sensors

MDPI

Article

Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems

Georgios Kavallieratos, Georgios Spathoulas and Sokratis Katsikas *

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, N-2815 Gjøvik, Norway; georgios.kavallieratos@ntnu.no (G.K.); georgios.spathoulas@ntnu.no (G.S.)
* Correspondence: sokratis.katsikas@ntnu.no; Tel.: +47-91138581

Abstract: The increasingly witnessed integration of information technology with operational technology leads to the formation of Cyber-Physical Systems (CPSs) that intertwine physical and cyber components and connect to each other to form systems-of-systems. This interconnection enables the offering of functionality beyond the combined offering of each individual component, but at the same time increases the cyber risk of the overall system, as such risk propagates between and aggregates at component systems. The complexity of the resulting systems-of-systems in many cases leads to difficulty in analyzing cyber risk. Additionally, the selection of cybersecurity controls that will effectively and efficiently treat the cyber risk is commonly performed manually, or at best with limited automated decision support. In this work, we propose a method for analyzing risk propagation and aggregation in complex CPSs utilizing the results of risk assessments of their individual constituents. Additionally, we propose a method employing evolutionary programming for automating the selection of an optimal set of cybersecurity controls out of a list of available controls, that will minimize the residual risk and the cost associated with the implementation of these measures. We illustrate the workings of the proposed methods by applying them to the navigational systems of two variants of the Cyber-Enabled Ship (C-ES), namely the autonomous ship and the remotely controlled ship. The results are sets of cybersecurity controls applied to those components of the overall system that have been identified in previous studies as the most vulnerable ones; such controls minimize the residual risk, while also minimizing the cost of implementation.

Keywords: cybersecurity; cyber physical systems; cyber risk propagation; cybersecurity controls; autonomous vessels

Citation: Kavallieratos, G.; Spathoulas, G.; Katsikas, S. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems. *Sensors* **2021**, *21*, 1691. https://doi.org/10.3390/s21051691

Academic Editor: Sherali Zeadally

Received: 24 January 2021
Accepted: 23 February 2021
Published: 1 March 2021

1. Introduction

Cyber-Physical Systems (CPSs) are characterized by the strong coupling of the physical and the cyber worlds. The inevitable dependence on highly automated procedures and the increasing integration of *physical parts* to highly interconnected *cyber parts* render CPSs vulnerable to cyber attacks. On the other hand, the wide use of such systems in various critical domains [1] (e.g., Smart Grid, Intelligent Transportation Systems, Medical devices, Industrial Control Systems, etc.) increases the impact of such cyber attacks. Furthermore, the *System of Systems* (SoS) nature of interconnected, complex CPSs [2] introduces challenges in addressing security risks. In this context, a complex CPS comprises other CPSs that are interconnected, and control and information flows exist among them. These flows constitute pathways that a cyber attack may leverage to propagate from component to component. More specifically, both or either of the likelihood of the attack and its impact, if successful, may propagate. Because likelihood and impact are the constituents of risk, the cyber risk of the overall system is related to the individual cyber risk of each interconnected component. This in principle means that knowledge of the cyber risk of the individual components of a complex CPS may be leveraged to assess the cyber risk of the overall system, thus also facilitating the analysis of large scale, complex CPSs through a divide-and-conquer-like approach to cyber risk assessment.

The assessment of risk is one of the steps in the risk management process [3] that concludes with treating the risk by means of controls that aim at achieving retention, reduction, transfer, or avoidance of the risk [4]. In the general case, each risk can be treated by a number of possible cybersecurity controls, each of which with varying effectiveness and efficiency characteristics. Note that the same control may be effective and efficient in treating more than one risk. Therefore, an important task in formulating the risk treatment plan is the selection of the optimal set of cybersecurity controls, the criterion of optimality in this context being effectiveness and efficiency. Because of the complexity of formulating this as a formal optimization problem, particularly when there are more than one criteria of optimality, the selection of the cybersecurity controls is largely performed empirically, at best with some automated decision support.

In this paper, we propose a novel method for identifying a set of effective and efficient cybersecurity controls for large scale, complex CPSs comprising other CPSs as components. We also propose a method for assessing the aggregated risk that results by taking into account the risk of the individual components and the information and control flows among these components. Specifically, we leverage evolutionary computing to develop a cybersecurity control selection algorithm that uses the aggregated cyber risk of a complex CPS to generate a set of effective and efficient cybersecurity controls to reduce this risk. The algorithm selects the cybersecurity controls among the list of such controls in the NIST Guidelines for Industrial Control Systems Security [5]. We illustrate the workings of the proposed method by applying it to the navigational systems of two instances of the Cyber-Enabled Ship (C-ES), i.e., vessels with enhanced monitoring, communication, and connection capabilities that include remotely controlled and fully autonomous ships [6]. The C-ES comprises a variety of interconnected and interdependent CPSs [7], and, as such, it constitutes a complex CPS. Specifically, we derive the set of cybersecurity controls for both the autonomous and the remotely controlled vessel.

Thus, the contribution of this work is as follows:

- A novel method for assessing the aggregate cybersecurity risk of a large scale, complex CPS comprising components connected via links that implement both information and control flows, by using risk measures of its individual components and the information and control flows among these components.
- A novel method for selecting a set of effective and efficient cybersecurity controls among those in an established knowledge base, that reduce the residual risk, while at the same time minimizing the cost.
- Sets of cybersecurity controls for the navigational systems of two instances of the C-ES, namely the remotely controlled ship and the autonomous ship, derived by employing the two methods.

The remainder of this paper is structured as follows: Section 2 reviews the related work in the areas of cyber risk propagation and aggregation; optimal selection of cybersecurity controls; and C-ES risk management. Section 3 provides the background knowledge on genetic algorithms, and on the STRIDE (*S*poofing, *T*ampering, *R*epudiation, *I*nformation disclosure, *D*enial of Service, and *E*levation) and DREAD (*D*amage, *R*eproducibility, *E*xploitability, *A*ffected, and *D*iscoverability) risk assessment methods that is necessary to make the paper self-sustained. Sections 4 and 5 present the proposed method for risk aggregation in complex CPSs and the proposed method for optimal cybersecurity control selection, respectively. In Section 6, we apply the proposed methods to the remotely controlled and the autonomous ship cases and discuss the results. Finally, Section 7 summarizes our conclusions and outlines topics for future research work.

2. Related Work

Cyber risk is evaluated as a function of the likelihood of an adverse event, such as an attack, occurring; and of the impact that will result when the event occurs. In order for an adverse event to occur, a threat has to successfully exploit one or more vulnerabilities; this can be done by launching one of a number of possible attacks. Hence, the likelihood

of the event occurring is, in turn, determined by the likelihood of the threat successfully exploiting at least one vulnerability. Accordingly, in order to analyze how the cyber risk propagates in a complex system made up by interconnected components that are systems by themselves requires analyzing how both the likelihood of the event and its impact propagates. Once this analysis is accomplished, the aggregate cyber risk of the complex system can be assessed.

Several security risk assessment methods applicable to general purpose IT systems have appeared in the literature (see Reference [8] for a comprehensive survey). Even though several of these methods can be and have been applied to CPSs, they cannot accurately assess cyber risks related to CPSs according to Reference [9], where a number of approaches for risk assessment for CPSs are listed. A review of risk assessment methods for CPSs, from the perspective of safety, security, and their integration, including a proposal for some classification criteria was made in Reference [10]. A survey of IoT-enabled cyberattacks that includes a part focused on CPS-based environments can be found in Reference [11]. Cyber risk assessment methods for CPSs more often than not are domain specific, as they need to take into account safety as an impact factor additional to the "traditional" impact factors of confidentiality, integrity, and availability. For example, an overview of such methods specific to the smart grid case is provided in Reference [12]. A review of the traditional cybersecurity risk assessment methods that have been used in the maritime domain, is provided in Reference [13]. Additionally, various risk assessment methods have been proposed to analyze cyber risk in autonomous vessels [14–16].

