



Article

QISS: Quantum-Enhanced Sustainable Security Incident Handling in IoT

Carlos Blanco ^{1,†}  0000-0001-9001-0904, Antonio Santos-Olmo ^{2,†}  0000-0002-2349-3894 and Luis Enrique Sánchez ^{2,†}  0000-0003-0086-1065

¹ Department of Computer Science and Electronics, University of Cantabria, Spain; Carlos.Blanco@unican.es

² Technologies and Information Systems Department, University of Castilla-La Mancha, Spain; antonio.santosolmo@uclm.es, luise.sanchez@uclm.es

* Correspondence: Carlos.Blanco@unican.es

† These authors contributed equally to this work.

Abstract: As Internet of Things (IoT) environments play an increasingly relevant role in various fields, such as healthcare, energy supply and industrial automation, the risk of cyber vulnerabilities and attacks also increases. In response to these challenges, the fundamental role of the Information Security Management System (ISMS) in protecting critical information assets is highlighted. Risk management plays a crucial role in this system, since in the presence of a cybersecurity incident scenario and possible response alternatives, they are responsible for re-establishing the system in an appropriate manner. To do that, they have to evaluate what is the best response. The time to implement a course of action must be considered, as the time in which the ISMS is restored is a critical aspect. However, in an environmental consciousness world, the sustainability dimension should also be considered, choosing more sustainable responses. This paper represents a significant evolution in risk management and incident response, aligning security practices with broader objectives of sustainability and corporate responsibility. It proposes a method for managing cybersecurity incidents that takes into account response time and the sustainability dimension. The method allows to choose whether we want to favor response time, sustainability or both in a given percentage, and based on that, it selects the most appropriate courses of action to restore the security of the system. This method is implemented using a quantum approach that ensures adequate and consistent response times, regardless of the number of incidents. Finally, this proposal is applied to real cases using our framework, MARISMA, demonstrating its effectiveness and relevance in the current context of risk management.

Keywords: Cybersecurity; Sustainability; Incident Response; Quantum Programming; Quantum Annealing

Citation: Blanco, C.; Santos-Olmo, A.; Sánchez, L.E. QISS: Quantum-Enhanced Sustainable Security Incident Handling in IoT. *Journal Not Specified* **2024**, *1*, 0. <https://doi.org/>

Received:

Revised:

Accepted:

Published:

Copyright: © 2024 by the authors. Submitted to *Journal Not Specified* for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In current society, Cyber-Physical Systems (CPS) and Internet of Things (IoT) environments play an increasingly important role. These connected devices enable interaction between the physical and digital worlds. They include computing, storage and communication functions that enable them to manage objects in the physical world (Orojloo and Azgomi, Alguliyev et al.) and provide services that deliver significant benefits in numerous areas such as healthcare, energy supply, transportation, industrial automation or the smart home (Priyadarshini et al., Jindal et al., Khalid et al., Kumar et al.).

However, their fast evolution and adoption has led to many of them being designed and launched into the market without adequate attention to security aspects, resulting in an increased number of vulnerabilities that can be exploited by malicious actors. In addition, the wide variety and large number of connected devices further increases the threat landscape. From security cameras and smart home appliances to vehicles and industrial systems, all these devices can be potential targets for cyber attacks. Heterogeneity

in terms of manufacturers, communication protocols and operating systems makes it difficult to implement consistent and effective security measures across the entire CPS and IoT infrastructure (Griffor et al., Lezzi et al.).

Therefore, CPS and IoT systems present significant challenges in terms of security that should be adequately addressed, otherwise they would have considerable consequences in terms of security and privacy. On the one hand, their application areas often correspond to critical infrastructures, where the disruption or compromise of these systems can have devastating consequences, ranging from disruptions to public services to risks to security and human life. On the other hand, they collect and process large amounts of sensitive data, such as personal information, health data or confidential business data. Lack of security in these systems can result in data leaks, theft of personal or financial information, and potential reputational damage to organisations.

To address these threats, the ISO/IEC 27.001 standard establishes key guidelines. According to this standard, the Information Security Management System (ISMS) is central to an overall management structure that seeks to preserve the security of information within organisations. By implementing an ISMS, organisations can establish policies, processes and controls to protect their critical information assets. This allows them to mitigate risks and safeguard the confidentiality, integrity and availability of the sensitive data they handle.

Risk management plays a fundamental role within an ISMS and the current scenario, in which cybersecurity incidents are increasing in both intensity and impact, making necessary both methodologies and tools that allow companies to address, understand and manage their cybersecurity risk in an adequate manner (Glantz et al., Thakur et al., Wang et al.).

Risk assessment and risk management solutions face challenges in their applicability and effectiveness. Lack of awareness and inaccurate risk assessment contribute to the majority of security incidents (Turskis et al.). Moreover, current approaches offer a static view of risks, despite the fact that risks are dynamic and evolve along with threats and vulnerabilities (Paltrinieri and Reniers).

To overcome these limitations, in previous works we have developed a methodology called "MARISMA" (Methodology for the Analysis of Risks in Information Systems, using Meta-Patterns and Adaptability) (Santos-Olmo et al.) supported by a technological environment called "eMARISMA" (www.emarisma.com). MARISMA is a methodology based on the reuse of knowledge for RAM purposes, using structures known as "patterns" that allow different types of cases to be supported. In this sense, a pattern was developed to manage and control risks in CPS considering the inherent needs of this type of systems (MARISMA-CPS) (Rosado et al.). This template is based on the main standards and recommendations on CPS, IoT and risk management (ISO/IEC 27.000 and IEC 62443, the recommendations of ENISA (European Union Agency for Network and Information Security) (Ross et al.) and the framework for CPSs developed by NIST (Griffor et al.).

However, there are still many challenges to be addressed. Systems are exposed to a large number of incidents on a daily basis that need to be corrected to restore system security. But each incident can be resolved by applying various course of actions, and it is necessary to have mechanisms in order to select the most appropriate response.

In a previous work (Serrano et al.), we have developed a quantum algorithm that selects as a response the minimum set of courses of action that cover all incidents. However, that work leaves out crucial aspects that are improved in this proposal.

On the one hand, the time needed to apply the course of action is a crucial aspect since it minimizes the possible damages suffered (Bhardwaj and Sapra). But on the other hand, in a society involved in the ecological transition, the responsible use of resources should also be taken into account and the most sustainable course of action should be favored (Salam, Zubair et al.).

This paper contributes to this challenge by improving incident response in a risk analysis and management system, considering both the speed and sustainability of the response.

In a typical production-level operation, a large volume of security incidents can occur on a regular basis, even more so if we consider environments consisting of several IoT devices. That is why for the design of our solution we design a quantum computing approach, which allows us to respond adequately and in near-constant time to scenarios with a large number of incidents.

The article continues in Section 2 by analyzing the background and related works on sustainable security incidents response and quantum optimization; Section 3 presents our proposal based on quantum programming for the selection of the courses of action set needed to restore system security considering response time and sustainability criteria; our proposal is validated in Section 4 by means of an application example; and finally, Section 5 shows the main conclusions obtained during the research and future works to be carried out.

2. Background and Related Work

This section includes background content about the research topics addressed in this paper, sustainable security incident response and quantum optimization. In particular, the first subsection provides an overview of the sustainable security incident response process and discuss some open research problems. In the next subsection, we discuss the foundation on which quantum computing is based applying it to optimization problems.

2.1. Sustainable Managing of Security Incidents

As mentioned in the introduction section, security incidents are undesired events that impact on the different dimensions of the valuable assets that make up a company's information systems ([Mahima](#)). These incidents are caused by failures in the implementation of the security controls that protect these assets, i.e. by vulnerabilities that exist in the information systems. These vulnerabilities are exploited by threats to reach these assets and cause damage to them ([Dion](#)).

