XA4AS: Adaptive Security for Multi-Stage Attacks

Elias Seid, Oliver Popov and Fredrik Blix
Department of Computer and Systems Sciences, Stockholm University, Sweden

Keywords: Security Engineering, Control Theory, Adaptive Systems, Security Solution, Multiple Failure, Cyber-Physical Systems.

Abstract: Identifying potential system threats that define security requirements is vital to designing secure cyber systems. Furthermore, the high frequency of attacks poses an enormous obstacle in analysing cyber-physical systems (CPS). The paper argues for the idea that any security solution for cyber-physical systems (CPS) should be adaptive and tailored to the specific types of threats and their frequency. Specifically, the solution should consistently monitor its surroundings in order to protect itself from a cyber-attack by adjusting its defensive measures. Understanding cyberattacks and their potential consequences on both internal and external assets in cyberspace is essential for preserving cyber security. The importance appears in the work of the Swedish Civil Contingencies Agency (MSB), which collects IT incident reports from vital service providers required by the NIS directive of the European Union and Swedish government agencies. The proposed solution is the Adaptive security framework, which aims to simplify the development of analytical models for implementing model predictive control and adaptive security solutions in the field of CPS. This study analyses security attacks and corresponding security measures for Swedish government agencies and organisations under the European Union's NIS mandate. A thorough analysis of adaptive security was conducted on 254 security incident reports provided by vital service providers. As a result, an overall total of five security measures were identified.

1 INTRODUCTION

The confluence of digital technology has led to substantial tangible consequences arising from mishaps in the virtual realm. A recent study conducted by Van den Berg et al. (2022) differentiates between the immediate and indirect consequences of cyber attacks. The direct impact on cyberinfrastructure relates to the potential ramifications of actions that could lead to unauthorised entry, modification, or removal of digital assets. The immediate effect is comparable to classifiers that evaluate the operational and informational consequences (Pursiainen, C. et al., 2018). The indirect impact refers to the consequences of an event that takes place outside of the digital domain (Van den Berg et al., 2022). Furthermore, the investigation undertaken in citation (Wang, E.K. et al., 2010) evaluated both the primary and secondary consequences of cyber incidents.

The organisation, stakeholders, government, and society might face significant repercussions as a result of data fraud, destruction, or compromise. When evaluating cyberattacks on critical service providers, it is imperative to take into account these consequences (Uzunov, A.V. et al 2012). The main secondary impacts on an institution typically involve financial consequences. Organisational risk assessments employ anticipated financial and economic damages to evaluate the probability and consequences of certain situations. The commercial and financial consequences are major when a loss of competitive advantage occurs as a result of the disclosure of sensitive information or a disruption. A comprehensive investigation was carried out to determine the typical expenses associated with cyber incidents across several industry sectors, with a specific emphasis on identifying the most severe categories. Financial loss is considered a factor in their cyber risk model (Gopstein, A. et al., 2020; Mancuso, V.F.et al., 2014).

Most software systems today are cyber-physical system components. CPSs include robots, mobile devices, and humans. CPS constituents are autonomous but work together to achieve system requirements. Healthcare, government, and financial services software systems are often CPS (Griffor et al., 2017; Boyes, 2018). Smart things have diverse, dynamic, and flexible sensor networks. These networks have distributed intelligent devices that can be easily at-

Seid, E., Popov, O. and Blix, F.
XA4AS: Adaptive Security for Multi-Stage Attacks.
DOI: 10.5220/0012707400003705

In *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)*, pages 284-293
ISBN: 978-989-758-699-6; ISSN: 2184-4976

tached to physical objects. These devices measure temperature, sound, vibration, pressure, and motion. They can also send data to remote software systems.

In the last ten years, different sectors in society have undergone a rapid process of digitalization. A notable trend is the transfer of vital information resources and organisational procedures from physical to digital platforms. The introduction of innovative socio-technical solutions has resulted in several benefits by dramatically enhancing operational efficiency in both corporate and governmental organisations, thus transforming the way information and processes are managed. Nevertheless, technology has also introduced new and unique challenges. The growing dependence on systems and networks has resulted in heightened susceptibility for crucial service providers, such as government agencies and healthcare institutions, to incidents that disrupt their operations (Urbach, N. et al., 2019).

CPS security breaches have cost large corporations millions of dollars in monetary losses. Furthermore, these expenses are rising (Ponemon et al., 2015). The complexity of CPS, including people, procedures, technology, and infrastructure, contributes to the occurrence of breaches. The inclusion of diverse components in a system might increase security concerns and attack potential, unlike homogenous software systems. Breach causes include trusted insiders, malware, SQL injections, compromised devices, and other factors. CPS are vulnerable to multistage attacks due of the increasing frequency of attacks. Attackers can execute more dangerous attacks by integrating atomic attack procedures with diverse components (Shostack, 2014).

