A Concept-Based Validation Approach to Validate Security Systems for Protection of Interconnected Critical Infrastructures

Tim H. Stelkens-Kobsch
German Aerospace Center (DLR)
tim.stelkens-kobsch@dlr.de

Hilke Boumann
German Aerospace Center (DLR)
hilke.boumann@dlr.de

Florian Piekert
German Aerospace Center (DLR)
florian.piekert@dlr.de

Meilin Schaper
German Aerospace Center (DLR)
meilin.schaper@dlr.de

Nils Carstengerdes
German Aerospace Center (DLR)
nils.carstengerdes@dlr.de

ABSTRACT

When it comes to securing critical infrastructures, it is evident to not only provide a toolbox which allows to detect when vulnerabilities are exploited but also to support the operations in performing mitigation procedures. This paper explains how a validation was conducted in the Horizon 2020 project PRAETORIAN to evaluate the operational feasibility of a system which observes and manages security within interconnected critical infrastructures. To this end, a concept-based approach involving presentation of scenarios with the help of narrations and visual elements, hands-on experience as well as discussions and questionnaires was used. Some results are discussed to demonstrate the applicability of this approach.

KEYWORDS

Critical infrastructure protection, validation, cybersecurity, cyber-physical security, hybrid security

ACM Reference Format:
Tim H. Stelkens-Kobsch, Hilke Boumann, Florian Piekert, Meilin Schaper, and Nils Carstengerdes. 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*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3600160.3605025

1 INTRODUCTION

With the increasing political focus on security for Critical Infrastructures (CI), the need for solutions providing a holistic, complete and entire frame for securing these infrastructures is gaining a stronger momentum. Finished and on-going programs like Horizon 2020 or Horizon Europe place a high priority on the preparation of novel operational concepts and technical enablers for early deployment. The work which is reported herein bases on previous experiences gathered in projects in the area of Air Traffic Management (ATM) and airport environments. For ATM this specific project is GAMMA[1] and for airports the relevant project is SATIE[2]. In GAMMA the methodological approach was developed [1] [2] [3] [4] and updated in SATIE [5] [6], where it also received some adaptation.

The PRAETORIAN[3] project funded under the Horizon 2020 Program of the European Commission, stems from the growing need for targeted research in security for critical infrastructures. In particular the project aims to complement the developments of previous projects in this area. A major shortcoming of established validation approaches is the primary focus on the safety perspective. One vital contribution of the PRAETORIAN project is therefore – next to the development of security capabilities – to demonstrate and complement the validation activities for critical infrastructures with respect to security.

The history of validating security systems and tools is rather short and the methodology is still shaped and adapted to achieve satisfactory results and end-user acceptance for the technologies under consideration. The de-facto standard for validations in ATM and the aviation industry is the European Operational Concept Validation Methodology (E-OCVM) [7]. This methodology was already successfully applied in the above-mentioned projects which are located in different domains. Therefore, the logical decision was to also apply and adapt E-OCVM for the validation tasks in PRAETORIAN.

This paper starts to report on the preparatory action within the PRAETORIAN project to validate the newly developed solution, continues to describe the activities during the validation phase and finishes with a description of the approaches taken for evaluating the results. It represents therefore a stepping stone to integrate the validation of security functions within the wider context of validation for security in critical infrastructures.

2 THE PRAETORIAN PROJECT

In recent years, CIs receive an increasing amount of physical and cyber-attacks. These can be furbished as sole attacks (either cyber or physical) or as combined cyber-physical. Also, the risk to be attacked by so called hybrid[4] attacks increased, which typically are multi-faceted attacks being minor when experienced as a single

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605025

[1] https://www.gamma-project.eu/
[2] https://satie-h2020.eu/
[3] https://praetorian-h2020.eu/
[4] See e.g. Hybrid threats as a concept - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats.