In order to minimise the damage of these incidents, organizations try to apply the most appropriate incident response methods ([Prasad and Rohokale](#)). In fact, the management of security incidents and the correlation of these events is a topic of great interest to the scientific community ([Salvi et al.](#)). Many organizations have focused on managing risks through integrated services in Computer Security Incident Response Teams (CSIRT), as these have proven to be one of the best solutions to improve cybersecurity by collaborating with each other, sharing knowledge and learning from cross experiences ([Tanczer et al.](#)). However, the implementation of a CSIRT comes at a considerable cost, which makes it only suitable for large organizations, with the need to create simpler and more effective incident management systems for small and medium-sized enterprises ([Pléta et al.](#)).

Security incident management and response can be considered a hot research topic with some relevant open questions ([Grispos et al.](#)). One of the most relevant question is how to achieve a reasonable situational awareness to know the situation regarding vulnerabilities, threats and possible security incidents ([Ahmad et al.](#)). In this area, there is recent intense research, for example proposing models to explain how organizations should achieve situational awareness of cybersecurity ([Ahmad et al.](#)), arguing that providing a rapid and efficient response to security incidents clearly supports cybersecurity awareness and improves the overall cybersecurity performance of companies ([Naseer et al.](#)), or considering misinformation as one of the key reasons for the lack of situational awareness ([Ahmad et al.](#)). Indeed, it is often claimed that attackers take advantage of the lack of corporate communication following cybersecurity incidents ([Knight and Nurse](#)) and the lack of learning from their experiences in incidents ([Ahmad et al.](#), [Ahmad et al.](#), [Ahmad et al.](#)).

It is, therefore, necessary for any type of company to have adequate and efficient tools to support incident management processes. And above all, utilities and processes providing them with mechanisms that facilitate decision-making to optimise the selection and prioritisation of security incidents to be resolved ([Ahmad et al.](#)). This is mainly due

to the fact that the incidence workload can be very high throughout the lifecycle of an information system, especially in typical cases such as the release of a new version of an application or an operating system upgrade. Thus, there is a strong need to take into account the specific efficiency and effectiveness needs of these new incident management support systems (van der Kleij et al.).

But for us, in this work, the most relevant problem faced by organizations is agility in managing and responding to security incidents (Tam et al.). This agility translates into the need to respond to these incidents in the shortest possible time (van der Kleij et al., He et al.). But this problem is becoming increasingly difficult to address, due to the growing number of incidents and their interconnection. When systems receive hundreds of events, we find that incident response teams must make a decision on which are the top incidents to start analyzing. In this sense, when planning the resolution of an incident, we encounter different types of scenarios. In some cases, responding to an incident is straightforward and involves activating a specific control (for example, installing antivirus software). However, we often find that the resolution of the incident is more complex and involves the execution of procedures with multiple action steps and even the intervention of different resources (technical and human). It is therefore necessary to apply the concept of a Course of Action (CoA), which NIST defines as "A time-phased or situationally dependent combination of risk response actions" (Initiative et al.).

In this sense, when organising and prioritising incident resolution, it is vital to choose the most appropriate course of action. In traditional decision-making systems, resolution time is often the key factor in determining the best choice. However, as sustainability becomes an increasingly relevant aspect in measuring the efficiency of an information system (Kniaz et al.), it is becoming increasingly necessary for decision making in this area to consider which possible course of action is more sustainable. In this way, given a set of incidents to resolve, we would achieve a balance between time and sustainability when calculating the most efficient courses of action to apply. But this prioritization cannot be done manually, as it would delay decision-making. According to some researchers, security incident response requires complex event processing (to capture, process, integrate and analyze data in real time), as well as investigation the cause-effect relationship between incidents (Naseer et al.).

We have seen this in practice through MARISMA (Rosado et al., Rosado et al.), which is our dynamic approach to risk analysis and management that we have designed, improved and extended, and which we have been applying to many types of companies and technologies (electric, hydrocarbons, governments, health, shipbuilding, chemical industry, etc.) for more than a decade with clients in eight Latin American countries. MARISMA is conceived as a complete and adaptable risk management framework, which includes a detailed methodology, a tool that automates many of the tasks of the methodology, and a support for improvement and extension to different technological contexts based on metadata, metamodels, ontologies and risk patterns.

In MARISMA and our tool we have implemented a workflow for the management of security incidents that considers key information (such as threats and threat types, assets and asset groups, risk dimensions and security controls) and has the following steps: i) collect the security incident information (description, cause, responsible person, and time limits to be solved), ii) select from the stored information and the available metadata the hierarchy of elements that are involved with the security incident (threats, assets and controls), defining other related information such as the severity of the incident, and quarantine the affected controls by temporarily lowering their coverage level while the incident is resolved, and finally, once the incident is solved, iii) support knowledge management and learning from the security incidents occurred by recording the lesson learned, incident resolution costs and some concluding remarks. Obviously, when a security incident occurs and is recorded, a set of chain changes are automatically applied on the risk components according to the stored metainformation. This is because the level of compliance with security controls is penalized if a threat has compromised the control,

which affect the risk level of many other assets, and which implies that those controls need to be reviewed and strengthened.

However, the key problem is that a typical scenario in incident management is the heavy workload involved in organizing and prioritizing incidents in order to define the most efficient way to resolve them in the shortest possible time and sustainably using available resources. The organization and efficient distribution of incidents becomes even more complicated at peak activity, such as the first production start-up of a system or the registration of a new service, when the number of incidents can reach large amounts, with the added complication of managing them properly. Thus, it is common to have to prioritize and plan dozens (or even hundreds) of incidents in a short time, which involves complex calculations, a high level of difficulty, and a high cost in time.

To illustrate this problem, we will show an example (see Table 1) that considers the unique identifier of the incidents, the threat that has caused the incident together with the course of action intended to mitigate that threat, the main control that has been affected by the threat, and the estimate of number of hours required to resolve the incident through the proposed course of action. As seen in Table 1, each incident involves a single threat. Still, each incident may affect one or more controls whose implementation must be reviewed and corrected to resolve the incident and try to prevent its recurring, so different courses of action can be considered to resolve the incident.

Table 1. Datasets of incidents

IdIncident	IdThreat	Threat	CoA	IdControl	Control	Time (h)	Sustainability
1	DD	DDoS	C11	GP-TM-16	Mechanisms for self-diagnosis and self-repair/healing	6	A
1	DD	DDoS	C12	GP-TM-17	Ensure standalone operation	6	E
2	DSIL	Data / Sensitive information leakage	C21	GP-TM-47	Risk Segmentation	3	B
3	IOI	Interception of information	C31	GP-PS-06	Implement test plans to verify whether the product performs as it is expected	8	F
4	CPH	Communication protocol hijacking	C41	GP-PS-09	Perform privacy impact assessments before any new applications are launched	40	B
4	CPH	Communication protocol hijacking	C42	GP-TM-25	Protect against 'brute force'	40	C
5	FOD	Failures of devices	C51	GP-PS-05	Design architecture by compartments	24	B
6	FOS	Failure of system	C61	GP-TM-17	Ensure standalone operation	8	A
7	MI	Modification of information	C71	GP-PS-09	Perform privacy impact assessments before any new applications are launched	24	F
7	EK	Exploit Kits	C72	GP-TM-20	Backward compatibility of firmware updates	2	B
7	SV	Software vulnerabilities	C73	GP-TM-16	Mechanisms for self-diagnosis and self-repair/healing	6	B
8	ED	Environment Disaster	C81	GP-TM-06	Restore Secure State	72	B
8	IOI	Interception of information	C82	GP-TM-25	Protect against 'brute force'	16	C
9	CPH	Communication protocol hijacking	C91	GP-TM-43	IoT devices should be restrictive in communicating	8	B

Traditionally, the management and response to security incidents have been focused on rapid resolution, often overlooking sustainability. However, efficient and environmentally friendly resource management is essential. Incorporating sustainability into these practices not only enhances effectiveness in immediate recovery but also strengthens organizational resilience and sustainability in the long term, in a context where social and environmental responsibility is increasingly important.

