water

MDPI

Article

Bridging the Cyber–Physical Divide: A Novel Approach for Quantifying and Visualising the Cyber Risk of Physical Assets

Cael Keenan [1,*], Holger R. Maier [1], Hedwig van Delden [1,2] and Aaron C. Zecchin [1]

[1] School of Architecture and Civil Engineering, The University of Adelaide, Adelaide, SA 5005, Australia
[2] Research Institute for Knowledge Systems (RIKS), P.O. Box 463, 6200 AL Maastricht, The Netherlands
* Correspondence: cael.keenan@adelaide.edu.au

Abstract: Critical infrastructures and their physical assets are under increasing threat of cyber-attacks as technological integration creates cyber–physical systems (CPSs). This has led to an urgent need to better understand which physical assets in these systems are most at risk, but this requires crossing the divide between cyber and physical risk assessments. However, existing cyber-security methods generally focus solely on the vulnerabilities and security of the cyber network and efforts to quantify the impacts of these cyber vulnerabilities on physical assets are generally limited to the consideration of individual attacks, rather than system-wide risk assessments. Similarly, risk assessments of physical infrastructure systems generally ignore potential impacts due to cyber-attacks. To overcome this cyber–physical divide in risk assessment, we introduce a novel approach for assessing risk across this divide. The proposed approach assesses the cyber risk of physical assets as a function of the vulnerabilities of their connected cyber components, and the contribution of cyber components to this risk. The approach is demonstrated with a case study of the C-Town water distribution system. The results indicate that the approach shows a modified prioritisation of risk compared to that obtained using conventional cyber or physical assessments, highlighting the importance of considering the connection between cyber and physical components in risk assessments of critical infrastructure and their physical assets.

Keywords: cyber–physical systems; risk assessment; cyber security; water distribution systems; risk modelling; cyber–physical attack

check for updates

Citation: Keenan, C.; Maier, H.R.; van Delden, H.; Zecchin, A.C. Bridging the Cyber–Physical Divide: A Novel Approach for Quantifying and Visualising the Cyber Risk of Physical Assets. *Water* **2024**, *16*, 637. https://doi.org/10.3390/w16050637

Academic Editors: Christos Makropoulos and Rita Maria Ugarelli

Received: 30 January 2024
Revised: 14 February 2024
Accepted: 20 February 2024
Published: 21 February 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The infrastructure required to maintain our societies' way of life is increasingly connected to cyber networks [1,2]. This is generally the result of the application of connected cyber control technology to infrastructure networks, such as water or electricity distribution systems [3,4]. This incorporation of technology has transformed these critical infrastructure networks into cyber–physical systems (CPSs)—complex interconnected physical and cyber networks (Figure 1a) that continually exchange information and control [5–7].

A key aspect of the function of CPSs, and what facilitates their interconnection, is the link between physical assets and cyber components. For example, in the case of water distribution systems, this could be a tank with a water level sensor and a router that will send that water level data to a pump, which will then turn on/off as a function of this level (Figure 1b). Whilst this link improves the efficiency and automation of the operation of the physical system, it also exposes the physical infrastructure and its operations to cyber threats, in addition to existing physical threats [8]. Not only have the cyber threats and vulnerabilities of CPSs become more prevalent and numerous over the past few years [9–12], the number of infrastructure systems exposed to these threats is also growing [13,14].

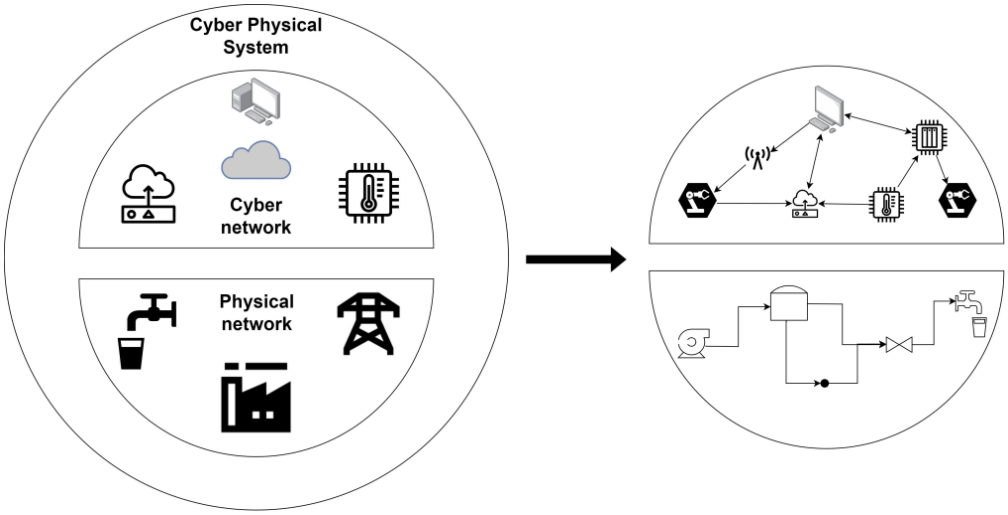


Figure 1. The cyber–physical system, where (**a**) the cyber network (represented by common components such as a router, sensor, cloud, and workstation) and the physical network (represented by common infrastructure networks: water, manufacturing, and power generation) work together as a cyber–physical system (CPS). (**b**) An example water distribution system CPS incorporates a physical network (bottom) of pump, valve, and storage tank where arrows indicate the flow of water. The cyber network (top) depicts common components including sensors, actuators, router, Supervisory Control and Data Acquisition (SCADA) workstation, and their potential configuration where arrows represent flow of information/control.

Cyber threats to physical infrastructure systems are caused by attacks upon the cyber network that have an impact in the physical network, which are referred to as cyber–physical attacks (CPAs) [15,16] (Figure 2). As a result, the need to safeguard physical assets against potential cyber-attacks has received increasing attention [17–21]. However, common domain-specific approaches to quantifying associated risks, such as cyber-threat modelling [22] or physical asset performance analysis [23–25], fall short of providing a system-wide assessment of the actual cyber-risk of critical infrastructure. This is because they primarily focus either on the cyber or physical domains of CPSs, without bridging the gap between them, or focus on enterprise networks rather than the operational technology networks that directly control infrastructure operations [8,17,26]. The small number of studies that do bridge the cyber–physical divide are "attack-focussed" [17], which means that they only consider the impact of specific cyber-attacks. While this can allow for the stress testing of the systems in question (e.g., Nikolopoulos and Makropoulos [27]), it generally does not provide a snapshot of the systemic risk of the combined CPS.

While there are existing approaches to assessing the system-wide risk of failure of physical assets (e.g., that the asset will not meet desired performance requirements, such as the inability of a water supply system to deliver water of suitable quality and pressure to customers), these are either attribute-based or performance-based, involving an assessment of factors such as the critical failure modes of the asset, its expected performance drop during failure, and the likelihood of this occurring based on historical data [23]. However, the risk or vulnerability of failure of specific physical assets due to their connection to cyber systems is often ignored, with generalised network-wide impacts considered instead [8,17]. This is likely because all the other risk factors and failure modes originate in the physical system itself and can therefore be considered at any particular point relatively easily. In contrast, consideration of the risk CPAs pose to the ability to maintain the desired performance of a physical system requires the development of a method for translating risks in the cyber domain to those in the physical domain.

Similarly, while there are existing approaches for quantifying system-wide risk in cyber networks, these generally do not translate to risk in the physical domain. For example, security/vulnerability-based assessments, such as maturity models [28], focus on assessing cyber-security attributes and the security policy of the cyber system, resulting in cyber-security policy recommendations that are silent on potential impacts on the physical assets of a CPS. In the same vein, threat-based assessments [29–32] focus on different approaches to simulating the behaviour of the attacker performing the CPA [33] with the goal of identifying strategies that assist with protecting cyber assets from these attacks, without crossing the cyber–physical divide to quantify the risk to specific physical assets due to these attacks.

Another assessment method commonly utilised within the cyber domain to understand its level of risk is the assessment of vulnerabilities using the Common Vulnerability Scoring System (CVSS) [34]. This scoring system is used to quantitatively score common vulnerabilities and exposures (CVEs), which are information system weaknesses that may be present in the cyber system [34]. These CVSS scores range from zero to ten and incorporate an exploitability score and an impact score in an effort to quantify the severity of a vulnerability and are commonly used in industry to prioritise mitigation responses across managed cyber networks. The exploitability score is influenced by a series of exploitability metrics describing the "ease and technical means by which the vulnerability can be exploited" [34]. The impact score and subsequent metrics reflect the consequences of the vulnerability being successfully exploited to either the primary cyber system or the downstream cyber systems. The most recent version of the CVSS (v4.0) also incorporates a safety metric, which identifies if the interconnected system may have an impact on the safety of human life. Whilst this again fails to cross the cyber–physical divide as it does not assess impact in the physical domain explicitly, nor provide a way to translate this vulnerability information to the physical domain, it does highlight an increased interest and desire for interconnected cyber–physical risk assessments.

As mentioned above, a common feature of all existing methods for quantifying system-wide risks in cyber networks is that they primarily provide an assessment of the security of the cyber domain of CPSs. This makes the implicit assumption that the most vulnerable components in the cyber domain have the largest impact in the physical domain. However, this is unlikely to be the case, highlighting the need for an approach that crosses the cyber–physical divide to enable the relative risk to physical assets due to components in the cyber network, as well as the relative influence of different components in the cyber network on this risk, to be quantified explicitly. This would not only provide a quantitative assessment of the actual risk of physical assets due to their cyber connectivity but would also provide the information needed to target and justify investment in mitigation measures in the cyber domain that result in the largest reduction in risk in the physical domain.

In order to address the shortcomings of existing approaches, the overarching aim of this paper is to introduce and assess the utility of a novel approach to assessing the relative systemic risk of cyber–physical systems by considering the interactions between the cyber and physical components of such systems explicitly. By crossing the cyber–physical divide, the proposed approach is able to quantify (i) the relative risk of physical assets due to cyber components and (ii) the relative influence of cyber components on physical asset risk (Objective 1). This enables physical asset managers to understand another aspect of the risk their assets face, namely the risk due to cyber threats, and enables the identification of the cyber components that have the largest influence on these risks, and hence the most effective risk reduction strategies.

The application and potential benefits of the proposed approach are illustrated on a water distribution system case study from the literature for three different cyber network configurations (Objective 2):

1. Demonstrating how the approach can be used to obtain (a) quantitative estimates of the relative risk of physical assets due to their connection to cyber components and how they differ for different cyber network configurations (Objective 2a) and (b) the

relative contribution of different cyber components to this risk and how they differ for different cyber network configurations (Objective 2b).

2. Illustrating how currently used risk assessment approaches can give misleading results, as determined by the relative risk rankings of the assets in the physical domain and the components in the cyber domain obtained using the proposed and more conventional approaches for the three different cyber network configurations considered, when determining (c) the relative vulnerabilities of cyber components in CPSs (Objective 2c) and (d) the relative impacts of physical assets in CPSs (Objective 2d).

The remainder of this paper is structured as follows: The proposed approach is introduced in Section 2, followed by details of the case study and how the proposed approach is applied to it in Section 3. The case study results are presented and discussed in Section 4, before the conclusions are outlined in Section 5.

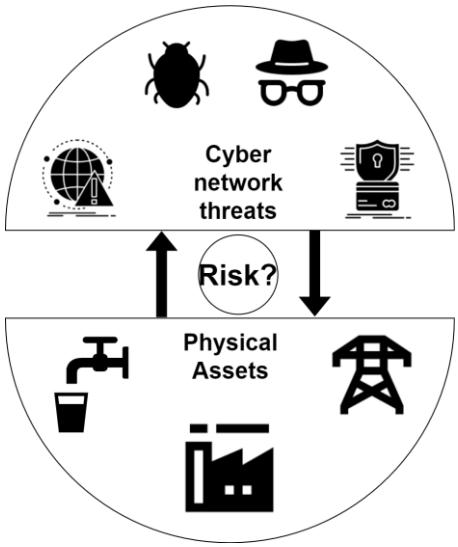


Figure 2. A divide exists in risk assessment, in which the systemic risk of cyber-attacks and threats originating in the cyber network are not necessarily assessed for physical assets.

2. Methodology

A conceptual representation of the proposed approach to assessing the relative systemic risk of cyber–physical systems by considering the interactions between the cyber and physical components of such systems explicitly (Objective 1) is given in Figure 3. A key feature of the approach is that it uses information from both the cyber (Step 1) and physical (Step 2) domains, as well as the way these are connected (Step 3), to quantify the relative cyber vulnerability (i.e., the relative likelihood of being attacked) (Step 4) and risk (Step 6) of each component in the physical system, in addition to the relative contribution of each cyber component to the impact (i.e., the physical infrastructure response to the attack) (Step 5) and risk (Step 7) in the physical domain. Risk is defined as the product of the vulnerability (likelihood) and impact (consequence) [35].

Another key feature of the proposed approach is that it has been designed to be easy to use, catering to users with differing degrees of expertise, knowledge, resources, and requirements. Consequently, it can be used either by generalists or specialists working to reduce the risks to physical infrastructure due to cyber threats. Furthermore, it can be easily modified to incorporate different types of data sources to suit the context of the assessment. The outputs produced can also be visualised in heat maps for improved understanding and communication of the risks to CPSs.

Details of each of the steps in the proposed approach (Figure 3) are given in the following sub-sections. It should be noted that although the approach is illustrated here through

an application to water infrastructure, it is designed as a generic approach applicable to all types of CPS infrastructure networks.

