Making (Implicit) Security Requirements Explicit for Cyber-Physical Systems: A Maritime Use Case Security Analysis

Tope Omitola(✉), Abdolbaghi Rezazadeh, and Michael Butler

Cyber-Physical Systems Research Group, Electronics and Computer Science, University of Southampton, Southampton, UK
{tobo,ra3,mjb}@ecs.soton.ac.uk

Abstract. The increased connectivity of critical maritime infrastructure (CMI) systems to digital networks have raised concerns of their vulnerability to cyber attacks. As less emphasis has been placed, to-date, on ensuring security of cyber-physical maritime systems, mitigating these cyber attacks will require the design and engineering of secure maritime infrastructure systems. Systems theory has been shown to provide the foundation for a disciplined approach to engineering secure cyber-physical systems. In this paper, we use systems theory, and concepts adapted from safety analysis, to develop a systematic mechanism for analysing the security functionalities of assets' interactions in the maritime domain. We use the theory to guide us to discern the system's requirement, likely system losses, potential threats, and to construct system constraints needed to inhibit or mitigate these threats. Our analyses can be used as springboards to a set of principles to help enunciate the assumptions and system-level security requirements useful as the bases for systems' security validation and verification.

Keywords: Maritime security · Systems theory · System Theoretic Process Analysis (STPA) · Threat analysis · Cyber-Physical System Security

1 Introduction

With over 80% of global trade by volume and more than 70% of its value being carried on board ships and handled by seaports worldwide [1], the importance of a well-functioning national maritime industry cannot be over-emphasised. As key nodes in global transport chains providing access to markets, supporting supply chains, and linking consumers and producers, global ports are under constant pressure to adapt to changes in the economic, institutional, regulatory and

This work has been conducted within the ENABLE-S3 project that has received funding from the ECSEL Joint Undertaking under Grant Agreement no. 692455.

G. Anderst-Kotsis et al. (Eds.): DEXA 2019 Workshops, CCIS 1062, pp. 75–84, 2019.
https://doi.org/10.1007/978-3-030-27684-3_11

operating landscape. Many studies, e.g. [2], have identified maritime infrastructure and vessels to be potentially vulnerable to interference from cyber-threats. This potential vulnerability stems from a combination of increased connectivity and reliance on digital components, globally accessible navigation systems, and increasing levels of autonomous control. All such attacks have safety repercussions, with potentially serious impacts on human life, the environment and the economy. In this paper, we investigate how systems theory can be used for security requirements elicitation and analysis of an exemplar cyber-physical system (CPS), i.e., the communication systems enabling the interactions between maritime ships and their control centres.

2 Related Work on Security Analyses of Maritime Communication System

Due to their importance, safety and security impose constraining requirements that need to be fulfilled in the design and implementation of the communication systems of maritime assets. Maritime communication systems (MCS), as exemplar cyber-physical systems, have a coupling between the computational and physical elements, and correct system behaviour depends on correct functioning of the "interaction" of control logic with the physical system dynamics. Engineering such complex cyber-physical systems requires a holistic view on both product and process, where safety and security need to be incorporated across the engineering life-cycle to ensure such systems are safe from hazards and accidents, and secure from intentional and unintentional threats.

Traditional security analysis methods, such as **THROP** [6], work with threat models that are based on the fault-error-failure chain model. While these models are valid to describe threats to isolated components, they are insufficient to describe system threats in complex interconnected systems, as we have in modern CPS. **STRIDE** [7] takes a threat-centric approach to security analysis associating each threat with a particular asset from attackers' perspective. Although an advantage of STRIDE is that it helps change a designer's focus from the identification of specific attacks to focusing on the end results of possible attacks, one major disadvantage is that it mainly targets software systems.

In security, there can be a tendency to consider the assurance of security to be one of simply applying one particular solution, e.g. authentication or cryptography, or adhering to a best practice, such as threat modelling. But systems security, like safety and other system quality properties, is an emergent property of a system. This means that system security results from many things coming together to produce a state or condition that is free from asset loss, and the resulting loss consequences.

3 System Theoretic Process Analysis for Safety and Security Analysis

System Theoretic Process Analysis (STPA) [3] is an accident causality model based on systems theory, expanding the traditional model of causality beyond

a chain of directly-related failure events or component failures to include more complex processes and unsafe interactions among system components. It is based on the three concepts of (a) safety constraints, (b) a hierarchical safety control structure, and (c) process models. STPA considers events leading to accidents occur because safety constraints were not successfully enforced.