Several works in the literature have studied how individual elements of cyber risk propagate in a network of interconnected systems; both deterministic and stochastic approaches have been used to this end. A threat likelihood propagation model for information systems based on the Markov process was proposed in Reference [17]. An approach for determining the propagation of the design faults of an information system by means of a probabilistic method was proposed in Reference [18]. A security risk analysis model (SRAM) that allows the analysis of the propagation of vulnerabilities in information systems, based on a Bayesian network, was proposed in Reference [19]. Methods for evaluating the propagation of the impact of cyber attacks in CPSs have been proposed in Reference [20–22], among others. Epidemic models were initially used to study malware propagation in information systems [17]. The propagation of cybersecurity incidents in a CPS is viewed as an epidemic outbreak in Reference [23] and is analyzed using percolation theory. The method was shown to be applicable for studying malware infection incidents, but it is questionable whether the epidemic outbreak model fits other types of incidents. Percolation theory was also used in Reference [24] to analyze the propagation of node failures in a network of CPSs comprising cyber and physical nodes organized in two distinct layers, such as in the case of the power grid. The Susceptible–Exposed–Infected–Recovered (SEIR) infectious disease model was used in Reference [25] to study malware infection propagation in the smart grid. A quantitative risk assessment model that provides asset-wise and overall risks for a given CPS and also considers risk propagation among dependent nodes was proposed in Reference [26].

A method for assessing the aggregate risk of a set of interdependent critical infrastructures was proposed in References [27,28]. The method provides an aggregate cyber risk value at the infrastructure level, rather than a detailed cyber risk assessment at the system/component level. Thus, it is suitable for evaluating the criticality of infrastructure sectors, but not for designing cybersecurity architectures or for selecting appropriate cybersecurity controls. A similar approach for the Energy Internet [29] was followed to develop an information security risk algorithm based on dynamic risk propagation in Reference [30]. A framework for modeling and evaluating the aggregate risk of user activity patterns in social networks was proposed in Reference [31]. A two-level hierarchical model was used in Reference [32] to represent the structure of essential services in the national cyberspace, and to evaluate the national level (aggregate) risk assessment by taking into account cyber threats and vulnerabilities identified at the lower level.

Based on the above discussion, it is evident that the problem of risk propagation and risk aggregation for complex systems, on one hand, and the problem of optimal selection of cybersecurity controls, on the other, have been individually studied. The conjunct problem of identifying the optimal set of cybersecurity controls that reduces the aggregate risk in a complex CPS cannot be approached by sequential application of methods each of which addresses the problem's components, due to the inherent nonlinearity of the risk propagation, risk aggregation, and control selection processes on one hand, and the intertwining of these processes. To the best of our knowledge, no method that solves this conjunct problem is currently available.

On the other hand, the systematic selection of cybersecurity controls has been mostly examined in the literature in attempting to identify the optimal set of controls for IT systems within a specified budget; examples of such approaches are those in References [33–35]. The outline of a programming tool that supports the selection of countermeasures to secure an infrastructure represented as a hierarchy of components was provided in Reference [36]. A methodology based on an attack surface model to identify the countermeasures against multiple cyberattacks that optimize the Return On Response Investment (RORI) measure is proposed in Reference [37]. However, to the best of our knowledge, a method that selects a set of cybersecurity controls that simultaneously optimizes both effectiveness and efficiency, by minimizing the residual risk and the cost of implementation, is still to be proposed.

The work described in this paper addresses these research gaps.

3. Background

3.1. Evolutionary/Genetic Algorithms

Genetic algorithms (GAs) are randomized search algorithms that imitate the structures of natural genetics and the mechanisms of natural selection [38]. They imitate biological genomes by means of strings structures that represent individuals and are composed of characters belonging to a sepcified alphabet. These structures form populations that evolve in time by means of a randomized exchange scheme that implements the principle of survival of the fittest; in every new generation, a new set of individuals is created, using parts of the fittest members of the old set, whilst also possibly retaining some of the fittest members of the old generation. GAs can be very useful when it comes to problems with very large solution spaces, where it is infeasible to exhaustively search the solution space. It should, however, be noted that GAs are not guaranteed to find the global optimum solution to a problem; however, they do find "acceptably good" solutions.

For designing a GA, a *coding scheme* that codes the parameter space; a set of *operators* to be used to each generation to generate the next generation; and a *fitness function* that measures the fitness of each individual as a functional of the function that we are trying to optimize need to be defined. The coding scheme and the fitness function to be used depend on the characteristics of the optimization problem on which the GA will be applied. However, a commonly used coding scheme is to use the binary alphabet to represent each element (gene) in a string (genome). On the other hand, the most commonly used operators are the *reproduction* operator, the *crossover* operator, and the *mutation* operator. These have been found to be both computationally simple and effective in a number of optimization problems [39].

The operators are used to evolve populations by creating new individuals that will form the new generation. To this end, the reproduction operator tentatively selects individuals with high fitness function values as candidate parents for the next generation, by means of a randomized technique, such as a *roulette wheel selection scheme*. The selected parents may mate by means of the crossover operator, that randomly selects pairs of mates and creates new individuals, by combining elements of both parents, these elements being selected at random. As in biological populations, random genetic alterations (mutations) sometimes result in genetically fitter individuals. Such alterations, that happen with small probability, are implemented in GAs by means of the mutation operator.

The generic GA addresses unconstrained optimization problems. However, constrained optimization problems are encountered more often than not, including the problem addressed in this work, as will be seen in the sequel. Constraints can be modeled as either equality relations, that can be incorporated within the function to be optimized; or as inequality relations, that may be handled either by simply evaluating the fitness of each individual and then check to see whether any constraints are violated, or by employing a penalty method. In the former (reactive) strategy, if an individual violates a constraint, it is assigned a fitness value equal to zero. In the latter (proactive) strategy, the fitness of an individual that violates a constraint is decreased by an amount proportional to the cost of the violation.

3.2. STRIDE

STRIDE [40] is a cyber security threat modeling method that was developed at Microsoft in 1999. It facilitates the process of identifying and analyzing six types of threats, namely *S*poofing, *T*ampering, *R*epudiation, *I*nformation disclosure, *D*enial of Service, and *E*levation of privileges, in which the initials form the acronym *STRIDE*. Each of these threats corresponds to the violation of a desirable property (security objective) of the system under study, as follows:

- Spoofing corresponds to violation of authenticity;
- Tampering corresponds to violation of integrity;
- Repudiation corresponds to violation of non-repudiability;
- Information disclosure corresponds to violation of confidentiality;
- Denial of service corresponds to violation of availability; and
- Elevation of privileges corresponds to violation of authorization.

STRIDE can be used to analyze threats for systems being in a variety of development phases, even for systems at the design phase; thus, it enables adherence to security-by-design principles [41]. Furthermore, even though originally designed for software systems, STRIDE has been also used in ecosystem environments where CPSs are prominently present [42–44]. In particular, a modified version of STRIDE was proposed and used in Reference [6] to model threats, to develop cyber attack scenarios, and to qualitatively assess the accordant risks for a number of CPSs in the C-ES ecosystem.

3.3. DREAD

DREAD is a security risk assessment model that, like STRIDE, was developed as part of Microsoft's threat modeling and risk analysis process. The name is an acronym made up from the initials of the characteristics of the risk associated with each attack scenario being analyzed, namely *D*amage (what is the extent of the damage that the attack is expected to inflict on the system); *R*eproducibility (how easy it is to reproduce the attack); *E*xploitability (the extent of the resources that the adversary needs to launch the attack); *A*ffected users/systems (how many people and/or systems will be affected); and *D*iscoverability (how easy is it for the adversary to identify vulnerabilities to exploit for launching the attack) [45].

STRIDE and DREAD are interrelated: the former allows the qualitative security analysis of the system, whilst the latter quantifies the identified risks. According to the approach in Reference [22], the values (High, Medium, Low) of the DREAD variables associated with each STRIDE threat $t \in \{S, T, R, I, D, E\}$ are determined by applying a specific set of criteria, shown in Table 1; these have been adapted from those in Reference [45], so as to include CPS aspects, and are further analyzed in Reference [22].

Table 1. Criteria for determining the values of the DREAD (*D*amage, *R*eproducibility, *E*xploitability, *A*ffected, and *D*iscoverability) variables [22,44].

	High (3)	Medium (2)	Low (1)
D	The adversary is able to bypass security mechanisms; get administrator access; upload/modify the CPS content.	Leakage of confidential information of the CPSs (functions/source code); partial malfunction/disruption of the system.	Leakage of non-sensitive information; the attack is not possible to extend to other CPSs on-board.
R	The attack can be reproduced at anytime.	The adversary is able to reproduce the attack, but under specific risk conditions.	Although the attacker knows the CPS's vulnerabilities/faults, they are unable to launch the attack.
E	The attack can be performed by a novice adversary, in a short time.	A skilled adversary may launch the attack.	The attack requires an extremely skilled person and in-depth knowledge of the targeted CPS.
A	All CPSs are affected.	Some users/systems, with non-default configuration are affected.	The attack affects only the targeted CPS.
D	The CPS's vulnerabilities are well known, and the attacker is able to access the relevant information to exploit them.	The CPS's vulnerabilities/faults are not well known and the adversary needs to access the CPS.	The threat has been identified, and the vulnerabilities have been patched.