Designing a security solution for CPS is more complex than for software systems, as it involves considering both individual components (e.g., sensing, communication, processing) and their interaction with the physical environment (Banerjee,2012). Adversaries can target vulnerable and risky CPS elements. This is because components like sensors operate in an unprotected environment without adequate security measures. Not considering various attacks during CPS design can make them vulnerable to exploitation. This phenomena is due to the low risks and potential for significant returns. Recent technological breakthroughs like cloud computing, AI, and the Internet of Things have created new vulnerabilities and cybersecurity challenges. Progress highlights the need to address cyber threats to essential service providers and the potential consequences of attacks.

Adaptive Security. Service providers that are critical and employ CPS are required to operate in dynamic environments and effectively accomplish many objectives. Upon detecting a failure, particularly when a goal is not accomplished due to external disruptions like high traffic or unpredictable user actions, a new configuration is executed. Nevertheless, devising a strategy to alleviate the consequences of alterations presents a major challenge (K. Angelopoulos et al., 2014). The main challenge arises from the undesired interference of multiple parameters in the configuration space, each with its own distinct objectives. The execution of the adaptation process may potentially lead to the restoration of security goal satisfaction. However, it also bears the risk of failure or exacerbation of security objectives.

A considerable amount of research on cyberattacks relies on sources such as media reports, open-source intelligence, and expert interviews [Ponemon, L. et al., 2015; Shostack, et al., 2014; Markopoulou, D. et al., 2021; Calderaro, et al., 2022; Hsieh, et al., 200516). At the same time, the European Union Agency of Cybersecurity (ENISA) has determined that publicly reported incidents only account for a small portion of the overall total. This suggests that a considerable number of incidents go unnoticed or unreported. The lack of research dedicated to studying the nature and impact of attacks targeting important service providers might be seen as harmful from multiple perspectives. As stated by sources [9,18], it has been suggested that this pattern could potentially affect the ability of businesses to accurately evaluate risk. This is because of a restricted comprehension of the likelihood and attributes of possible attacks (Papakonstantinou et al., 2022; Osei-Kyei, et al., 2021). The little investigation on the adverse effects of cyber attacks impedes researchers' understanding of the organisational and social ramifications of these criminal acts (Caldarulo, M et al., 2022;Agrafiotis et al., 2018). The objective of this study is to look into the following research question (RQ).

RQ1. How can adaptive security solutions be integrated into into current critical infrastructure systems to enhance the overall cybersecurity posture?

The remaining parts of this paper are organised as follows. Section 2 establishes the theoretical foundation of our research, whereas Section 3 introduces the XA4AS framework. The fourth section of the paper presents case studies, while the fifth section is dedicated to the experiment and its results. Section 6 has discussions. Section 7 offers a conclusion and considers potential areas for further study.

2 RESEARCH BASELINE

2.1 Digitising Critical Service Providers

Digitalization linked physical and digital domains, speeding up and connecting society. Technology has heightened social instability, uncertainty, complexity, and ambiguity (Urbach, 2019). Due to its complexity, modern society has become a risk society requiring advanced risk management (Kaiya, 2014). Beck suggests that digitization and globalisation may have led to transboundary disasters, impacting emergency response (Boin, A, 2019). Disasters can impact geography, time, and society (Boin, A, 2019). Recent socio-technical advancements, including increased system and software dependence and complicated supply networks, have led to increased occurrences (Kaiya, 2014). Due to key infrastructure disruptions, modern society must adapt to mitigate cross-border crisis risks (Boin, A, 2019).

Protecting critical information systems and networks from damage and disruption has been a policy goal since the 21st century to avoid incidents from worsening. To maintain IT-dependent service continuity and integrity, strategic goals such societal resilience and robustness enable quick recovery and endurance of events. According to(Harry, 2018), precise measurements are necessary as more information and operations shift to technology. This aligns with the need to secure cyberspace and address risks to national security (Pursiainen, 2018).

Cyberattacks on society services and infrastructure create complicated and unforeseen risks. Thus, interdisciplinary approaches are necessary to address these difficulties. Researchers propose a comprehensive method to address all dangers, including society safety and security (Syafrizal, 2021). Sweden normally considers all hazards in its policy. Swedish Civil Contingencies Agency (MSB) incorporates hostile threats into national risk assessments (Mitnick, K.D, 2011). As the EU highlights cyber threats to its internal market, merging becomes more apparent (Calderaro, 2022). (Shevchenko, 2023) found that the EU's cyber governance thinking is more influenced by reality than other governing organisations. The integration of physical and digital worlds has accelerated society's pace and interconnectedness due to digitalization.

