conforms to my expectations.	3.67	0.82	✓
	28. The PRAETORIAN system conforms to my mental model of how the system should work.	3.54	0.93	✓

Better Understanding of Attacks and Consequences

From Table 2 it can be seen that the results for the first objective were satisfying with regard to situation awareness, a faster detection of cyber and physical threats, the relevance of provided information and the quality of decision support (ACs A1, A2, A4, A5). Especially the enhanced situation

awareness (items 1 and 2) and the quality of decision support (item 7) were rated positively. However, in the context of AC A3 "The PRAETORIAN solution does not induce operator overload", participants slightly agreed that the system displays too much information (item 4). In this case, the cut-off criterion was not met.

Better Resilience and Improved Coordinated Response

Table 2 shows that all items relating to the second objective (comprising B1, B2, B3) were on average rated sufficiently high. Participants indicated slight agreement that the system could enable a faster coordinated response to cyber and physical threats (items 8 to 10), that it could improve the resilience of CIs (item 11) and that it could enhance teamwork between the involved parties (items 12 and 13).

Usability and Acceptance of Solution

The results for the third objective were heterogeneous, see Table 2. Regarding system acceptance (C1), the average ratings met the cut-off criterion except for item 17: On average, participants agreed that the PRAETORIAN system needs improvement. However, they also overall indicated, e.g., that the system provides advantages (item 16) and innovations (item 18). While mean ratings regarding the compatibility of PRAETORIAN with existing procedures and systems (item 14) passed the cut-off criterion, it should be noted that participants' average agreement about this item was comparably low.

Overall, participants indicated sufficient trust in the information provided by the system (item 19, C2).

Concerning usability (C3), not all results met the cut-off criterion. Participants' average agreement about the user-friendliness of the system was neutral (item 20) and therefore still sufficient. However, participants slightly disagreed that the interfaces used to share data with external sources and organizations are easy to use (item 21). The overall mean SUS score was $M = 53.02$ ($SD = 16.45$), which corresponds to a usability slightly above "OK" according to Brooke (2013).

Furthermore, participants on average did not agree that the system is intuitive to use (item 22, C4).

In the context of the system's conformance to participants' mental models (C5), results for most items met the cut-off criterion. Among all items related to this AC, participants on average indicated the highest agreement that PRAETORIAN should raise warnings on system outage (item 25) and that there should be consultable status and historical data (item 26). However, on average they did not agree that PRAETORIAN could be easily integrated into their current workflows (item 23).

To summarize, while satisfying results were achieved for most items, some shortcomings were identified regarding acceptance, usability, intuitive use and conformance with operators' mental models.

DISCUSSION

In the following section, the reported results will be discussed with regard to the three objectives. In addition to the statistical evaluation, verbal and textual responses gathered in the questionnaires and debriefings will be regarded, and limitations of the validation exercises will be considered. It must be noted that it is not possible to include all data collected during the validation exercises in the scope of this work. Based on selected results, a more global evaluation that does not consider all feedback in detail is therefore provided.

Better Understanding of Attacks and Consequences

Within this objective, the ACs regarding situation awareness, a faster detection of cyber and physical threats, the relevance of information and helpfulness of decision support were considered to be satisfying. The enhancement of situation awareness and the helpfulness of the decision support provided by the system were identified as benefits of the PRAETORIAN system in particular. Regarding the topic of situation awareness, some participants also named the integration of cyber and physical threats and the integration of safety and security issues as benefits during the debriefing. Regarding the relevance of information, some participants positively mentioned the availability of real-time information, sensor information, information about cascading effects and about previous or on-going attacks at other CIs.

In the debriefings, participants expressed several ideas for additional features which could further improve the system in relation to the mentioned ACs. This included, e.g., additional types of sensors, a weather forecast or a more extensive integration of individual CIs' resources.