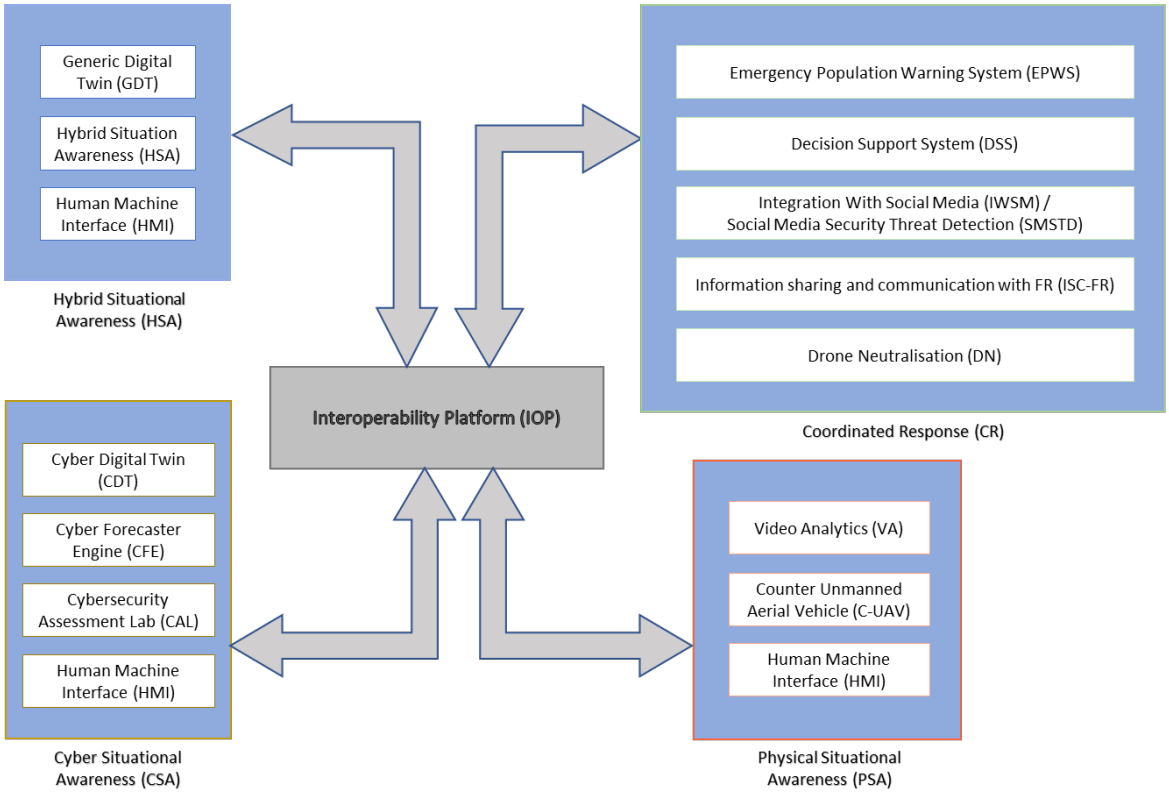

Figure 1: Main PRAETORIAN architectural components

attack but being critical when applied as composed and targeted attacks. In order to increase CI's resilience, advanced security and protection systems are required. To achieve this, the EU-funded PRAETORIAN project delivers a multidimensional installation-specific solution comprising a physical situation awareness system, a cyber situation awareness system, a hybrid situation awareness system (including digital twins), and a coordinated response system including a decision support system. The solution assists security managers of critical infrastructures in their decision-making to prevent and resist against potential cyber, physical and/or combined security threats to their own CIs and other interrelated infrastructures. The project intends to handle human-made cyber- and physical attacks and mitigate their negative effects on society. The applicability and usability of its solutions is demonstrated in four finally selected attack scenarios which are co-located at two international airports, two ports, two hospitals and two power plants and a medical laboratory. The scenarios also consider potential cascading effects, which are managed by the PRAETORIAN solution.

The strategic goal of PRAETORIAN is to increase the security and resilience of European critical infrastructures, facilitating the coordinated protection of interrelated CIs against combined physical and/or cyber threats. To that end, the project provides a multidimensional (economical, technological, policy, societal) yet installation-specific solution. The consortium consists of 23 participating entities which represent a broad cross section of stakeholders of critical infrastructures. CI operating companies as well as research institutions work hand in hand aiming to enable CI for mitigating variety of crises which may also propagate through connected CIs.

2.1 The PRAETORIAN Solution

As shown in Figure 1, the PRAETORIAN solution is mainly composed of four principal components and their respective different modules – Physical Situation Awareness (PSA), Cyber Situation Awareness (CSA), Hybrid Situation Awareness (HSA) and Coordinated Response (CR). All these four modules are interconnected with one another through the use of the Interoperability Platform (IOP).

2.1.1 The Cyber Situation Awareness System. The Cyber Situation Awareness (CSA) system is a system capable of:

1. Preventing and detecting stealth cyber threats.
2. Anticipating problems to avoid or limit them as much as possible.

It is realised by two main modules: The Cyber Forecaster Engine (CFE) and the Cybersecurity Assessment Lab (CAL), along with a Human Machine Interface (HMI) that includes new visualization paradigms for the cyber space. The CFE and CAL modules operate on different Cyber Digital Twins (CDTs), which mimic the real Information Technology / Operational Technology (IT/OT) systems of the CIs. The CSA HMI acts as the main point of command for

cyber threats. It allows the end-users to view events and alerts in real time and in a conventional list format while also including other data representation formats to enable better situation awareness and overall picture comprehension.

2.1.2 The Physical Situation Awareness System. The Physical Situation Awareness (PSA) system collects data from the legacy systems installed in CIs as well as from the newly deployed sensors (e.g., sound sensors, video / IR cameras, presence sensors, sonar, ...), which were introduced as situation awareness indicators by the project. It provides features such as dynamic location of resources and assets, security perimeter control, real time video analysis (through the Video Analytics [VA] module) and rogue drone detection (using the Counter Unmanned Aerial Vehicle [C-UAV] module). The main visual component is the PSA HMI, including a Geographical Information System (GIS) on which to represent geolocated data such as security staff & vehicles, sensors, alarms related with physical incidents and the 3D cartography of some areas of the CI.

2.1.3 The Hybrid Situation Awareness System. The Hybrid Situation Awareness System (HSA) system receives alarms from both cyber and physical domains (through the CSA and PSA) and correlates them to calculate the potential propagation of threats. It is supported by a Generic Digital Twin, which models the most relevant assets of the individual CIs and the relationships among them, and reflects the potential consequences or effects of the detected threat over a single CI as well as over its related ones. The HSA HMI or front end is the main interface for interacting with the HSA system. It provides means and interfaces to configure data sources (connection to CSA and PSA) as well as data sinks (connection to Emergency Population Warning System [EPWS] and Decision Support System [DSS]) as well as all the required parameters of the system itself (data storage, communications mechanisms, thresholds, etc.).