Then, the risk value R_t^s associated with each STRIDE threat $t \in \{S, T, R, I, D, E\}$ for system s is calculated by using the following formulas [41,44,45]:

$$Impact_t^s = \frac{Damage + Affectedsystems}{2}, \quad (1)$$

$$Likelihood_t^s = \frac{Reproducibility + Exploitability + Discoverability)}{3}, \quad (2)$$

$$Risk_t^s = \frac{(Impact_t^s + Likelihood_t^s)}{2}. \quad (3)$$

$Impact_t^s$ represents a measure of the effect a successful attack materializing threat t has on the component s; $Likelihood_t^s$ represents a measure of how likely it is for threat t to materialize on s.

Both STRIDE and DREAD have been used in Reference [44] to assess the cyber risk of Cyber-Physical Systems (CPSs) on board the C-ES paradigm.

4. Cyber Risk Propagation and Aggregation

4.1. System Model

Assume a CPS consisting of N interconnected components, each denoted by c_i, $i = 1, ...N$. This system can be represented by a directed graph of $N + 1$ nodes, the system itself being one of the nodes, denoted as c_0. The edges of the graph represent information and control flows between the nodes. An edge from node A to node B indicates the existence of either an information flow or a control flow, from A to B. A consequence of the existence of such an edge is that a cybersecurity event at node A affects node B, as well. For example, in the simple graph of Figure 1, a cybersecurity event at node A will have effect on node B, as well, while a cybersecurity event at node B will have effect on both nodes A and C. The relationship "has effect" can be quantified by assigning an *effect coefficient* to each flow.

These are denoted henceforth by eff^{a}_{AB}, where $a = I$ for the information flow, and $a = C$ for the control flow, respectively. One way of assigning values to these coefficients is to use the inverse of the *in degree centrality*, i.e., the number of flows arriving to that node, denoted by IDC. Following this approach, the case in which information arrives to node B only through node A, will result in a much higher eff^{I}_{AB} than the case where information arrives to node B from a large number of nodes, including A. By definition, the values of all effect coefficients lie in the [0, 1] range and provide an indication of the percentage of the damage that is propagated from one node to the other. The *total effect coefficient* eff^{T}_{AB} is computed as a function of eff^{I}_{AB} and eff^{C}_{AB}, as in Equation (4).

The function f in Equation (4) has to be instantiated according to the requirements of the domain to which the methodology is applied and/or to specific characteristics of components A and B with regards to the criticality of information and control flows between them. For example, one option is to select f as the average of the effect coefficients. This option reflects equal importance of the information and the control flows in risk propagation, and it has been used in the illustrative application of the method presented in Section 6.

$$eff^{T}_{AB} = f(eff^{I}_{AB}, eff^{C}_{AB}), \tag{4}$$

where $eff^{I}_{AB} = \frac{1}{IDC^{I}_{B}}$, $eff^{C}_{AB} = \frac{1}{IDC^{C}_{B}}$.

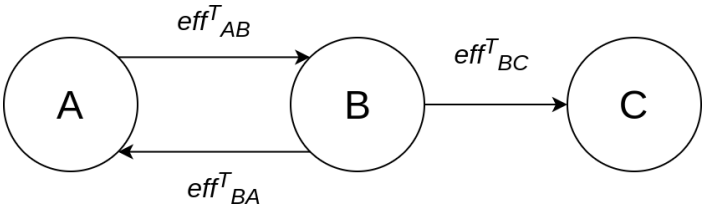

Figure 1. Effect relationship between nodes.

Another example is that of a cyber-physical system that mainly aims at sensing and processing data coming from a process, e.g., an electric power smart meter. In such systems, information workflows are more significant than control flows, and a function f of the form $eff^{T}_{AB} = a \times eff^{I}_{AB} + b \times eff^{C}_{AB}$ with $a + b = 1, a > b$ would be a good choice. On the other hand, for a cyber-physical system that aims at controlling a process, e.g., a smart grid digital switch, a variant of the same function f but with $a + b = 1, b > a$ would be more appropriate, as control flows are more likely to enable cyber risk propagation between components.

4.2. Aggregate Risk

For any threat t, the *aggregate* risk $R_t^{agg_{c_j}}$ of component c_j is (applying the worst case scenario principle [28]) given by:

$$R_t^{agg_{c_j}} = \max(R_t^{dir_{c_j}}, R_t^{prop_{c_j}}), \tag{5}$$

where $R_t^{dir_{c_j}}$ (*direct* risk) is the risk when c_j is not connected to any other component c_k, $k \neq j$, which is calculated by means of Equations (1)–(3), and $R_t^{prop_{c_j}}$ (*propagated* risk) is the risk that c_j faces because of its connections to other components. These connections may be over any, possibly multi-hop, path p_l from any node k to j, $k \neq j$. Applying again the worst case scenario principle, $R_t^{prop_{c_j}}$ is calculated as:

$$R_t^{prop_{c_j}} = \max_{p_l} R_t^{prop_{c_j}^{p_l}}, \tag{6}$$

where $R_t^{prop_{c_j}^{p_l}}$ is the risk of component c_j associated with threat t and propagated along path p_l.

When a threat materializes against component c_i, it will also create an effect to component c_j, if c_i and c_j are connected. In the absence of controls, the likelihood that this will happen is equal to the likelihood that the threat will materialize against c_i in the first place. In contrast, the impact that this event has on c_j is only a fraction of the impact the event has on any c_k on any path p_l from c_i to c_j. This fraction is represented by $eff_{p_l}^T$ and is calculated by

$$eff_{p_l}^T = \prod_{i=1}^{j-1} eff_{c_i c_{i+1}}^T. \tag{7}$$

Accordingly, the risk propagated over path p_l, originating at component (node) c_i and terminating at component (node) c_j, is calculated by:

$$R_t^{prop_{c_j}^{p_l}} = \frac{eff_{c_i c_j}^{T_{p_l}} \times Impact_t^{c_i} + L_t^{c_i}}{2}. \tag{8}$$

The system as a whole is represented by c_0; therefore, the (global) risk of threat t for the system is given by:

$$R_t^s = R_t^{agg_{c_0}} = \max(R_t^{dir_{c_0}}, R_t^{prop_{c_0}}), \tag{9}$$

where the direct risk for the system is not applicable ($R_t^{dir_{c_0}} = 0$) and the propagated risk for the system is calculated as for any other node ($R_t^{prop_{c_0}} = \max_{p_l} R_t^{prop_{c_0}^{p_l}}$), thus

$$R_t^s = \max_{p_l} R_t^{prop_{c_0}^{p_l}} \tag{10}$$

In order to showcase how the global risk calculation works and also to shed light on an underlying subtle assumption, consider the example system shown in Figure 2. In order to calculate the aggregate risk of each c_i, $i = 1, 2, 3$, we need to calculate the propagated risks, and this requires identifying all possible paths originating at any node and terminating at c_i, $i = 1, 2, 3$, respectively. The propagated risk for c_3 is equal to zero, as there is no such path. Nodes c_1 and c_2 are interconnected; therefore, a loop exists between them. Consequently, if we allow circular paths to be considered, there are infinite paths between these two nodes, and the computation in Equation (7) would be endless. However, by noticing that the value of the total effect coefficient becomes, by definition, negligible after a couple of hops, we are able to disregard circular paths in its computation.

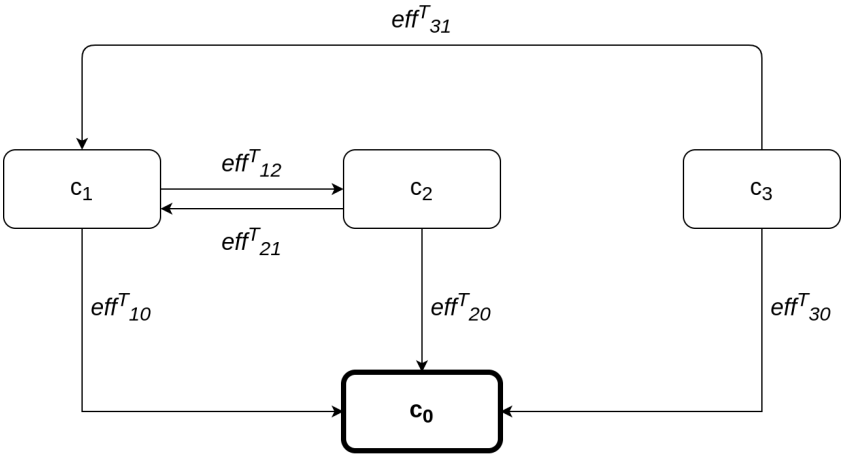

Figure 2. An example of a system.