In this framework, each response strategy to incidents (each course of action) is rated with a sustainability label, ranging from A, being the most sustainable, to G, the least

sustainable. This approach ensures that decisions are not made solely based on immediate efficiency or speed but also considering the long-term environmental impact.

This approach balances the need for quick and effective responses to security incidents with the commitment to act sustainably and responsibly. By integrating sustainability as a key factor in decision-making, organizations not only effectively manage current risks but also strengthen their future resilience, sustainability, and reputation among stakeholders, marking a significant evolution in risk management and incident response.

2.2. Quantum Optimization

Quantum computing represents a novel paradigm that leverages the unique aspects of quantum physics, offering substantial potential advancements in the computing arena. This potential is well-acknowledged in scholarly works, as highlighted in key publications (IBM). Crucial to the practical application of quantum computing is the development of programming languages and methodologies. These tools are imperative for providing structured and elevated descriptions of quantum algorithms that are independent of the specific hardware utilized (Clairambault et al.).

The field of quantum programming has garnered significant attention following the development of efficient quantum algorithms by pioneers such as Shor (Shor) and Grover (Grover). This interest persists, although the discovery of new quantum algorithms remains a formidable challenge. One of the primary reasons for this is the inherent complexity of quantum programs, which are typically depicted as quantum circuits (Altenkirch and Grattage).

A key differentiation between quantum and classical programming lies in the use of quantum bits or qubits, as opposed to standard bits (Sánchez and Alonso). In quantum programming, qubits are manipulated through quantum gates to perform various operations. Quantum computation, especially under the circuit model of quantum programs (QP), involves these gates. They serve as fundamental operations for altering the qubits' amplitude and phase (Sánchez and Alonso). Quantum circuits and their corresponding gates can be visually represented, as illustrated in Figure 1. They are also expressible via syntax-based notations in various quantum programming languages such as Q# and QASM. These programming languages have been developed to simplify the articulation of quantum algorithms, transforming quantum circuit concepts into a sequence of textual programming statements. They address the core aspects of quantum programming and are tailored to meet the exigencies of practical quantum computing applications. Specifically, these languages facilitate the expression and conceptualization of quantum algorithms, which are vital for the real-world application of quantum computing. Thus, quantum programming environments are pivotal in advancing quantum computers from theoretical constructs to practical tools for scientific exploration and discovery (Gyongyosi and Imre).

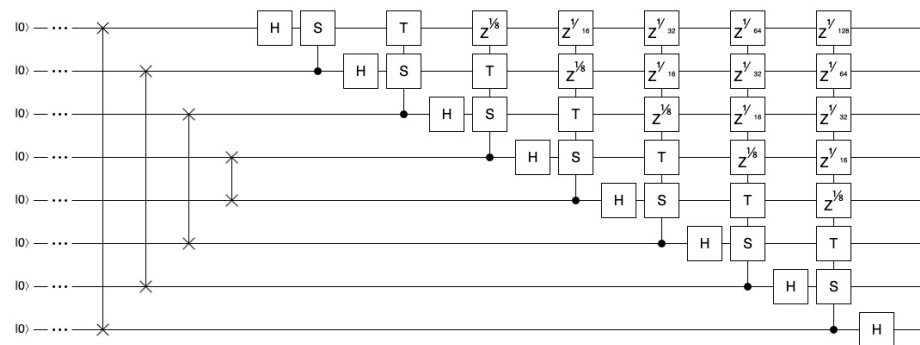


Figure 1. Example of Quantum circuit

Quantum computing presents revolutionary approaches to computational challenges, surpassing traditional computational methods in efficiency (Gyongyosi and Imre). A

qubit, the fundamental unit of quantum computing, can be represented through various subatomic particles, such as electron spins or photons. Unlike classical bits that are binary, a qubit exists in multiple states simultaneously due to quantum superposition. This attribute allows a qubit to hold a value of zero, one, or both simultaneously, with specific probabilities. The value of a qubit is only determined upon measurement, at which point the qubit collapses and requires resetting for further use. Quantum programming, therefore, focuses on navigating and identifying optimal solutions within this probabilistic framework (Piattini et al.).

Quantum optimization often employs search algorithms, notably Grover's algorithm (Grover), which conducts searches in an undetermined space by encoding solution criteria using quantum oracles. These oracles (Sutor, Johnston et al.) function similarly to high-level programming functions, aiding in constructing search algorithms with linear complexity.

Additionally, quantum environments like D-Wave's Quantum Leap¹ facilitate optimization for NP-hard combinatorial problems using adiabatic quantum optimization (Farhi et al., Das and Chakrabarti). This approach involves defining the optimization system as a Hamiltonian, representing both the objective and constraints, and the quantum computer seeks the solution that minimizes the system's energy. Approaches using Ising expressions for this type of optimization are discussed in (Lucas), while gate-based programming alternatives, such as those in the Qiskit textbook (Asfaw et al.), implement the quantum approximate optimization algorithm (QAOA) (Farhi et al.).

Quantum adiabatic computing marks a significant advancement in optimization algorithms. It complements classical algorithms, like backtracking, dynamic programming, heuristic searches (e.g., A*), and adversarial searches (e.g., Minimax, branch and bound), by offering new, more efficient techniques. Among these advancements are genetic algorithms (Rocke), classical annealers like simulated annealing (Kirkpatrick et al.), and benchmark functions algorithms (Dieterich and Hartke). However, these solutions often struggle with local minima and are less effective with exceedingly large or complex problems. Adiabatic quantum computation emerges as a promising solution for solving complex NP-complete optimization problems in polynomial time (Černý).

Quantum annealing algorithms typically begin by defining a problem with qubits in a superposition state. Through the annealing process, these qubits collapse to a classical state of either 0 or 1, representing the lowest energy solution. As depicted in Figure 2, the process starts with the qubits in a single-valley energy state (a), evolving through the annealing to a double-well potential state (b), and culminating with a deeper valley representing the optimal solution (c).

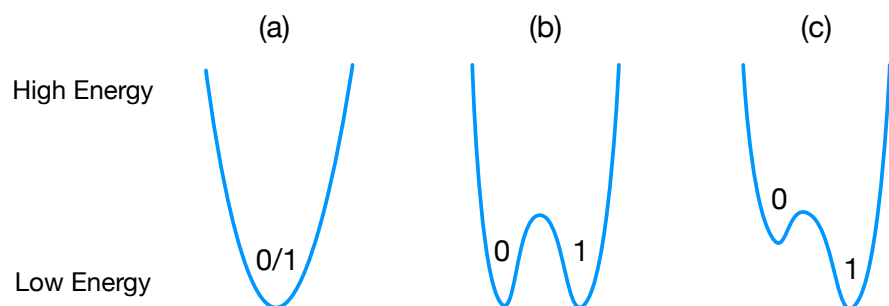


Figure 2. Quantum annealing process

In our work we apply a quantum computing approach to optimize incident response management in the context of a risk assessment and management framework. This quantum computing approach is applied on the dataset of detected security incidents, which has information on their associated threats, the courses of action needed to restore the system, the time required to apply them and their associated sustainability. On this dataset,

¹ <https://www.dwavesys.com/>

it searches for the minimum energy state that represents the best solution for incident resolution, prioritizing that the response time is the shortest possible, that the results are as sustainable as possible or a combination of both in an indicated percentage.