2.1.4 The Coordinated Response System. The Coordinated Response (CR) system is used for the coordination of the emergency plans of all the CIs, processing the information coming from the other three core components (CSA, PSA and HSA) to enable a more effective response to the hazards. There are five main modules that are part of the CR system: the DSS orchestrates the emergency plans of the CIs involved in the project by providing response(s) to detected threats in an automated manner; the EPWS implements the EU-ALERT service, based on ETSI TS 102 900 V1.3.1 (2019-02) [8], relying on special notifications to mobile phones geolocated in a specific area; the "Integration With Social Media" (IWSM) component allows to alert the population through social media channels; the "First Responders (FRs) Information sharing technologies" (ISC-FR) component is the communication channel through which the FRs and rescue teams will be contacted in case of an incident; the "Social Media Security Threat Detection" (SMSTD) component monitors social media channels to identify posts relevant to an incident; and finally, a C-UAV system (the Drone Neutralization [DN] module) provides technological foundation for countering drones.

2.1.5 The Interoperability Platform. The Interoperability Platform (IOP) interconnects all the modules of the PRAETORIAN solution, allowing the exchange of information between all systems and modules through multiple communication protocols (e.g., MQ Telemetry Transport [MQTT], Neural Autonomic Transport System [NATS], Distributed Data Protocol [DDP], and others). It also provides other functionalities such as information storage, avoidance of data duplication between modules, replication of changes and possible inconsistencies, thereby providing data for the whole platform through the usage of database technologies such as MongoDB.

3 METHODS USED

The process of validating the system under consideration followed the process shown in Figure 2. In earlier stages of the project, the CI related requirements and architectural information were already gathered. Then, in the preparation of the validation exercises the validation needs as well as the needs for setting up the validation platform were elaborated. In this respect, the validation platform has to be understood as the combination of the PRAETORIAN solution and the validation/ simulation environment. The needs were then aligned with the technological development of the validation platform and its timing, as this had to happen in parallel. Before the validation exercises could start, the different prototypes were connected utilising standard interfaces where applicable. PRAETORIAN also provides the opportunity to connect legacy systems of the CI. Within this step, the validation plan [9] was written and the scenarios were finalised, which were already available in a premature version when the preparations for the validation exercises started.

Having the validation plan, the interconnected systems and the scenario descriptions finally set, the first validation exercise was conducted. The data gathered in this first exercise was already considered for further development of the following validation exercises and so forth, i.e. an iterative approach was chosen ("iterative validation results"). After the last validation had finished, the evaluation of the entire set of validation results was conducted. Applying this approach means, that results from one validation can not necessarily be compared in entirety with the others. This was accepted in order to allow to further develop the PRAETORIAN solution still in the validation phase. However, subgroups of the questions could further be applied in the consecutive validation exercises, when the content, the questions were dealing with, was not changed from one exercise to the other. More details on the chosen methods, the gathered data and the results achieved are reported in the validation report of PRAETORIAN [10] (which was, however, labelled as a consortium confidential document by the EC and is therefore limited in access).

3.1 Sample group of participants for validations

Twenty-four participants attended the PRAETORIAN validation exercises overall. Participants were recruited from the CIs and from FR organisations involved in the validation scenarios, i.e., they were employees of partners in the PRAETORIAN consortium but not directly involved in the project. Participant roles included experts from a Hydro Power Plant (HPP), two hospitals, two ports, a power plant, two airports, a laboratory and three FR organisations. Scenario #1 additionally involved an external participant not directly employed by one of the involved CIs but by an affiliated company. This person was recruited due to their expertise in relation to cybersecurity of this one participating CI. Participants were selected

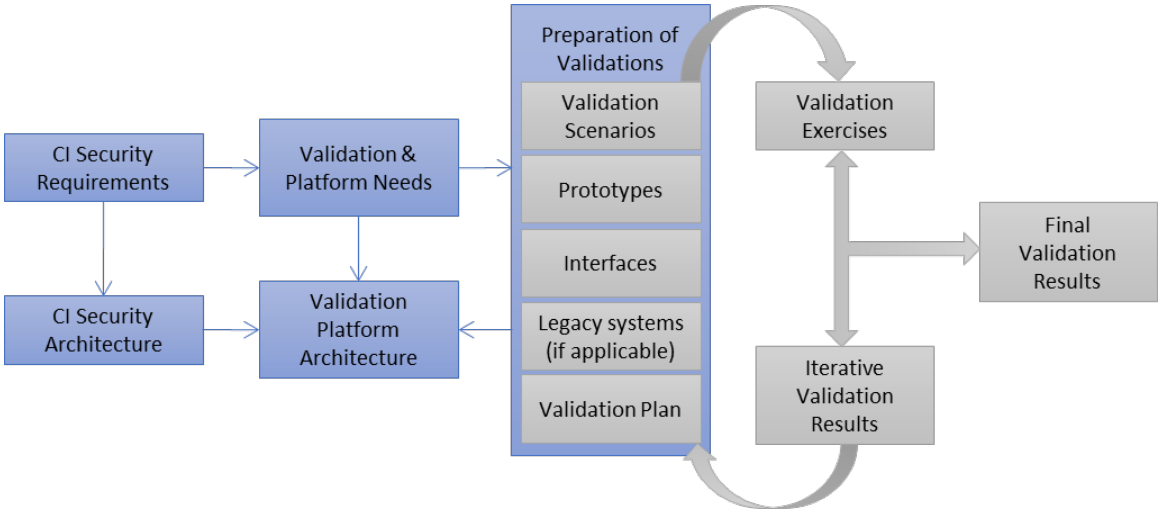

Figure 2: Process of setting up validations for CI security (adapted from [2]).

to represent one specific role of the validation scenario. Some participant roles were represented by more than one participant, and sometimes one participant represented several participant roles. Each validation scenario was exercised once and experienced only by one group of participants. Scenario #1 involved five participants, scenario #2 eight participants, scenario #3 six participants and scenario #4 involved five participants. Informed consent was obtained from participants in advance to the validation exercises.