The integration of technology has led to increasing social instability, uncertainty, complexity, and ambiguity (Urbach, 2019). Today's complex society necessitates advanced risk management (Kaiya, H, A, 2014). Digitalization and globalisation may have led to trans-boundary crises, as suggested by Beck and the impact of digitalization on emergency management (Boin, 2019). Crisis can have repercussions across time, place, and culture. Modern socio-technical advancements, such as reliance on diverse systems and software, and complicated supply networks, have led to increased occurrences (Kaiya, H, A, 2014). Modern civilization must adapt to lessen transboundary crisis risks due to infrastructure interruptions (Boin, 2019).

2.2 Security Attack Event Monitoring

The accelerated progress of cyber advancements has led to a dearth of agreement about understanding of cyberattacks and their impact on society (Simmons, C et al.,2014). The current analysis employs the cyberattack definition proposed by (Derbyshire, et al., 2018), which spans a broad spectrum of ”offensive actions”. an influence on the digital framework of a company. Offensive action involves both proactive attacks, like DDoS attacks, and reactive attacks, such cyber-exploitation, which entails unauthorised acquisition of information (Wang, E.K et al., 2010). Cyberattacks on the cyberinfrastructure might aim at compromising processes, hardware, and users. Multiple cyberattack strategies exist, including syntactic attacks that utilise malware and semantic attacks that employ social engineering techniques, with the aim of gaining unauthorised access to specific cyber systems.

This section presents the Asfalia framework that supports the monitoring of security attack events for CPSs, and the framework spans the three realms of a CPS. Moreover, the framework supports cross-realm analysis and monitoring, which spins off security events across realms. Our models focus on realm-specific adversaries, meaning that they span the three realms of a CPS (cyber, physical infrastructure, and social). We also analysed the interdependent relationships among realm-specific attack models. The AM depends on the VM model in revealing realm-specific vulnerabilities, and vulnerabilities captured by (the VM) spin off and provides inputs to the next realm (AM). Thus, a suitable attack mechanism is selected by taking advantage of the weaknesses of the VM. More detailed information can be found in (Seid, 2023).

2.3 Model Predictive Control

We present a receding horizon model predictive control (MPC) approach (E.Camacho et al.,2004; J. Maciejowski et al., 2002) that effectively addresses the management of multiple conflicting goals through the use of multiple control parameters. When the controller is enhanced with a Kalman Filter (KF) (L. Ljung et al., 2010), it has the capability to acquire knowledge in real-time and adjust the controller according to the behaviour of the system. This allows the controller to overcome inherent inaccuracies arising from dynamics that are not accounted for in model (2), as well as unknown disturbances affecting the system.

(MPC) is a control technique that employs an optimisation problem to determine a set of control parameters (actuators), denoted as u(·), in order to achieve a desired set of goals, denoted as $y\circ(\cdot)$, for a set of indicators, denoted as y(·), over a prediction horizon H. The control parameters u* are determined at each control instant t by minimising a cost function J(t), while adhering to specified constraints. The optimisation problem involves making predictions about the future behaviour of the system using the dynamic model (2).

As a result, a derived solution refers to a planned arrangement of forthcoming control parameter values $U^*= U_t^* + 1, ...U_t^* + H - 1$ across the anticipated time horizon. Effective planning is particularly crucial in situations where there is a delay in the occurrence of changes in control parameters.

The receding horizon principle applies only the first computed value u_t^* to the system, u(t)=u_t^*. Creating perfect models for real-world systems is impossible due to their dynamic behaviour. Therefore, plan corrections are necessary at each step and the horizon is reduced by one unit. The plan may fail due to external disturbances such as system workload changes. In essence, the plan would have been followed if a perfect model and no disturbances were present, which is not feasible. At the next control instant, a new plan is created based on the updated measured values of indicators to overcome this obstacle. This accounts for modelling uncertainties and unanticipated system behaviours (2). The model has been incorporated into our framework for adaptive security strategies and is integrated within our architecture, as detailed in the subsequent section.

3 XA4AS FRAMEWORK

The methodology we employ consists of two distinct stages: the design time phase and the runtime phase. In the initial stage, the necessary models for the synthesis and tuning of the MPC controller are obtained. As a result, in the subsequent stage, the controller is implemented within our adaptation framework and modifies the control parameters of the target system as necessary. We developed this framework and it has been published in our prior work (pending review, authors withheld).

Developing a comprehensive behavioural model for highly complex systems such as CPS, characterised by numerous complicated and diverse states, presents a significant challenge (Cailliau and van Lamsweerde et al., 2017). In order to comprehend how attackers achieve their objectives by compromising security concerns such as confidentiality, integrity, availability, and accountability, it is necessary to analyse the behaviour of the threat environment within the system and how adversaries can exploit vulnerabilities. Once the design phase has been finalised and the system has been successfully implemented, the XA4AS framework, which is focused on control-based security goals, can be effectively deployed to serve as the mechanism for adaptation. The figure presented as Figure 5 illustrates the five primary components of XA4AS. More detailed information can be found in (Seid,E et al., 2024)