3. A proposal for sustainable security incident management

In this section, we show the algorithmic solution proposed for the problem posed, using quantum algorithms. In order to correctly plan the algorithmic solution of the proposed problem, it is necessary to specify the variables and entities that are part of the algorithm. These variables can be defined as follows:

- **Definition 1.** Let be I_i an unique identifier of an incident. Corresponding with the IdIncident of Table 1.
- **Definition 2.** Let be C_{ij} a possible Course of Actions for solving control I_i . Being j an identifier for the course of actions
- **Definition 3.** Let be t_i the estimated time in minutes necessary for solving the incident I_i , mapping to the Time value.
- **Definition 4.** Let be **Sustainability** a label indicating the sustainability rating of the solution based on the course of actions selected. This rating is related to the energy and sustainability of the proposed solution, being A a more sustainable solution than G .
- **Definition 5.** Let be x_{ij} a binary variable that determines, at the algorithm solution, whether the course of actions C_{ij} is selected to be addressed.
- **Definition 6.** Let be P a penalty coefficient, which serves to modulate the weight of the constraints in the algorithm definition. It can be found empirically to be equal to the highest estimated cost among all the occurrences plus one, thus affecting the whole solution.

Basing on these definitions we can express algebraically the objective pursued by executing the quantum optimization algorithm that will be sent to the quantum computer. This problem is summarized as a small example within the scope of table 2; this table shows a dataset encapsulating a spectrum of security incidents within a computational system, accompanied by an array of potential resolution methodologies, termed 'courses of action'. The algorithm's core function lies in the strategic selection of these courses, prioritizing those that yield superior efficiency in terms of temporal cost or sustainability. This efficiency is quantified via a weighted average, governed by a coefficient α , facilitating adaptability to shifting real-time parameters. Our discourse aims to dissect the fundamental constructs and pivotal considerations integral to the crafting and execution of this optimization algorithm. Through this analytical lens, we endeavor to impart a thorough comprehension of its operational framework and the consequential impact it bears in the landscape of cybersecurity research and application.

Table 2. Incidents and controls example

Incident	Courses of Action	Time	Sustainability
I1	C11	10	B
I1	C12	20	A
I1	C13	60	G
I2	C21	50	A
I2	C22	100	B
I3	C31	1	G
I3	C32	20	F
I3	C33	50	E
I3	C34	10	E

As highlighted in Section 2, while genetic algorithms and classical annealers present viable strategies for addressing certain problems, they often fall short in solving complex optimization challenges within polynomial time. In the realm of quantum computation,

two predominant approaches are quantum gate-based circuits and adiabatic quantum algorithms. It is acknowledged that quantum gate-based methods, such as the Quantum Approximate Optimization Algorithm (QAOA), can tackle optimization problems comparably to quantum annealers. However, the formulation and implementation of these quantum circuits are notably more intricate and extensive than the Hamiltonian formulation used in quantum annealers, which is simpler, more comprehensible, and independent of the quantum platform's specifics.

To address the problem at hand, we propose modeling it as a *Quadratic Unconstrained Binary Optimization (QUBO)* problem, alternatively known as *unconstrained binary quadratic programming (UBQP)*. This approach will encapsulate the objectives and constraints of our problem, enabling the adiabatic quantum computer's solver to identify the minimum energy state. This state corresponds to the optimal combination of variables, or incidents, necessary for an effective solution.

QUBO-based optimization problems are defined through a Hamiltonian, which, in its summation form, delineates both the objectives and the constraints required by the solution. This Hamiltonian is articulated as a Binary Quadratic Model (BQM) and is subsequently transformed into a BQM matrix. This matrix is then processed by the adiabatic solver.

Our primary goal is the minimization of the total cost associated with the issues forming part of the solution. This objective could be articulated in the form of a BQM expression as follows (equation 1):

$$\text{Minimize} \left(\sum_{i=1} \sum_{j=1} (x_{ij} \times (\alpha \cdot T_{ij} + (1 - \alpha) \cdot S_{ij})) \right) \quad (1)$$

Being x_{ij} the binary variable that determines whether or not the course of actions C_{ij} is selected to solve the incident I_i , and T_{ij} the estimated time and S_{ij} is the sustainability rank related to the course of actions C_{ij} . Additionally, α is a tuning coefficient for indicating in operating time the weight of time and sustainability in the solution.

In this problem, the constraints are straightforward, we just have to make sure that at least one course of actions (C_{ij}) is selected for each incident I_i . This set of constraints can be modeled as shown in the equation 2.

$$\forall i \in N \sum_{j=1}^K x_{ij} \geq 1 \quad (2)$$

Based on the definition of the previous equations, the Python code shown in Figure 3 is generated, in which a QUBO matrix is filled in to be sent to the quantum sampler annealing. This algorithm creates a superior triangular matrix, which defines the QUBO matrix for the Binary Quadratic Model (BQM).

```

1 def createBQM(incidents, CoA, time, sustainability):
2     Q = defaultdict(int)
3     num_coa = len(CoA)
4     penalty = max(alfa * time[i] + (1-alfa) * sustainability[i]
5                 for i in range(num_coa)) + 1
6
7     for i in range(num_coa):
8         Q[(i, i)] = -(penalty/(time[i] + (1-alfa) * sustainability[i]))
9
10    for incident in incidents:
11        indices = [i for i, incident in enumerate(incidents)
12                  if CoA['incident'] == incident]
13        for i in indices:
14            for j in indices:
15                if i < j:
16                    Q[(i, j)] = Q[(i, j)] + penalty
17
```

Figure 3. Python code for quantum algorithm

4. Validation

In this section we validate our proposal by applying the developed algorithm to a dataset with real incident data.

The dataset used presents 50 incidents, together with the possible courses of action to respond, the time needed and the associated sustainability label. Table 3 shows the first 10 elements of this dataset.

Table 3. A subset of the incident dataset for validation

IdIncident	IdThreat	Threat	CoA	Time (h)	Sustainability
1	[SV]	Software vulnerabilities	C5	5	A
2	[ED]	Environment Disaster	C11	17	E
3	[IOI]	Interception of information	C7	41	F
3	[IOI]	Interception of information	C1	41	A
4	[IG]	Information gathering	C1	35	A
5	[DDoS]	DDoS	C5	4	A
5	[DDoS]	DDoS	C6	4	E
6	[VRRBL]	Violation of rules and regulations / Breach of legislation	C5	10	A
7	[LOSS]	Loss of support services	C15	11	D
8	[NO]	Network outage	C1	28	A
9	[CPH]	Communication protocol hijacking	C3	4	G
10	[MIM]	Man in the middle	C3	39	G

To validate our proposal, we applied the algorithm developed (Figure 3), which generate the input matrix for the quantum annealer sampler. That is, we generated the triangular QUBO matrix Q and we send it to the sampler with the code shown in Listing 4. We executed the algorithm utilizing a *D-Wave 2000Q lower-noise system* equipped with a *DW_2000Q_6* quantum processor, which boasts 2048 qubits arranged in a *[16,16,4] chimera topology*.

```

1 sampler = LeapHybridSampler()
2 sampleset = sampler.sample(bqm)
3

```

Figure 4. Python code for quantum sampling

We have carried out executions considering different configurations indicating different degrees of prioritization of response time (coefficient α) and sustainability (coefficient $1-\alpha$) in the selection of the set of courses of action. Specifically, it has been applied considering the following α values: 0.0, 0.2, 0.5 and 0.8. The results obtained are presented below.

After executing the coding, we get the results of the sampling as a text file in which we can observe the results of the algorithm and the energy of each of the found solutions. The solution with a minimum energy level is the one that fulfills the requirements and goals of our problem.

Figures 5, 6, 7 and 8 show the outputs of the algorithm for the data shown in table 3 considering different values of α : 0.0 (which fully prioritizes sustainability over response time), 0.2, 0.5 and 0.8 (which prioritizes time over sustainability).