Therefore, the global risk of a system can be calculated by the algorithm in Algorithm 1. As can be seen in Algorithm 1, nodes along a path are processed recursively, starting at the end of the path. If a node is already in the path, it is not included again, so as to avoid cyclic paths.

Algorithm 1: Global system risk calculation algorithm.

Result: Global system risk is calculated as R_t^s
Function `process_node`(c_j, eff, p_l)**:**
  $L = L_t^{c_j}$;
  $I = I_t^{c_j}$;
  $R = \frac{L+I}{2}$;
  foreach *edge from* c_i *to* c_j **do**
    if $c_i \notin p_l$ **then**
      $p_l = p_l \cup \{c_i\}$;
      $L', I' = process\_node(c_i, eff_{c_i c_j}, p_l)$;
      $R' = \frac{L'+I'}{2}$;
      if $R' > R$ **then**
        $L = L'$;
        $I = I'$;
        $R = R'$;
      end
    end
  end
  return $eff \times L, I$;
L, I=`process_node`(c_0, 1, $\{c_0\}$);
$R_t^s = \frac{L+I}{2}$;

5. Optimal Cybersecurity Control Selection

5.1. Cybersecurity Controls

We assume that there exists a list of controls available to apply to the components of the system. Each control m, when applied to component c_i, has a potential effect on the values of $Impact_t^{c_i}$ and $Likelihood_t^{c_i}$ that are used in the calculation of the cyber risk, such effect depending on the effectiveness and the nature of the control. We denote the new Likelihood and Impact values of threat t that result after the application of control m to c_i by $Likelihood_{tm}^{c_i}$ and $Impact_{tm}^{c_i}$, respectively. These values can be calculated by re-applying DREAD to the system, which is now protected by m.

Additionally, for each control m, a cost metric $Cost_m$ is defined. This metric is expressed on a 1–5 scale, corresponding to the qualitative classifications very low cost, low cost, medium cost, high cost, and very high cost. Note that the use of this scale was dictated by the fact that it is difficult to measure the cost of implementing a control. However, if such a measure is available, the replacement of the value in the 1–5 scale with the actual cost of the control is straightforward.

For a system with N components and a list with M controls with the cost metrics vector $C = [cost_1, cost_2, ..., cost_M]$, the following binary matrix AC compactly depicts the applied controls throughout the system:

$$AC = \begin{bmatrix} ac_{1,1} & ac_{1,2} & ... & ac_{1,N} \\ ac_{2,1} & ac_{2,2} & ... & ac_{2,N} \\ ... & ... & ... & ... \\ ac_{M,1} & ac_{M,2} & ... & ac_{M,N} \end{bmatrix}, \quad (11)$$

where

$$ac_{i,j} = \begin{cases} 0, \textit{if control } i \textit{ is not applied to component } j \\ 1, \textit{if control } i \textit{ is applied to component } j \end{cases}. \quad (12)$$

Then, the total cost TC_{AC} of the applied controls solution AC is given by $TC_{AC} = AC \times C$.

5.2. Optimization Method

The optimization problem to be solved is to select the optimal (effective and efficient) set of controls among a list of possible ones. This amounts to selecting the set of controls AC that minimizes the system *residual* risk $R^s_{t_{AC}}$, at the lowest total cost TC. A closed formula that would allow the application of an exact optimization method, and thus the calculation of the globally optimum solution to the problem, is not possible to construct, unless many, not necessarily realistic, assumptions are made. On the other hand, the large size of the search space (all candidate solutions) prohibits the exhaustive search approach. Hence, a heuristic optimization method has to be employed [46]; we have selected to use a genetic algorithm, even though any other heuristic optimization method would, in principle, be applicable.

The design parameters of the genetic algorithm are as follows:

- The search space comprises all possible combinations of controls applied to components.
- Each individual solution is represented by the matrix AC, which is transformed into a binary vector of size $M \times N$. The value of each element of the vector represents the decision to apply a specific control to a specific component or not. For example, for a system with three components and two controls, the solution would be denoted by the vector $[ac_{11}, ac_{21}, ac_{12}, ac_{22}, ac_{13}, ac_{23}]$, assuming that all controls are applicable to all components.
- The fitness function is defined as $fit(AC) = R^s_{t_{AC}} + C_{norm}(AC)$, where $C_{norm}(AC) = \frac{TC_{AC}}{TC_{max}}$, with TC_{max} being the largest possible cost, that results when applying all available controls to all system components.
- The initial population size is 100.
- The mutation probability is 0.1.
- The next generation is determined by uniform crossover, with crossover probability equal to 0.5, an elite ratio of 0.01, and 0.3 of the population consisting of the fittest members of the previous generation (aka parents).
- The algorithm terminates when the maximum number of allowed iterations is used. This number is calculated as $iter_{max} = 50 \times \sum_{i=1,j=1}^{i=M,j=N} ac_{ij}$.

The algorithm for selecting the optimal set of security controls is depicted in Algorithm 2.

Note that the fitness function consists of two elements, namely the residual risk (which takes values in [0, 3]) and the normalized cost (which takes values in [0, 1]). This non-symmetric approach has been selected to put emphasis on the importance of reducing the residual risk, even by bearing larger cost. This approach results in initial iterations of the algorithm tending to generate solutions that minimize the residual risk. In later iterations of the algorithm, the less costly combinations of controls prevail, among those that lead to the maximum possible risk reduction.

Algorithm 2: Algorithm for selecting the optimal set of security controls

Result: Optimal set of security controls is identified

Function `calc_fitness(`*control_sets*`):`

control_sets_fit_scores = [];

foreach *c in control_sets* **do**

control_sets_fit_scores[c] = fit_score(*c*);

end

return control_sets_fit_scores;

Function `select_parents(`*control_sets,control_sets_fit_scores*`):`

parents_control_sets = [] ;

foreach *c in control_sets* **do**

if *control_sets_fit_scores[c]* $\in$ *upper 30% of control_sets_fit_scores* **then**

parents_control_sets $\leftarrow$ *c*;

end

end

return parents_control_sets;

Function `select_elite(`*control_sets,control_sets_fit_scores*`):`

elite_control_sets = [] ;

foreach *c in control_sets* **do**

if *control_sets_fit_scores[c]* $\in$ *upper 1% of control_sets_fit_scores* **then**

elite_control_sets $\leftarrow$ *c*;

end

end

return elite_control_sets;

Function `crossover(`*parent_control_sets*`):`

control_sets = parent_control_sets;

pop = $|$control_sets$|$;

while *pop<100* **do**

$parent_a = random(parent\_control\_sets)$;

$parent_b = random(parent\_control\_sets)$;

$control\_set_{new} = crossover(parent_a, parent_b)$;

$control\_sets \leftarrow control\_set_{new}$;

$pop = pop + 1$;

end

return control_sets;

Function `mutation(`*control_sets,elite_control_sets*`):`

mutated_control_sets = [];

foreach *c in control_sets* **do**

if *c* $\in$ *elite_control_sets* **then**

$mutated\_control\_sets \leftarrow c$;

else

$mut\_c = mutate(c)$;

$mutated\_control\_sets \leftarrow mut\_c$;

end

end

return *mutated_control_sets*;

Algorithm 2: *Cont.*

```
Function find_solution():
    iter_max = 50 × Σ_{i=1,j=1}^{i=M,j=N} ac_ij;
    iter = 0;
    control_sets ← 100 random sets;
    while iter < iter_max do
        control_sets_fit_scores = calc_fitness(control_sets);
        parents_control_sets = select_parents(control_sets,control_sets_fit_scores);
        elite_control_sets = select_elite(control_sets,control_sets_fit_scores);
        control_sets = crossover(parents_control_sets);
        control_sets = mutation(control_sets);
        iter = iter + 1
    fittest_control_set = fittest c ∈ control_sets return fittest_control_set;
find_solution()
```

6. Application to the C-ES

Autonomous and remotely controlled ships—both variants of the Cyber-Enabled Ship (C-ES)—are being increasingly developed. At the same time, the maritime transportation sector contributes significantly to the gross domestic product of many countries around the world. It is not surprising, then, that the cybersecurity of the sector has been designated a very high priority by international organizations [47] and national governments [48] alike. The CPSs comprising the C-ES were identified, and the overall ICT architecture of the C-ES in the form of a tree structure was proposed in Reference [6]. An extended Maritime Architectural Framework (e-MAF) was proposed, and the interconnections, dependencies, and interdependencies among the CPSs of the C-ES were described in Reference [7]. These results are depicted in the form of directed graphs in Figures 3–6 for the two variants of the C-ES. Furthermore, an initial threat analysis of the generic ICT architecture of the C-ES identified the three most vulnerable onboard systems, namely the Automatic Identification System (AIS), the Electronic Chart Display Information System (ECDIS), and the Global Maritime Distress and Safety System (GMDSS) [6]. These results were verified by means of the comprehensive threat and risk analysis that was presented in Reference [44]. The most critical attack paths within the navigational CPSs of the C-ES were identified in Reference [22]. The cybersecurity and safety requirements for the CPSs of the C-ES were identified in References [49,50], and an initial set of cybersecurity controls that satisfy these requirements was proposed in Reference [44].

