applied sciences

MDPI

Article

Digital Twin of Food Supply Chain for Cyber Exercises

Tuomo Sipola *, Tero Kokkonen, Markku Puura, Kalle-Eemeli Riuttanen, Kari Pitkäniemi, Elina Juutilainen and Teemu Kontio

Institute of Information Technology, Jamk University of Applied Sciences, 40100 Jyväskylä, Finland; tero.kokkonen@jamk.fi (T.K.)
* Correspondence: tuomo.sipola@jamk.fi; Tel.: +358-50-310-3339

Abstract: The food supply chain is a critical part of modern societies. As with other facets of life, it is thoroughly digitalized, and uses network connections. Consequently, the cyber security of the supply chain becomes a major concern as new threats emerge. Cyber ranges can be used to prepare for such cyber security threats by creating realistic scenarios mimicking real-world systems and setups. Organizations can participate in cyber security training and exercises that present them with these scenarios. Cyber ranges can also be used efficiently for research and development activities, because cyber ranges are realistic environments and can be used for the generation of realistic data. The aim of this study is to describe a digital twin of the food supply chain built for cyber range-based cyber security exercises. The digital twin mirrors the real-world situation with sufficient detail, as required by the cyber exercise. This research uses the design science methodology, which describes the construction and evaluation of the proposed system. The study explains the general capabilities of the food supply chain digital twin and its use in the cyber range environment. Different parts of the supply chain are implemented as Node.js services that run on the Realistic Global Cyber Environment (RGCE) platform. The flow of ingredients and products is simulated using an apparatus model and message queues. The digital twin was demonstrated in a real live cyber exercise. The results indicate that the apparatus approach was a scalable and realistic enough way to implement the digital twin. The main limitations of the implemented system are the implementation on one specific platform, and the need for more feedback from multiple exercises. Creation of a digital twin enables the use of cyber ranges to train organizations related to the food supply chain.

Keywords: cyber security; cyber exercise; digital twin; critical systems; food supply chain

Citation: Sipola, T.; Kokkonen, T.; Puura, M.; Riuttanen, K.-E.; Pitkäniemi, K.; Juutilainen, E.; Kontio, T. Digital Twin of Food Supply Chain for Cyber Exercises. *Appl. Sci.* **2023**, *13*, 7138. https://doi.org/10.3390/app13127138

Academic Editor: Jose Machado

Received: 28 April 2023
Revised: 5 June 2023
Accepted: 13 June 2023
Published: 14 June 2023

1. Introduction

The food supply chain represents the interlinked flow of raw materials to food products. It consists of food production, processing, distribution, and retail [1]. Such systems include traditional and modern Internet of Things (IoT) devices. As a critical system, the resilience of the supply chain against any disturbances is important [2], including environmental [3] and pandemic [4] reasons. Cyber threats against supply chains have been identified earlier, e.g., using target IT systems to facilitate weapons trafficking, pharma sabotage, or cargo theft [5]. Similar threats could target any supply chain, taking into account their characteristics. The concept of the supply chain covers all aspects of society, including the use of subsidy schemes, which can be modeled mathematically [6]. Demand disruptions are possible, and the effects of such events can be modeled in a simplified setup of one manufacturer and one retailer [7]. Figure 1 illustrates the basic schematic structure of the food supply chain, adapted from [1,8].

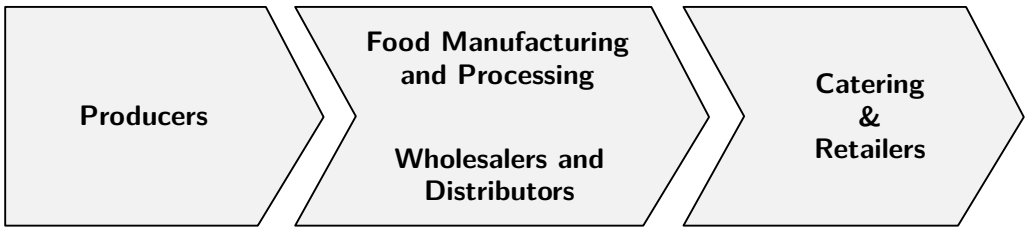

Figure 1. Food supply chain.