Finally, a comparison of the selected courses of action in each case is shown (Figure 4). We can observe how the different solutions vary in the selection of some courses of

```

1 Object x0 (incident: [SV], coa: C5, time: 5, energy: 1, cost: 1.0)
2 Object x3 (incident: [IOI], coa: C1, time: 41, energy: 1, cost: 1.0)
3 Object x4 (incident: [IG], coa: C1, time: 35, energy: 1, cost: 1.0)
4 Object x7 (incident: [VRRBL], coa: C5, time: 10, energy: 1, cost: 1.0)
5 Object x8 (incident: [LOSS], coa: C15, time: 11, energy: 30, cost: 30.0)
6 Object x9 (incident: [NO], coa: C1, time: 28, energy: 1, cost: 1.0)
7 Object x10 (incident: [CPH], coa: C3, time: 4, energy: 100, cost: 100.0)
8 Object x16 (incident: [MI], coa: C16, time: 4, energy: 1, cost: 1.0)
9 Object x18 (incident: [MIM], coa: C1, time: 30, energy: 1, cost: 1.0)
10 Object x19 (incident: [SH], coa: C7, time: 4, energy: 75, cost: 75.0)
11 Object x20 (incident: [NR], coa: C1, time: 45, energy: 1, cost: 1.0)
12 Object x22 (incident: [ED], coa: C4, time: 9, energy: 20, cost: 20.0)
13 Object x26 (incident: [ROM], coa: C6, time: 42, energy: 50, cost: 50.0)
14 Object x30 (incident: [EK], coa: C13, time: 27, energy: 20, cost: 20.0)
15 Object x31 (incident: [TPF], coa: C13, time: 13, energy: 20, cost: 20.0)
16 Object x34 (incident: [DSIL], coa: C15, time: 36, energy: 30, cost: 30.0)
17 Object x37 (incident: [DDoS], coa: C1, time: 7, energy: 1, cost: 1.0)
18 Object x38 (incident: [FOD], coa: C15, time: 4, energy: 30, cost: 30.0)
19 Object x40 (incident: [MW], coa: C14, time: 4, energy: 10, cost: 10.0)
20 Object x42 (incident: [FOS], coa: C3, time: 4, energy: 100, cost: 100.0)
21 Object x45 (incident: [TA], coa: C16, time: 33, energy: 1, cost: 1.0)
22 Object x51 (incident: [AP], coa: C2, time: 21, energy: 100, cost: 100.0)
23 Object x52 (incident: [CMD], coa: C16, time: 6, energy: 1, cost: 1.0)
24 Object x57 (incident: [DN], coa: C10, time: 33, energy: 10, cost: 10.0)
25 cost total: 606.0
26 Time: 12 seconds
27 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ... 66 energy num_oc.
28 2 1 0 0 1 1 0 0 1 1 1 1 0 0 0 0 0 ... 0 -1162.846667 1
29 3 1 0 0 1 1 0 0 1 1 1 1 0 0 0 0 0 ... 0 -1162.846667 1
30 1 1 0 0 1 1 0 0 1 1 1 1 0 0 1 0 0 ... 0 -1162.846667 1
31 8 1 0 0 1 1 0 0 1 1 1 1 0 0 0 0 0 ... 0 -1162.846667 1
32 14 1 0 0 1 1 0 0 1 1 1 1 0 0 1 0 0 ... 0 -1162.846667 1
33 27 1 0 0 1 1 0 0 1 1 1 1 0 0 1 0 0 ... 0 -1162.846667 1
34 66 1 0 0 1 1 0 0 1 1 1 1 0 0 0 0 0 ... 0 -1162.846667 1
35 68 1 0 0 1 1 0 0 1 1 1 1 0 0 0 0 0 ... 0 -1162.846667 1
36 76 1 0 0 1 1 1 0 1 1 1 1 0 0 0 0 0 ... 0 -1162.846667 1
37 19 1 0 0 1 1 1 0 1 1 1 1 0 0 0 0 0 ... 0 -1162.846667 1
38 ...
39

```

Figure 5. Results fully prioritizing sustainability (alpha equal to 0.0)

```

1 Object x0 (incident: [SV], coa: C5, time: 5, energy: 1, cost: 1.8)
2 Object x1 (incident: [ED], coa: C11, time: 17, energy: 50, cost: 43.4)
3 Object x4 (incident: [IG], coa: C1, time: 35, energy: 1, cost: 7.8)
4 Object x5 (incident: [DDoS], coa: C5, time: 4, energy: 1, cost: 1.6)
5 Object x7 (incident: [VRRBL], coa: C5, time: 10, energy: 1, cost: 2.8)
6 Object x8 (incident: [LOSS], coa: C15, time: 11, energy: 30, cost: 26.2)
7 Object x9 (incident: [NO], coa: C1, time: 28, energy: 1, cost: 6.4)
8 Object x10 (incident: [CPH], coa: C3, time: 4, energy: 100, cost: 80.8)
9 Object x16 (incident: [MI], coa: C16, time: 4, energy: 1, cost: 1.6)
10 Object x18 (incident: [MIM], coa: C1, time: 30, energy: 1, cost: 6.8)
11 Object x19 (incident: [SH], coa: C7, time: 4, energy: 75, cost: 60.8)
12 Object x20 (incident: [NR], coa: C1, time: 45, energy: 1, cost: 9.8)
13 Object x27 (incident: [ROM], coa: C7, time: 37, energy: 75, cost: 67.4)
14 Object x30 (incident: [EK], coa: C13, time: 27, energy: 20, cost: 21.4)
15 Object x31 (incident: [TPF], coa: C13, time: 13, energy: 20, cost: 18.6)
16 Object x34 (incident: [DSIL], coa: C15, time: 36, energy: 30, cost: 31.2)
17 Object x38 (incident: [FOD], coa: C15, time: 4, energy: 30, cost: 24.8)
18 Object x40 (incident: [MW], coa: C14, time: 4, energy: 10, cost: 8.8)
19 Object x42 (incident: [FOS], coa: C3, time: 4, energy: 100, cost: 80.8)
20 Object x45 (incident: [TA], coa: C16, time: 33, energy: 1, cost: 7.4)
21 Object x51 (incident: [AP], coa: C2, time: 21, energy: 100, cost: 84.2)
22 Object x52 (incident: [CMD], coa: C16, time: 6, energy: 1, cost: 2.0)
23 Object x57 (incident: [DN], coa: C10, time: 33, energy: 10, cost: 14.600000000000001)
24 Object x62 (incident: [IOI], coa: C10, time: 10, energy: 10, cost: 10.0)
25 cost total: 621.0000000000001
26

```

Figure 6. Results prioritizing 80% sustainability and 20% time (alpha equal to 0.2)

```

1 Object x0 (incident: [SV], coa: C5, time: 5, energy: 1, cost: 3.0)
2 Object x1 (incident: [ED], coa: C11, time: 17, energy: 50, cost: 33.5)
3 Object x5 (incident: [DDoS], coa: C5, time: 4, energy: 1, cost: 2.5)
4 Object x7 (incident: [VRRBL], coa: C5, time: 10, energy: 1, cost: 5.5)
5 Object x8 (incident: [LOSS], coa: C15, time: 11, energy: 30, cost: 20.5)
6 Object x9 (incident: [NO], coa: C1, time: 28, energy: 1, cost: 14.5)
7 Object x10 (incident: [CPH], coa: C3, time: 4, energy: 100, cost: 52.0)
8 Object x16 (incident: [MI], coa: C16, time: 4, energy: 1, cost: 2.5)
9 Object x18 (incident: [MIM], coa: C1, time: 30, energy: 1, cost: 15.5)
10 Object x19 (incident: [SH], coa: C7, time: 4, energy: 75, cost: 39.5)
11 Object x20 (incident: [NR], coa: C1, time: 45, energy: 1, cost: 23.0)
12 Object x26 (incident: [ROM], coa: C6, time: 42, energy: 50, cost: 46.0)
13 Object x30 (incident: [EK], coa: C13, time: 27, energy: 20, cost: 23.5)
14 Object x31 (incident: [TPF], coa: C13, time: 13, energy: 20, cost: 16.5)
15 Object x34 (incident: [DSIL], coa: C15, time: 36, energy: 30, cost: 33.0)
16 Object x38 (incident: [FOD], coa: C15, time: 4, energy: 30, cost: 17.0)
17 Object x40 (incident: [MW], coa: C14, time: 4, energy: 10, cost: 7.0)
18 Object x42 (incident: [FOS], coa: C3, time: 4, energy: 100, cost: 52.0)
19 Object x43 (incident: [TA], coa: C15, time: 31, energy: 30, cost: 30.5)
20 Object x51 (incident: [AP], coa: C2, time: 21, energy: 100, cost: 60.5)
21 Object x52 (incident: [CMD], coa: C16, time: 6, energy: 1, cost: 3.5)
22 Object x57 (incident: [DN], coa: C10, time: 33, energy: 10, cost: 21.5)
23 Object x62 (incident: [IOI], coa: C10, time: 10, energy: 10, cost: 10.0)
24 Object x66 (incident: [IG], coa: C4, time: 18, energy: 20, cost: 19.0)
25 cost total: 552.0
26