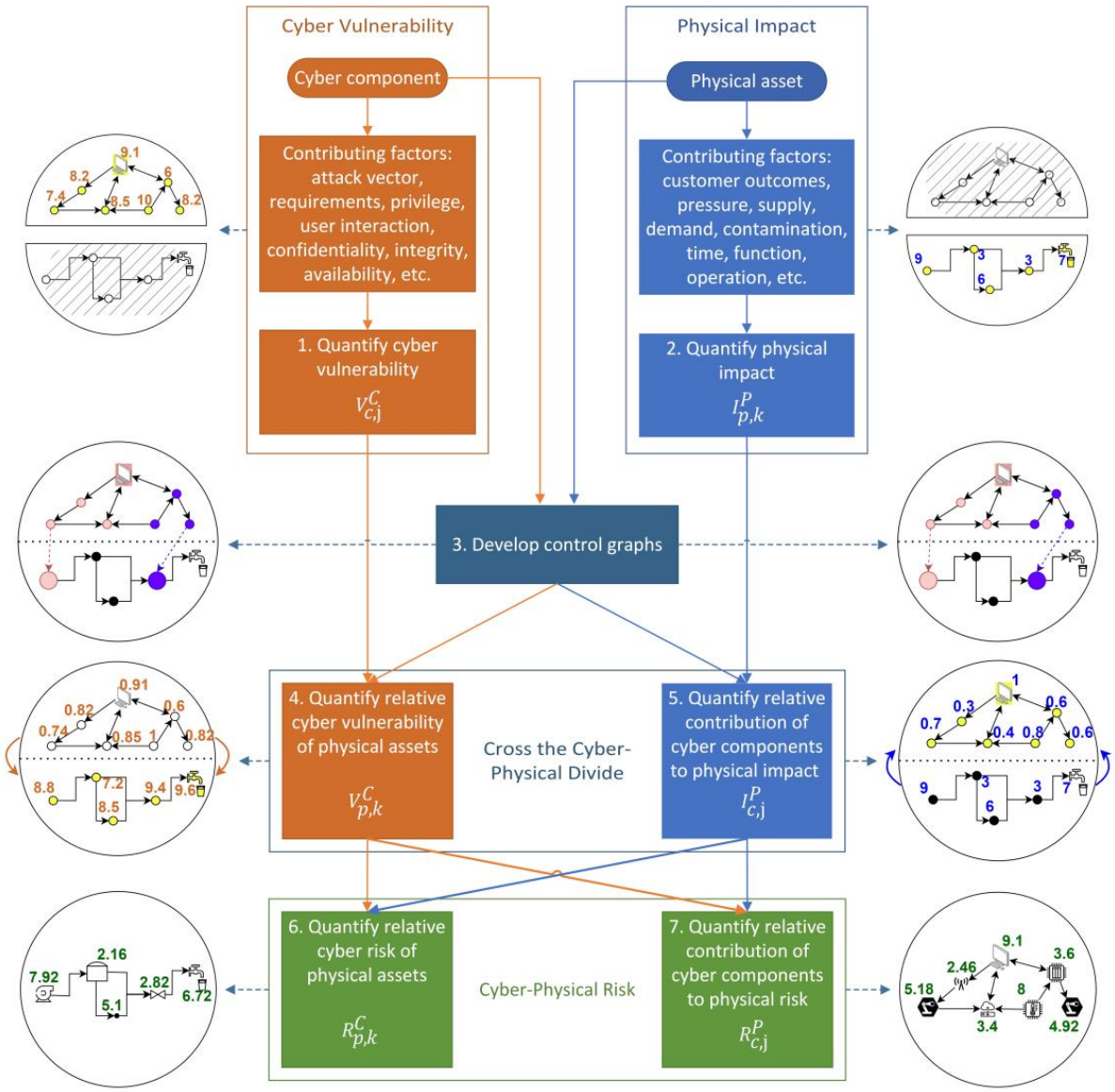


Figure 3. Proposed approach to assessing the relative systemic risk of cyber–physical systems by considering the interactions between the cyber and physical components of such systems explicitly.

2.1. Step 1—Quantify Cyber Vulnerability

As shown in Figure 3, the first step in the proposed approach involves the assignment of a vulnerability score ($V^C_{c,j}$) to each of the j components in the cyber network, as is generally performed when performing risk assessments that are restricted to the cyber domain. This score can be thought of as analogous to a probability of a successful attack at the component in question and is affected by contributing factors such as potential attack vectors, complexity, privileges required, user interaction needed, and effect on confidentiality, integrity, and availability.

Whilst this score can be informed by any metrics that may provide insight into the possibility of cyber compromise, the Common Vulnerability Scoring System (CVSS) described in Section 1 is recommended [34], as it is an existing scoring system that is used extensively in the literature [36–39] and industry [40]. As mentioned in Section 1, CVSS scores range from zero to ten and take account of a range of factors related to vulnerability

and impact in the cyber domain. In cases where there are multiple common vulnerability exposures (CVEs) related to a cyber component, these can be combined through determining the mean CVSS score, taking the maximum of the vulnerability scores, or by using other score aggregation techniques, as considered most appropriate for the case study under consideration.

2.2. Step 2—Quantify Physical Impact

As shown in Figure 3, the second step in the proposed approach involves the assignment of a physical impact score ($I^P_{p,k}$) to each of the k components in the physical network that could be susceptible to failure through a CPA. Such impacts are generally affected by contributing factors such as customer outcomes (pressure, supply), remediation requirements, and criticality to network function. While these impact scores can be obtained using a range of methods, such as hydraulic modelling in the case of water distribution systems [18,24], for the sake of simplicity and consistency, an approach that mirrors the development of CVSS 4.0 scores for individual cyber component vulnerabilities is proposed to determine the physical impact scores.

Following the CVSS 4.0 methodology, impact scores ranging from zero to ten are obtained for each physical asset by weighting scores from three metrics affecting the physical impact that are obtained for each asset using expert opinion (Equation (1)):

$$I^P_{p,k} = \frac{(TtF + SoF + TtR)}{3}. \quad (1)$$

These metrics include time to failure (*TtF*), severity of failure (*SoF*), and time to remediation (*TtR*), as these are simplified versions of commonly used performance-based measures when assessing the risk of failure of a water distribution system (WDS) (Table 1) [41–43]. Time to failure is defined as the expected time it takes until the system performance enters an unsatisfactory state. For example, should a pump fail, it is expected that customers will eventually have unmet demand. Despite this, water in holding tanks can be used to satisfy demand for a period of time, increasing the expected time to failure. Severity of failure is defined as the expected maximum potential impact of the failure of a physical asset and time to remediation is defined as the expected time it takes for a physical asset to return to a functional state following failure. As shown in Table 1, each of these metrics is assigned a score of 1, 5, or 10 depending on the perceived severity of the impact. It should be noted that as is the case for the cyber vulnerability scoring, other information regarding the physical assets under consideration can also be used to inform the impact score, such as the results of CPA stress testing [44].

Table 1. Scoring matrix for the physical impact score of a physical asset.

Metric	Score = 1	Score = 5	Score = 10
Time to failure (*TtF*)	Slow	Medium	Fast
Severity of failure (*SoF*)	Low	Medium	High
Time to remediation (*TtR*)	Fast	Medium	Slow

2.3. Step 3—Develop Control Graphs

As shown in Figure 3, the third step in the proposed approach involves the determination of which cyber components are connected to, and therefore have an influence on, each of the physical assets. This is achieved by determining the control graph [45] for each physical asset, which is defined as the connected sub-graph within the network that contains sensing and logic nodes (i.e., cyber components) that control the node of interest (i.e., physical asset). A key innovation is to utilise these cyber control graphs for each physical asset in risk assessment, directly connecting a set of cyber components to each physical asset. This enables the cyber risk of each asset in the physical realm to be

quantified based on an assessment of the vulnerability of individual components in the cyber realm, and vice versa (see Figure 3), thereby crossing the cyber–physical divide.

In order to determine the control graphs for each of the physical assets of interest, the entire CPS must first be represented as a directed graph, a common format for the depiction of a CPS [46]. Within this graph, nodes represent cyber components and physical assets, and the edges indicate a flow of information or control between components/assets. These directed edge relationships are determined either by a manual process of investigating the network dynamics, implied from infrastructure control rules, or can be automated with the aid of active or passive network scanning tools [10]. The nature of these directed edges can also be affected by cyber-security practices such as network segmentation and firewall rules that regulate the networks' communication. Identifying the boundary for such assessments is a challenge given the potential number of connected components; however, this is not the focus of the proposed approach. Once the overall CPS graph has been developed, the connectivity of each cyber component to physical assets is defined as the sub-graph of the parent and ancestor nodes for each physical asset.

The cyber components that are grouped into their sub-graph by their connection to physical assets constitute the control graph for that physical asset. This establishes the relationship between the cyber and physical network, crossing the divide between the two domains. In this implementation, it is assumed that a compromise of any of these components within the control graph will cascade to cause the failure of the physical asset to which it is connected, thereby providing an upper bound to risk.

2.4. Step 4—Quantify Relative Cyber Vulnerability of Physical Assets

As shown in Figure 3, the fourth step in the proposed approach involves the calculation of the relative cyber vulnerability of each of the physical assets under consideration ($V^C_{p,k}$) (Equation (2)). As can be seen from Equation (2), these values represent the ratio of the cyber vulnerability of physical asset k ($v^C_{p,\,k}$) (see Equation (3)) to the maximum cyber vulnerability of any of the physical assets under consideration ($\max v^C_p$), thereby providing information on the relative vulnerability of the different physical assets in the system under consideration to CPAs

$$V^C_{p,k} = \frac{v^C_{p,k}}{\max v^C_p}\,, \tag{2}$$

and

$$v^C_{p,k} = \sum_{j=1}^{m} w_i \cdot V^C_{c,\,j}\,. \tag{3}$$

As can be seen from Equation (3), the cyber vulnerability of physical asset k ($v^C_{p,\,k}$) is the weighted sum of the cyber vulnerability scores ($V^C_{c,\,j}$) of the m individual cyber components that are connected to physical asset k (i.e., the number of cyber components in the control graph of the physical asset under consideration). It should be noted that the vulnerability scores of the cyber components are determined in Step 1 and which m cyber components are connected to physical asset k is determined in Step 3. The weights (w_i) used in the calculation of the cyber vulnerability of physical asset k ($v^C_{p,\,k}$) (see Equation (3)) represent the relative perceived importance of each connected cyber component (e.g., based on its level of data traffic), thereby increasing the generality and flexibility of the proposed approach. In the absence of information on the relative importance of each cyber component, these weights should be set to 1.

It should be noted that the functional relationships used to calculate the cyber vulnerabilities of each of the physical assets under consideration (Equations (2) and (3)) can also be altered depending on user needs and preferences (see Appendix A, Table A1 for examples).

2.5. Step 5—Quantify Relative Contribution of Cyber Components to Physical Impact

As shown in Figure 3, the fifth step in the proposed approach involves the calculation of the relative contribution of each cyber component j to the impact in the physical domain ($I^P_{c,j}$) (Equation (4)). As can be seen from Equation (4), these values represent the ratio of the physical impact contributed to by cyber component j ($i^P_{c,\,j}$) (see Equation (5)) to the maximum physical impact contributed by any of the cyber components under consideration ($\max i^P_c$), thereby providing information on how important a particular cyber component is to the process function of the CPS

$$I^P_{c,j} = \frac{i^P_{c,j}}{\max i^P_c}\,, \tag{4}$$

and

$$i^P_{c,\,j} = \sum_{k=1}^{n} w_k \cdot I^P_{p,\,k}\,. \tag{5}$$

As can be seen from Equation (5), the contribution of cyber component j to the impact in the physical domain ($i^P_{c,\,j}$) is the weighted sum of the impacts of each of the n physical assets that cyber component j is connected to. It should be noted that the impact scores of the physical assets are determined in Step 2 and which n physical assets that cyber component j connects to is determined in Step 3. The weights (w_k) used in the calculation of the contribution of cyber component j to the impact in the physical domain ($i^P_{c,\,j}$) (see Equation (5)) represent the relative perceived importance of each connected physical asset (e.g., based on topological attributes of the assets [47,48]), thereby increasing the generality and flexibility of the proposed approach. In the absence of information on the relative importance of each physical asset, these weights should be set to 1.

It should be noted that the functional relationships used to calculate the relative contributions of each of the cyber components under consideration to the impact in the physical domain (Equations (4) and (5)) can be altered in the same way as Equations (2) and (3), depending on user needs and preferences (see Appendix A, Table A1 for examples).

2.6. Step 6—Quantify Relative Cyber Risk of Physical Assets

As shown in Figure 3, the sixth step in the proposed approach involves the calculation of the relative cyber risk of each of the physical assets under consideration ($R^C_{p,k}$) (Equation (6)). As can be seen from Equation (6), the relative cyber risk of physical asset k is the product of its relative cyber vulnerability (i.e., likelihood of being attacked successfully) ($V^C_{p,k}$) (Step 4—Equation (2)) and its physical impact score ($I^P_{p,\,k}$) (Step 2—Equation (1)):

$$R^C_{p,k} = V^C_{p,k} \cdot I^P_{p,\,k}\,. \tag{6}$$

These relative risk values can provide invaluable information to network managers on the relative risks of different physical assets to CPAs. The relative cyber risk scores for different physical assets can be colour coded (e.g., low, medium, high) and represented in a heat map to better assist managers with the identification of cyber risk "hot spots". This information can then be used in tandem with other asset management data (component criticality, asset life, etc.) to gain a more complete understanding of the risk of any connected physical asset and the topological distribution of risk. The use of a colour-coded visualisation is also a way to assess the relative effectiveness of different risk mitigation strategies. This type of output is intuitive and regularly used by physical asset managers, allowing the proposed approach to be incorporated into current physical risk assessment methods with ease. This interoperability afforded by a common output allows the outcomes of this methodology to be combined with existing infrastructure knowledge, such as that of physical performance and criticality analyses, to determine what the interplay between these different types of risk may be.