4 CASE STUDY: SECURITY INCIDENT OBTAINED FROM CRITICAL SERVICE PROVIDERS

The data source used in the present study comprises IT-incident reports that were submitted to MSB. Therefore, it can be regarded as an unorthodox examination of the written information, predominantly relying on sources that rely on documents as their primary basis of information. In addition, this study employed a secondary dataset comprised of written IT-incident reports that were submitted to MSB by various Swedish government departments and organisations, in accordance with the standards outlined in the European Union's NIS-directive. In Sweden and other countries, organisations have the option to retain information. The Swedish legislation governing public access to information and confidentiality, namely the Public Access to Information and Secrecy Act (SFS 2009:400) and the Protective Security Act (SFS 2018:585), imposes restrictions on the sharing of information within public administration, including government agencies.

Private corporations have the choice to retain information regarding attacks and their implications as a means to protect their valuable resources or uphold favourable connections with stakeholders. An inherent drawback of this strategy is that the secondary data used as the data source were not explicitly gathered for the aim of this study. This constraint restricts

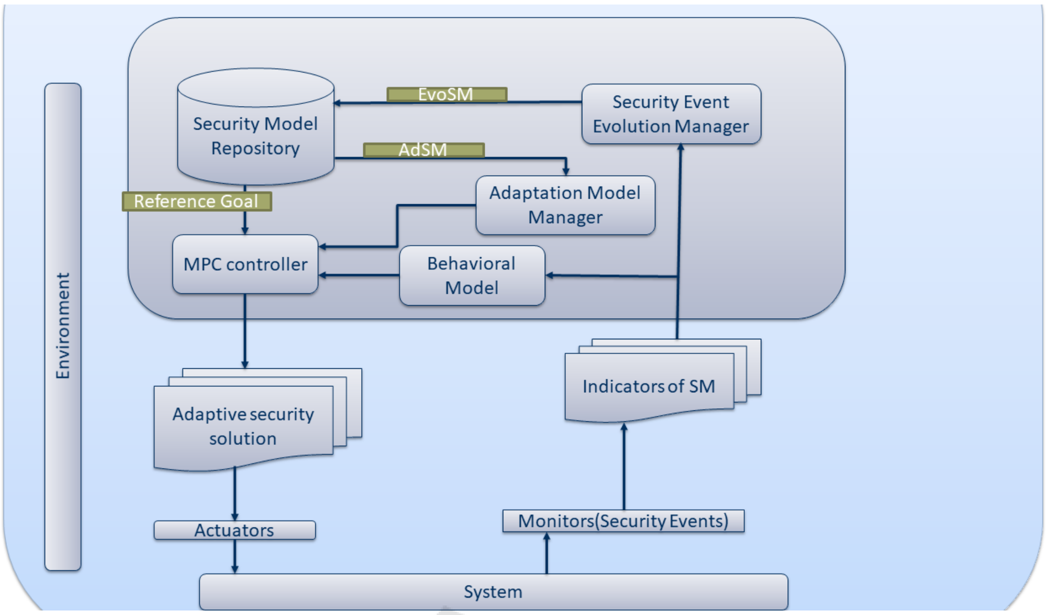

Figure 1: XA4AS.

the analysis. The conclusions that can be drawn rely on the attributes and excellence of the data acquired from the specific structure of MSB's IT-incident reports. Another limitation includes the dependence on recorded incidences as the foundation. To analyse the cyber threat landscape, it is important to consider that the findings drawn are heavily influenced by the reporting choices and methodologies employed by businesses.

4.1 Classification of Security Events

The data treatment procedure had four steps. Initially, all IT incidents recorded between 1 April 2019 and 1 April 2023 were analysed, focusing on harmful events. Rest were removed from the dataset. The IT-incident reports were categorised by vulnerability, attack mechanism, security events, and attack target in the second stage, and the results were quantified. Incidents lacking sufficient information for classification were classed as unknown. The third stage of data treatment involves summarising quantities within each category for frequency comparison. From April 2019 until 2023, (MSB) received 1332 IT-incident reports from major service providers. Only 256 reports were filed by NIS organisations, while the rest 1076 came from government agencies. The collection included 254 reports with detailed accounts of intentional and malevolent behaviours.

The remaining instances were attributed to various factors, such as technician and user errors, system failures, natural events, and unknown variables. Additionally, cyberattack frequency has remained steady from April 2019 to 2023. The period from 1 April 2019 to 2020 had a significant rise in reported cyberattacks, totaling 73 occurrences. Between 2022 and 2023, 67 cyberattacks were documented. From 2020 to 2021, cyberattacks increased significantly, with 61 documented cases. From April 2021 to 2022, cyber assaults targeting critical service providers were rare. Only 53 instances were reported.