3.2 Objectives and Acceptance Criteria

Five validation objectives (Obj.) were extracted based on objectives which were defined already in the planning phase of PRAETORIAN. These were further divided into seventeen Acceptance Criteria (AC). In order to validate the PRAETORIAN solution, it was evaluated in how far each AC and in consequence, objective, was satisfied. This was done by evaluating the bespoke validation questionnaire, the debriefing feedback and the System Usability Scale (SUS) [11], see section 3.3. Table 1 summarizes the objectives and AC. Tick marks indicate the metrics used to assess an AC. AC_10 "The PRAETORIAN solution is cost-effective" was not assessed with any dedicated questionnaire or debriefing questions. Nevertheless, participants provided some feedback related to cost-effectiveness on their own accord.

3.3 Validation Scenarios and Material

3.3.1 Validation Scenarios. Four scenarios involving physical and cyber-attacks on multiple CIs have been developed within the PRAETORIAN project. The scenarios were constructed in order to illustrate the functionalities of the different PRAETORIAN modules in a realistic way.

- Scenario #1 is a cross-border scenario involving a combined physical and cyber-attack on a hydro power plant. The attack results in a power blackout and a flooding in the region, both of which affect a nearby hospital.
- Scenario #2 includes combined cyber and physical attacks on both a port and a power plant.
- Scenario #3 focuses on a combined cyber and physical attack on a port, resulting in cascading effects for the area, a nearby hospital and an airport.
- Scenario #4 is a cross-border scenario about the theft of a biohazardous sample from a laboratory which is then transported to an airport.

For each of the validation scenarios, supporting roles (e.g., attackers, security staff) and participant roles (i.e., people from one of the involved CIs or FR organisations interacting with the PRAETORIAN system) were identified. Each participant represented one or more participant roles. For each step of the scenarios, the involvement of and interactions between supporting roles, participant roles and individual PRAETORIAN tools were extracted. The respective validation scenario was presented to participants using presentation slides. In the beginning, a short overview of the scenario was given. Following this, each scenario step was narrated in more detail, e.g. with the help of pictures or videos. The involved participants were asked about their current operations and systems in the context of the respective scenario step. Then, relevant PRAETORIAN tools were demonstrated to the participants. To this end, some of the alerts and notifications were simulated in the background and tool developers showed the resulting information on the human-machine interfaces (HMIs) via screensharing. An exception to this was scenario #2, in which some parts were executed live on the related digital twin. Participants also had the opportunity to try out the system on their own screens in parallel. In some cases, participants were asked to share their own screens and were guided through using the interfaces. The role-dependent log-in was processed before the start of each validation scenario. After the respective tools of the scenario step have been demonstrated, participants were asked to provide their feedback on the tools. The tools shown and the questions asked were designed specifically for the different validation scenarios.

Table 1: Validation objectives and acceptance criteria (tick marks indicate the metrics used to assess an AC)

			Metrics		
			Bespoke validation questionnaire	Debriefing	System Usability Scale
Obj. 1	Improve the understanding of any physical or cyber threats and their consequences in the interdependent network of critical infrastructures				
	AC_01	The PRAETORIAN solution **enhances situation awareness.**	✓	✓	
	AC_02	... **enables a faster detection of cyber and physical threats.**	✓	✓	
	AC_03	... **does not induce operator overload.**	✓	✓	
	AC_04	... **provides the relevant information.**	✓	✓	
	AC_05	... **provides helpful decision support.**	✓	✓	
Obj. 2	Improve the resilience of the CIs, their neighbouring population and environment and enable a coordinated response to an attack				
	AC_06a	... **enables a faster coordinated response to cyber and physical threats.**	✓	✓	
	AC_06b	... **improves the resilience of CIs.**	✓	✓	
	AC_07	... **enhances teamwork between the parties involved, e. g. operators and first responders.**	✓	✓	
Obj. 3	Share with the public pertinent information on the risks associated to an event and the emergency response actions planned to overcome the incident				
	AC_08	... **allows faster sharing of relevant information with the public.**	✓	✓	
Obj. 4	Validate the project results in real contexts of interdependent CIs to improve its efficiency, cost-effectiveness and societal benefit				
	AC_09	... **is efficient.**	✓	✓	
	AC_10	... **is cost-effective.**			
	AC_11	... **has societal benefit.**	✓	✓	
Obj. 5	The overall PRAETORIAN solution as well as its individual tools and functionalities are accepted and easy to use.				
	AC_12	... **is accepted.**	✓	✓	
	AC_13	... **is trustworthy.**	✓	✓	
	AC_14	... **is usable.**	✓	✓	✓
	AC_15	... **is intuitive to use.**	✓	✓	
	AC_16	... **conforms to operators' mental models.**	✓	✓	

3.3.2 Debriefing Questions. Seven debriefing questions were asked at the end of each of the validation scenarios and discussed with all participants of the respective validation exercise. The first block consisted of these four questions:

1. *Which benefits do you see in the **concept** of PRAETORIAN?*
2. *Which benefits do you see in PRAETORIAN's **technology**?*
3. *How could the **concept** of the PRAETORIAN system be improved?*
4. *How could PRAETORIAN's **technology** be improved?*

Then, there was a second part consisting of three questions which were introduced by the following sentence:

PRAETORIAN can share the information you received during the previous attacks with other critical infrastructures on a European scale.