As the PRAETORIAN system seems to display too much information in some instances, it might cause operator overload. Therefore, AC A3 (no operator overload) cannot be considered fulfilled. As pointed out during one of the scenario playouts by participants, filtering options could help to mitigate this. However, the reported (slight) overload of operators could also be a result of a lack of training or familiarization with the PRAETORIAN system, as participants did not receive training prior to the validation exercises. More extensive tool related trainings could be an additional mitigation step. Considering this, the AC was evaluated to be partially satisfied.

Better Resilience and Improved Coordinated Response

The results concerning the resilience and coordinated response to attacks were satisfying overall. This includes participants' opinions about PRAETORIAN enabling a faster coordinated response to cyber and physical threats, improving the resilience of CIs and enhancing teamwork between the involved parties.

In the debriefings, the possibility of exchanging experiences and transferring knowledge between different actors was highlighted as a strength of the system multiple times, along with the ability to adjust or

prepare responses to an incident. Positive remarks regarding communication, coordination and information exchange were received. Nevertheless, participants also pointed out challenges, e.g., ensuring interoperability between CIs and establishing standardized conditions. Furthermore, it became apparent that more useful communication paths need to be constituted within the system. For example, some participants expressed that communication should run across a central communication point instead of direct inter-CI communication. As one lesson learned from the validation exercises, additional actors should be included in the system in order to reflect the communication workflows of end-users appropriately, e.g., authorities or additional groups of First Responders.

Usability and Acceptance of the PRAETORIAN Solution

The third objective comprises ACs concerning acceptance, trust, usability, intuition and conformance with operators' mental models. Acceptance of the system was evaluated to be satisfying overall. For example, participants agreed that PRAETORIAN would provide advantages and innovations compared to their current systems. When asked about the advantages provided by PRAETORIAN, participants named several advantages related to both the concept and the technology. This included, e.g., advantages related to teamwork, the integration of cyber and physical components or receiving real-time information. Nevertheless, participants also indicated that improvements are needed. A large proportion of proposed improvements concerned usability-related aspects. PRAETORIAN's compatibility with applied procedures and systems should be further investigated, seeing that participants expressed neutral attitudes in this regard. For example, participants voiced concerns that PRAETORIAN might be incompatible with procedures for sharing of confidential data, or General Data Protection Regulation. Furthermore, when asked which challenges they foresee in implementing PRAETORIAN, participants' answers included, e.g.: challenges related to the compatibility with systems, procedures and regulations already in place, cost of the system, ensuring security of PRAETORIAN itself, or willingness of companies to share data.

Trust in the system was rated to be satisfactory, though some participants stressed that it is essential to ensure the security and integrity of the PRAETORIAN system itself in real operations. The integration of a large amount of sensitive (and partially confidential) data introduces the risk of elevating the system to a single-point-of-failure.

In particular usability and intuitive use of the system were identified as areas for improvement, as participants did not find the overall system intuitive. Therefore, the results regarding intuition were considered unacceptable. This again highlights the need for extensive training. While in need of improvement, the usability of the overall system was still considered partially satisfying. The overall SUS score indicated low usability in a marginal, but not yet unacceptable range (Bangor, Kortum and Miller, 2009; Brooke, 2013) and the participants indicated an overall neutral attitude concerning the system's user-friendliness. Some participants proposed that

there should be a more consistent look and use between the different HMIs, or less HMIs overall. Seeing that the PRAETORIAN system was not at a fully mature stage during the validation exercises, weaknesses regarding usability were to be expected and will likely be enhanced with increasing maturity level.

Concerning the system's conformance with end-users' mental models (i.e., in how far the system fulfils end-users' expectations), the participants mostly expressed neutral to positive attitudes. Nevertheless, this AC was evaluated to be only partially satisfying. This is because the easy integration of the system in participants' current workflows seems to need improvement.

CONCLUSION AND RECOMMENDATIONS FOR FUTURE WORK

In conclusion, participants attributed several potential benefits to the PRAETORIAN system. The overall positive questionnaire results point towards operational feasibility in principle. The validation results must, of course, be interpreted within the context of the conducted validation exercises and their limitations. However, improvements on different levels are necessary in order to establish an overarching, holistic concept ready for implementation. This includes improvements regarding systems and HMIs, procedures, and responsibilities.