Building upon earlier work, and as a step towards defining the cybersecurity architecture of such vessels, we selected the CPSs of the C-ES to illustrate the applicability of the methods proposed in this paper. The results are presented in the sequel for the autonomous and the remotely controlled vessel.

6.1. The Cyber-Enabled Ship

The CPSs of the C-ES were identified and described in Reference [6], where a threat analysis and a qualitative risk analysis were carried out, and the most vulnerable onboard systems were identified. Three distinct sub-groups of onboard CPSs were identified, namely the bridge CPSs; the engine CPSs; and the Shore Control Center (SCC) CPSs. The SCC is a sub-component of the remotely controlled vessel, that aims to control and navigate one or more ships from the shore. The interconnections, dependencies, and interdependencies of these CPSs were identified in Reference [7] and were later used to define the cybersecurity requirements of the C-ES in Reference [49]. The CPSs considered herein are:

- The Autonomous Navigation System (ANS) is responsible for the navigational functions of the vessel. ANS controls all the navigational sub-systems and communicates with the SCC by transmitting dynamic, voyage, static, and safety data to ensure the vessel's safe navigation.

- The Autonomous Ship Control (ASC) acts as an additional control for the C-ES and aims to assess the data derived from the sensors and from the SCC.
- The Advanced Sensor Module (ASM) automatically analyzes sensor data to enhance the environmental observations, such as ships in the vicinity. By leveraging sensor fusion techniques, this module analyzes data derived from navigational sensors, such as the Automatic Identification System (AIS) and the Radar.
- The Automatic Identification System (AIS) facilitates the identification, monitoring, and locating of the vessel by analyzing voyage, dynamic, and static data. Further, the AIS contributes to the vessel's collision avoidance system by providing real time data.
- The Collision Avoidance (CA) system ensures the safe passage of the vessel by avoiding potential obstacles. The system analyzes the voyage path by leveraging anti-collision algorithms conforming to the accordant COLREGs regulations [51].
- The Electronic Chart Display Information System (ECDIS) supports the vessel's navigation by providing the necessary nautical charts, along with vessel's attributes, such as position and speed.
- The marine RADAR provides the bearing and distance of objects in the vicinity of the vessel, for collision avoidance and navigation at sea.
- The Voyage Data Recorder (VDR) gathers and stores all the navigational data of the vessel specifically related to vessel's condition, position, movements, and communication recordings.
- The Auto Pilot (AP) controls the trajectory of the vessel without requiring continuous manual control by a human operator.

The methods proposed in Sections 4 and 5 used as input prior results, namely the system components and their interconnections that make up the system graph representation; the impact and likelihood values associated with the STRIDE threats and computed by means of DREAD for each individual component; and the list of available cybersecurity controls, along with information on their cost and effectiveness. Figures 3–6 depict the graph representations of the onboard navigational CPSs of the autonomous and of the remotely controlled ship, respectively, along with their interconnections and interdependencies [6,22,44]. Impact and likelihood values associated with the STRIDE threats and computed by means of DREAD are depicted in Tables 2 and 3 [44]. Each line of Tables 2 and 3 represents one of the STRIDE threats, indicated by the corresponding initial. Each column of the Table represents individual CPSs, indicated by their corresponding initials, as defined in Section 6.1. The values inside the cells are the corresponding impact (left table) and likelihood (right table) values per STRIDE threat and per individual component; these have been calculated by means of Equations (1) and (2), respectively. These values are subsequently used as input to Algorithm 1, to calculate the aggregate risk of each CPS.

The list of available cybersecurity controls has been defined based on the NIST guidelines for Industrial Control Systems security [5] by following a systematic process proposed in Reference [44]. The effectiveness and the cost of each security control are estimated considering their applicability, the extent to which each control reduces the impact or/and the likelihood, and the resources needed to implement it.

Table 2. Impact values.

	Impact									
	ANS	**ASC**	**ASM**	**AIS**	**CA**	**ECDIS**	**SCC**	**RADAR**	**AP**	**VDR**
S	2.5	3	2.5	2	2.5	2.5	2.5	2.5	2	2
T	2.5	2	1.28	2.5	2.5	2	2	2.5	2.5	2
R	2	2.5	1.5	2	1.5	1.5	1.5	2	1.5	1.5
I	2.5	2.5	2	2	1.5	3	1.5	1	2	2
D	2.5	2.5	2	2	2.5	3	2.5	2	2.5	2
E	3	3	1.5	2.5	1.5	3	1.5	2	2	2

Table 3. Likelihood values.

	Likelihood									
	ANS	**ASC**	**ASM**	**AIS**	**CA**	**ECDIS**	**SCC**	**RADAR**	**AP**	**VDR**
S	1.33	1.33	2	2.66	1.33	2.32	1.66	2	1	1
T	1.33	2	1.28	2.33	1.66	2.33	1.33	1.66	1	1
R	1	1	1	2.66	1	1	1.33	1.33	1	1
I	1	1	1.33	2.66	1.33	1.66	1.33	1	1	1
D	1.33	1.66	2	2	1.33	2	1.66	2	1	1
E	1.33	1	1	1.33	1	1.66	1	1	1	1

6.2. Optimal Controls for the Autonomous Ship

Autonomous ships are equipped with advanced interconnected CPSs able to navigate and sail the vessels without human intervention. The onboard navigational CPSs of the autonomous ship are described by the directed graphs $G_I(V, E)$ and $G_C(V, E)$ depicted in Figures 3 and 4, respectively, as discussed in detail in References [6,44]. $G_I(V, E)$ represents information flow connections and $G_C(V, E)$ control flow connections. Table 4 depicts the effect coefficients between all the considered systems. Each line and each column of Table 4 represents a CPS of the C-ES, indicated by their corresponding initials, as defined in Section 6.1 above. The values inside the cells are the effect coefficients between each pair of these systems; specifically, the value in the cell at row i and column j is the value of eff_{ij}^{T}. These have been calculated by means of Equation (13), which derives from Equation (4) when the function f is the average of the information and control effect coefficients. These values are also subsequently used as input to Algorithm 1, to calculate the aggregate risk of each CPS.

$$eff_{AB}^{T} = \frac{eff_{AB}^{I} + eff_{AB}^{C}}{2}. \tag{13}$$

It is worth noticing that CPSs with high information and control flows, such as the ANS and the ASC, are characterized by high values of the effect coefficient.

Table 4. Effect coefficients—Autonomous ship.

	C-ES	**AIS**	**ECDIS**	**VDR**	**ASM**	**RADAR**	**AP**	**CA**	**ANS**	**ASC**
C-ES	0	0	0	0	0	0	0	0	0	0
ANS	0.208	0.208	0.208	0.208	0.208	0.166	0.208	0.208	0	0
ASC	0.055	0.055	0.055	0.055	0.055	0	0.055	0.055	0.055	0
ASM	0.321	0.071	0.071	0	0	0	0.071	0.321	0.071	0.071
AIS	0.041	0	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041
CA	0.211	0.211	0.045	0.045	0.045	0.045	0.045	0	0.211	0.045
ECDIS	0.05	0.05	0	0.05	0.05	0.05	0.05	0.05	0.05	0.05
RADAR	0,055	0	0.055	0.055	0	0	0.055	0.055	0.555	0
AP	0,045	0.045	0.045	0	0	0.045	0	0.045	0.045	0.045
VDR	0,062	0.062	0.062	0	0	0.062	0	0	0.062	0.062

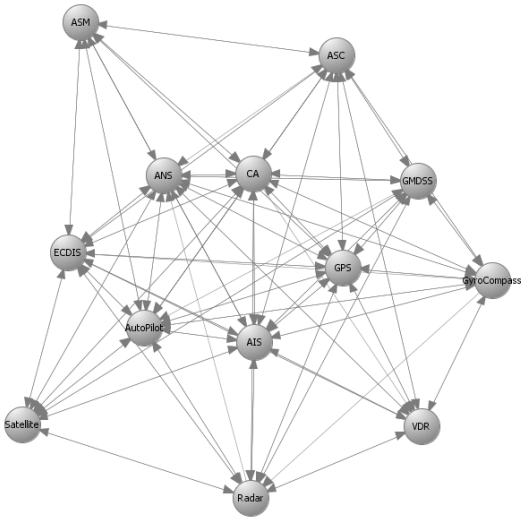

Figure 3. Autonomous ship—Navigational Cyber-Physical Systems (CPSs)–$G_I(V, E)$–Information flow connections.