2.7. Step 7—Quantify Relative Contribution of Cyber Components to Physical Risk

As shown in Figure 3, the seventh step in the proposed approach involves the calculation of the relative contribution of a particular cyber component j to physical risk $(R^P_{c,j})$ (Equation (7)). As can be seen from Equation (7), the relative contribution of cyber component j to the risk in the physical domain is the product of its vulnerability in the cyber domain (i.e., likelihood of being attacked successfully) $(V^C_{c,j})$ (Step 1) and its relative contribution to the impact in the physical domain $(I^P_{c,j})$ (Step 5—Equation (4)):

$$R^P_{c,i} = V^C_{c,j} \cdot I^P_{c,j}\,. \tag{7}$$

These values of the relative contribution of different cyber components to the physical risk provide invaluable information to network managers on where to prioritise risk mitigation efforts. These values can also be visualised through a heat map, providing a rapid overview of which cyber components are of most concern.

3. Case Study

3.1. Study Description

The approach proposed in Section 2 has been applied to a fictional water distribution system (WDS) CPS, C-Town [49] (Figure 4). This network was chosen primarily due to its specific use in the previous stress testing of CPA scenarios for water CPSs [27,44,50]. Furthermore, it has had extensive use in the literature ([42,51], among others) and is often used as a benchmark model within the water distribution field. It also features a balance between a realistic level of complexity for a medium-scale water distribution system and computational efficiency.

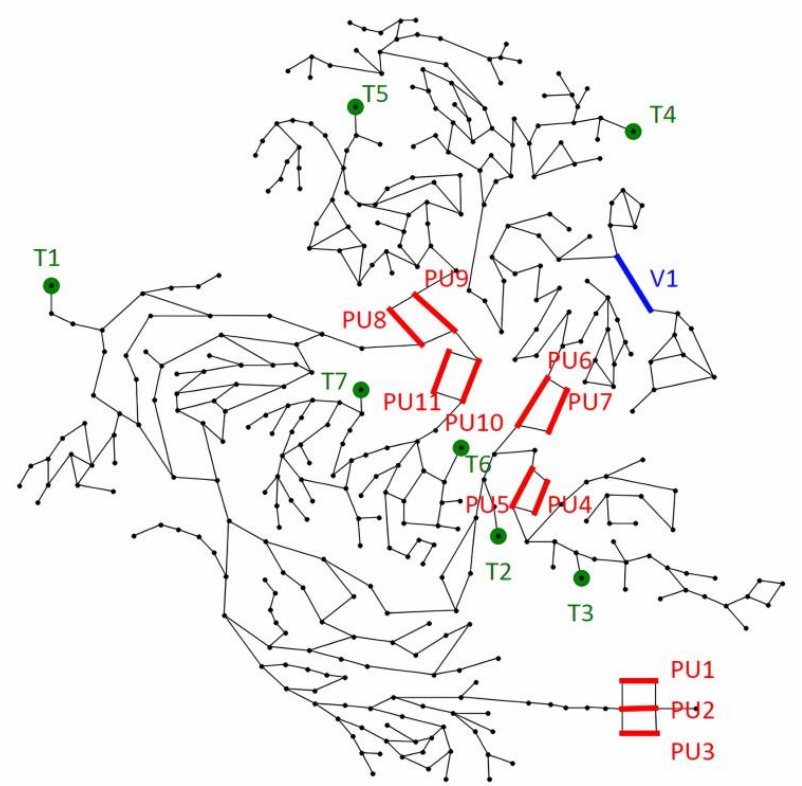


Figure 4. Basic configuration of the C-Town water distribution system. Red indicates a link with a pump asset (PU1 –PU11), blue indicates a link with a valve asset (v1), and green indicates the location of a tank asset (T1–T7).

The C-Town WDS distributes water via pumping from a source reservoir to storage tanks and then to users throughout the network (Figure 4). The physical domain of the C-Town WDS includes 11 pumps in 5 pump stations, 1 valve, 7 tanks to supply demand nodes across the network, and in Networks 2 and 3, 5 isolation valves and 5 flushers (Table 2), with the specification of the network informed by [15,27]. These pumps operate according to the trigger levels of the tanks, and pump station 1 (incorporating pumps 1 through 3) draws water from the singular water source.

Table 2. Physical network components of the C-Town WDS.

Physical Component	Number
Nodes	388
Pipes	429
Tanks	7
Pump stations (pumps)	5 (11)
Valves	1 in use
(Networks 2 and 3) Isolation valves	5
(Networks 2 and 3) Flushers	5

Three realisations of the connected SCADA cyber infrastructure are investigated (Figure 5) to enable the generality of findings across different cyber network structures and degrees of connectivity to be assessed. Two of these realisations have been used in previous studies and the third has been developed for this case study to provide an intermediate level of connectivity. It should be noted that as C-Town is a fictional benchmark WDS, none of these cyber network configurations are from actual systems and are used for illustration purposes. Details of the three cyber network configurations used are as follows:

- Network 1 (limited cyber connectivity) (Figure 5a) has been adapted from Taormina, Galelli, Tippenhauer, Salomons, and Ostfeld [15] and is a mostly disconnected CPS network. This cyber network acts as a simple control network for the CPS, without a central SCADA unit. The original configuration in [15] contain a central SCADA workstation, but this has been removed in this study to enable a disconnected network to be considered.
- Network 2 (high level of cyber connectivity) (Figure 5b) was developed by Nikolopoulos and Makropoulos [27] and is an interconnected CPS network. This cyber network incorporates water quality sensors, and its associated physical infrastructure is connected to a central SCADA cyber component. The water quality-related infrastructure includes the cyber components required for the sensing and reporting of contamination within the network and includes physical assets that isolate parts of the network and flush contaminated water from the system.
- Network 3 (intermediate level of cyber connectivity) (Figure 5c) is an adaptation of Network 2 that has been developed for this case study to provide a network with an intermediate level of interconnection (i.e., a connectivity level that lies between that of Networks 1 and 2).

A legend providing details of the asset and cyber component codes used is included in Appendix B, Table A2. Further information relating to the function of and the differences between the three realisations of the CPS are included in Appendix B, Tables A3–A5.

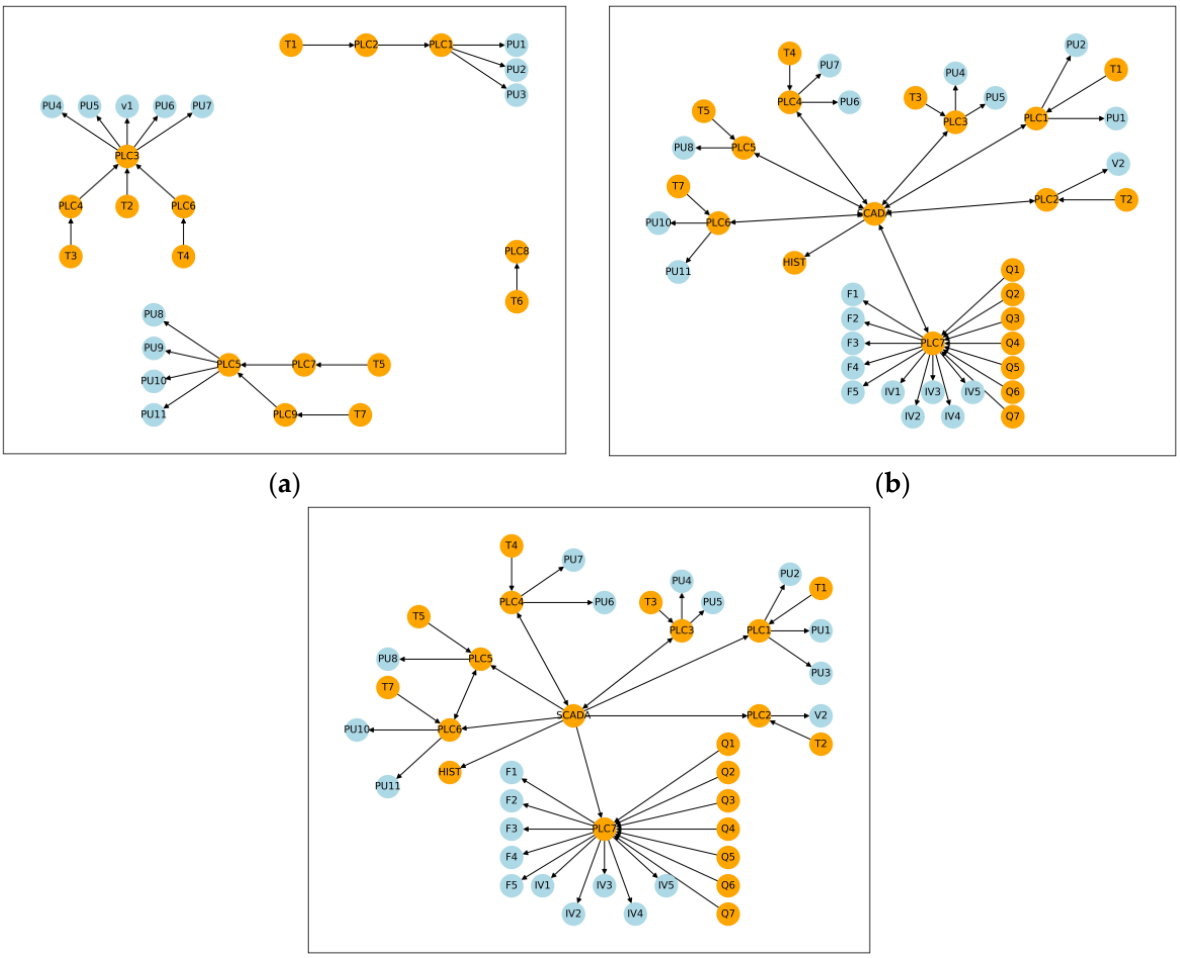


Figure 5. Different CPS network configurations investigated: (**a**) Network 1. (**b**) Network 2. (**c**) Network 3. Blue indicates physical asset nodes, orange indicates cyber component nodes, directed edges indicate the flow of information and control.

3.2. Application of Proposed Approach

The application and potential benefits of the proposed approach are illustrated on the C-Town WDS with the three different cyber network configurations outlined in Section 3.1 (see Figure 6). As can be seen from Figure 6, this is achieved by demonstrating how the approach can be used to obtain (i) quantitative estimates of the relative risk to physical assets due to their connection to cyber components (Objective 2a) and (ii) the relative contribution of cyber components to this risk (Objective 2b), as well as (iii) comparing the relative vulnerabilities of the cyber components obtained using the proposed approach that crosses the cyber–physical divide (Step 7, Figure 6) with those obtained using the commonly used approach of considering vulnerabilities in the cyber domain in isolation (Step 1, Figure 6) (Objective 2c) and (iv) comparing the relative impacts of the physical assets obtained using the proposed approach that crosses the cyber–physical divide (Step 8, Figure 6) with those obtained using the commonly used approach of considering impacts in the physical domain in isolation (Step 2, Figure 6) (Objective 2d).

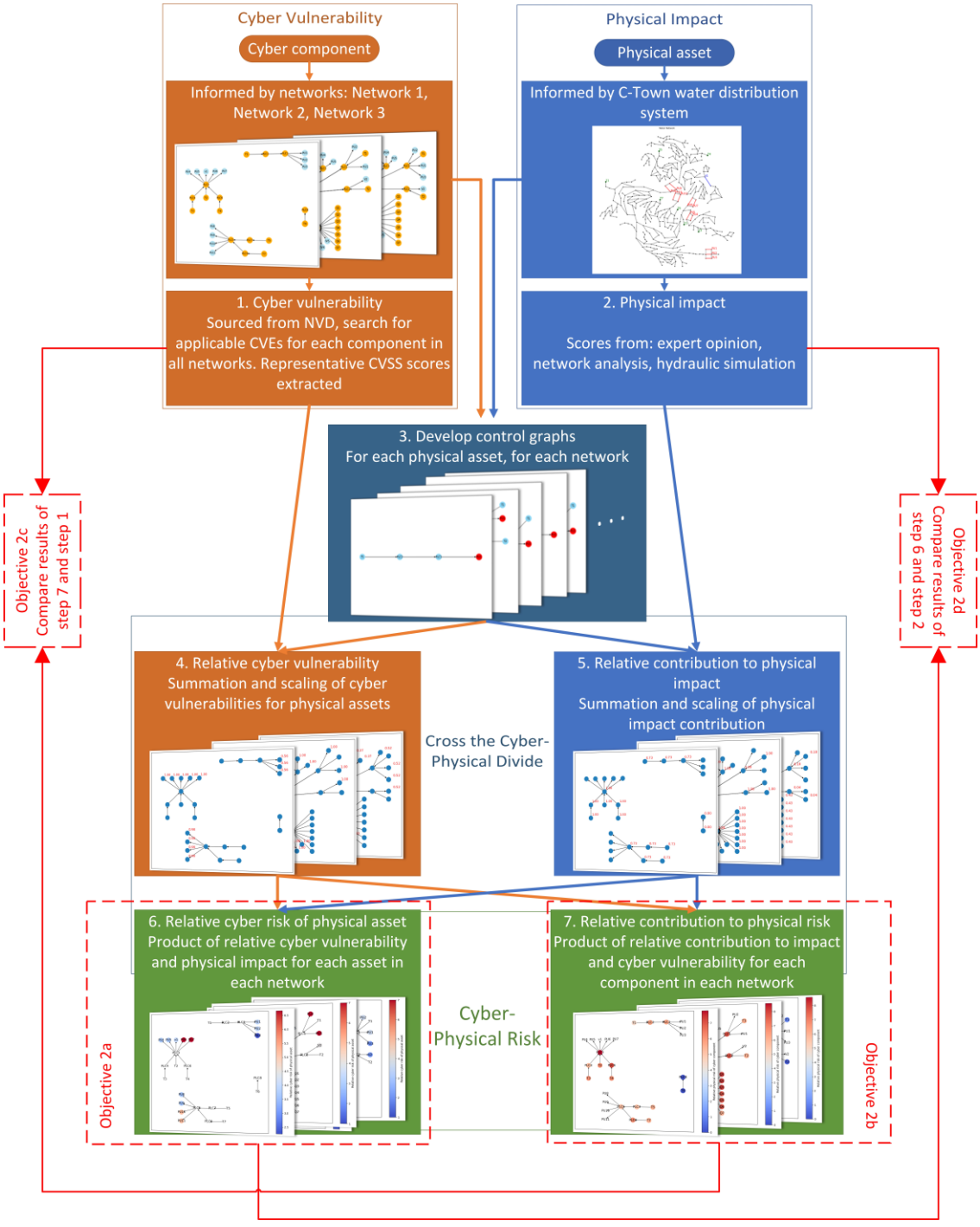


Figure 6. Details of application of proposed approach to WDS case study for three different cyber networks.