5 SECURITY ATTACK ANALYSIS USING ASFALIA FRAMEWORK

This section presents an analysis of security attacks for critical service providers using the Asfalia framework. The framework facilitates the monitoring of security breach incidents and encompasses all three domains of a Cyber-Physical System (CPS).Moreover, the framework facilitates evaluation and monitoring of many domains, allowing for the detection of security incidents that occur across various domains. Our models explicitly focus on adversaries that are present in specific domains, which include the three domains of a CPS (cyber, physical infrastructure, and social). We developed this framework and it has been published in our prior work (pending review, authors withheld).

Attack patterns are classified into two distinct categories: The initial classification of cyberattack is domain-based, wherein specific domains or networks are targeted. The second category is mechanism-based harm, which aims to exploit flaws in different systems or procedures. As an illustration, 'social engineering' falls into the domain-based attack category, whereas 'collect and analyse' falls into the mechanism-based attack category. A total of 18 cyber security incidents have been categorised as cyber attacks, depending on the manner of attack, while seven of them have been categorised as domain-based cyber attacks. The reports were classified into two main categories related to cybersecurity and cyberattacks. A study was conducted on five major cyber incidents to analyse the tendencies of cyber security attacks. The occurrences were identified and categorised based on a domain-specific attack. Among the 254 reported cyber security incidents, Asfalia has detected 7 vulnerabilities and 5 major incidents. Furthermore, all six targets that were subjected to cyberattacks have been captured.

5.1 Security Attack Analysis of DDoS

Attack-Mechanism Model (AM). This model captures design strategies, different attack pattern mechanisms. More importantly, it builds attack mechanisms by employing goal models, domain assumptions, attack mechanisms, and task operationalisation artifacts. Each attack pattern captures knowledge about how specific parts of an attack are designed and executed, providing the adversary's perspective on the problem and the solution, and gives guidance on ways to mitigate the attack's effectiveness. AM model depends on VM model since it prepares its attacking mechanism based on the threat explored in VM model as shown in Figure 5. However, threats can be refined not only linearly but also iteratively. The second sub-attack mechanism consists of three sequential steps. Prior to initiating an attack, the attacker must acquire a comprehensive understanding of the targeted system. After that, they launch a specific operation within the system. Finally, they investigate whether the target condition reveals a deadlock condition.

Event Model (EM). This model captures events that are derived from behavioural models (BM). From the perspective of the event log, these events can be categorised into observable and non-observable events. Specifically, our focus is directed towards events that can be directly perceived or witnessed. Security events are generated from the behavioural model, also referred to as the BM model. For instance, the occurrence of distributed denial of service (DDoS) attacks has been captured, with one specific event identified as E1: the initiation of the exploratory phase. E2: "An action was triggered and initiated", and E3: "A denial of service occurred"

5.2 Security Attack Analysis of Installed Malware

Attack-Mechanism Model (AM). (1) Cross zone scripting, (2) exploit systems susceptible to the attack, (3) find the insertion point for the payload, and (4) craft and inject the payload. Tasks: (1) Leverage knowledge of common local zone functionality, (2) find weakness in the functionality used by both privileged and unprivileged users, (3) make the maliciously vulnerable functionality to be used by the victim, (4) leverage cross-site scripting vulnerability to inject payload, and domain assumption: insufficient input validation by the system.

Event Model (EM). This model captures the security events E1: Internet and local zone enabled, E2: enable functionality failed, E3: internet and local zone disabled, E4: weakness found, E5: weakness failed, E6: victim-injected payload, and E7: payload injected.

5.3 Security Attack Analysis of Installed Web Compromise (XSS Through HTTP Query String)

Seven attack mechanisms were captured, namely, (1) XSS through HTTP query string; (2) use a browser or an automated tool; (3) attempt variations in input parameters; (4) exploit vulnerabilities; (5) steal session IDs, credentials, page contents; (6) content spoofing; and (7) forceful browsing. Tasks: 10 specific tasks have been captured, namely: (1) use spidering tool to follow and record all links, (2) use a proxy tool to record all links visited, (3) use a browser to manually explore and analyse the website, (4) use a list of XSS probe strings to inject in the parameter of known URLs; (5) use a proxy tool to record the results of the manual input of XSS probes in known URls, (6) develop malicious JavaScript that is injected through vectors and send information to the attacker, (7) develop malicious JavaScript that is injected through vectors and take and cause the browser to execute it, (8) develop malicious JavaScript that is injected through vectors and perform actions on the same website, (9) develop malicious JavaScript that is injected through vectors, and (10) cause the browser to execute requests to other websites .

Event Model (EM). This model captures the security events E1: links recorded, E2: website explored, E3: visited links recorded, E4: known URLs injected, E5: results of manual input of XSS probes recorded: E6:

information sent, E7: attacker's command executed by the browser, E8: action performed on the same website, E9: request executed to other website, and E8: invalid information exposed to the user.