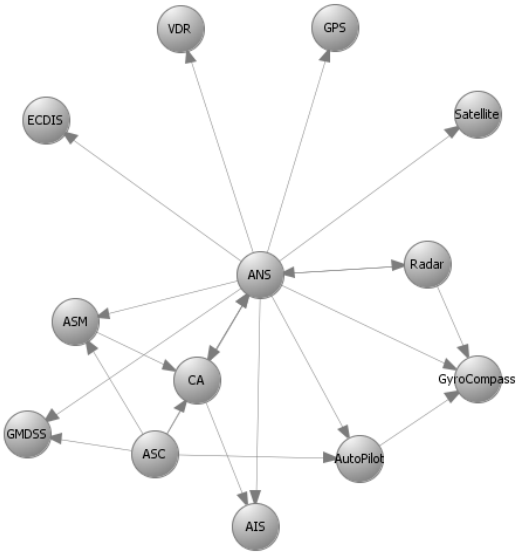

Figure 4. Autonomous ship—Navigational CPSs–$G_C(V, E)$–Control flow connections.

The security controls in the optimal set are selected from the initial list of available controls by applying the method described in Section 5. Table 5 depicts the optimal set of security controls per STRIDE threat and per CPS component. It also depicts the associated initial global risk (without controls) and the residual global risk (with the optimal controls applied). These values have been calculated by employing Algorithm 1.

Each line of Table 5 represents one of the STRIDE threats. The first column represents the global initial risk (i.e., without any security controls in place) of the C-ES, as assessed by means of Algorithm 1. The second column represents each constituent CPS, and the third column the optimal set of security controls identified by means of Algorithm 2. Finally, the fourth column represents the residual risk (i.e., with the optimal set of security controls in place) of the C-ES, as assessed by applying again Algorithm 1 with the risks of each individual CPS updated according to the effectiveness of the applied controls.

Table 5. Optimal controls—Autonomous ship.

Threat	Initial Risk	Component	Controls	Residual Risk
Spoofing	1.651	ECDIS ASM AIS Radar	Time Stamps (AU-8) Unsuccessful Logon Attempts (AC-7) Remote Access (AC-17) Security Assessments (CA-2)	0.964
Tampering	1.615	AIS Radar CA ECDIS ASC	Information Input Restrictions (SI-9) Tamper Protection (PE-3(5)) Tamper Protection (PE-3(5)) Port and I/O Device Access (SC-41) Tamper Protection (PE-3(5))	1.087
Repudiation	1.555	Radar AIS	Device Identification and Authentication (IA-3) Information System Component Inventory (CM-8 (4))	0.725
Information Disclosure	1.629	AIS CA ECDIS	Cryptographic Protection (SC-13) Information System Component Inventory (CM-8 (4)) Protection of Information at Rest (SC-28)	0.89
Denial of Service	1.373	AIS Radar CA ANS ASC ECDIS ASM	Denial of Service Protection (SC-5) Fail-Safe Procedures (SI-17) Denial of Service Protection (SC-5) Fail-Safe Procedures (SI-17) Power Equipment and Cabling (PE-9) Device Identification and Authentication (IA-3) Fail-Safe Procedures (SI-17)	0.89
Elevation of Privileges	1.129	ANS AIS ECDIS	Device Identification and Authentication (IA-3) Internal System Connections (CA-9) Unsuccessful Logon Attempts (AC-7)	0.725

6.3. Optimal Controls for the Remotely Controlled Ship

Remotely controlled vessels are equipped with CPSs that allow the control and operation of the vessel from the shore. Similarly with the autonomous vessel variant, the navigational CPSs of the remotely controlled ship are described by the directed graphs $G'_I(V, E)$ and $G'_C(V, E)$ in Figures 5 and 6. The SCC is a critical component in this variant of the C-ES, since the control and monitoring of the vessel critically depends on the SCC's normal operation. This is why the effect coefficients attain high values between systems that support the remote operations, such as the SCC, ANS, and ECDIS. All effect coefficients between the CPSs of the remotely controlled vessel are depicted in Table 6. Similarly to the case of the autonomous ship, the total effect coefficients have been calculated by means of Equation (13).

The security controls in the optimal set are selected from the initial list of available controls by applying the method described in Section 5. Table 7 depicts the optimal set of security controls per STRIDE threat and per CPS component. It also depicts the associated initial global risk (without controls) and the residual global risk (with the optimal controls applied). These values have been calculated in the same manner as the corresponding ones of the first C-ES variant.

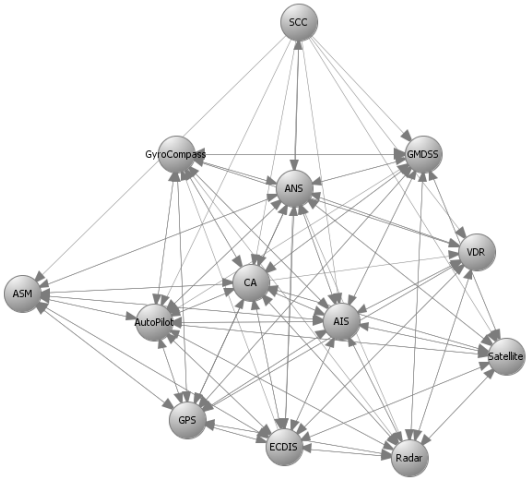

Figure 5. Remotely controlled ship—Navigational CPSs–$G'_I(V, E)$–Information flows.

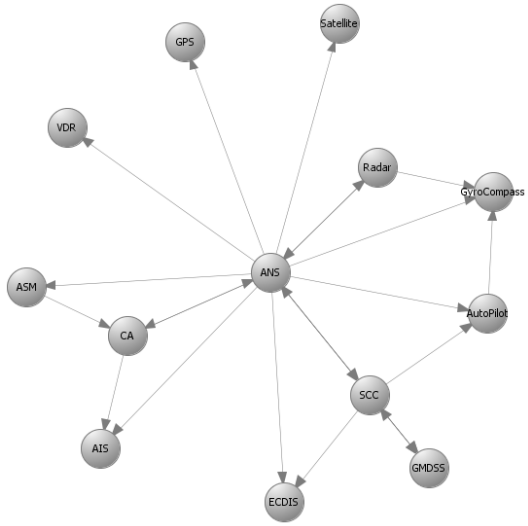

Figure 6. Remotely controlled ship—Navigational CPSs–$G'_C(V, E)$–Control flows.

Table 6. Effect coefficients—Remotely controlled ship.

	C-ES	AIS	ECDIS	VDR	ASM	RADAR	AP	CA	ANS	SCC
C-ES	0	0	0	0	0	0	0	0	0	0
ANS	0.208	0.208	0.208	0.208	0.208	0.106	0.208	0.208	0	0.208
SCC	0.75	0.5	0.75	0.5	0.5	0	0.75	0.5	0.75	0
ASM	0	0.071	0.071	0	0	0	0.071	0.321	0.071	0
AIS	0.041	0	0.041	0.041	0.041	0.041	0.041	0.041	0.041	0.041
CA	0	0.295	0.045	0.045	0.045	0.045	0.045	0	0.295	0
ECDIS	0.05	0.05	0	0	0.05	0.05	0.05	0.05	0.05	0.05
RADAR	0.166	0.166	0.166	0.166	0	0	0.166	0.166	0.666	0.166
AP	0.045	0.045	0.045	0	0.045	0.045	0	0.045	0.045	0
VDR	0	0.062	0.062	0	0	0.062	0	0	0.062	0

Table 7. Optimal controls–Remotely controlled ship.