The vulnerability scores for each cyber component (Step 1, Figure 6) are representative of CVSS scores of historical CVEs relevant to industrial control system/operational technology cyber components [52], as suggested in Section 2.1. The resulting vulnerability scores for the cyber network components are given in Appendix B, Table A6. Similarly, the physical impact of each asset (Step 2, Figure 6) was determined using the approach outlined in Section 2.2. The relevant physical impact scores were informed by an analysis of the hydraulic function of the network and expert opinion. The resulting scores for the assets in the physical network are given in Appendix B, Table A7. It should be noted that

while these cyber and physical scores are realistic and every effort was made to ensure they are as representative as possible, they are primarily used for the purposes of illustrating the proposed approach.

Control graph development (Step 3, Figure 6) was undertaken using the approach outlined in Section 2.3, using a manual method to identify the relevant parent and ancestor nodes, based on the directed edges pre-defined by the flow of information and control, for the asset in question. With each of the control graphs developed for the physical assets, the cyber components relevant to each physical asset were identified. Details of the resulting control graphs for Network 1 are given in Appendix C, Figure A1a–l.

The relative cyber vulnerability (Step 4, Figure 6) and risk (Step 6, Figure 6) of each physical asset were determined using the approaches outlined in Sections 2.4 and 2.6, respectively (Objective 2a). The weightings in Equation (3) were set to 1 to facilitate the easiest-to-use and understand application of the proposed approach. The quantitative estimates of the relative risk to physical assets due to their connection to cyber components are represented as colour-coded heat maps for ease of understanding and the illustration of the visualisation capacity of the approach.

The relative contributions of cyber components to the physical impact (Step 5, Figure 6) and risk (Step 7, Figure 6) were determined using the approaches outlined in Sections 2.5 and 2.7, respectively (Objective 2b). The weightings in Equation (5) were set to 1 to facilitate the easiest-to-use and understand application of the proposed approach. The quantitative estimates of the relative contribution of the different cyber components to the risk in the physical domain are represented as colour-coded heat maps for ease of understanding.

As mentioned above, in order to assess the potential benefits of the proposed approach, (i) the relative vulnerabilities of the cyber components obtained using the proposed approach that crosses the cyber–physical divide (Step 7, Figure 6) were compared with those obtained using the commonly used approach of considering vulnerabilities in the cyber domain in isolation (Step 1, Figure 6) (Objective 2c) and (ii) the relative impacts of the physical assets obtained using the proposed approach that crosses the cyber–physical divide (Step 6, Figure 6) were compared with those obtained using the commonly used approach of considering the impacts in the physical domain in isolation (Step 2, Figure 6) (Objective 2d). This was achieved by comparing the relative risk rankings of the assets in the physical domain and the components in the cyber domain obtained using the proposed and more conventional approaches for the three different cyber network configurations considered (Figure 5).

4. Results and Discussion

4.1. Application of Proposed Approach

The heatmaps of the relative cyber risks of physical assets (Objective 2a) and the relative contribution of different cyber components to these risks (Objective 2b) for the C-Town WDS are shown in Figures 7 and 8, respectively, with the corresponding numerical values given in Tables 3 and 4. As can be seen in Table 3, due to the relative nature of the proposed risk metric (Equation (6)), the highest risk score is equal to the physical impact score (Equation (1)) at that location, with scores for all other assets scaled down from that level based on their relative cyber vulnerability (Equation (2)). Similarly, as can be seen in Table 4, due to the relative nature of the proposed metric for quantifying the relative contribution of different cyber components to risks to physical assets (Equation (7)), the highest score is equal to the cyber vulnerability score at that location (see Section 2.1), with scores for all other cyber components scaled down from that level based on their relative physical impact (Equation (4)).

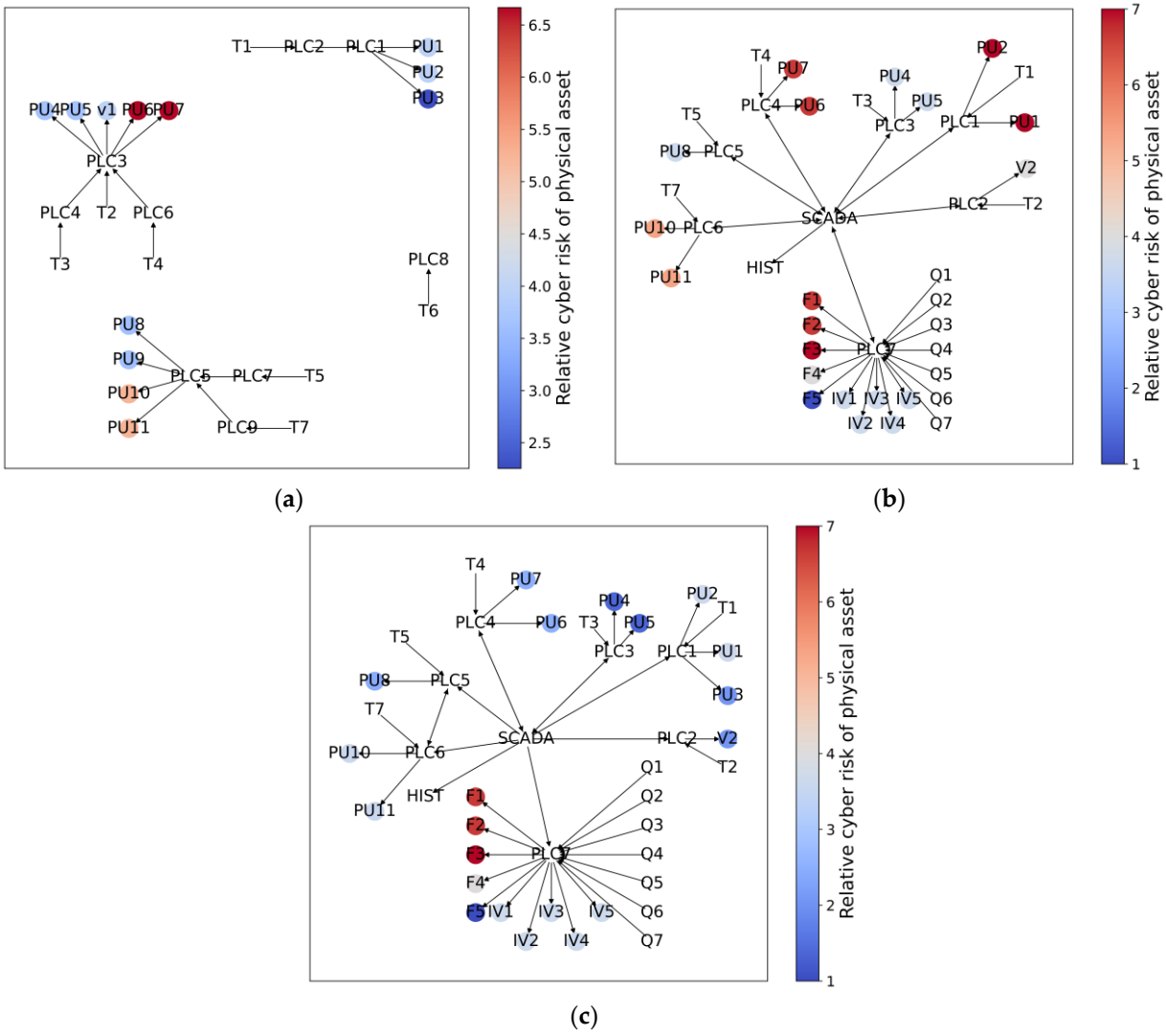


Figure 7. Heatmap of relative cyber risk of physical assets in the C-Town CPS for (**a**) Network 1. (**b**) Network 2. (**c**) Network 3.

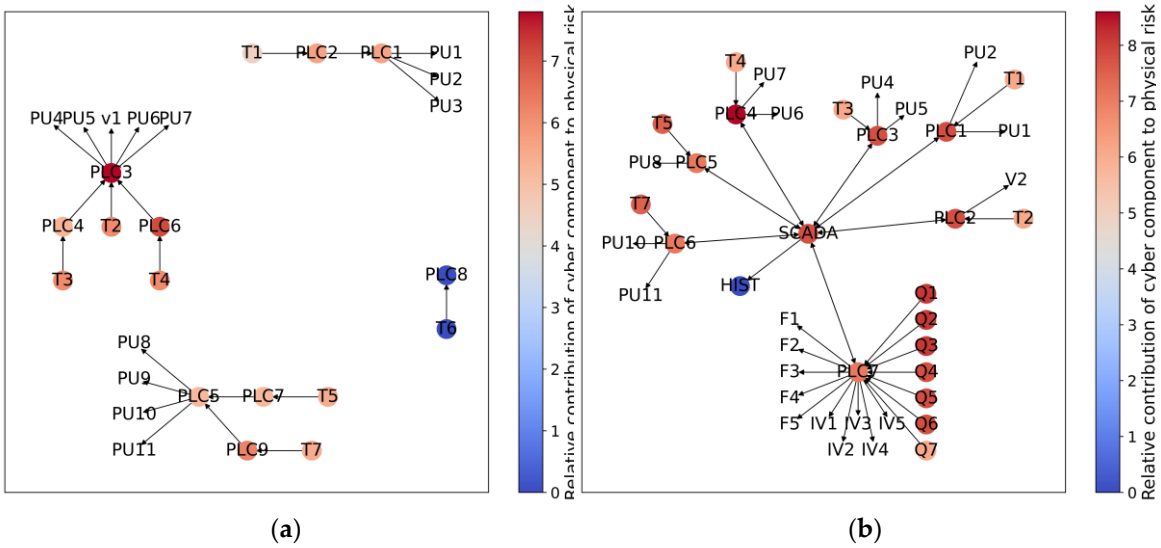
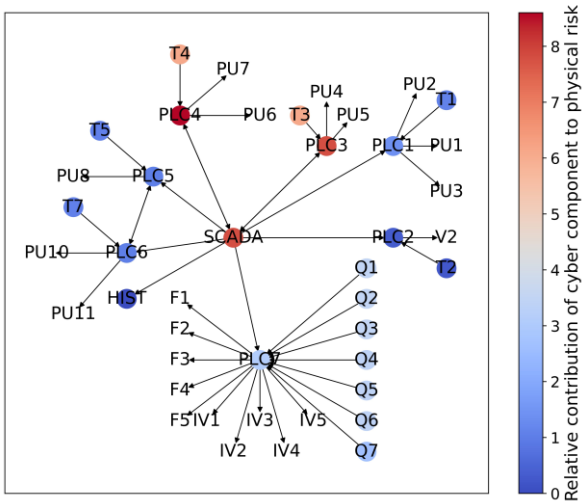


Figure 8. *Cont.*



(**c**)

Figure 8. Heatmap of relative contribution of cyber components to physical risk in the C-Town CPS for (**a**) Network 1. (**b**) Network 2. (**c**) Network 3.

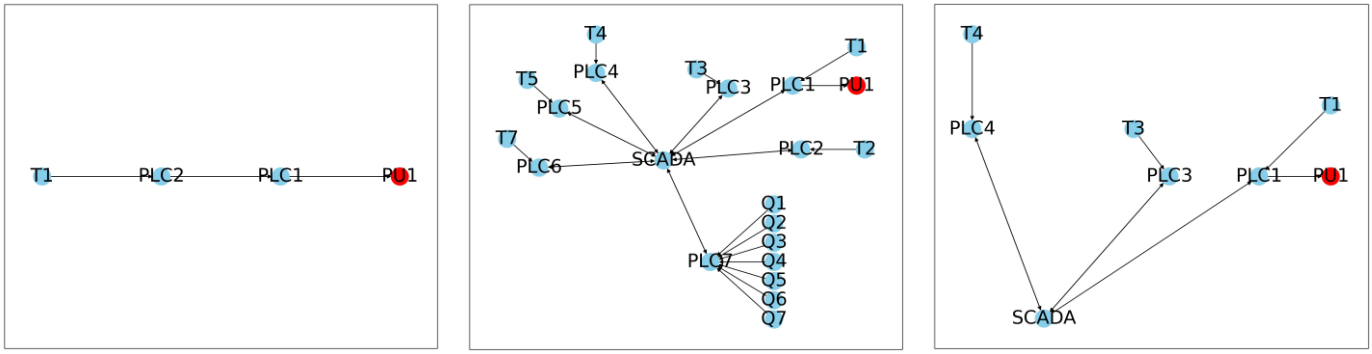
Table 3. Quantification of relative cyber risk of physical assets in Network 1, 2, and 3.