```

Figure 7. Results prioritizing 50% sustainability and 50% time (alpha equal to 0.5)

```

1 Object x0 (incident: [SV], coa: C5, time: 5, energy: 1, cost: 4.2)
2 Object x5 (incident: [DDoS], coa: C5, time: 4, energy: 1, cost: 3.4000000000000004)
3 Object x7 (incident: [VRRBL], coa: C5, time: 10, energy: 1, cost: 8.2)
4 Object x8 (incident: [LOSS], coa: C15, time: 11, energy: 30, cost: 14.799999999999999)
5 Object x9 (incident: [NO], coa: C1, time: 28, energy: 1, cost: 22.6)
6 Object x10 (incident: [CPH], coa: C3, time: 4, energy: 100, cost: 23.199999999999996)
7 Object x16 (incident: [MI], coa: C16, time: 4, energy: 1, cost: 3.4000000000000004)
8 Object x19 (incident: [SH], coa: C7, time: 4, energy: 75, cost: 18.199999999999996)
9 Object x22 (incident: [ED], coa: C4, time: 9, energy: 20, cost: 11.2)
10 Object x25 (incident: [NR], coa: C14, time: 28, energy: 10, cost: 24.400000000000002)
11 Object x26 (incident: [ROM], coa: C6, time: 42, energy: 50, cost: 43.6)
12 Object x30 (incident: [EK], coa: C13, time: 27, energy: 20, cost: 25.6)
13 Object x31 (incident: [TPF], coa: C13, time: 13, energy: 20, cost: 14.399999999999999)
14 Object x38 (incident: [FOD], coa: C15, time: 4, energy: 30, cost: 9.2)
15 Object x40 (incident: [MW], coa: C14, time: 4, energy: 10, cost: 5.199999999999999)
16 Object x42 (incident: [FOS], coa: C3, time: 4, energy: 100, cost: 23.199999999999996)
17 Object x43 (incident: [TA], coa: C15, time: 31, energy: 30, cost: 30.799999999999997)
18 Object x48 (incident: [DSIL], coa: C9, time: 38, energy: 75, cost: 45.4)
19 Object x51 (incident: [AP], coa: C2, time: 21, energy: 100, cost: 36.8)
20 Object x52 (incident: [CMD], coa: C16, time: 6, energy: 1, cost: 5.000000000000001)
21 Object x57 (incident: [DN], coa: C10, time: 33, energy: 10, cost: 28.400000000000002)
22 Object x62 (incident: [IOI], coa: C10, time: 10, energy: 10, cost: 10.0)
23 Object x64 (incident: [MIM], coa: C2, time: 28, energy: 100, cost: 42.4)
24 Object x66 (incident: [IG], coa: C4, time: 18, energy: 20, cost: 18.4)
25 cost total: 471.9999999999999
26

```

Figure 8. Results prioritizing 20% sustainability and 80% time (alpha equal to 0.8)

action, such as C11, which presents poor sustainability (label E) and is not selected when the configuration fully prioritizes sustainability. However, when this criterion is relaxed, it begins to be selected. In this sense, we can also observe how in the last configuration, where the response time is strongly prioritized, the selection of C9 appears, which is an even less sustainable course of action with a label F.

On the other hand, the courses of action C8 and C12 have the worst sustainability labels, F and G respectively. There are alternative courses of action that cover the same incidents and are better in terms of time and sustainability, so C8 and C12 are never selected.

Table 4. Comparison of results obtained according to different alpha values

CoA	Alfa 0.0	Alfa 0.2	Alfa 0.5	Alfa 0.8
C1	x	x	x	x
C2	x	x	x	x
C3	x	x	x	x
C4	x		x	x
C5	x	x	x	x
C6	x		x	x
C7	x	x	x	x
C8				
C9				x
C10	x	x	x	x
C11		x	x	
C12				
C13	x	x	x	x
C14	x	x	x	x
C15	x	x	x	x
C16	x	x	x	x

The quantum algorithm becomes more important when we move into real scenarios where the number of incidents is high, in the order of hundreds or thousands. This number is even greater if we consider a centralized incident management system serving multiple organizations. In these cases, the quantum algorithm responds in a constant time, independent of the number of incidents handled, which is a critical aspect for an incident response system.

5. Conclusions

The significance of security management, risk analysis, and particularly risk management, underscored by effective handling and learning from security incidents, is escalating in importance. However, the sustainability aspect of such security management is frequently overlooked. It is crucial, nevertheless, to consider security solutions and controls in light of their sustainability. This approach is not only feasible but necessary in an era of increasing environmental consciousness. Our focus in this paper has been on the context of the Internet of Things environments, which are proliferating globally and contributing to a significant rise in security incidents.

In this context, the efficiency with which incidents are addressed and system security is reinstated is of paramount importance for the prompt resolution of security breaches. However, addressing these issues in a sustainable manner, by opting for the most suitable course of action, is not only preferable but also aligns with the environmental policies.

The field of quantum computing research is diversifying rapidly, finding applications in numerous and varied contexts. Specifically, in this paper, we have developed an experimental quantum computing application aimed at optimizing the selection of security courses of action in response to various security incident scenarios. This application not only evaluates the required time for each security solution but also considers its sustainability. We have designed and implemented a quantum computing algorithm and, following extensive testing and execution, can affirm that its results are accurate and align with expectations based on quantum principles. The algorithm has high efficiency in execution time, effectively solving the problem in a near-constant timeframe. This paper illustrates the efficacy of our quantum algorithm in addressing this specific security challenge.

Therefore, it is reasonable to assert that, despite the numerous unresolved challenges in security incident management, particularly in the context of handling extensive datasets, certain issues can be effectively addressed using quantum algorithms. In fact, a key component of our future research involves an in-depth exploration of quantum algorithms and swarm intelligence applied to the extensive dataset of security risks and incidents collected from various organizations. This endeavour aims to enable real-time correlation of security incidents, offering a more comprehensive and efficient approach to responding to security threats.

Author Contributions: Conceptualization, all authors; methodology, C. Blanco.; software, A. Santos-Olmo; validation, L.E. Sánchez; writing, review and editing, all authors; All authors have read and agreed to the published version of the manuscript.