STPA performs system safety hazard analyses, while our work focusses on system security. To some extent, system safety and security can be viewed as analogues of each other. Whilst system safety, and STPA in particular, focusses on analysing the system for potential accidents and identifying the hazards that could lead to those accidents, system security considers potential losses to the system and the associated threats that could lead to those losses, so that security constraints and mechanisms can be identified and integrated into the design to address the causes of these potential threats and to reduce the risk associated with the potential losses.

STPA has the following seven steps: (1) Stating system *purpose*, (2) Identifying *accidents*, (3) Identifying system *hazards* associated with accidents, (4) Constructing high-level *control structure*, (5) Translating system hazards into high-level *safety requirements*, (6) Identifying *unsafe control actions*, and (7) Using the results to *create or improve system design*.

Applying STPA concepts to security analysis, we have focussed on identifying **losses** (instead of accidents), **threats** (instead of hazards), translating the threats to a set of **security constraints** (instead of safety requirements), and identifying **insecure actions** (instead of unsafe control actions).

Figure 1 shows the entities of interest of our analysis, the MCS between an SBB controller and a Ship that the SBB controls. The first step in STPA is identifying the system's purpose.

3.1 System Purpose

Identifying the system purpose may require a few iterations, by the security analysis team, of what the system is supposed to achieve. After doing this, we identified the purpose of the MCS to be: "*the provision of timely, confidential, and correct communication of navigation data, acknowledgements and route updates, between SBB and Ship*". As our focus is on the MCS, we have made use of the two primitives of *SEND* and *RECEIVE* to model the actions of data being sent and received. The next stage is to identify the losses to the system. We start by defining what a loss is.

3.2 System Losses

A **loss** is a circumstance, event or operation that can adversely impact, and/or cause failure to, a system's purpose. We can see from Sect. 3.1 that unauthorised reading and modification of data, as well as any operation that can affect timely data reception will adversely affect our system's purpose. Taking these into consideration, the system losses, from the points of view of both the Ship and SBB, are listed in Table 1. From Table 1, we see the correspondence between a loss,

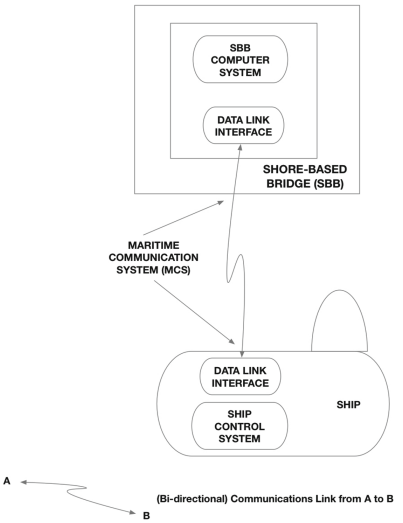

Fig. 1. Entities of interest (MCS, SBB, and Ship)

such as "Receiving Incorrect Ship Location data" (L_2), and its impact on one of the items of the purpose statement, i.e. "correctness". The next stage in STPA is to identify the system threats.

Table 1. System losses

Loss	Description of loss (from SBB's perspective)	Loss	Description of loss (from Ship's perspective)
L_1	Not receiving ship location data (at set periodic times)	L_5	Not receiving navigation data from SBB
L_2	Receiving incorrect Ship Location data	L_6	Receiving incorrect navigation data from SBB
L_3	Receiving Ship location/status data very late	L_7	Receiving navigation data very late from SBB
L_4	Un-authorised agent able to read Ship location/status data sent by Ship to SBB	L_8	Un-authorised agent able to read navigation data sent by SBB to Ship

3.3 System Threats

For the MCS to be effectively protected, we must resolve the security challenges inherent to that protection. These challenges can be looked at from the lens of the Confidentiality, Integrity and Availability, (C-I-A), triad. A loss of availability