	Relative Cyber Risk of Physical Asset		
Asset	**Network 1**	**Network 2**	**Network 3**
PU1	3.95	7.00	3.62
PU2	3.95	7.00	3.62
PU3	2.25	-	2.07
PU4	3.67	3.67	2.47
PU5	3.67	3.67	1.37
PU6	6.67	6.67	6.67
PU7	6.67	6.67	6.67
PU8	3.60	3.67	3.67
PU9	3.60	-	-
PU10	5.24	5.33	3.60
PU11	5.24	5.33	3.60
v1	4.00	-	-
V2	-	4.00	2.07
F1	-	6.67	2.49
F2	-	6.67	2.49
F3	-	7.00	7.00
F4	-	4.00	4.00
F5	-	1.00	1.00
IV1	-	3.67	3.67
IV2	-	3.67	3.67
IV3	-	3.67	3.67
IV4	-	3.67	1.37
IV5	-	3.67	3.67

Table 4. Quantification of relative contribution of cyber components to physical risk in Network 1, 2, and 3.

	Relative Contribution of Cyber Components to Physical Risk		
Component	**Network 1**	**Network 2**	**Network 3**
PLC1	5.69	7.8	3.38
PLC2	5.69	7.8	7.8
PLC3	7.8	7.8	1.39
PLC4	5.3	8.6	8.6
PLC5	5.18	7.1	3.08
PLC6	7.1	7.1	1.01
PLC7	5.18	7.1	1.01
PLC8	0	-	-
PLC9	6.28	-	-
T1	4.45	6.1	1.09
T2	6.1	6.1	6.1
T3	6.1	6.1	0.24
T4	6.1	6.1	6.1
T5	5.47	7.5	1.07
T6	0	-	-
T7	5.47	7.5	1.07
Q1	-	8.1	3.51
Q2	-	8.1	3.51
Q3	-	8.1	3.51
Q4	-	7.8	3.38
Q5	-	7.8	7.8
Q6	-	7.8	3.38
Q7	-	6.1	2.65
SCADA	-	7.8	0.31
HIST	-	0	0

The importance of using a risk assessment approach for CPSs that crosses the cyber–physical divide is highlighted clearly by comparing the risk assessment results for the three different cyber network configurations (Figures 7 and 8 and Tables 3 and 4). As can be seen, there are significant differences in the cyber risk scores of particular physical assets (Figure 7 and Table 3) and the relative contributions of the different cyber components to this risk (Figure 8 and Table 4), which would not be the case if such assessments were performed solely in the physical and cyber domains, respectively. For example, as can be seen in Figure 7 and Table 3, the cyber risk of pump 1 and pump 2 (PU1, 2) changes across the three cyber network configurations. From Network 1 to 2, the cyber risk level changes due to the large increase in connectivity, where pumps 1 and 2 are now connected to all cyber components (Figures 7 and 9). However, despite still being a physically critical part of the network and also being connected to more components in the cyber network in Network 3 than in Network 1, due to higher risks elsewhere in the CPS, the relative cyber risk of both pump 1 and 2 in Network 3 has decreased.



(**a**) (**b**) (**c**)

Figure 9. Control graphs showing connectivity of PU1 across (**a**) Network 1. (**b**) Network 2. (**c**) Network 3. Red denotes node of interest and blue denotes the connected cyber components.

For similar reasons, differences exist across the different cyber network configurations for the relative contributions of particular cyber components to this risk, as can be seen in Table 4. For example, in Network 1, programmable logic controller 1 (PLC1) has a different relative contribution compared with its contribution in Network 2 as it is connected to far more physical assets. In contrast, in Network 3, it is only connected to the control of the same assets as in Network 1, but elsewhere in the network, there are components with higher connectivity and a higher relative contribution to risk, causing the contribution of PLC1 to drop accordingly (Figure 8).

Across both the physical and cyber networks, the fact that risk values change with different cyber network configurations highlights another potential mitigation option for network managers. In cases like that of Network 2, where the network is highly interconnected, if there is a particular network segment, cyber component, or physical asset that could benefit from risk mitigation, there is potential to achieve this (respective to other parts of the network) through changing the connectivity or disconnection. This can then be achieved without the additional investment required for traditional mitigation options such as network monitoring, firewalls, and other cyber-security options. This is partially explored in the existing literature, which discusses the use of other network topologies [47], and as discussed previously, further work in the development of control graphs and their use to determine cyber network-specific mitigation has already been undertaken by Barrère et al. [53].

By using an approach that crosses the cyber–physical divide, these results provide new insights into the actual risks to physical assets in CPSs (Figure 7, Table 3), the relative importance of different cyber components in causing these risks (Figure 8, Table 4), and the influence the configuration of the cyber components has on both of these. These new insights have the potential to be of significant value to both cyber and physical network managers. For example, by understanding the relative contributions cyber components make to physical risks, cyber-security professionals can implement mitigating technologies to eliminate the vulnerabilities of most importance. Due to the critical infrastructure nature of CPS networks, when multiple CVEs exist and network downtime is required to mitigate them, prioritisation can be particularly useful in managing the balance between network security and availability.

In the physical domain, understanding the cyber risk of the assets in the network can enable network operators to establish physical mitigation measures. These can potentially come in the form of the decentralised control of certain parts of the network, the implementation of backup assets, or keeping a higher volume of water in reserve in holding tanks to account for the extra risk of downtime from a pump station with high cyber risk.

4.2. Comparison with Conventional Approaches

The comparisons of the relative risk rankings of the assets in the physical domain and the components in the cyber domain obtained using the proposed and more conventional approaches for the three different cyber network configurations considered (Objectives 2c and 2d) are given in Tables 5 and 6. As can be seen, the results clearly highlight the importance of crossing the cyber–physical divide in risk assessments of CPSs. This is because the relative order of which physical assets have greater cyber risk levels (Table 5) and which cyber components are the greatest contributors to these risks (Table 6) is significantly different when the proposed approach is used. For example, the risk ranks of 58% of physical assets and 100% of cyber components change when cyber–physical connections are considered.

More specifically, as can be seen from Table 6, in Network 3, the historian server (HIST) poses the largest cyber vulnerability when assessed in isolation, but has the lowest contribution to cyber risk once the connections between the cyber and physical domains are taken into account, while water quality sensor 7 (Q7) has the lowest level of cyber vulnerability, but contributes considerably more to the cyber risk of physical assets in the network. This is because the HIST has, in this case, been assessed to have a CVE with a score of 8.8 (for example purposes, CVE-2020-24674 [54]). This could result in a denial-of-service attack, taking this component offline. In contrast, Q7 and its related cyber infrastructure has a lower cyber risk—a CVE with a CVSS of 6.1, which is the joint-lowest score in the CPS. However, these vulnerabilities in isolation ignore the impact each of these components can have in the physical domain. By considering the potential to cause physical impacts due to the compromise of these components, their relative contribution to risk changes, with the risk ranking of Q7 rising 5 ranks so that Q7 now has a greater risk contribution than the HIST (Table 6). This is because Q7, as defined by the connectivity of the network, can potentially have an impact on physical assets F1–5 and IV1–5, whereas the HIST component is disconnected from the control of any assets and has no relative contribution to the risk of any physical assets. Consequently, despite the higher isolated cyber vulnerability of the HIST, it has a lower contribution to risk when crossing the cyber–physical divide. The comparison between the conventional approach of assessing cyber vulnerability and the relative contribution to cyber risk in the network is visualised in Appendix D, Figures A2–A4.

Similarly, as can be seen in Table 5, pump 1 (PU1) has the highest physical impact when assessed conventionally within the physical domain. As a primary pump within the pump station that draws from the reservoir source—the singular input of water into the C-Town WDS—this has been assessed to have a high impact score of 7. This score embodies the slow time to failure (due to water held in tanks throughout the WDS), high potential severity of failure, and slow time to remediation. Contrastingly, pump 11 (PU11) poses a middle level of physical impact, resulting in an impact score of 5.33. However, these impacts ignore the potentially heightened level of vulnerability that each of these assets faces from a CPA occurring in the cyber domain. By considering the relative cyber risk of these physical assets, the prioritisation of risk changes. In Network 1, PU1 drops by 5 ranks and PU11 rises by 2, such that PU11 is now the priority for mitigation targeting (Table 5). This is because PU1 is vulnerable to compromises at three cyber components (T1, PLC1, and PLC2), whilst PU11 is vulnerable to compromises at five cyber components (T5, PLC7, PLC5, PLC9, and T7), including PLC9, which has one of the highest cyber vulnerability scores. As such, despite the higher potential physical impact of PU1, it has a lower level of risk when crossing the cyber–physical divide due to the level of vulnerability faced by PU11. This comparison between the conventional physical impact assessment and the cyber risk faced by physical assets is visualised in Appendix D, Figures A5–A7.

For some network connectivities, however, there is no marked difference in relative risk rank when the proposed approach is used. This is seen in the prioritisation of physical assets being consistent in Network 2. Due to the highly interconnected nature of Network 2, all physical assets are connected to all of the same cyber components, resulting in no relative

change. This is because the proposed approach determines *relative* values within a given cyber–physical system to enable the relative risks to different physical assets and the relative contribution of different cyber components to these risks to be identified. Consequently, *relative* risk values are the same whether physical components are fully connected to all cyber components or not connected to any of them. In order to determine the absolute values of risk, an independent benchmark value would need to be used in the denominator in Equations (2) and (4).

An additional insight gained from the use of the proposed approach comes from the control graph visualisations (see Appendix C, Figure A1a–l). For example, these visualisations can identify that pumps within the same pump stations have the same cyber component dependencies (Figure A1a–c). This allows for the simplification of control schemes, with a main pump being controlled by the same logic as the backup pumps, but this can also be seen as a potential risk to the CPS operation. This kind of dependency creates scenarios in which, should a pump be compromised in this station through a CPA, backup pumps are much more likely to also be unavailable. This would suggest that redundancy within the physical network for this pump station is required, or cyber redundancy is needed to ensure the pump station can stay online during a CPA event.

Table 5. Using the physical impact score only, physical assets for each network are ordered by the severity of the potential impact, the priority list for mitigation efforts. Subsequent to the application of the proposed method, they are then ordered by their level of cyber risk and the change in priority recorded. Δ represents "change in".

Network 1		Network 2		Network 3	
Physical Impact (Rank)	**Cyber Risk Altered (Δ Rank)**	**Physical Impact (Rank)**	**Cyber Risk Altered (Δ Rank)**	**Physical Impact (Rank)**	**Cyber Risk Altered (Δ Rank)**
PU1 (1)	PU6 (+2)	PU1 (1)	PU1 (0)	PU1 (1)	F3 (0)
PU2 (1)	PU7 (+2)	PU2 (1)	PU2 (0)	PU2 (1)	F2 (+2)
PU6 (3)	PU10 (+2)	F3 (1)	F3 (0)	F3 (1)	F1 (+2)
PU7 (3)	PU11 (+2)	F2 (4)	F2 (0)	F2 (4)	F4 (+6)
PU10 (5)	v1 (+2)	F1 (4)	F1 (0)	F1 (4)	IV5 (+8)
PU11 (5)	PU1 (−5)	PU6 (4)	PU6 (0)	PU6 (4)	IV3 (+8)
PU3 (7)	PU2 (−5)	PU7 (4)	PU7 (0)	PU7 (4)	IV2 (+8)
v1 (7)	PU4 (+1)	PU10 (8)	PU10 (0)	PU10 (8)	IV1 (+8)
PU4 (9)	PU5 (+1)	PU11 (8)	PU11 (0)	PU11 (8)	IV4 (+8)
PU5 (9)	PU8 (−1)	V2 (10)	V2 (0)	V2 (10)	PU1 (−9)
PU8 (9)	PU9 (−1)	F4 (10)	F4 (0)	PU3 (10)	PU2 (−9)
PU9 (9)	PU3 (−5)	IV4 (12)	IV4 (0)	F4 (10)	PU10 (−4)
		PU5 (12)	PU5 (0)	PU5 (13)	PU11 (−4)
		PU4 (12)	PU4 (0)	IV4 (13)	PU7 (−10)
		IV1 (12)	IV1 (0)	PU4 (13)	PU6 (−10)
		IV2 (12)	IV2 (0)	IV1 (13)	PU8 (−3)
		IV3 (12)	IV3 (0)	IV2 (13)	V2 (−7)
		PU8 (12)	PU8 (0)	IV3 (13)	PU3 (−7)
		IV5 (12)	IV5 (0)	PU8 (13)	PU5 (−6)
		F5 (20)	F5 (0)	IV5 (13)	PU4 (−6)
				F5 (21)	F5 (0)

Table 6. Using cyber vulnerability only, cyber components for each network are ordered by the severity of the vulnerability, the priority list for mitigation efforts. Subsequent to the application of the proposed method, they are then ordered by their level of contribution to physical risk and the change in priority recorded. Δ represents "change in".