1. *Which benefits do you see in this kind of cooperation?*
2. *Which obstacles do you see in this kind of cooperation?*
3. *Do you want to share any final comments?*

3.3.3 Questionnaires. An online questionnaire was created using LimeSurvey [12], which is an internet based free and open source online statistical survey web app, enabling users using a web interface to develop and publish online surveys, collect responses, create statistics, and export the resulting data to other applications. The questionnaires were sent to participants at the end of each validation exercise or in retrospect via e-mail. It consisted of the bespoke validation questionnaire and the SUS.

Bespoke validation questionnaire

The bespoke validation questionnaire comprised statements and questions about the integrated PRAETORIAN solution, the validation scenarios as well as statements and questions about individual PRAETORIAN tools. Each statement and question were assigned to one of the AC in advance or considered additional feedback if no AC could be assigned.

Statements and questions regarding the integrated PRAETORIAN solution and the validation scenarios were shown to all participants. Statements and questions regarding individual tools were

Table 2: Types of questions in the bespoke validation questionnaire

Topic	No. of questions per question type			Total no.
	Rating scale	Free text	Other	
Validation scenario	2	0	0	2
Integrated system	31	6	0	37
PSA	12	3	0	15
CSA	12	4	0	16
HSA	10	0	0	10
CR	13	2	1	16
General	1	1	1 (Multiple select)	3
DSS	5	1	0	6
Chat tool	1	0	0	1
ISC-FR	2	0	0	2
EPWS	1	0	0	1
IWSM	2	0	0	2
SMSTD	1	0	0	1

shown only to those participants who interacted with said tools during the validation scenario according to the participant role they assumed. One exception to this was "Security officers should be alerted in case of a detection of a suspicious post (e.g. a tweet) of high criticality" about the SMSTD, which was answered by all participants who experienced scenario #3 (instead of only the one participant who interacted with the SMSTD) to increase the number of data samples.

Statements were 5-point Likert items, with 1 = "strongly disagree" and 5 = "strongly agree". Means (M) and standard deviations (SD) were calculated per statement. In order to be considered acceptable, a mean rating equal to or higher than the neutral rating of 3 ("neither agree nor disagree") had to be reached. For inverse statements, the mean rating had to be lower than 3. In addition, there were free text questions and one multiple select question which were also assigned to one AC each. Some free text questions were presented as follow-up questions only if participants' ratings of a specific statement exceeded or fell below a certain criterion (e.g., an agreement lower than 3). Table 2 provides an overview of the types of questions in the bespoke validation questionnaire.

System Usability Scale

The SUS [11] was filled in by all participants in order to assess the usability of the PRAETORIAN solution (AC_14 "The PRAETORIAN solution is usable."). It is made up of ten statements which are rated as 5-point Likert items, with 1 = "strongly disagree" and 5 = "strongly agree". SUS scores ranging between 0 and 100 were calculated from the ratings of the ten statements as described in Brooke [11]. In keeping with Bangor et al. [13] SUS scores under 50 were considered unacceptable and SUS scores above 70 were considered acceptable. The range between 50 and 70 constitutes a range of marginal acceptability. Bangor et al. [13] divided this further into a "high marginal" range for scores just over 60 to 70 and a "low marginal" range for scores between 50 and just over 60.

3.4 Procedure of Validation Exercises

There was one validation exercise per validation scenario. The validation exercises were conducted remotely with the help of video-conferencing tools. Each exercise took place over the course of one day. In the morning, participants were welcomed and informed consent was ensured. After an introduction to the validation exercises, participants were given an overview of the PRAETORIAN solution as well as more detailed presentations about its individual modules and tools (CSA, PSA, HSA, CR as well as DD and DN). Participants were informed that asking questions was allowed at all times and a question-and-answer session was offered after all PRAETORIAN tools were presented.

In the afternoon, participants logged in to the different PRAETORIAN modules. Then the validation scenario was presented to participants as outlined in 3.3.1. At the end of the validation scenario, the debriefing questions were asked and discussed with all participants of the validation exercise. Finally, participants received a link to the online questionnaire including the bespoke validation questions as well as the SUS. Due to time restraints, the link to the online questionnaire was shared via mail after the respective validation exercise in most cases, so the majority of participants filled in the questionnaire unsupervised after some time had passed following the validation exercise.

The conduct of validation exercise #2 deviated from this procedure because four participants were unable to attend the validation exercise live. Instead, these participants provided their written feedback based on recordings of the validation exercise.

3.5 Methods for Data Analysis

Quantitative data analysis (participants' ratings of statements in the bespoke validation questionnaire and the SUS) was conducted descriptively using IBM SPSS Statistics version 26.0.0.1 [14]. Mean SUS scores as well as M and SD for statements about the integrated system were calculated per scenario and also in an aggregated manner over all 24 participants. M and SD for bespoke statements about individual tools were calculated in an aggregated manner for all participants who interacted with the tool in question and

Table 3: Number of answers to the bespoke validation questionnaire included in data analysis

Topic	No. of answers analysed
Validation scenario	24
Integrated system	24
PSA	11
CSA	7
HSA	11
CR	
General	24
DSS	16
Chat tool	15
ISC-FR	5 / 6
EPWS	7
IWSM	5
SMSTD	6

were therefore presented with such statements. The SUS and the bespoke validation questionnaire were analysed in the context of the assigned ACs.