For example, to improve usability, the individual tools should be harmonized regarding their design and use. Furthermore, the validations showed that PRAETORIAN's compatibility with end-users' workflows, communication paths, currently used procedures and systems needs to be considered. Following a holistic approach, PRAETORIAN is intended to be used by heterogenous CIs and end-users in Europe. To ensure compatibility with existing systems, procedures, workflows and legislations is therefore a challenging endeavour, as harmonized standards often do not exist between national CIs, not to speak about cross-border connections. Some participants viewed standardization as a necessary prerequisite for the implementation of PRAETORIAN and the interoperability between different CIs. Other participants added to the discussion that the implementation of a holistic system such as PRAETORIAN could also foster the establishment of standardized conditions. On the one hand, PRAETORIAN will likely need to adhere to differing (national or CI-specific) regulations regarding, e.g., data handling or drone neutralization. On the other hand, it is also imaginable that some regulations will be adapted in the future in order to enable a holistic, inter-CI security management, which will ideally reach cross-border. Additionally, decision-making responsibilities should be determined, e.g., whether the involvement of higher authorities is needed for risk-management decisions.

It would therefore be of interest for future research to further evaluate the concept of overarching security management of linked CIs. This should again be accompanied by validations. Based on the conducted validation exercises, some recommendations can be derived.

When evaluating a new system, a challenge lies in the selection of the right end-users for a workplace that does not yet exist. As an example, some of

the participants were not ideally suited for their assigned participant roles, e.g., due to limited IT knowledge when evaluating cyber security aspects. In future validations, more and more diverse end-users need to be included to get a more holistic picture. Generally, a bigger sample size would be advisable in order to achieve more representative results.

Furthermore, the applied validation approach was focused on subjective feedback based on the presented scenario and introduced PRAETORIAN tools, with limited hands-on experiences. Based on this, further developments of the system could be achieved. With increasing maturity, the execution of high-fidelity Human-in-the-Loop simulations with the fully developed system is recommended. This ensures a higher external validity and also allows for collection of objective performance metrics like response times. Establishing a more realistic environment would enable participants to provide more meaningful assessments of the examined AC. Performance data would be especially valuable when evaluating, e.g., in how far PRAETORIAN enables a faster detection of threats (AC A2) or a faster coordinated response (AC B1), but also for other AC.

Finally, it is noteworthy that the participants proposed several interesting ideas for additional features to be included in the system. This included, e.g., the integration of a function that monitors the current risk level for certain attacks. While a discussion of all proposed ideas is outside the scope of this work, this shows that there are potential features worth exploring in future research.

ACKNOWLEDGMENT

The authors would like to thank Andrei-Vlad Predescu and the PRAETORIAN partners' team members for their support in the project and the validation exercises. This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 101021274.

REFERENCES

Asgari, Hamid. Stelkens-Kobsch, Tim H. Montefusco, Patrizia. Abhaya, Lalitha. Koelle, Rainer. Markarian, Garik. D'Auria, Giuliano. (2017). "Provisioning for a Distributed ATM Security Management: the GAMMA Approach" in IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 11, pp. 5–21, Nov. 2017, doi: 10.1109/MAES.2017.170037.

Bangor, Aaron. Kortum, Philip. Miller, James. (2009). "Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale", Journal of Usability Studies, vol. 4, no. 3, pp. 114–123.

BBC. (2023). "Brussels explosions: What we know about airport and metro attacks," bbc.com. https://www.bbc.com/news/world-europe-35869985 (accessed Aug. 14, 2024).

Brooke, John. (1996). "SUS - A Quick and Dirty Usability Scale," in Usability Evaluation In Industry, P. W. Jordan, B. Thomas, M. I. L. and B. Weerdmeester, Eds., London, Taylor & Francis Ltd., pp. 189–194.