Network 1		Network 2		Network 3	
Cyber Vulnerability (Rank)	**Relative Contribution to Physical Risk (Δ Rank)**	**Cyber Vulnerability (Rank)**	**Relative Contribution to Physical Risk (Δ Rank)**	**Cyber Vulnerability (Rank)**	**Relative Contribution to Physical Risk (Δ Rank)**
PLC9 (1)	PLC3 (+3)	HIST (1)	PLC4 (+1)	HIST (1)	PLC4 (+1)
PLC8 (1)	PLC6 (+7)	PLC4 (2)	Q3 (+1)	PLC4 (2)	PLC3 (+4)
T6 (3)	PLC9 (−2)	Q1 (3)	Q2 (+1)	Q1 (3)	SCADA (+4)
PLC1 (4)	T2 (+8)	Q3 (3)	Q1 (+1)	Q3 (3)	T3 (+14)
PLC2 (4)	T3 (+8)	Q2 (3)	PLC1 (+1)	Q2 (3)	T4 (+14)
PLC3 (4)	T4 (+8)	Q4 (6)	SCADA (+1)	PLC3 (6)	Q3 (−3)
T5 (7)	PLC1 (−3)	PLC3 (6)	Q5 (+1)	SCADA (6)	Q2 (−3)
T7 (7)	PLC2 (−3)	Q5 (6)	PLC2 (+1)	PLC2 (6)	Q1 (−3)
PLC6 (9)	T5 (−2)	SCADA (6)	Q4 (+1)	Q5 (6)	Q5 (−3)
PLC5 (9)	T7 (−2)	Q6 (6)	PLC3 (+1)	Q6 (6)	Q4 (−3)
PLC7 (9)	PLC4 (+5)	PLC1 (6)	Q6 (+1)	PLC1 (6)	Q6 (−3)
T1 (12)	PLC5 (−3)	PLC2 (6)	T5 (+1)	Q4 (6)	PLC7 (+3)
T2 (12)	PLC7 (−3)	T5 (13)	T7 (+1)	T5 (13)	Q7 (+5)
T3 (12)	T1 (−2)	T7 (13)	PLC5 (+1)	T7 (13)	PLC1 (−8)
T4 (12)	T6 (−12)	PLC6 (15)	PLC6 (+1)	PLC6 (15)	T1 (+3)
PLC4 (16)	PLC8 (−14)	PLC7 (15)	PLC7 (+1)	PLC7 (15)	T7 (−3)
		PLC5 (15)	T1 (+1)	PLC5 (15)	T5 (−3)
		T1 (18)	T4 (+1)	T1 (18)	PLC6 (−3)
		T3 (18)	T3 (+1)	T3 (18)	PLC5 (−3)
		T2 (18)	T2 (+1)	T2 (18)	PLC2 (−14)
		T4 (18)	Q7 (+1)	T4 (18)	T2 (−3)
		Q7 (18)	HIST (−21)	Q7 (18)	HIST (−21)

5. Conclusions

Critical infrastructure systems around the world have become cyber–physical systems (CPSs). These systems are becoming more advanced, resulting in more interdependence within the system and leading to an increased risk of cyber–physical attacks (CPAs). Despite the close ties between the operation of cyber and physical networks, there exists a divide between these domains in the assessment and management of risk.

This paper presents a novel approach to quantifying the cyber risk faced by physical assets in a CPS and the physical risk of a cyber component being compromised. This assessment bridges the cyber–physical divide between the two domains. This is achieved by using control graphs, assigning scores to the relevant cyber components and physical assets, and aggregating the relevant information in the other domain at each physical asset or cyber component. Furthermore, this information can then be conveyed such that physical asset managers can understand the cyber risks across their network with a heat map of the cyber risk of physical assets. By mapping this risk spatially in the physical domain rather than at the cyber network, the proposed method can facilitate decision-making and mitigation in the physical network through redundancies and other methods.

When applied to a benchmark case study CPS from the literature, the water distribution system of C-Town, the results obtained using the proposed approach showed that the quantitative estimates of the relative risk of physical assets due to their connection to cyber

components (Objective 2a) and the relative contribution of different cyber components to this risk (Objective 2b) varied significantly for the three different configurations of the cyber network considered, highlighting the importance of considering the connection between cyber and physical systems in risk assessments of cyber–physical systems. The importance of crossing the cyber–physical divide was reinforced further by the results of the comparison of the relative risk rankings obtained using the proposed and more conventional approaches to risk assessment (Objectives 2c and 2d), as there was a difference in risk prioritisation in almost all cases. In addition, the results of this comparison also showed that different network structures changed the risk posture of the CPS.

While the proposed approach is a novel way to assess cyber–physical risk within a CPS, which can provide insights that have previously not been possible, there are a number of potential issues that need to be overcome when the approach is applied in practice:

- In the case study networks tested, a CVE and corresponding CVSS score is assumed to exist at every cyber component. In real networks, this may not be the case, or the CVEs may be distributed amongst the supporting firmware, software, and communication channels between the components, making them difficult to assign to a particular component. However, other cyber vulnerability information could be used instead of the CVE and CVSS system, which could address some of these potential issues. Alternatively, these issues can be dealt with using a participatory approach with networking professionals that understand the CPS network in detail. The proposed approach is sufficiently flexible to accommodate these alternatives.
- The case study networks have simplified the sensor hardware, software, firmware, and supporting communications channels by assuming they exist as one cyber component sensor node, with an associated vulnerability. In practice, this may need to be expanded to better convey accurate information to cyber-security professionals looking to mitigate these risks.
- The assumption has been made that any failure from a vulnerability at a component will cause a downstream failure of the physical asset. Whilst this is a necessary simplification to make for the assessment process, this does not hold true in all situations—some cyber vulnerabilities are specific to the confidentiality of data as opposed to the availability of the service that facilitates operations. Similarly, some cyber-related incidents may not be CPA events, but other forms of intrusion, such as to gain information or a foothold into the network for further exploitation. Despite this, the assumption that any vulnerability can cause a failure is a worst-case-scenario outlook and can be considered appropriate for a risk assessment for such critical infrastructure.
- The proposed assessment methodology is difficult to validate in practice. Due to the human agency involved in a CPA, validation of a method such as this is impractical. In order to combat this, when using this approach, the individual parts of the method that can be validated should be. These include undertaking process and logic validation through consultation with peers [55] regarding the scoring determined for each component and the development of the network graph, to ensure the correct flow of information and control.

Despite these potential limitations, the results obtained clearly demonstrate the need for and value of the proposed approach. By crossing the cyber–physical divide, the approach is able to provide more accurate assessments of the relative risk of physical assets that result from their connection to cyber components, as well as more accurate assessments of the relative contribution of different cyber components to this risk, showing promise in its ability to join the often disparate cyber and physical risk assessment methodologies. This also opens to the door to more effective ways of prioritising cyber risk mitigation strategies.

Author Contributions: Conceptualisation, C.K., H.R.M. and H.v.D.; data curation, C.K.; formal analysis, C.K.; funding acquisition, H.R.M.; investigation, C.K.; methodology, C.K., H.R.M., H.v.D. and A.C.Z.; project administration, C.K. and H.R.M.; resources, C.K.; software, C.K.; supervision, H.R.M., H.v.D. and A.C.Z.; validation, C.K.; visualisation, C.K.; writing—original draft, C.K.; writing—review and editing, H.R.M., H.v.D. and A.C.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was undertaken while the lead author was supported by funding from the Australian Department of Education Skills and Employment, Australian Government Research Training Program Scholarship. SA Water Corporation, the industry partner, has also provided funding.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: The authors would like to acknowledge the industry partner, SA Water Corporation, for the support they have provided.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A Alternative Mathematical Methods

Table A1. Alternative options for the calculation of the cyber vulnerability of physical assets (Equation (2)) and for the aggregation of these scores (Equation (3)). Each equation is represented for physical asset k, connected to cyber component j, with m relevant cyber components.

Summation Option (Equation (2))	Equation	Notes
Summation	Equation (2)	Recommended due to simplicity of application and increasing nature of score.
Independent event probabilities	$v^C_{p,k} = 1 - \frac{\left(\prod_{j=1}^{m}\left(1 - V^C_{c,j}\right)\right)}{10}$	Captures the marginal increase in vulnerability due to new vulnerabilities effectively. Due to the skew of CVSS scores toward the high-end, as the number of vulnerabilities increases, values asymptote to maximum possible value (i.e., 10).
Arithmetic mean	$v^C_{p,k} = \frac{1}{m}\sum_{j=1}^{m} V^C_{c,j}$	Simple to use, but the vulnerability can be reduced significantly by a CVSS with a low score. This is counter-intuitive, as vulnerabilities that are added, even if they are not severe, should not reduce the overall vulnerability.
Geometric mean	$v^C_{p,k} = \prod_{j=1}^{m} V^{C\ \frac{1}{m}}_{c,j}$	Consistent with the approach of probabilities of independent events and less sensitive to outliers. Fails if there is a cyber component with no vulnerability (score of 0).
Aggregation option (Equation (3))	**Equation**	**Notes**
Relative to maximum	Equation (3)	Recommended. Enables the comparison of values within the CPS network.
Relative to benchmark	$V^C_{p,k} = \frac{v^C_{p,k}}{Benchmark}$	Enables the comparison of values to those of other networks outside the CPS being assessed. Requires choice of suitable/meaningful benchmark value.
Absolute value	$V^C_{p,k}$	Does not account for the effect of numerous components and does not provide a base from which to assess.

Appendix B Case Study Details

The codes used for assets and components within the three case study networks are detailed in Table A2.

Table A2. Legend of asset and component codes used within the three case study networks.

Asset/Component	Codes
Pumps	PU1–11
Valve	V1/V2
Isolation valves	IV1–5
Flusher	F1–5
Tank level sensors	T1–7
Programmable logic controllers	PLC1–9
Water quality sensors	Q1–5
Supervisory control and data acquisition unit	SCADA
Historian server	HIST

Network 1 (Figure 5a) of the C-Town CPS has an associated SCADA cyber network developed to describe how the physical assets are controlled [15]. The key cyber components and the control scheme are detailed in Table A3, with this control scheme originally developed in [15]. As stated above, this has been adapted to investigate a more disconnected cyber network structure in the CPS. As can be seen, the programmable logic controllers (PLC) are listed, along with information on which sensors and/or actuators they are connected to. The connected physical assets to be assessed are identified by the actuators, which directly interact with the asset and these actuators are listed with their corresponding controlling sensor. Where this sensor is associated with another PLC, a connection between the actuators' and sensors' PLC exists. The physical assets to be assessed are pumps 1 through 11 (PU1–PU11) and valve 1 (v1). This basic structure is maintained for Network 2 and 3, with the changes listed below.

Table A3. Control scheme of the C-Town CPS, adapted with permission from [15]. 2017, American Society of Civil Engineers.

Controlling PLC	Connected Sensors and Actuators (Corresponding Sensor)
PLC1	PU1 (T1), PU2 (T1), PU3 (N/A)
PLC2	T1
PLC3	T2, V1 (T2), PU4 (T3), PU5 (T3), PU6 (T4), PU7 (T4)
PLC4	T3
PLC5	PU8 (T5), PU9 (N/A), PU10 (T7), PU11 (T7)
PLC6	T4
PLC7	T5
PLC8	T6
PLC9	T7

Network 2 of the C-Town CPS adapts this network to include water quality-related infrastructure and changes the control scheme to a more interconnected and centralised cyber network, see Table A4, with changes informed by [27] and Figure 5b.

Table A4. Changes from Network 1 to Network 2 of the C-Town CPS.

Components/Assets and Controls	Elements
Additional sensors	Seven additional water quality sensors added, placed at junctions J301, J385, J109, J292, J494, J67, J297. Designated here as Q1–7.
DMA isolation valves actuators	Five additional isolation valves and actuators. Placed at pipes P409, P424, P310, P796, and P237. Designated here as IV1–5.

Table A4. *Cont.*

Components/Assets and Controls	Elements
DMA isolation valves control logic	Control logic implemented through PLC7, 'If concentration readings of ANY sensor above 0.001 mg/L close ALL DMA isolation valves'
Flushing units	New flushing nodes adjacent to present nodes J1056, J416, J1208, J185, and J87. These are designated here as F1–5.
Flushing unit control logic	Control logic implemented through PLC7, 'If concentration readings of the DMA's sensor above 0.001 mg/L open the DMA's flushing unit's isolation valve'
Historian	Historian cyber component added, receiving information from the SCADA system component.
SCADA	A central SCADA system cyber component added, acting as a central hub for all control and information flow.
Removed pump	Pump 3 removed from the active network
Valve change	Valve 1 not considered; Valve 2 used
Moved sensors	T1 connected to PLC1, T2 and V2 connected to PLC2, T3 connected to PLC3, PU6 and PU7 and T4 connected to PLC4, T5 connected to PLC5, PU10 and PU11 and T7 connected to PLC6

Network 3 includes the same infrastructure as Network 2; however, it incorporates a different realisation of the connectivity of the network (Table A5), see Figure 5c. This realisation is born from an analysis of the control of the CPS and communication channels through which information can potentially flow. For example, the connection between PLC7 and the SCADA node is changed to a uni-directional connection, as none of the data procured by sensors in this network segment are used for the control of physical assets in other network segments. These changes are made in an attempt to understand the generality of the assessment method across various network structures and connectivity.

Table A5. Changes in connectivity from Network 2 to Network 3.

Connected Nodes	Change
SCADA/PLC7	Now a one-way connection from SCADA to PLC7
SCADA/PLC6	Now a one-way connection from SCADA to PLC6
SCADA/PLC5	Now a one-way connection from SCADA to PLC5
PLC5/PLC6	New multi-direction connection between PLC5 and PLC6
PLC1/PU3	Re-added PU3, controlled by PLC1

The following tables (Tables A6 and A7) are the quantification of the cyber vulnerabilities, sourced from [52] and physical impact scores used within the C-Town CPS case study.

Table A6. Cyber component vulnerability scores.

CYBER Component	Example CVE CVSS Score
PLC1	7.8
PLC2	7.8
PLC3	7.8
PLC4	8.6
PLC5	7.1
PLC6	7.1
PLC7	7.1

Table A6. *Cont.*

CYBER Component	Example CVE CVSS Score
PLC8	8.6
PLC9	8.6
T1	6.1
T2	6.1
T3	6.1
T4	6.1
T5	7.5
T6	8.2
T7	7.5
HIST	8.8
SCADA	7.8
Q1	8.1
Q2	8.1
Q3	8.1
Q4	7.8
Q5	7.8
Q6	7.8
Q7	6.1

Table A7. Physical asset impact scores.