The feedback received during the validation scenarios was evaluated qualitatively on scenario-level and lessons learned were extracted. Participants' answers to the debriefing questions and free text questions from the bespoke validation questionnaire were analysed in an aggregated manner and categorized by AC. If no AC could be identified as fitting, feedback was categorized as additional feedback.

The following steps were taken for data cleansing: Some questionnaire answers regarding certain tools were excluded from data analysis because specific participants reported not being the right users for said tool, either in the questionnaire or during the validation exercise. This applied to two participants with regards to the PSA and two participants with regards to the CSA. The statement "Compared to my current situation, it is easier for me to send EU_ALERT messages in selected areas using the Emergency Population Warning System." about the EPWS was excluded from data analysis entirely because most participants reported not having sufficient permits for alerting the population.

The number of answers analysed per topic in the bespoke validation questionnaire are summarized in Table 3. This serves to give an impression of the underlying data basis.
In order to accommodate the diverse pool of participants utilizing the ISC-FR, the evaluation was thoughtfully divided into two distinct parts, ensuring a proper reflection of the different end-users. Just answers from participating FRs were considered for the statement "The information provided by the Coordinated Response tool enables first responders to respond effectively to an ongoing incident.". This delivered five answers (see Table 3). On the other hand, no answers from FRs were considered for the statement "The operators can dispatch information about ongoing incidents to the first responders in a user-friendly way". This resulted in six answers (see Table 3).

4 EVALUATION OF VALIDATION EXERCISES

In this section, a final condensed summary of the results is presented in order to demonstrate the applicability of the validation approach that was used. The evaluation was a multi-step approach including the analysis of individual statements and questions from the bespoke validation questionnaire, SUS scores, debriefing feedback and feedback from the validation scenarios. First of all, the achievement of objectives due to the fulfilment of the different AC was evaluated. This was reached with the help of the bespoke validation questionnaire, the SUS and the debriefing. Secondly, lessons learned based on the feedback received during the validation scenarios were extracted. Lastly, additional feedback that does not fall into one of the before mentioned categories is summarized.

4.1 Achievement of Objectives

The main outcome of a validation exercise is to assess if the validation objectives have been fulfilled. In order to measure this, the

Table 4: Objectives assessed in the validation

Objective No.	Description	No. of related acceptance criteria	OK/ partially OK/ Not OK/ not assessed	No. of corresponding questionnaire items
1	Improve the understanding of any physical or cyber threats and their consequences in the interdependent network of critical infrastructures.	5	4/1/0/0	22
2	Improve the resilience of the CIs, their neighbouring population and environment and enable a coordinated response to an attack.	3	3/0/0/0	12
3	Share with the public pertinent information on the risks associated to an event and the emergency response actions planned to overcome the incident.	1	1/0/0/0	1
4	Validate the project results in real contexts of interdependent CIs to improve its efficiency, cost-effectiveness and societal benefit.	3	2/0/0/1	3
5	The overall PRAETORIAN solution as well as its individual tools and functionalities are accepted and easy to use.	5	2/2/1/0	51

Table 5: Lessons learned from validation exercises

ID	Source	Lesson learned
1	Scenario #1	Reflect end-users' communication workflows accurately for validations.
2	Scenario #1	Consider use of a central point of communication between CIs.
3	Scenario #1	Realise, show and connect assets on all logical levels.
4	Scenario #2	Improve user interface design and tools' customization capabilities (adaptation of level of detail).
5	Scenario #2	Ensure interoperability with existing systems.
6	Scenario #3	Assess existing communication channels and the need for new or additional communication channels.
7	Scenario #3	Improve user interface design and tools' customization capabilities (adaptation of level of detail).
8	Scenario #3	Improve user interface design and tools' customization capabilities (filtering of information).
9	Scenario #3	Add more sensors to the system.
10	Scenario #3	Provide training for participants to be able to explore full functionality of the system.
11	Scenario #4	Consider all necessary end-users in conceptualisation of scenario.
12	Scenario #4	Encourage relevant stakeholders to participate in validations.
13	Scenario #4	Consider national/regional legislations as well as CI-specific responsibilities and regulations.
14	Scenario #4	Evaluate if whether operating the system under consideration might require implementation of new jobs and re-definition of responsibilities.
15	Scenario #4	Re-evaluate events that trigger alerts in the system (not all events displayed were considered meaningful).
16	Scenario #4	Include a database of lessons learned from previous incidents in order to gather information on how to handle certain incidents.
17	Scenario #4	Provide practical guidance on how to react when faced with possible cascading effects (probabilistic information about cascading effects might not be sufficient for end-users).

PRAETORIAN project defined specific acceptance criteria as reported in section 3.2. Table 4 shows the extent to which the AC were satisfied. The majority of the assessed acceptance criteria was rated with "OK" (66.7% and more), whereas there seems to be some potential for improvement for the PRAETORIAN solution functionality (40% "OK"), see objective 5.

In detail (see Table 1 and Table 4), the AC_03 (objective 1), AC_14 (objective 5) and AC_16 (objective 5) were evaluated as partially OK. Rated as Not OK was AC_15 (objective 5), while AC_10 (objective 4) was not assessed. Following up on that (and without weighing the different AC against each other), it can be claimed that the majority of objectives was met while the fulfilment of objective 4 and objective 5 can be discussed and improved in future work.