Brooke, John. (2013). "SUS: A Retrospective " in Journal of Usability Studies, vol. 8, no 2, pp. 29–40.

Connor, Tracy. Winter, Tom. Gosk, Stephanie. (2015). "Iranian Hackers Claim Cyber Attack on New York Dam". nbcnews.com. https://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611 (accessed Aug. 14, 2024).

Davis, Jessica. (2020). "Millions of IoT Medical Devices Impacted by Ripple20 Vulnerabilities." healthitsecurity.com. https://healthitsecurity.com/news/millions-of-iot-medical-devices-impacted-by-ripple20-vulnerabilities (accessed Aug. 14, 2024).

DPR. (2017). "WannaCry Ransomware Attack Summary," dataprotectionreport.com. https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary (accessed Aug. 14, 2024).

EUROCONTROL. (2010). "European Operational Concept Validation Methodology, EOCVM Version 3.0, Volume I," Brussels, Belgium.

Gallagher, Ryan. Bloomberg. (2020). "Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus." fortune.com. https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus (accessed Aug. 14, 2024).

Gooch, Paul. (2020). "Five reasons why cyber physical damage attacks may increase." tmkiln.com. https://www.tmkiln.com/news-insights/insights/five-reasons-why-cyber-physical-damage-attacks-may-increase (accessed Aug. 09, 2023).

Greenburg, Andy. (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." wired.com. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world (accessed Aug. 14, 2024).

IBM Corp. (2019). IBM SPSS Statistics for Windows, Version 26.0, Armonk, NY: IBM Corp.

LimeSurvey GmbH. (2024). "LimeSurvey: An Open Source survey tool" LimeSurvey GmbH, Hamburg, Germany, [Online]. Available: https://www.limesurvey.org.

Pagliery, Jose (2016). "Hackers destroy computers at Saudi aviation agency." money.cnn.com. https://money.cnn.com/2016/12/01/technology/saudi-arabia-hack-shamoon (accessed Aug. 14, 2024).

Papadopoulos, Lazaros. Demestichas, Konstantinos. Muñoz-Navarro, Eva Maria. Hernández-Montesinos, Juan José. Paul, Stéphane. Museux, Nicolas. König, Sandra. Schauer, Stefan. Climente Alarcón, Alfonso. Perez Llopis, Israel. Stelkens-Kobsch, Tim H. Hadjina, Tamara. Levak, Jelena. (2023). "Protection of critical infrastructures from advanced combined cyber and physical threats: The PRAETORIAN approach" in International Journal of Critical Infrastructure Protection, vol. 44, pp. 100657. doi: 10.1016/j.ijcip.2023.100657.

Ranger, Steven. (2018). "GitHub hit with the largest DDoS attack ever seen." zdnet.com. https://www.zdnet.com/article/github-was-hit-with-the-largest-ddos-attack-ever-seen (accessed Aug. 14, 2024).

Stelkens-Kobsch, Tim H. Carstengerdes, Nils. Reuschling, Fabian. Burke, Kelly. Mangini, Matteo. Lancelin, David. Georgiou, Eftichia. Hrastnik, Sven. Branchini, Elena. (2021). "Security Challenges for Critical Infrastructures in Air Transport" in Cyber-Physical Threat Intelligence for Critical Infrastructures Security – Securing Critical Infrastructures in Air Transport, Finance, Gas, Healthcare, and Industry.

Stelkens-Kobsch, Tim H. Boumann, Hilke. Piekert, Florian. Schaper, Meilin. Carstengerdes, Nils. (2023). "A Concept-Based Validation Approach to Validate Security Systems for Protection of Interconnected Critical Infrastructures" in The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29-September 01, 2023, Benevento, Italy. doi: 10.1145/3600160.3605025.

Winder, Davey. (2020). "COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online." forbes.com. https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online (accessed Aug. 14, 2024).
Zetter, Kim. (2016). "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." wired.com. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid (accessed Aug. 14, 2024).