5.4 Design-Time

Our methodology originates by extracting diverse security goals and security methods associated with the target system. Once all goals have been clarified, ASm are allocated to those that meet the criteria. Considered the most crucial and prone to failure. An ASM defines a desired target, denoted as R_i, for the controller's output.

The assault pattern referred to as "Forced Deadlock" can be described using the following behavioural annotations: (G2, G3#, and G4#). The annotations specify that the sub-attack mechanism "Get familiar with system" should be accomplished first, followed by the instances of "Trigger an action" and "Explore if the target condition has a deadlock condition."

Interleaving refers to the process of combining or alternating two or more things in a specific order or sequence. The formal behavioural annotation for the action of triggering an action is represented as (T2#DA1). This annotation signifies the simultaneous fulfilment of the target host providing an API to the user and the subsequent triggering of the first action, followed by the initiation of a second action. The formal behavioural annotation for the sub-attack, which investigates the presence of a deadlock state in the target situation, is denoted as (T3#DA2). This annotation indicates the consecutive execution of two actions: firstly, examining the programme for a deadlock situation, and secondly, presuming that the target programme does indeed have a deadlock condition.

Table 1: Reference Security Goal.

CRq	**Reference**
ASm1	R1=80
ASm2	R2=75
ASm3	R3=100
ASm4	R4=90
ASm5	R5=90
ASm6	R6=100

In this situation, the initial EvoSm operation is started, leading to a change in the reference objective from 80% to 70%, as can be seen in Table 4. The second EvoSm operation is triggered when there is a failure in T2, leading to the restoration of the threshold to its prior value. T2 and T3 have the potential to undergo multiple iterations sequentially, as they await each other's completion.

The reference security targets have been modified to a lower level, namely reduced from 90% to 80% and from 80% to 60%, respectively.If ASm4 and ASm5 encounter a failure lasting more than three days, the reference security aim will be temporarily loosened for a period of one week.

If goal G1 fails more than three times per week in the context of ASm6, the restriction is continually adjusted to four times per week. If ASm4 encounters a failure lasting more than three consecutive days, the adaptation mechanism will then ignore it for a period of three days. The Analytic Hierarchy Process (AHP) is used to assign weights to each indication based on their levels of relevance. Generally, security objectives that are considered critical are prioritised over those that are non-critical. The weights are associated with the elements of matrix Q in the cost function. The controller use the optimisation function to determine a state of balance for each aim, devoting more resources towards achieving the goals that are more important. The weights of the control parameters are set through empirical elicitation, with lower weights allocated to the parameters that require less frequent tweaking. The values of matrix P in the cost function represent weights.

Our security analysis for XSS throught HTTP, DDoS, has found that Disable scripting languages such as JavaScript in browser is a more cost-effective solution than Regularly patch all software. Additionally, the previous method also provides the benefit of immediate efficacy. The priority for the indicators and the weights for control parameters were determined using elicitation, as shown in table 3 and table 4, respectively.

The remaining security goals to be identified pertain to the adaptive security mechanism (ADSM). The attainment of these objectives imposes constraints on the process of adaptation itself. Model Predictive Control (MPC) uses an Adaptive Horizon Determination Strategy (ADSM) to establish the receding horizon of the controller. This approach establishes the specific time period towards which the adaptation plan should be focused on in the future. The term "ADSM" may also denote the degree to which control parameters are allowed to fluctuate.

In the end, it is important to construct a numerical model. In order to replicate the MERS system in the absence of natural laws, we conducted a complete simulation with regular modifications to control parameters, while also documenting the input and output data. We employ Matlab and the System Identification toolkit to ascertain the analytical model of the system. While it is not possible to simulate the system with complete accuracy, the model can be enhanced upon deployment by incorporating a learning mechanism that operates during runtime.

Table 2: EvoSm Operations.

CRq	EvoSm Execution
ASm1	Relax(ASm1,ASm1'_70), Strengthen(ASm1,ASm1'_80)
ASm2	Relax (ASm2, ASm2'_60)
ASm3	Relax (ASm3, ASm3'_90)
ASm4	Relax (ASm4, ASm4'_80)
ASm5	Wait(3 days)
ASm6	Replace (ASm6, ASm6'_3)

6 DISCUSSION

The cyberattack is mechanism-based. There have been 18 cyber attacks, depending on the technique used, and seven domain-based cyber attacks. The reports were divided into cybersecurity and cyberattack categories. Five major cyber incidents were studied to determine cyber security attack trends. A domain-specific attack recognised and categorised the instances. From 254 reported instances, Asfalia detected 7 vulnerabilities and 5 critical cyber security events. Additionally, all five cyberattack targets were successfully captured.

The framework also includes 24 attack mechanisms, 32 tasks, 23 behavioural annotations, 10 domain assumptions, and 35 security events. According to their behaviours, the experiment's security issues can be characterised as password recovery exploitation, authentication abuse, buffer overflows, cross-site scripting, phishing, and brute force assaults. Our technique aids security analysts in incident analysis and critical service provider security solution development.