Overall, PRAETORIAN seems to be a sufficiently accepted and trustworthy system that offers benefits and innovations. Nevertheless, there is certainly room for improvements in some cases. This mainly concerns usability of the system, intuitive use and compatibility with end-users' current workflows.

4.2 Lessons Learned

The identification of lessons learned is a prominent part for the evaluation of validation exercises and contributes to the further development of systems as well as future research. The input originates from subject matter experts and operators who handle security events in their daily work, as well as observations made during the validation exercises. Table 5 summarises the lessons learned which were identified during and after the validation exercises.

4.3 Additional Feedback

Unrelated to any of the AC or objectives, the answers of the participants indicated some important items:

1. Possible competition in the market needs to be considered. Depending on the needed time-to-market and having it fully developed soon, PRAETORIAN might set new standards for other security systems to come as it would be the first holistic, inter CI security solution to be available.
2. National regulations could restrict the use of some PRAETORIAN functions. As an example, rules for drone neutralization differ between countries. In addition, it should be evaluated whether differing legislations could impair cooperation on a European scale.
3. Responsibilities regarding decision-making for risk-management must be decided when determining the roles of end-users of the PRAETORIAN system. For example, involvement of higher authorities might be necessary.

Furthermore, participants' answers to the bespoke validation questionnaire statements about the validation scenarios indicated that all validation scenarios could be considered adequately understandable and realistic.

5 DISCUSSION AND CONCLUSIONS

This section provides the wrap-up of the result interpretation from the PRAETORIAN validation and reflects the suitability of the concept-based validation approach that was taken, also mentioning the limitations that apply.

The approach explained by the E-OCVM [7] was taken and adapted to the security management research conducted in PRAETORIAN to identify whether the developed system is considered operationally feasible by experts participating in the validation exercises. To answer this question, the formulated validation claim ("it is operationally feasible") was broken down into independent validation objectives (see table 1 in section 3.2). These objectives

are high level but operationally more graspable that the validation claim. Further, several acceptance criteria (AC) were defined (see table 1 in section 3.2) that detail the objectives further. To assess if an AC was successfully achieved, suitable metrics were chosen and designed. This comprised the debriefing and the questionnaires. Then the designed validation exercises were executed and relevant data were gathered from participants. Their answers were analysed and interpreted in the context of each AC as described in section 3. Tables 2 (section 3.3.3) and 4 (section 3.5) allow to assess the confidence level that may be put into the results. Based on these analyses, a status (OK/partially OK/not OK) was applied to each AC. Compiling an overall answer from the set of AC for a given validation objective, the objectives were discussed with regards to benefits, areas of improvement and other noteworthy participant feedback that was identified. Based on the overall view on the entirety of objectives, the central validation claim was positively answered.

In conclusion, following the E-OCVM notion [7], the selected concept-based validation approach is suitable of validating the addressed E-OCVM levels 1 (proof of concept/scope) and 2 (proof of feasibility) (i.e. Technological Readiness Level [TRL] 1-3). The proof of operational feasibility (E-OCVM level 2; TRL 2/3) of a cross-CI approach to attack-detection was achieved. Reformulating this central claim, confidence was achieved to the question "are we building the right system?", although the evaluation still indicates some areas of improvement. E-OCVM level 3 (deriving the operational benefit and pre-industrial development and integration; TRL 4/5) includes the prototypical implementation in a suitable environment. A distributed and simulated approach is the only feasible way to ensure that adequate attack scenarios can be performed against the system, without actual generation of harm at any involved critical infrastructure installation. Further, waiting for suitable attacks to happen is no choice either, for completeness. Since the taken approach was concept-based and did lack the dynamic aspect of a live system in a near-to-the-target environment that E-OCVM prescribes, the PRAETORIAN solution did not reach sufficient maturity for E-OCVM level 3 until the end of the validation exercises. This again is another proof that the E-OCVM methodology as such can be applied to this research domain, as it clearly provided boundaries regarding maturity assessments/achievements. However, the application of the methodology as shown in this paper would benefit from an additional validation conducted in a more realistic and interactive set up. This could confirm the confidence in those AC like operator overload or situation awareness and enable the measurement of e.g., the time-to-detect cyber-physical attacks with feasible objective metrics.

Further, the selected validation approach was robust against adaptations of the underlying technical system due to development and functionality implementation progress, as it was not fully clear how mature the system and especially its HMIs would be for the validation execution. The approach of explaining the development of an attack situation to the participants while showing them the corresponding indications and events in the PRAETORIAN tools and supporting this with explanatory presentation slides was deemed to be the most feasible and applicable approach for receiving interpretable results. This again is fully compliant with the E-OCVM methodology for the anticipated maturity level. Another indication of robustness was observed when, e.g., some participants had time constraints and could not attend for the full exercise duration. As a consequence, they were only able to fill in the questionnaires the following days and not directly in the aftermath of the exercise. The chosen approach allowed to gather their answers retrospectively even though their memory might have been blurred. Furthermore, one stakeholder group could not participate to the live validation exercises due to a short-notice union strike on the day of the exercise. To cope with this situation, it was decided to record the respective validation exercise and let the specific group of participants watch and answer the questionnaires and debriefing questions at a later point. Nevertheless, the feedback provided by these participants seemed sufficiently high in quality and was therefore included in the data analysis. It becomes clear that the chosen concept-based validation approach allowed for the necessary level of flexibility in order to react to the challenges that occurred in the process of preparing and conducting the validation exercises.