Funding: This work has been developed within the ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521), ALBA-UC (TED2021-130355B-C33, id.3611130630-130630-28-521), AETHER-UCLM (PID2020-112540RB-C42), PRESECREL (PID2021-124502OB-C42) and CHIST-ERA (PCI2023145980-2) funded by MCIN/AEI/10.13039/501100011033 and Unión Europea Next GenerationEU/PRTR

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: <https://github.com/GSYAtools/QISS>

Acknowledgments: We thank the support of the companies Sicaman Nuevas Tecnologías S.L. (<https://www.sicaman.com>) and Marisma Shield S.L. (<https://www.emarisma.com>) that have facilitated the validation of case studies and the use of the eMARISMA tool

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

References

- Orojloo, H.; Azgomi, M.A. A game-theoretic approach to model and quantify the security of cyber-physical systems. *Computers in Industry* **2017**, *88*, 44–57. <https://doi.org/10.1016/j.compind.2017.03.007>.
- Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Computers in Industry* **2018**, *100*, 212–223. <https://doi.org/10.1016/j.compind.2018.04.017>.
- Priyadarshini, I.; Kumar, R.; Tuan, L.M.; Son, L.H.; Long, H.V.; Sharma, R.; Rai, S. A new enhanced cyber security framework for medical cyber physical systems. *SICS Software-Intensive Cyber-Physical Systems* **2021**, *35*, 159–183. <https://doi.org/10.1007/s00450-021-00427-3>.
- Jindal, A.; Aujla, G.S.; Kumar, N.; Chaudhary, R.; Obaidat, M.S.; You, I. SeDaTiVe: SDN-Enabled Deep Learning Architecture for Network Traffic Control in Vehicular Cyber-Physical Systems. *IEEE Network* **2018**, *32*, 66–73. <https://doi.org/10.1109/MNET.2018.1800101>.
- Khalid, A.; Kirisci, P.; Khan, Z.H.; Ghrairi, Z.; Thoben, K.D.; Pannek, J. Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry* **2018**, *97*, 132–145. <https://doi.org/10.1016/j.compind.2018.02.009>.
- Kumar, R.; Narra, B.; Kela, R.; Singh, S. AFMT: Maintaining the safety-security of industrial control systems. *Computers in Industry* **2022**, *136*, 103584. <https://doi.org/10.1016/j.compind.2021.103584>.
- Griffor, E.; Wollman, D.; Greer, C. Framework for Cyber-Physical Systems: Volume 1, Overview. Technical Report June, National Institute of Standards and Technology, Gaithersburg, MD, 2017. <https://doi.org/10.6028/NIST.SP.1500-201>.
- Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry* **2018**, *103*, 97–110. <https://doi.org/10.1016/j.compind.2018.09.004>.
- Glantz, C.; Lenaues, J.; Landine, G.; O'Neil, L.R.; Leitch, R.; Johnson, C.; Lewis, J.; Rodger, R., Implementing an Information Security Program. In *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges*; Martellini, M.; Malizia, A., Eds.; Terrorism, Security, and Computation, Springer International Publishing: Cham, 2017; book section Chapter 9, pp. 179–197. https://doi.org/10.1007/978-3-319-62108-1_9.
- Thakur, K.; Qiu, M.; Gai, K.; Ali, M.L. An Investigation on Cyber Security Threats and Security Models. In Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, nov 2015; pp. 307–311. <https://doi.org/10.1109/CSCloud.2015.71>.
- Wang, T.; Gao, S.; Li, X.; Ning, X. A meta-network-based risk evaluation and control method for industrialized building construction projects. *Journal of Cleaner Production* **2018**, *205*, 552–564. <https://doi.org/10.1016/j.jclepro.2018.09.127>.
- Turskis, Z.; Goranin, N.; Nurusheva, A.; Boranbayev, S. Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach. *Informatica* **2019**, *30*, 187–211. <https://doi.org/10.15388/Informatica.2019.203>.

13. Paltrinieri, N.; Reniers, G. Dynamic risk analysis for Seveso sites. *Journal of Loss Prevention in the Process Industries* **2017**, *49*, 111–119. <https://doi.org/10.1016/j.jlp.2017.03.023>. 488
14. Santos-Olmo, A.; Sánchez, L.E.; Rosado, D.G.; Serrano, M.A.; Blanco, C.; Mouratidis, H.; Fernández-Medina, E. Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals. *Frontiers of Computer Science* **2024**, *18*, 183808. 489
15. Rosado, D.G.; Santos-Olmo, A.; Sanchez, L.E.; Serrano, M.A.; Blanco, C.; Mouratidis, H.; Fernández-Medina, E. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Comput. Ind.* **2022**, *142*, 103715. <https://doi.org/10.1016/j.compind.2022.103715>. 490
16. Ross, M.; Jara, A.J.; Cosenza, A. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. Technical Report November, European Union Agency For Network And Information Security, 2017. <https://doi.org/10.2824/03228>. 491
17. Serrano, M.A.; Sánchez, L.E.; Santos-Olmo, A.; García-Rosado, D.; Blanco, C.; Barletta, V.S.; Caivano, D.; Fernández-Medina, E. Minimizing incident response time in real-world scenarios using quantum computing. *Software Quality Journal* **2024**, *32*, 163–192. <https://doi.org/10.1007/s11219-023-09632-6>. 492
18. Bhardwaj, A.; Sapra, V. Security Incidents & Response Against Cyber Attacks, 2021. <https://doi.org/https://doi.org/10.1007/978-3-030-69174-5>. 493
19. Salam, A., Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends. In *Internet of Things for Sustainable Community Development: Wireless Communications, Sensing, and Systems*; Springer International Publishing: Cham, 2020; pp. 299–327. https://doi.org/10.1007/978-3-030-35291-2_10. 494
20. Zubair, S.; Ahmed, M.; Sikos, L.; Islam, N. Toward a Sustainable Cybersecurity Ecosystem. *Computers* **2020**, *9*, 74. <https://doi.org/10.3390/computers9030074>. 495
21. Mahima, D. Cyber Threat in Public Sector: Modeling an Incident Response Framework. In Proceedings of the 2021 International Conference on Innovative Practices in Technology and Management (ICIPTM), 2021, pp. 55–60. <https://doi.org/10.1109/ICIPTM52218.2021.9388333>. 496
22. Dion, M. Cybersecurity policy and theory. In *Theoretical Foundations of Homeland Security*; Routledge: London, 2020; pp. 257–284. 497
23. Prasad, R.; Rohokale, V., Secure Incident Handling. In *Cyber Security: The Lifeline of Information and Communication Technology*; Springer International Publishing: Cham, 2020; pp. 203–216. https://doi.org/10.1007/978-3-030-31703-4_14. 498
24. Salvi, A.; Spagnoletti, P.; Noori, N.S. Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security* **2022**, *112*, 102507. <https://doi.org/https://doi.org/10.1016/j.cose.2021.102507>. 499
25. Tanczer, L.M.; Brass, I.; Carr, M. CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy* **2018**, *9*, 60–66. <https://doi.org/https://doi.org/10.1111/1758-5899.12625>. 500
26. Plèta, T.; Tvaronavičienė, M.; Della Casa, S. Cyber effect and security management aspects in critical energy infrastructures. *Insights into Regional Development* **2020**, *2*, 538–548. [https://doi.org/10.9770/IRD.2020.2.2\(3\)](https://doi.org/10.9770/IRD.2020.2.2(3)). 501
27. Grispos, G.; Glisson, W.B.; Storer, T. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. *Digital Investigation* **2017**, *22*, 62–73. <https://doi.org/https://doi.org/10.1016/j.diin.2017.07.006>. 502
28. Ahmad, A.; Maynard, S.B.; Desouza, K.C.; Kotsias, J.; Whitty, M.T.; Baskerville, R.L. How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security* **2021**, *101*, 102122. <https://doi.org/10.1016/j.cose.2020.102122>. 503
29. Ahmad, A.; Desouza, K.C.; Maynard, S.B.; Naseer, H.; Baskerville, R.L. How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology* **2020**, *71*, 939–953. <https://doi.org/10.1002/asi.24311>. 504
30. Naseer, A.; Naseer, H.; Ahmad, A.; Maynard, S.B.; Masood Siddiqui, A. Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management* **2021**, *59*, 102334. <https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2021.102334>. 505
31. Ahmad, A.; Webb, J.; Desouza, K.C.; Boorman, J. Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security* **2019**, *86*, 402–418. <https://doi.org/10.1016/j.cose.2019.07.001>. 506
32. Knight, R.; Nurse, J.R. A framework for effective corporate communication after cyber security incidents. *Computers & Security* **2020**, *99*, 102036. <https://doi.org/https://doi.org/10.1016/j.cose.2020.102036>. 507
33. Ahmad, A.; Maynard, S.B.; Shanks, G. A case analysis of information systems and security incident responses. *International Journal of Information Management* **2015**, *35*, 717–723. <https://doi.org/10.1016/j.ijinfomgt.2015.08.001>. 508
34. Ahmad, A.; Hadgkiss, J.; Ruighaver, A.B. Incident response teams - Challenges in supporting the organisational security function. *Computers and Security* **2012**, *31*, 643–652. <https://doi.org/10.1016/j.cose.2012.04.001>. 509
35. van der Kleij, R.; Schraagen, J.M.; Cadet, B.; Young, H. Developing decision support for cybersecurity threat and incident managers. *Computers & Security* **2021**, p. 102535. <https://doi.org/https://doi.org/10.1016/j.cose.2021.102535>. 510
36. Tam, T.; Rao, A.; Hall, J. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security* **2021**, *109*, 102385. <https://doi.org/https://doi.org/10.1016/j.cose.2021.102385>. 511
37. He, Y.; Zamani, E.D.; Lloyd, S.; Luo, C. Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management* **2022**, *62*, 102435. <https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2021.102435>. 512