The Adaptation manager of XA4AS framework only classified 15% of reported security incidents as critical. Essential aspect of XA4AS is its ability to adapt to non-linear system behaviours. The simulator employs nonlinear interactions between inputs and outputs for more realistic behaviour. In actuality, most systems have nonlinear input-output interactions. To be effective, the adaptation process must address model faults. In Model Predictive Control (MPC), the Kalman Filter (KF) enhances model correction during system operation, resulting in more precise predictions. In the security model scenario, a linear model predicted system behaviour. This may not always be possible. Custom models or sophisticated system identification approaches can manage non-linear systems (L. Ljung, 2010). Non-linear model predictive control (MPC) formulations by F. Allgower, in 2000 are also relevant.

Our investigation shows that building the security model bottom-up in the framework works. Based on domain task specifications, differentiation occurs. This identifies domain-specific attacks. We prioritise cyber, physical infrastructure, and social aspects of CPS for essential service providers in our models. We also analysed attack model interconnectivity across domains. The VM method detects domain-specific vulnerabilities. Once vulnerabilities are found by VM, attack (AM) uses them to identify an acceptable attack method. This option exploits well-documented VM vulnerabilities. XA4AS analytical models require simulations or historical data. This is a major system defect. System designers face a hurdle because there are no methods to simulate a model that generates data that closely reflects the actual system. This is because CPS lacks exclusive methods. Security engineering approaches and MPC configuration optimisation guidelines are our future study.

7 CONCLUSION

This study builds on our previous research on monitoring security attack events and assessing attack patterns, focusing on the Asfalia framework. Another goal is to include Model Predictive Control (MPC) into cyber-physical system adaptive security mechanisms. Thus, we provide XA4AS (Extended Asfalia (Framework) for Adaptive Security of Cyber-Physical Systems). Facilitating the creation of analytical models for model predictive control and adaptive security solutions in CPS is the goal of this approach.

The proposed model predicts system behaviour with significant precision. XA4AS can quickly adapt to environmental changes and create adaptable solutions. The approach was assessed using 254 critical service provider security incident reports. According to our case study, Swedish service providers' IT incident reports to MSB show that denial-of-service attacks and disruptions have the biggest impact on operations and information. Many of the 254 cyberattacks analysed had no obvious direct or indirect effects. Social engineering attacks often have little immediate impact. While social engineering for initial access and user attacks is declining, it remains widespread. Malware infestation is rare. A few dangerous IT incidents endangered critical service providers' information resources.

The analysis shows that control-theoretic concepts can create effective cyber-physical system adaptability strategies, often outperforming human skill. Our approach aids security analysts in event analysis and CPS security solution development. (VM) detects and captures adversaries and vulnerabilities, then analyses the attack's target using a domain-specific technique. The Attack Model (AM) is created by building a model based on the adversaries provided in the VM. The behavioural model (BM) annotates system behaviours of the VM and AM. EM events are derived from behavioural models. The models above help the XA4AS Security Evolution Manager and Adaptation Manager. Our approach needs more case studies in order to demonstrate its efficacy.

REFERENCES

Van den Berg, B.; Kuipers, S. Vulnerabilities and Cyberspace: A New Kind of Crises. In Oxford Research Encyclopedia of Politics; Universiteit Leiden—LUMC: Leiden, The Netherlands, 202

Pursiainen, C. Critical infrastructure resilience: A Nordic model in the making? Int. J. Disaster Risk Reduct. 2018, 27, 632–641.

Wang, E.K.; Ye, Y.; Xu, X.; Yiu, S.-M.; Hui, L.C.K.; Chow, K.-P. Security issues and challenges for cyber physical system. In Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, Hangzhou, China, 18–20 December 2010; pp. 733–738.

Uzunov, A.V.; Ferncez, E.B.; Falkner, K. Engineering security into distributed systems: A survey of methodologies. J. UCS 2012, 18, 2920–3006.

Gopstein, A.; Gopstein, A.; Nguyen, C.; Byrnett, D.S.; Worthington, K.; Villarreal, C. Framework and Roadmap for Smart Grid Interoperability Standards Regional Roundtables Summary Report; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.

Mancuso, V.F.; Strang, A.J.; Funke, G.J. ; Finomore, V.S. Human factors of cyber attacks: A framework for human-centered research. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Chicago, IL, USA, 27–31 October 2014; SAGE Publications: Los Angeles, CA, USA, 2014; Volume 58, pp. 437–441.

Urbach, N.; Roeglinger, M. Introduction to Digitalization Cases: How Organizations Rethink Their Business for the Digital Age; Springer: Berlin/Heidelberg, Germany, 2019

Ponemon, L. Cost of Data Breach Study: Global Analysis; Technical Report; Poneomon Institute: Traverse City, MI, USA, 2015.