Threat	Initial Risk	Component	Controls	Residual Risk
Spoofing	1.952	SCC ASM AIS Radar	Monitoring Physical Access (PE-6 (1)) Unsuccessful Logon Attempts (AC-7) Remote Access (AC-17) Security Assessments (CA-2)	1.663
Tampering	1.663	ECDIS ANS Radar CA SCC AIS	Device Identification and Authentication (IA-3) Port and I/O Device Access (SC-41) Tamper Protection (PE-3(5)) Tamper Protection (PE-3(5)) Physical Access Control (PE-3) Information Input Validation (SI-10)	1.04
Repudiation	1.828	AIS Radar SCC	Device Identification and Authentication (IA-3) Security Assessments (CA-2) Non-repudiation (AU-10)	0.875
Information Disclosure	1.828	AIS SCC	Cryptographic Protection (SC-13) Information System Component Inventory (CM-8 (4))	1.47
Denial of Service	1.622	ECDIS AIS CA SCC Radar ANS ASM	Internal System Connections (CA-9) Information System Backup (CP-9 (1), (2), (3), (5)) Denial of Service Protection (SC-5) Denial of Service Protection (SC-5) Security Assessments (CA-2) Emergency Shutoff (PE-10) Fail-Safe Procedures (SI-17)	0.99
Elevation of Privileges	1.205	ANS AIS ECDIS	Device Identification and Authentication (IA-3) Internal System Connections (CA-9) Unsuccessful Logon Attempts (AC-7)	0.875

6.4. Discussion

The overall process followed to carry out the case studies is depicted graphically in Figure 7. In this figure, rectangles represent processing steps, and skewed rectangles represent input/output; solid lines link processing steps, whilst dashed ones link input/output to processing steps. The shaded area delineates the content of this paper.

As can be seen in Table 5, in the case of the autonomous ship, twenty different security controls are recommended for application to seven of the ten navigational CPSs. The fact that these CPSs have been found in previous works [6,44] to be the most vulnerable onboard navigational systems, verifies the consistency of the proposed methods. Similarly, as can be seen in Table 7, twenty different security controls are recommended for application to six out of the ten navigational CPSs; again, these CPSs are the most vulnerable.

The optimal controls sets are different in the two variants of the C-ES. This reflects the difference in the level of autonomy of each variant: According to the IMO classification, the remotely controlled vessel lies at the second or third autonomy level, while the autonomous ship lies at the fourth level [52]. Different levels of autonomy mean different levels of interaction with humans and different levels of importance of the SCC in the ship's operation, which, in turn, mean different levels of risk for the same threat.

The security controls that are recommended by any automated decision support method, including the methods proposed herein, need to be *re-considered*, *consolidated*, and *checked for applicability* by domain experts and stakeholders together. The proposed methods enable the execution of what-if scenarios, including by modifying the initial list of the available security controls, and/or by modifying parameters of the genetic algorithm.

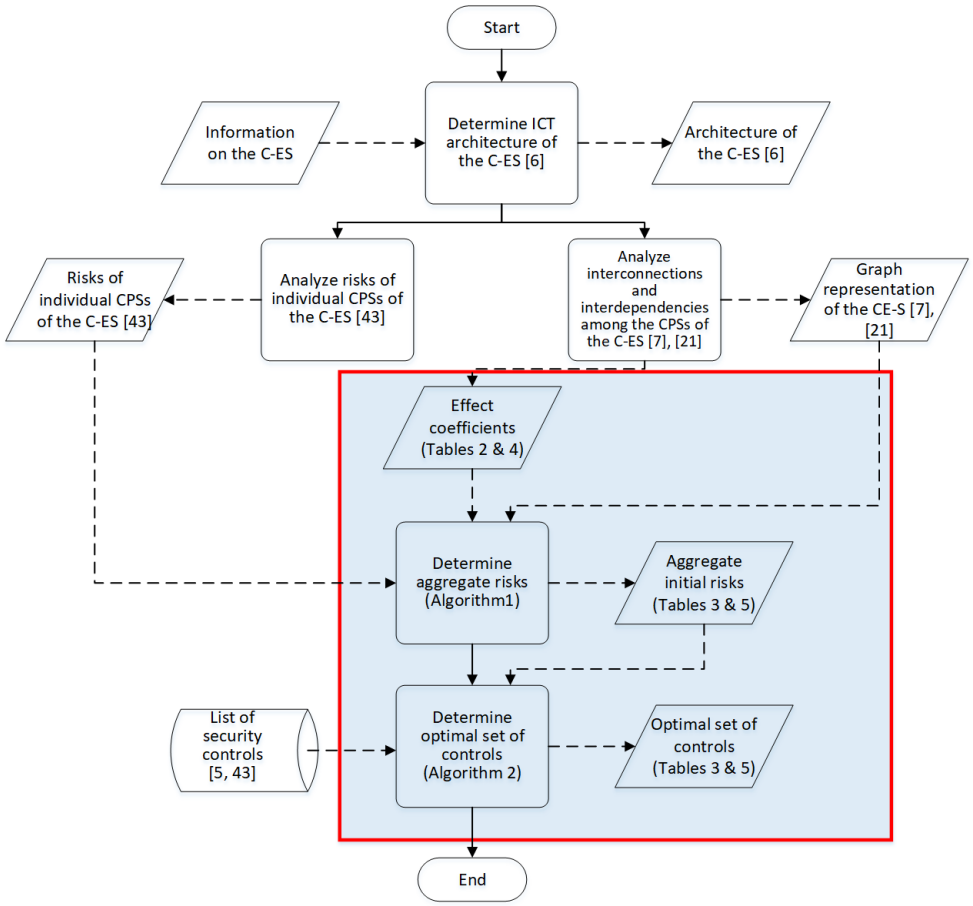

Figure 7. Overall process.

7. Conclusions

The growing utilization of highly interconnected CPSs in critical domains increases the attack surface, making the infrastructure more vulnerable to cyber attacks. In this paper, we model a complex CPS as a digraph in which nodes represent sub-CPSs and in which edges represent information and control flows among these subsystems. By leveraging this model, we proposed a novel method for assessing the aggregate cybersecurity risk of large scale, complex CPSs comprising interconnected and interdependent components, by using risk measures of its individual components and the information and control flows among these components. Building upon this method, we proposed a novel method, based on evolutionary programming, for selecting a set of effective and efficient cybersecurity controls among those in an established knowledge base, that reduces the aggregate residual risk, while at the same time minimizing the cost. We then used both methods to select optimal sets of cybersecurity controls for the navigational systems of two instances of the C-ES, namely the remotely controlled ship and the autonomous ship. These sets lead to the definition of the cybersecurity architecture of such vessels. They have been found to be in line with previous results that identified the most vulnerable navigational CPSs of the C-ES, and to minimize the global residual risk. In the future, we intend to develop a software tool that will implement the proposed methods, and to use it to experientially examine the usability of the proposed approach with domain experts and stakeholders, in the C-ES and other critical application domains.