Physical Asset	Physical Impact Score
PU1	7.0
PU2	7.0
PU3	4.0
PU4	3.67
PU5	3.67
PU6	6.67
PU7	6.67
PU8	3.67
PU9	3.67
PU10	5.33
PU11	5.33
V1	4.00
V2	4.0
F1	6.67
F2	6.67
F3	7.0
F4	4.0
F5	1.0
IV1	3.67
IV2	3.67
IV3	3.67
IV4	3.67
IV5	3.67

Appendix C Network 1 Control Graph Examples

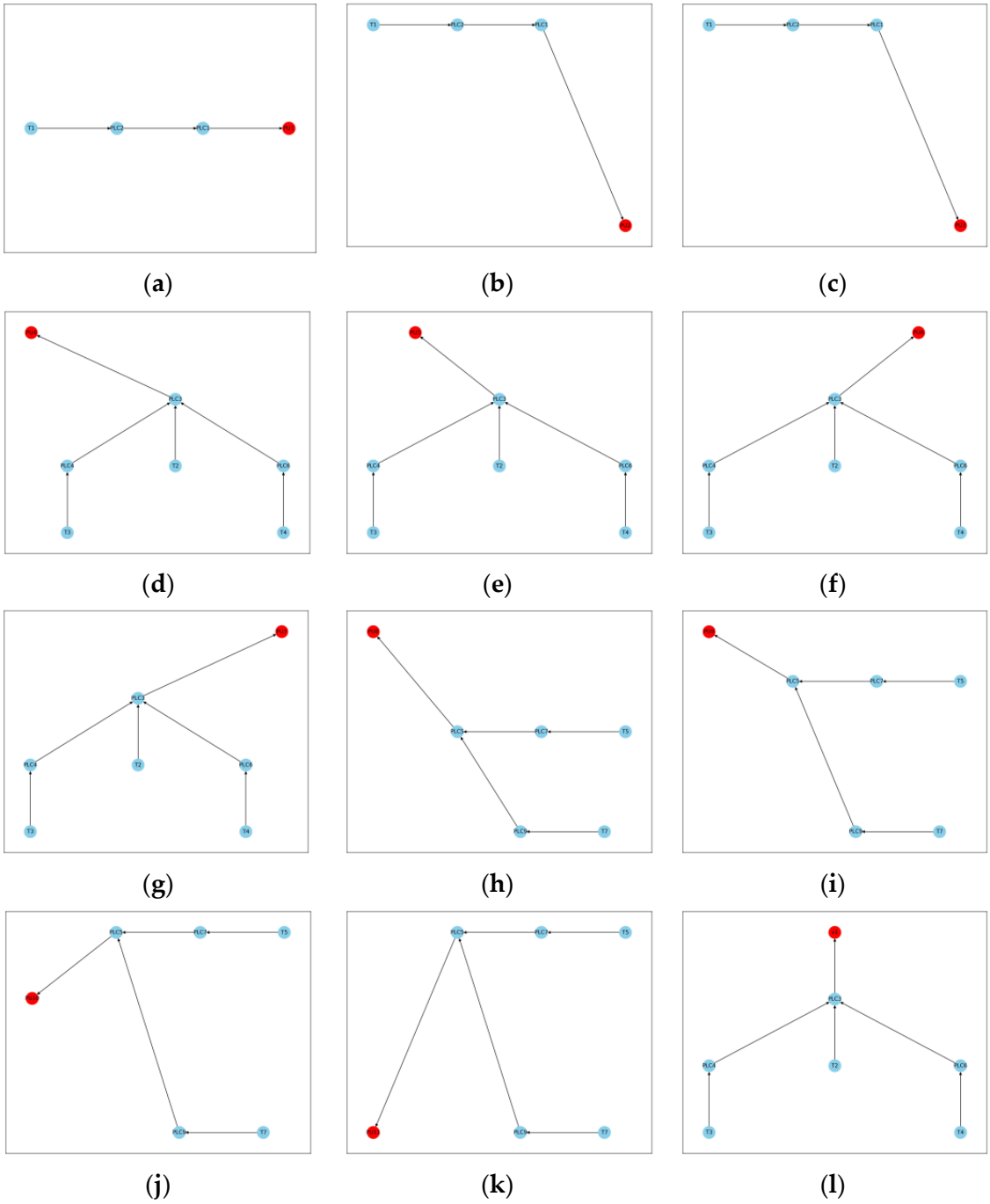


Figure A1. Control graphs developed for Network 1, for physical asset: (**a**) PU1, (**b**) PU2, (**c**) PU3, (**d**) PU4, (**e**) PU5, (**f**) PU6, (**g**) PU7, (**h**) PU8, (**i**) PU9, (**j**) PU10, (**k**) PU11, (**l**) v1. Red denotes the physical asset in question, blue the connected cyber components.

Appendix D Case Study Comparison Result Heatmaps

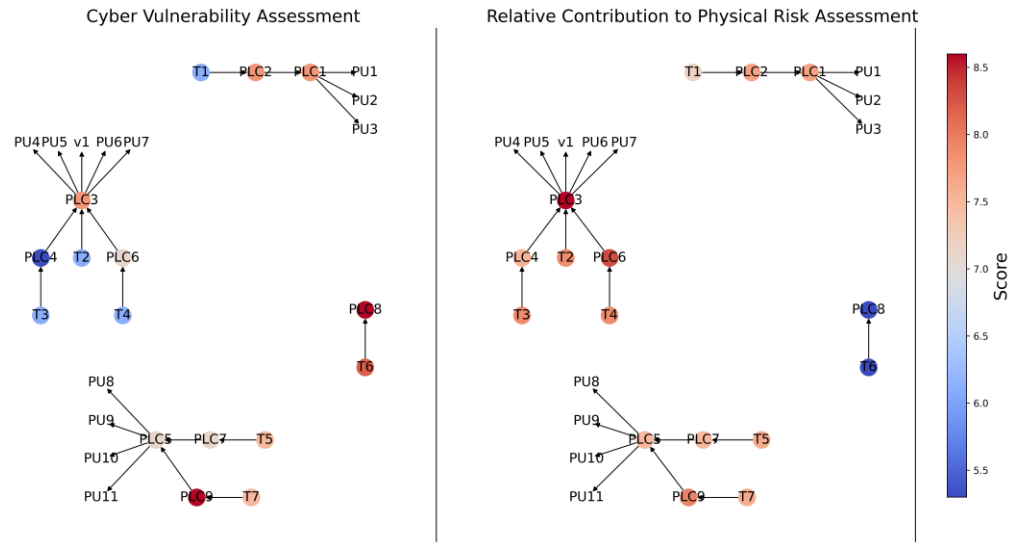


Figure A2. Comparison between a solely cyber vulnerability assessment, and an assessment of the relative contribution of cyber components to physical risk for cyber components in Network 1 of the C-Town CPS.

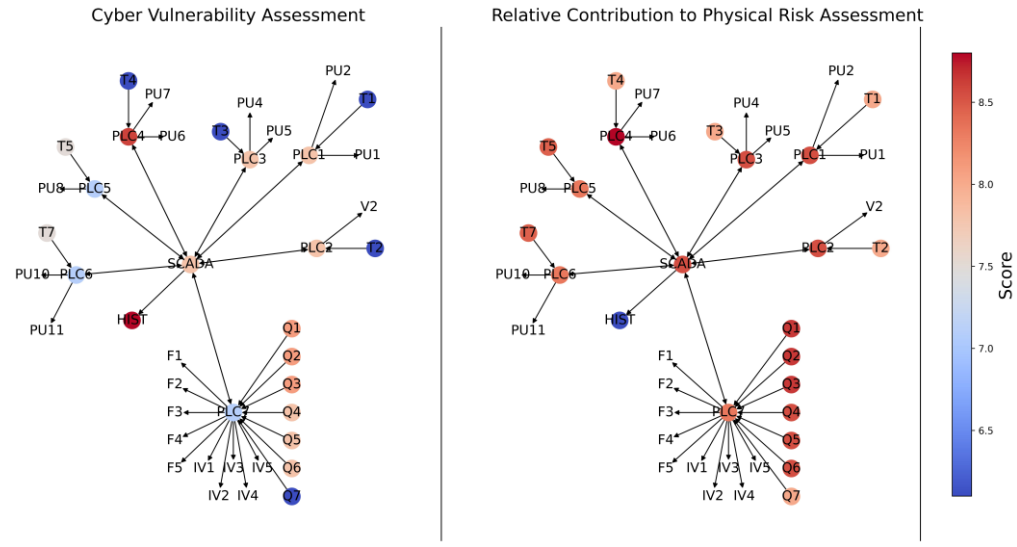


Figure A3. Comparison between a solely cyber vulnerability assessment, and an assessment of the relative contribution of cyber components to physical risk for cyber components in Network 2 of the C-Town CPS.

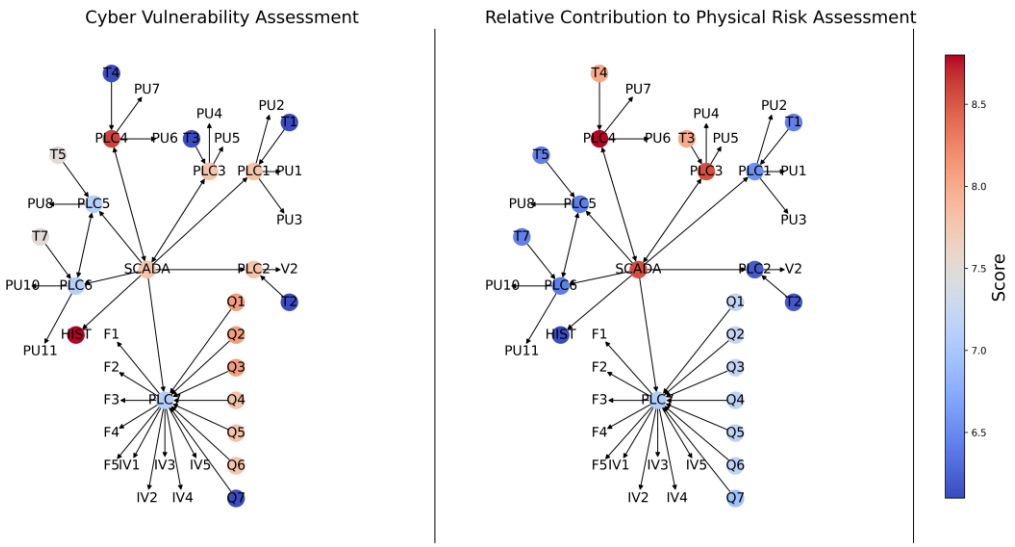


Figure A4. Comparison between a solely cyber vulnerability assessment, and an assessment of the relative contribution of cyber components to physical risk for cyber components in Network 3 of the C-Town CPS.

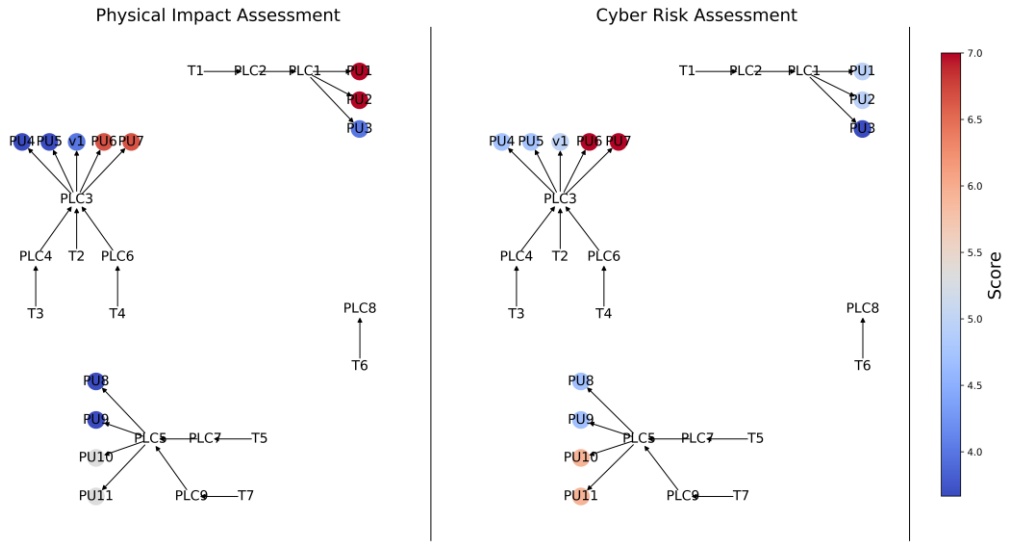


Figure A5. Comparison between a solely physical impact assessment, and the relative cyber risk assessment for physical assets in Network 1 of the C-Town CPS.

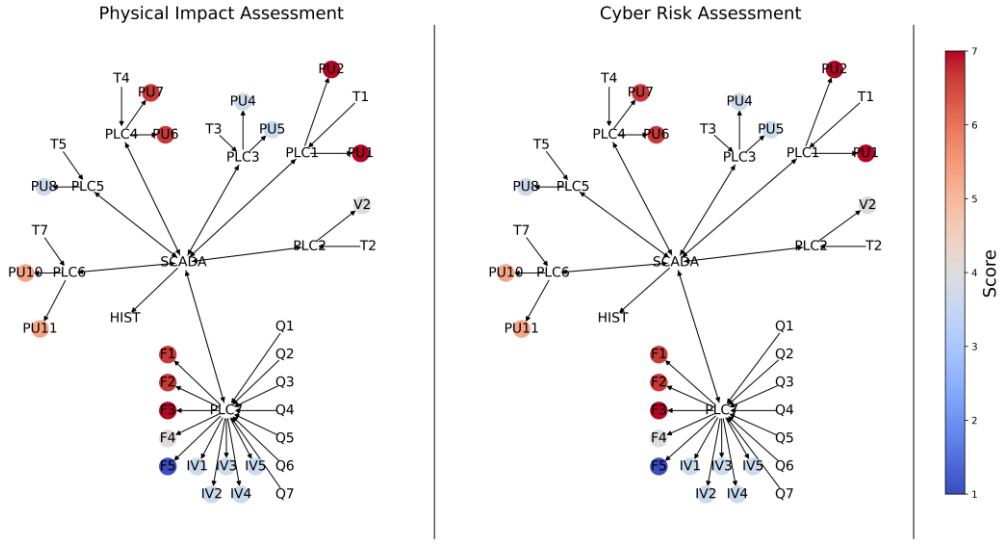


Figure A6. Comparison between a solely physical impact assessment, and the relative cyber risk assessment for physical assets in Network 2 of the C-Town CPS.