38. Initiative, J.T.F.T.; et al. *SP 800-39. managing information security risk: Organization, mission, and information system view*; National Institute of Standards & Technology: USA, 2011.
39. Kniaz, S.; Brych, V.; Marhasova, V.; Tyrkalo, Y.; Skrynkovskyy, R.; Sumets, A. Modeling of the information system of environmental risk management of an enterprise. In Proceedings of the 2022 12th International Conference on Advanced Computer Information Technologies (ACIT). IEEE, 2022, pp. 215–218.
40. Rosado, D.G.; Moreno, J.; Sánchez, L.E.; Santos-Olmo, A.; Serrano, M.A.; Fernández-Medina, E. MARISMA-BiDa pattern: Integrated risk analysis for big data. *Computers & Security* **2021**, *102*, 102155. <https://doi.org/10.1016/j.cose.2020.102155>.
41. IBM. *The Quantum Decade. A playbook for achieving awareness, readiness, and advantage*; IBM, 2021.
42. Clairambault, P.; De Visme, M.; Winskel, G. Game semantics for quantum programming. *Proceedings of the ACM on Programming Languages* **2019**, *3*, 1–29.
43. Shor, P. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings of the Proceedings 35th Annual Symposium on Foundations of Computer Science, Ieee, Santa Fe, NM, USA, 2002; pp. 124–134. <https://doi.org/10.1109/SFCS.1994.365700>.
44. Grover, L.K. Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Physical Review Letters* **1997**, *79*, 325–328. <https://doi.org/10.1103/PhysRevLett.79.325>.
45. Altenkirch, T.; Grattage, J. A Functional Quantum Programming Language. In Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science (LICS' 05), Chicago, IL, USA, 2005; pp. 249–258, [arXiv:quant-ph/0409065]. <https://doi.org/10.1109/LICS.2005.1>.
46. Sánchez, P.; Alonso, D. On the Definition of Quantum Programming Modules. *Applied Sciences* **2021**, *11*, 5843.
47. Gyongyosi, L.; Imre, S. A Survey on quantum computing technology. *Computer Science Review* **2019**, *31*, 51–71. <https://doi.org/10.1016/j.cosrev.2018.11.002>.
48. Gyongyosi, L.; Imre, S. A Survey on quantum computing technology. *Computer Science Review* **2019**, *31*, 51–71. <https://doi.org/10.1016/j.cosrev.2018.11.002>.
49. Piattini, M.; Serrano, M.; Perez-Castillo, R.; Petersen, G.; Hevia, J.L. Toward a Quantum Software Engineering. *IT Professional* **2021**, *23*, 62–66. <https://doi.org/10.1109/MITP.2020.3019522>.
50. Sutor, R. *Dancing with Qubits*; Packt Publishing: Birmingham, UK, 2019.
51. Johnston, E.R.; Harrigan, N.; Gimeno-Segovia, M. *Programming Quantum Computers: essential algorithms and code samples*; O'Reilly Media: Gravenstein Highway North, USA, 2019.
52. Farhi, E.; Goldstone, J.; Gutmann, S.; Lapan, J.; Lundgren, A.; Preda, D. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. *Science* **2001**, *292*, 472–475.
53. Das, A.; Chakrabarti, B.K. Colloquium: Quantum annealing and analog quantum computation. *Reviews of Modern Physics* **2008**, *80*, 1061.
54. Lucas, A. Ising formulations of many NP problems. *Frontiers in physics* **2014**, *2*, 5. <https://doi.org/10.3389/fphy.2014.00005>.
55. Asfaw, A.; Corcoles, A.; Bello, L.; Ben-Haim, Y.; Bozzo-Rey, M.; Bravyi, S.; Bronn, N.; Capelluto, L.; Vazquez, A.C.; Ceroni, J.; et al. *Learn Quantum Computation Using Qiskit*; IBM, 2020.
56. Farhi, E.; Goldstone, J.; Gutmann, S. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028* **2014**.
57. Rocke, D. Genetic Algorithms+ Data Structures= Evolution programs (3rd. *Journal of the American Statistical Association* **2000**, *95*, 347.
58. Kirkpatrick, S.; Gelatt Jr, C.D.; Vecchi, M.P. Optimization by simulated annealing. *science* **1983**, *220*, 671–680.
59. Dieterich, J.M.; Hartke, B. Empirical review of standard benchmark functions using evolutionary global optimization. *arXiv preprint arXiv:1207.4318* **2012**.
60. Černý, V. Quantum computers and intractable (NP-complete) computing problems. *Phys. Rev. A* **1993**, *48*, 116–119. <https://doi.org/10.1103/PhysRevA.48.116>.

Short Biography of Authors



Carlos Blanco has a Ph.D. in Computer Science from the University of Castilla-La Mancha (Spain). He is working as an Assistant Professor at the University of Cantabria (Spain) and is a member of several research groups: GSyA (University of Castilla-La Mancha) and ISTR (University of Cantabria). His research activity is in the field of Security for Information Systems and its specially focused on assuring Big Data, Data Warehouses and OLAP systems by using MDE approaches. He has published several international communications, papers and book chapters related with these topics (DSS, CSI, INF50F, ComSIS, TCJ, ER, DaWaK, etc.).



Antonio Santos-Olmo is M.Sc and PhD. in Computer Science by the University of Castilla-La Mancha. He is an Assistant Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha in Ciudad Real (Spain). M.Sc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Software Factory departments of the company Sicaman Nuevas Tecnologías S.L. His-research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real (Spain).

593



Luis Enrique Sánchez holds a PhD in Computer Science from the University of Castilla-La Mancha (Spain), a MSc in Computer Science from the Polytechnic University of Madrid (Spain), and holds a degree in Computer Science from the University of Granada (Spain). He is Certified Information System Auditor by ISACA and Leader Auditor of ISO27001 by IRCA. He participates at the GSyA research group and he is Assistant Professor of the Technologies and Information Systems Department of the University of Castilla-La Mancha. He has directed more than 50 projects in multinational companies. He has more than 60 national and international papers and conference on Software Engineering and Teaching. He belongs to various professional and research associations (COIILCLM, ALI, ASIA, TUV Rheinland, ISACA, eSec INTECO, SC27 AENOR, etc.).

594

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

595

596

597