Table 2. Possible system threats

Threat	Threat definition	Threat	Threat definition
$\mathbf{T}_1$ Message congestion	Overload of the communication system persisting for a time significantly longer than service time	$\mathbf{T}_2$ Interference	Unauthorised signal disruption
$\mathbf{T}_3$ Tampering	Unauthorised data modification	$\mathbf{T}_4$ Injection Attack	Introduction of false messages
$\mathbf{T}_5$ Replay Attack	Valid communication is maliciously repeated or delayed	$\mathbf{T}_6$ Relay Attack	Man-in-the-middle attack where all messages are forwarded verbatim between a valid sender and a valid receiver
$\mathbf{T}_7$ Identity spoofing	Accessing a system disguised as a different actor	$\mathbf{T}_8$ Loss of communications infrastructure	Unavailability of communication provisioning
$\mathbf{T}_9$ Denial of service attack	Denial of service attack definition	$\mathbf{T}_{10}$ Traffic analysis	Unauthorised study of communication patterns between Ship and SBB
$\mathbf{T}_{11}$ Eavesdropping	Unauthorised listening to or reading of Ship and/or SBB's data and communication		

is the loss of the ability to access network resources. A loss of integrity is the intentional or unintentional changes to transmitted and stored data, while a loss of confidentiality is the unauthorised disclosure of transmitted and stored data.

A **threat** is a system state or a set of conditions that will lead to a system loss [3]. Table 2 shows the potential threats we identified for the MCS. These threats refer to specific opportunities by adversaries to defeat the system purpose and/or engender system losses. Table 3 shows the connection between threats and the losses they may cause, with a threat leading to more than one loss (e.g. T_1 being a causation factor to losses L_1, L_3, L_5 and L_7), or interactions of threats leading to a particular type of system loss (e.g. T_1, T_4, T_8, and T_9 as contributing factors to L_1).

3.4 System Control Structure

The control structure captures functional relationships and interactions of the main components of the MCS, as a set of command actions and feedback loops.

Table 3. System losses and threats

Losses & threats	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8
T_1	X		X		X		X	
T_2		X	X	X		X	X	X
T_3		X				X		
T_4	X	X	X		X	X	X	
T_5		X		X		X		X
T_6				X				X
T_7				X				X
T_8	X		X		X		X	
T_9	X		X		X		X	
T_{10}				X				X
T_{11}				X				X

The questions to ask when constructing the control structure are: what are the main components in the system, what role does each play, and what are the command actions being used to interact. Figure 2 shows the control structures of the secure (Fig. 2A) and insecure (Fig. 2B) interactions between SBB and Ship.

3.5 Defining High-Level Security Constraints

After identifying the threats and constructing the control structures, the next major goal is to identify the security-related constraints necessary to prevent the threats from occurring. The question STPA enabled us to ask to help us identify the constraints was: "What constraints need to be in place to prevent the aforementioned threat conditions from occurring"? The constraints we identified are listed in (Table 4).

The security constraints together with the control structure helped us to answer questions such as: (a) what are we controlling (in the case of the MCS, it is data communication security between SBB and Ship), (b) what happens when the control actions go wrong (in our case, it is the likelihood that the identified threats may manifest), and (c) how can we mitigate those things we have identified can go wrong. Therefore, looking at the threats enumerated in Table 2, the security engineers can start identifying the constraints (Table 4) that need to be in place in order to mitigate those threats. For example, a threat such as "*an adversary interfering in the communication between SBB and Ship*" ($\mathbf{T}_2$), the system constraint is to guarantee against such threat occurring.

3.6 Identifying Insecure Actions

After the preliminary threat analyses carried out in Tables 2 and 4, the next step is to use STPA's four general categories of insecure control actions [3], to identify