Author Contributions: Conceptualization, G.K., G.S. and S.K.; methodology, G.K., G.S. and S.K.; software, G.K. and G.S.; validation, G.K. and G.S.; formal analysis, G.K., G.S. and S.K.; investigation, G.K. and G.S.; resources, S.K.; writing—original draft preparation, G.K. and G.S.; writing—review and editing, S.K.; visualization, G.K. and S.K.; supervision, S.K.; project administration, S.K.; funding acquisition, S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This paper has been partially funded by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 773960 (DELTA project).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Giraldo, J.; Sarkar, E.; Cardenas, A.A.; Maniatakos, M.; Kantarcioglu, M. Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Des. Test* **2017**, *34*, 7–17. [CrossRef]
2. Cyber-Physical Systems Public Working Group (CPS PWG). *Framework for Cyber-Physical Systems*; NIST Special Publication 1500-201: Volume 1, Overview. Version 1.0; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2017.
3. International Organization for Standardization, ISO. *ISO 31000:2018 Risk Management—Guidelines*; ISO: Geneva, Switzerland, 2018.
4. International Organization for Standardization, ISO. *ISO/IEC 27005:2018 Information Technology—Security Techniques—Information Security Risk Management*; ISO: Geneva, Switzerland, 2018.
5. Stouffer, K.; Pillitteri, V.; Marshall, A.; Hahn, A. Guide to industrial control systems (ICS) security. *NIST Spec. Publ.* **2015**, *800*, 247.
6. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Cyber-attacks against the autonomous ship. In Proceedings of the SECPRE 2018, CyberICPS 2018, Barcelona, Spain, 6–7 September 2018; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2018; Volume 11387, pp. 20–36.
7. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Modelling Shipping 4.0: A Reference Architecture for the Cyber-Enabled Ship. In Proceedings of the Asian Conference on Intelligent Information and Database Systems, Phuket, Thailand, 23–26 March 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 202–217.
8. Kouns, J.; Minoli, D. *Information Technology Risk Management in Enterprise Environments*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2010.
9. Ali, S.; Balushi, T.; Nadir, Z.; Hussain, O. Risk Management for CPS Security. In *Cyber Security for Cyber Physical Systems*; Springer International Publishing AG: Cham, Switzerland, 2018; pp. 11–34.
10. Lyu, X.; Ding, Y.; Yang, S.H. Safety and security risk assessment in Cyber-Physical Systems. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 221–232. [CrossRef]
11. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
12. Lamba, V.; Šimková, N.; Rossi, B. Recommendations for smart grid security risk management. *Cyber-Phys. Syst.* **2019**, *5*, 92–118. [CrossRef]
13. You, B.; Zhang, Y.; Cheng, L.C. Review on Cyber Security Risk Assessment and Evaluation and Their Approaches on Maritime Transportation. In Proceedings of the 30th Annual Conference of International Chinese Transportation Professionals Association, Houston, TX, USA, 19–21 May 2017; pp. 19–21.
14. Tam, K.; Jones, K. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU J. Marit. Aff.* **2019**, *18*, 129–163. [CrossRef]
15. Tam, K.; Jones, K. Cyber-risk assessment for autonomous ships. In Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, UK, 11–12 June 2018; pp. 1–8.
16. Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU J. Marit. Aff.* **2019**, *18*, 509–520. [CrossRef]
17. Kim, Y.G.; Jeong, D.; Park, S.H.; Lim, J.; Baik, D.K. Modeling and simulation for security risk propagation in critical information systems. In Proceedings of the International Conference on Computational and Information Science, Guangzhou, China, 3–6 November 2006; Springer: Berlin/Heidelberg, Germany, 2006; pp. 858–868.
18. Kondakci, S. A new assessment and improvement model of risk propagation in information security. *Int. J. Inf. Comput. Secur.* **2007**, *1*, 341–366. [CrossRef]
19. Feng, N.; Wang, H.J.; Li, M. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Inf. Sci.* **2014**, *256*, 57–73. [CrossRef]
20. Orojloo, H.; Azgomi, M.A. A method for evaluating the consequence propagation of security attacks in cyber–physical systems. *Future Gener. Comput. Syst.* **2017**, *67*, 57–71. [CrossRef]
21. Wang, T.; Wei, X.; Huang, T.; Wang, J.; Valencia-Cabrera, L.; Fan, Z.; Pérez-Jiménez, M.J. Cascading failures analysis considering extreme virus propagation of cyber-physical systems in smart grids. *Complexity* **2019**, *2019*, 7428458. [CrossRef]
22. Kavallieratos, G.; Katsikas, S. Attack Path Analysis for Cyber Physical Systems. In *Computer Security: ESORICS 2020 International Workshops, CyberICPS, SECPRE, and ADIoT, Guildford, UK, 14–18 September 2020, Revised Selected Papers*; Lecture Notes in Computer Science Book Series (LNCS); Springer International Publishing: Cham, Switzerland, 2020; Volume 12501, pp. 19–33.
23. König, S.; Rass, S.; Schauer, S.; Beck, A. Risk propagation analysis and visualization using percolation theory. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2016**, *7*, 1–8. [CrossRef]
24. Qu, Z.; Zhang, Y.; Qu, N.; Wang, L.; Li, Y.; Dong, Y. Method for quantitative estimation of the risk propagation threshold in electric power CPS based on seepage probability. *IEEE Access* **2018**, *6*, 68813–68823. [CrossRef]
25. Zhu, B.; Deng, S.; Xu, Y.; Yuan, X.; Zhang, Z. Information security risk propagation model based on the SEIR infectious disease model for smart grid. *Information* **2019**, *10*, 323. [CrossRef]

26. Malik, A.A.; Tosh, D.K. Quantitative Risk Modeling and Analysis for Large-Scale Cyber-Physical Systems. In Proceedings of the 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020; pp. 1–6.
27. Theoharidou, M.; Kotzanikolaou, P.; Gritzalis, D. A multi-layer criticality assessment methodology based on interdependencies. *Comput. Secur.* **2010**, *29*, 643–658. [CrossRef]
28. Theoharidou, M.; Kotzanikolaou, P.; Gritzalis, D. Risk assessment methodology for interdependent critical infrastructures. *Int. J. Risk Assess. Manag.* **2011**, *15*, 128–148. [CrossRef]
29. Zhou, X.; Wang, F.; Ma, Y. An overview on energy internet. In Proceedings of the 2015 IEEE International Conference on Mechatronics and Automation (ICMA), Beijing, China, 2–5 August 2015; pp. 126–131. [CrossRef]
30. Hong, Q.; Jianwei, T.; Zheng, T.; Wenhui, Q.; Chun, L.; Xi, L.; Hongyu, Z. An information security risk assessment algorithm based on risk propagation in energy internet. In Proceedings of the IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017; pp. 1–6.
31. Li, S.; Zhao, S.; Yuan, Y.; Sun, Q.; Zhang, K. Dynamic security risk evaluation via hybrid Bayesian risk graph in cyber-physical social systems. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 1133–1141. [CrossRef]
32. Karbowski, A.; Malinowski, K. Two-Level System of on-Line Risk Assessment in the National Cyberspace. *IEEE Access* **2020**, *8*, 181404–181410. [CrossRef]
33. Sawik, T. Selection of optimal countermeasure portfolio in IT security planning. *Decis. Support Syst.* **2013**, *55*, 156–164. [CrossRef]
34. Viduto, V.; Maple, C.; Huang, W.; López-Peréz, D. A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decis. Support Syst.* **2012**, *53*, 599–610. [CrossRef]
35. Schilling, A.; Werners, B. Optimal selection of IT security safeguards from an existing knowledge base. *Eur. J. Oper. Res.* **2016**, *248*, 318–327. [CrossRef]
36. Baiardi, F.; Telmon, C.; Sgandurra, D. Hierarchical, model-based risk management of critical infrastructures. *Reliab. Eng. Syst. Saf.* **2009**, *94*, 1403–1415. [CrossRef]
37. Gonzalez-Granadillo, G.; Garcia-Alfaro, J.; Alvarez, E.; El-Barbori, M.; Debar, H. Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the RORI index. *Comput. Electr. Eng.* **2015**, *47*, 13–34. [CrossRef]
38. Goldberg, D.E. *Genetic Algorithms in Search, Optimization and Machine Learning*, 1st ed.; Addison-Wesley Longman Publishing Co., Inc.: Boston, MA, USA, 1989.
39. Blickle, T.; Thiele, L. A Comparison of Selection Schemes Used in Evolutionary Algorithms. *Evol. Comput.* **1996**, *4*, 361–394. [CrossRef]
40. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
41. Zinsmaier, S.; Langweg, H.; Waldvogel, M. A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria. In Proceedings of the 6th International Conference on Information Systems Security and Privacy—Volume 1: ICISSP, Valletta, Malta, 25–27 February 2020; pp. 473–480. [CrossRef]
42. Kavallieratos, G.; Gkioulos, V.; Katsikas, S.K. Threat analysis in dynamic environments: The case of the smart home. In Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 234–240.
43. Seifert, D.; Reza, H. A security analysis of cyber-physical systems architecture for healthcare. *Computers* **2016**, *5*, 27. [CrossRef]
44. Kavallieratos, G.; Katsikas, S. Managing Cyber Security Risks of the Cyber-Enabled Ship. *J. Mar. Sci. Eng.* **2020**, *8*, 768. [CrossRef]
45. Microsoft. Chapter 3—Threat Modeling. 2010. Available online: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN (accessed on 28 February 2021).
46. Rothlauf, F. Optimization Methods. In *Design of Modern Heuristics: Principles and Application*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 45–102. [CrossRef]
47. BIMCO; CLIA; ICS; INTERCARGO; INTERMANAGER; INTERTANKO; IUMI; OCIMF; World Shipping Council. The Guidelines on Cyber Security Onboard Ships. Version 4. Available online: https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx (accessed on 28 February 2021).
48. The President of the United States. *National Maritime Cybersecurity Plan*; White House Office: Washington, DC, USA, 2020. Available online: https://www.hsdl.org/?view&did=848704 (accessed on 28 February 2021).
49. Kavallieratos, G.; Diamantopoulou, V.; Katsikas, S. Shipping 4.0: Security requirements for the Cyber-Enabled Ship. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6617–6625. [CrossRef]
50. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. SafeSec Tropos: Joint security and safety requirements elicitation. *Comput. Stand. Interfaces* **2020**, *70*, 103429. [CrossRef]
51. International Maritime Organization. Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs). 1972. Available online: https://www.imo.org/en/About/Conventions/Pages/COLREG.aspx (accessed on 24 January 2021).
52. International Maritime Organization. IMO Takes First Steps to Address Autonomous Ships. 2018. Available online: http://www.imo.org/en/mediacentre/pressbriefings/pages/08-msc-99-mass-scoping.aspx (accessed on 21 September 2020).