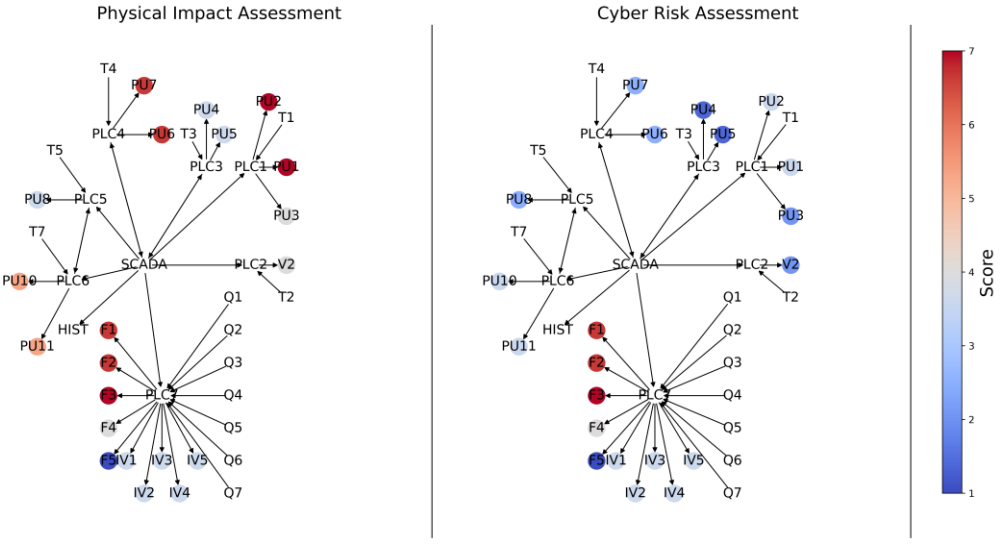


Figure A7. Comparison between a solely physical impact assessment, and the relative cyber risk assessment for physical assets in Network 3 of the C-Town CPS.

References

1. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4.
2. Adedeji, K.B.; Hamam, Y. Cyber-Physical Systems for Water Supply Network Management: Basics, Challenges, and Roadmap. *Sustainability* **2020**, *12*, 9555. [CrossRef]
3. Cardenas, A.A.; Amin, S.; Sastry, S. Secure Control: Towards Survivable Cyber-Physical Systems. In Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008.
4. Wang, Z.; Song, H.; Watkins, D.W.; Ong, K.G.; Xue, P.; Yang, Q.; Shi, X. Cyber-physical systems for water sustainability: Challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 216–222. [CrossRef]
5. Energetics Incorporated. *Foundations for Innovation in Cyber-Physical Systems*; National Institute of Standards and Technology (NIST): Columbia, MD, USA, 2013.
6. Wolf, W. Cyber-physical systems. *Computer* **2009**, *42*, 88–89. [CrossRef]
7. Gill, H. From vision to reality: Cyber-physical systems. In Proceedings of the HCSS National Workshop on New Research Directions for High Confidence Transportation CPS: Automotive, Aviation, and Rail, Washington, DC, USA, 18–20 November 2008; pp. 1–29.

8. Tuptuk, N.; Hazell, P.; Watson, J.; Hailes, S. A systematic review of the state of cyber-security in water systems. *Water* **2021**, *13*, 81. [CrossRef]
9. Djenna, A.; Harous, S.; Saidouni, D.E. Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Appl. Sci.* **2021**, *11*, 4580. [CrossRef]
10. Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S. *Guide to Operational Technology (OT) Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
11. Dragos, I. *ICS/OT Cybersecurity Year in Review 2022*; Dragos: Hanover, MD, USA, 2023.
12. Clark, R.M.; Panguluri, S.; Nelson, T.D.; Wyman, R.P. Protecting drinking water utilities from cyberthreats. *Am. Water Work. Assoc.* **2017**, *109*, 50–58. [CrossRef]
13. Chu, Z.; Pinceti, A.; Kaviani, R.; Khodadadeh, R.; Li, X.; Zhang, J.; Saikumar, K.; Sahraei-Ardakani, M.; Mosier, C.; Podmore, R. A Verifiable Framework for Cyber-Physical Attacks and Countermeasures in a Resilient Electric Power Grid. *arXiv* **2021**, arXiv:2104.13908.
14. Rasekh, A.; Hassanzadeh, A.; Mulchandani, S.; Modi, S.; Banks, M.K. Smart Water Networks and Cyber Security. *J. Water Resour. Plan. Manag.* **2016**, *142*, 01816004. [CrossRef]
15. Taormina, R.; Galelli, S.; Tippenhauer, N.O.; Salomons, E.; Ostfeld, A. Characterizing Cyber-Physical Attacks on Water Distribution Systems. *J. Water Resour. Plan. Manag.* **2017**, *143*, 04017009. [CrossRef]
16. Moraitis, G.; Nikolopoulos, D.; Bouziotas, D.; Lykou, A.; Karavokiros, G.; Makropoulos, C. Quantifying Failure for Critical Water Infrastructures under Cyber-Physical Threats. *J. Environ. Eng.* **2020**, *146*, 04020108. [CrossRef]
17. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
18. Shin, S.; Lee, S.; Burian, S.J.; Judi, D.R.; McPherson, T. Evaluating Resilience of Water Distribution Networks to Operational Failures from Cyber-Physical Attacks. *J. Environ. Eng.* **2020**, *146*, 04020003. [CrossRef]
19. Fan, H.; Ni, M.; Zhao, L.; Li, M. Review of cyber physical system and cyber attack modeling. In Proceedings of the 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Nanjing, China, 20–23 September 2020.
20. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064. [CrossRef]
21. Alanazi, M.; Mahmood, A.; Chowdhury, M.J.M. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Comput. Secur.* **2023**, *125*, 103028. [CrossRef]
22. Magar, A. *State-of-the-art in Cyber Threat Models and Methodologies*; Defence Research and Development Canada: Ottawa, ON, Canada, 2016.
23. Cassottana, B.; Aydin, N.Y.; Tang, L.C. Quantitative Assessment of System Response during Disruptions: An Application to Water Distribution Systems. *J. Water Resour. Plan. Manag.* **2021**, *147*. [CrossRef]
24. Qi, Z.; Zheng, F.; Guo, D.; Zhang, T.; Shao, Y.; Yu, T.; Zhang, K.; Maier, H.R. A Comprehensive Framework to Evaluate Hydraulic and Water Quality Impacts of Pipe Breaks on Water Distribution Systems. *Water Resour. Res.* **2018**, *54*, 8174–8195. [CrossRef]
25. Broad, D.R.; Maier, H.R.; Dandy, G.C.; Nixon, J.B. Estimating Risk Measures for Water Distribution Systems Using Metamodels. In *Impacts of Global Climate Change*; American Society of Civil Engineers: Reston, VA, USA, 2005; pp. 1–12. [CrossRef]
26. Leszczyna, R. Review of cybersecurity assessment methods: Applicability perspective. *Comput. Secur.* **2021**, *108*, 102376. [CrossRef]
27. Nikolopoulos, D.; Makropoulos, C. Stress-testing water distribution networks for cyber-physical attacks on water quality. *Urban Water J.* **2021**, *19*, 256–270. [CrossRef]
28. Commonwealth of Australia. *Essential Eight Maturity Model*; Directorate, A.S., Ed.; Commonwealth of Australia: Canberra, Australia, 2023.
29. Hussain, S.; Kamal, A.; Ahmad, S.; Rasool, G.; Iqbal, S. Threat modelling methodologies: A survey. *Sci. Int.* **2014**, *26*, 1607–1609.
30. Tatam, M.; Shanmugam, B.; Azam, S.; Kannoorpatti, K. A review of threat modelling approaches for APT-style attacks. *Heliyon* **2021**, *7*, e05969. [CrossRef] [PubMed]
31. Nweke, L.O.; Wolthusen, S. A Review of Asset-Centric Threat Modelling Approaches. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 1–6. [CrossRef]
32. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based threat modeling for cyber-physical systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 26–29 September 2017.
33. Fernandez, E.B. Threat modeling in cyber-physical systems. In Proceedings of the 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Auckland, New Zealand, 8–12 August 2016; pp. 448–453.
34. FIRST. Common Vulnerability Scoring System. 2024. Available online: https://www.first.org/cvss/ (accessed on 23 November 2023).
35. *ISO 31000:2018(en)*; Risk management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018.
36. Cheimonidis, P.; Rantos, K. Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. *Future Internet* **2023**, *15*, 324. [CrossRef]

37. Wolthuis, R.; Phillipson, F.; Jongsma, H.-J.; Langenkamp, P. A framework for quantifying cyber security risks. *Cyber Secur. A Peer-Rev. J.* **2021**, *4*, 302–316.
38. Peng, X.; Li, J.H.; Xinming, O.; Peng, L.; Levy, R. Using Bayesian networks for cyber security analysis. In Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), Chicago, IL, USA, 28 June–1 July 2010.
39. Huang, K.; Zhou, C.; Tian, Y.-C.; Yang, S.; Qin, Y. Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Electron.* **2018**, *65*, 8153–8162. [CrossRef]
40. The MITRE Corporation. *Common Vulnerability and Exposures Program*; The MITRE Corporation: McLean, VA, USA, 2024.
41. Hashimoto, T.; Stedinger, J.R.; Loucks, D.P. Reliability, resiliency, and vulnerability criteria for water resource system performance evaluation. *Water Resour. Res.* **1982**, *18*, 14–20. [CrossRef]
42. Diao, K.; Sweetapple, C.; Farmani, R.; Fu, G.; Ward, S.; Butler, D. Global resilience analysis of water distribution systems. *Water Res.* **2016**, *106*, 383–393. [CrossRef]
43. Butler, D.; Ward, S.; Sweetapple, C.; Astaraie-Imani, M.; Diao, K.; Farmani, R.; Fu, G. Reliable, resilient and sustainable water management: The Safe & SuRe approach. *Glob. Chall.* **2017**, *1*, 63–77. [CrossRef]
44. Nikolopoulos, D.; Moraitis, G.; Bouziotas, D.; Lykou, A.; Karavokiros, G.; Makropoulos, C. Cyber-Physical Stress-Testing Platform for Water Distribution Networks. *J. Environ. Eng.* **2020**, *146*, 04020061. [CrossRef]
45. Nicolaou, N.; Eliades, D.G.; Panayiotou, C.; Polycarpou, M.M. Reducing Vulnerability to Cyber-Physical Attacks in Water Distribution Networks. In Proceedings of the 2018 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), Porto, Portugal, 10–13 April 2018; pp. 16–19.
46. Guan, J.; Graham, J.H.; Hieb, J.L. A digraph model for risk identification and mangement in SCADA systems. In Proceedings of the 2011 IEEE International Conference on Intelligence and Security Informatics, Beijing, China, 10–12 July 2011.
47. Meng, F.; Fu, G.; Farmani, R.; Sweetapple, C.; Butler, D. Topological attributes of network resilience: A study in water distribution systems. *Water Res.* **2018**, *143*, 376–386. [CrossRef]
48. Hwang, H.; Lansey, K. Water Distribution System Classification Using System Characteristics and Graph-Theory Metrics. *J. Water Resour. Plan. Manag.* **2017**, *143*, 04017071. [CrossRef]
49. Ostfeld, A.; Salomons, E.; Ormsbee, L.; Uber, J.G.; Bros, C.M.; Kalungi, P.; Burd, R.; Zazula-Coetzee, B.; Belrain, T.; Kang, D.; et al. Battle of the Water Calibration Networks. *J. Water Resour. Plan. Manag.* **2012**, *138*, 523–532. [CrossRef]
50. Taormina, R.; Galelli, S.; Tippenhauer, N.O.; Ostfeld, A.; Salomons, E. Assessing the Effect of Cyber-Physical Attacks on Water Distribution Systems. In *World Environmental and Water Resources Congress 2016*; American Society of Civil Engineers: Reston, VA, USA, 2016; pp. 436–442. [CrossRef]
51. Douglas, H.C.; Taormina, R.; Galelli, S. Pressure-Driven Modeling of Cyber-Physical Attacks on Water Distribution Systems. *J. Water Resour. Plan. Manag.* **2019**, *145*, 06019001. [CrossRef]
52. Byers, R.; Turner, C.; Brewer, T. National Vulnerability Database. 2022. Available online: https://data.nist.gov/od/id/1E0F15DAAEFB84E4E0531A5706813DD8436 (accessed on 20 November 2023).
53. Barrère, M.; Hankin, C.; Nicolaou, N.; Eliades, D.G.; Parisini, T. Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. *J. Inf. Secur. Appl.* **2020**, *52*, 102471. [CrossRef]
54. CVE-2020-24674. Available online: https://nvd.nist.gov/vuln/detail/CVE-2020-24674 (accessed on 20 November 2023).
55. Chen, S.H.; Pollino, C.A. Good practice in Bayesian network modelling. *Environ. Model. Softw.* **2012**, *37*, 134–145. [CrossRef]

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.