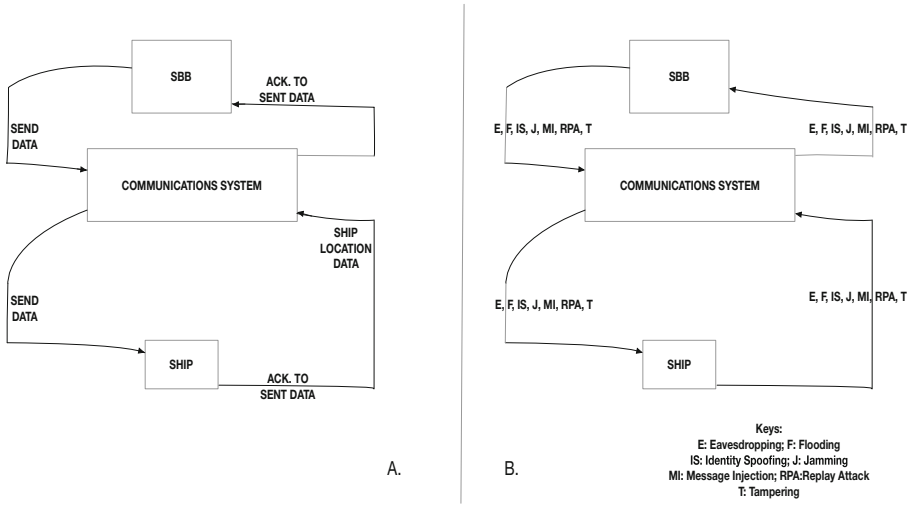

Fig. 2. Control structures for both the secure and insecure interactions between SBB and Ship

the conditions under which the actions of sending and receiving navigation data could lead to system threats. The security environment is dynamic, sometimes adversarial, with malicious actors that can learn how to subvert the system. In this kind of environment, the actions of interest to us are delineated as normal and malicious.

Malicious and Normal Control Actions. The system's normal control actions include: the *send*-ing and *receive*-ing of navigation and acknowledgement data from both the SBB and Ship. The malicious control actions are the actions a malicious agent is likely to make that can lead to a threat. These actions include: (a) Spoofing the address resolution and the IP protocols of the underlying communication network; (b) Eavesdropping actions; as well as (c) Traffic analysis actions.

Tables 5 and 6 present our use of STPA to analyse some controls and outputs issued by the MCS. **N.B.** We have used the following abbreviations in the two tables(**T**: Tampering, **I**: Interference, **IA**: Injection Attack, **RPA**: Replay Attack, **RLA**: Relay Attack, **IS**: Identity Spoofing, **DoS**: DoS Attack, **TA**: Traffic Analysis, **E**: Eavesdropping).

We found that the effect of the normal actions is binary: either they leave the system fool-proof or vulnerable to all of the threats described in Sect. 3.3, while the malicious actions expose the system to all of these security threats. This may be due to the existence of an operational communication system exposes it to such threats. In addition, our choice of primitives of *SEND* and *RECEIVE* are at a level that these states are binary, either a message is sent or not, and if a message is not sent, then no security threat arises.

Table 4. High-level security constraints for the MCS

Threat	System constraint
$\mathbf{T}_1$ Communications requests exceed link capacity (**Message Congestion**)	$\mathbf{SC}_1$ The system shall be able to prove the identity of agents during transactions
$\mathbf{T}_2$ An adversary interferes in the communication between SBB and Ship (**Interference**)	$\mathbf{SC}_2$ The system shall guarantee against communication interference between SBB and Ship
$\mathbf{T}_3$ Valid communication between SBB and Ship is intercepted and data are maliciously modified (**Tampering**)	$\mathbf{SC}_3$ The system shall maintain strong mutual continuous authentication, of SBB and Ship, during all operations' transactions
$\mathbf{T}_4$ False messages, pretending to come from a valid source, are introduced into the system (**Injection Attack**)	$\mathbf{SC}_4$ The system shall maintain strong mutual continuous authentication, of SBB and Ship, during all operations' transactions
$\mathbf{T}_5$ The system maliciously repeats or delays valid communication between SBB and Ship (**Replay Attack**)	$\mathbf{SC}_5$ The system shall maintain strong mutual continuous authentication, of SBB and Ship, during all operations' transactions
$\mathbf{T}_6$ Valid communication is forwarded verbatim between SBB and Ship by a malicious agent (**Relay Attack**)	$\mathbf{SC}_6$ The system shall maintain strong mutual continuous authentication, of SBB and Ship, during all operations' transactions
$\mathbf{T}_7$ A malicious agent is pretending to be the SBB, the Ship or the Communication System (**Identity Spoofing**)	$\mathbf{SC}_7$ The system shall maintain strong mutual continuous authentication, of agents, during all operations' transactions
$\mathbf{T}_8$ There is discernible delay or a denial of service between the SBB and Ship (**Loss of Communications Infrastructure**)	$\mathbf{SC}_8$ The system shall detect the loss of infrastructure
$\mathbf{T}_9$ There is discernible delay or a denial of service between the SBB and Ship (**Denial of Service Attack**)	$\mathbf{SC}_9$ The system shall ensure and maintain the specific turn-around time for each requested operation
$\mathbf{T}_{10}$ A malicious agent observes patterns of communication traffic between SBB and Ship (**Traffic Analysis**)	$\mathbf{SC}_{10}$ The system shall ensure protection over all communication
$\mathbf{T}_{11}$ An un-authorised agent listens into communication between SBB and Ship (**Eavesdropping**)	$\mathbf{SC}_{11}$ The system shall ensure that all the communications are not readable by any un-authorised party