Shostack, A. Threat Modeling: Designing for Security; John Wiley & Sons: Hoboken, NJ, USA , 2014.

Griffor, E. R., Greer, C., Wollman, D. A., Burns, M. J., et al. (2017). Framework for cyber-physical systems: Volume 1, overview.

Boyes, H., Hallaq, B., Cunningham, J., and Watson, T. (2018). The industrial internet of things (iiot): An analysis framework

Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., and Gupta, S. K. S. (2012). Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. Proceedings of the IEEE, 100(1):283–299.

K. Angelopoulos, V. E. S. Souza, and J. Mylopoulos. Dealing with multiple failures in zanshin: a control-theoretic approach. In SEAMS 14, pages 165–174. ACM, 2014.

Markopoulou, D.; Papakonstantinou, V. The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Comput. Law Secur. Rev. 2021, 41, 105502.

Calderaro, A.; Blumfelde, S. Artificial intelligence and EU security: The false promise of digital sovereignty. Eur. Secur. 2022, 31, 415–434. .

Hsieh, H.F.; Shannon, S.E. Three approaches to qualitative content analysis. Qual. Health Res. 2005, 15, 1277–1288

Papakonstantinou, V. Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? Comput. Law Secur. Rev. 2022, 44, 105653

Osei-Kyei, R.; Tam, V.; Ma, M.; Mashiri, F. Critical review of the threats affecting the building of critical infrastructure resilience. Int. J. Disaster Risk Reduct. 2021, 60, 102316

Caldarulo, M.; Welch, E.W.; Feeney, M.K. Determinants of cyber-incidents among small and medium US cities. Gov. Inf. Q. 2022, 39, 101703.

Agrafiotis, I.; Nurse, J.R.; Goldsmith, M.; Creese, S.; Upton, D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. 2018, 4, tyy006

Kaiya, H.; Kono, S.; Ogata, S.; Okubo, T.; Yoshioka, N.; Washizaki, H.; Kaijiri, K. Security requirements analysis using knowledge in capec. In Advanced Information Systems Engineering Workshops; Springer: Berlin/Heidelberg, Germany, 2014; pp. 343–348.

Boin, A. The transboundary crisis: Why we are unprepared and the road ahead. J. Contingencies Crisis Manag. 2019, 27, 94–99.

Harry, C.; Gallagher, N. Classifying cyber events. J. Inf. Warf. 2018, 17, 17–31.

Syafrizal, M.; Selamat, S.R.; Zakaria, N.A. AVOIDITALS: Enhanced Cyber-attack Taxonomy in Securing Information Technology Infrastructure. Int. J. Comput. Sci. Netw. Secur. 2021, 21, 1–12.

Mitnick, K.D.; Simon, W.L. The Art of Deception: Controlling the Human Element of Security; John Wiley & Sons: Hoboken, NJ, USA, 2011

Shevchenko, P.V.; Jang, J.; Malavasi, M.; Peters, G.W.; Sofronov, G.; Trück, S. The nature of losses from cyber-related events: Risk categories and business sectors. J. Cyberse-Curity 2023, 9, tyac016

Simmons, C.; Ellis, C.; Shiva, S.; Dasgupta, D.;Wu, Q. AVOIDIT: A Cyber Attack Taxonomy. In Proceedings of the 9th Annual Symposium on Information Assurance, Kyoto, Japan, 4–6 June 2014; pp. 12–22.

Derbyshire, R.; Green, B.; Prince, D.; Mauthe, A.; Hutchison, D. An analysis of cyber security attack taxonomies. In Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 24–26 April 2018; pp. 153–161.

Fernandez-Buglioni, E. Security Patterns in Practice: Designing Secure Architectures Using Software Patterns; John Wiley & Sons: Hoboken, NJ, USA, 2013.

V. Souza, A. Lapouchnian, and J. Mylopoulos. Requirements-driven qualitative adaptation. On the Move to Meaningful Internet Systems: OTM 2012, volume 7565 of Lecture Notes in Computer Science, pages 342–361. Springer Berlin Heidelberg, 2012.

L. Ljung. Approaches to identification of nonlinear systems. In Control Conference (CCC), 2010 29th Chinese, pages 1–5, July 2010.

V. E. S. Souza, A. Lapouchnian, W. N. Robinson, and J. Mylopoulos. Awareness requirements for adaptive systems. In 2011 ICSE Symposium on Software Engineering for Adaptive and Self-Managing Systems, SEAMS, pages 60–69, 2011.

E. Camacho and C. Bordons. Model Predictive Control. Springer London, 2004.

J. Maciejowski. Predictive Control: With Constraints. Prentice Hall, 2002.

Cailliau, A.van Lamsweerde, Runtime monitoring and resolution of probabilistic obstacles to system goals. In Software Engineering for Adaptive and Self- Managing Systems (SEAMS), 2017 IEEE/ACM