To conclude, based on the experience gathered during the PRAETORIAN validation, the concept-based approach to validate security systems for the protection of interconnected CIs proved applicable. In the PRAETORIAN project, the concept-based approach offered the possibility to gather valuable feedback and insights from experts. In highly complex, interrelated environments with a multitude of systems with different individual maturity levels, the concept-based approach offers unique possibilities. It is a flexible, efficient and effective option for early validation exercises (low E-OCVM or TRL levels) within an iterative evaluation process.
Further reading about PRAETORIAN can also be found in [15] [16].

ACKNOWLEDGMENTS

This work has received funding by the EU H2020 research and innovation programme under grant agreement No 101021274. (PRAETORIAN, https://praetorian-h2020.eu/).

REFERENCES

[1] Patricia Montefusco, Rosana Casar, Rainer Koelle and Tim H. Stelkens-Kobsch, "Addressing Security in the ATM Environment: From Identification to Validation of Security Countermeasures with Introduction of New Security Capabilities in the ATM System Context," 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 2016, pp. 532-541, doi: 10.1109/ARES.2016.67.

[2] Tim H. Stelkens-Kobsch, Michael Finke, Denis Kolev, Rainer Koelle and Roul Lahaije, "Towards validating a security situation management capability," 2016 Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, USA, 2016, pp. 1A1-1-1A1-9, doi: 10.1109/ICNSURV.2016.7486320.

[3] Meilin Schaper, Tim H. Stelkens-Kobsch and Nils Carstengerdes, "From preparation to evaluation of integrated ATM-security-prototype validations," 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, 2017, pp. 1-8, doi: 10.1109/DASC.2017.8102100.

[4] Tim H. Stelkens-Kobsch, Michael Finke and Nils Carstengerdes, "A comprehensive approach for validation of air traffic management security prototypes: A case study," 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, 2017, pp. 1-10, doi: 10.1109/DASC.2017.8102082.

[5] John Soldatos, Isabel Praça, Aleksandar Jovanović (Eds.). (2021). Chapter 10: Security Challenges for Critical Infrastructures in Air Transport; Tim H. Stelkens-Kobsch, Nils Carstengerdes, Fabian Reuschling, Kelly Burke, Matteo Mangini, Davide Lancelin, Eftichia Georgiou, Sven Hrastnik and Elena Branchini. In Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry (pp. 232–253). Now Publishers. https://doi.org/10.1561/9781680838237

[6] John Soldatos, Isabel Praça, Aleksandar Jovanović (Eds.). (2021). Chapter 11: Toolkit to Enhance Cyber-physical Security of Critical Infrastructures in Air Transport; Fabian Reuschling, Nils Carstengerdes, Tim H. Stelkens-Kobsch, Kelly Burke, Thomas Oudin, Meilin Schaper, Filipe Apolinário, Isabel Praça

and Leonidas Perlepes. In Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry (pp. 254–287). Now Publishers. https://doi.org/10.1561/9781680838237

[7] EUROCONTROL, European Commission, European Operational Concept Validation Methodology, E-OCVM, Version 3, Volume I, February 2010.

[8] ETSI TS 102 900 V1.3.1 (2019-02). Retrieved May 10, 2023 from https://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.03.01_60/ts_102900v010301p.pdf

[9] Hilke Boumann, Andrei-Vlad Predescu, Tim H. Stelkens-Kobsch, Yves Günther, Nils Carstengerdes, Helena Opower, Ev Muñoz, Juan José Hernández, Frédéric Guyomard, Siham Farina, Franck Bouzon, Mourad Leslous, Mohammed Hibti, Tamara Hadjina, Lazaros Papadopoulos, Klemen Gregorc, Markus Plass, Israel Pérez, Javier Hingant, Jelena Levak and Stefan Schauer. (2022). PRAETORIAN D7.2 Validation Plan (Consortium Confidential). European Commission.

[10] Hilke Boumann, Andrei-Vlad Predescu, Tim H. Stelkens-Kobsch, Florian Piekert, Meilin Schaper, Nils Carstengerdes, Eva Muñoz Navarro, Juan José Hernández, Alfonso Climente, Javier Hingant, Tamara Hadjina and Lazaros Papadopoulos (2023). PRAETORIAN D7.4 Validation Report (Consortium Confidential). European Commission.

[11] John Brooke, (1996). SUS - A Quick and Dirty Usability Scale. In Patrick W. Jordan, B. Thomas, Ian Lyall McClelland and Bernard Weerdmeester (Eds.), Usability Evaluation In Industry (pp. 189-194). Taylor & Francis Ltd.

[12] Limesurvey: An Open Source survey tool. LimeSurvey GmbH. http://www.limesurvey.org

[13] Aaron Bangor, Pilip Kortum and James Miller (2009). Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. Journal of Usability Studies, 4(3), 114-123.

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

[15] Sandra König and Abdelkader Magdy Shaaban. 2022. Parametrization of Probabilistic Risk Models. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for Computing Machinery, New York, NY, USA, Article 129, 1–6. https://doi.org/10.1145/3538969.3544454

[16] Florian Piekert, Nils Carstengerdes, Meilin Schaper, Hilke Boumann, Tim H. Stelkens-Kobsch, and Andrei-Vlad Predescu (2023). Mitigation of Operational Impacts on Airports by early Awareness of malicious Events impacting linked Critical Infrastructures [Manuscript submitted for publication]. Air Transport Research Society ATRS World Conference 2023, Kobe, Japan.