Table 5. Normal control actions of the MCS

Normal control action	Not providing exposes system to threats	Providing exposes system to threats	Wrong time or wrong order exposes system to threats	Stopped too soon or applied too long exposes system to threats
SBB sends navigation data to ship	None	**UCA1**. T, I, IA, RPA, RLA, IS, DoS, TA, E	As in UCA1	As in UCA1
Ship receives Navigation data	None	As in UCA1	As in UCA1	As in UCA1
Ship sends Ack to SBB	None	As in UCA1	As in UCA1	As in UCA1
SBB receives Ack data from Ship	None	As in UCA1	As in UCA1	As in UCA1

Table 6. Malicious control actions of the MCS

Malicious control action	Not providing exposes the system to threats	Providing exposes the system to threats	Wrong time or wrong order exposes the system to threats	Stopped too soon or applied too long exposes the system to threats
Address resolution protocol (ARP) spoofing command	None	**UCA2**. IS, T, RPA, RLA, IA	As in UCA2	As in UCA2
IP spoofing command	None	As in UCA2	As in UCA2	As in UCA2
Packet tampering command	None	As in UCA2	As in UCA2	As in UCA2
Eavesdropping command (e.g. via a Network sniffer)	None	**UCA3**. Eavesdropping. Usually a passive attack	As in UCA3	As in UCA3
Traffic analysis command (e.g. via using Wireshark or P0f)	None	**UCA4**. Traffic Analysis. Normally a passive attack	As in UCA4	As in UCA4

3.7 Use Results to Create or Improve Design

The next step in STPA is to use the results of the analyses to help in designing a more secure system. Security is about risk management, and a purpose of risk management is to reduce losses. The C-I-A triad conjoined with the system losses and threats (Table 3) and with the high-level security requirements (Table 4) can help in assessing risk and weighting value. Depending on one's application domain, one can assign different values to the threats in Tables 3 and 4.

4 Conclusions and Future Work

This paper showed how systems theory and concepts from safety analyses, especially STPA, can be applied to the security analysis of a critical maritime infrastructure system (an exemplar cyber-physical system). We showed how STPA's systematic approach can help in eliciting the appropriate system's purpose, and to identify the losses and threats that may severely impact that purpose. We also showed how to derive the system constraints that can be used to inhibit or mitigate these threats, and described appropriate mitigation techniques.

For future work, we shall employ the Event-B [5] modelling methodology to help verify the completeness of the system constraints to mitigate or inhibit the threats that generated them.

References

1. United States Navy Biography. http://www.navy.mil/navydata/leadership/quotes.asp?q=253&c=6. Accessed 28 Nov 2018
2. UK Cabinet Office: National Cyber Security Strategy 2016 to 2021. UK Cabinet Office, November 2016
3. Leveson, N.G., Thomas, J.P.: STPA Handbook (2018)
4. Howard, G., Butler, M., Colley, J., Sassone, V.: Formal analysis of safety and security requirements of critical systems supported by an extended STPA methodology. In: 2nd Workshop on Safety & Security aSSurance (2017). https://doi.org/10.1109/EuroSPW.2017.68
5. Abrial, J.-R.: Modeling in Event-B: System and Software Engineering. Cambridge University Press, Cambridge (2010)
6. Dürrwang, J., Beckers, K., Kriesten, R.: A lightweight threat analysis approach intertwining safety and security for the automotive domain. In: Tonetta, S., Schoitsch, E., Bitsch, F. (eds.) SAFECOMP 2017. LNCS, vol. 10488, pp. 305–319. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66266-4_20
7. Potter, B.: Microsoft SDL threat modelling tool. In: Network Security, vol. 1, pp. 15–18 (2009)