1.1. Cyber Exercises

Like all IT systems, the food supply chain is vulnerable to cyber security threats, e.g., in the areas of smart farming and cyber–physical systems [9]. Cyber attacks against food supply chains can be devastating. Therefore, preparing for such scenarios in a safe environment is important. An effective solution to enhance the knowledge and skills of staff members against cyber threats is the cyber security exercise, where the learning audience participates in a realistic scenario using a technical infrastructure that mirrors the systems and networks in the real world [10]. Such technical infrastructure is called cyber range and/or cyber arena, especially when an expansive environment is considered. Karjalainen and Kokkonen introduce the requirements for cyber arena environments [11]: (i) realism, (ii) isolated and controlled environment, (iii) internet simulation, (iv) user and network traffic generation, (v) attack execution and simulation, (vi) organizations' infrastructures, (vii) collaboration, and (viii) planning, executing, monitoring, and analyzing. When creating new target domains for cyber arenas, the requirements of realism, user and network traffic generation, and organizations' infrastructures in particular become essential.

Cyber arenas need services that replicate the real-world environments where the staff members would face realistic cyber attacks. One way of replicating the food supply chain is to create a digital twin, which mirrors the production cycle and factory setups of the domain. Digital models such as digital twins have their roots in life-cycle management, with a focus on computational modeling; they are virtual representations mirroring physical systems [12]. These models are, naturally, software programs that copy the behavior of their real-world counterparts. The exact definition of a digital twin is an elusive concept that is perhaps not enough distinguished from computing models and simulations [13].

Figure 2 illustrates a typical cyber exercise conducted in a cyber arena. Domain expertise defines the scenario, which can be realized with digital twins and models. The white team (WT), also known as exercise control, controls the planning and execution of the exercise. The blue team (BT) is the learning audience of the exercise defending their systems: by implementing required incident response and forensics maneuvers, for example. The BT is usually modeled in accordance with real organizational structures, and there can be one or several BTs in the exercise. The red team (RT) acts as the threat actor by executing real cyber attacks against the exercise assets of the BTs [14,15]. There is also a green team (GT); they act as system administrations for the whole exercise environment. Basically, the GT enable the technical exercise and assist the other teams if there are out-of-scenario technical issues during the exercise. In this paper, the domain is the food supply chain, the organizations are companies in that domain, and the Realistic Global Cyber Environment (RGCE) [16] serves as the cyber arena.

The cyber arena models the whole networked information security infrastructure required for the cyber exercise. Consequently, it can be realized using digital twins, which meet the requirements set by cyber security exercises. Themes related to digital twins, such as physical and virtual processes and virtual environments [17], are relevant in the cyber arena.

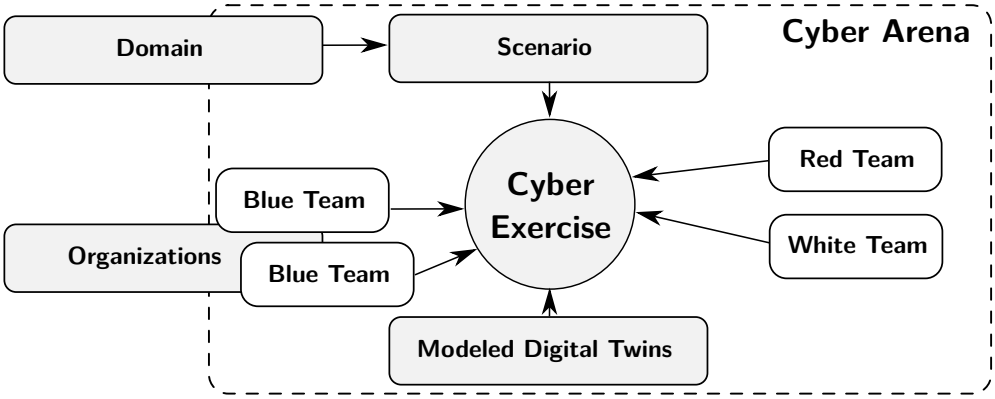

Figure 2. Elements of a cyber exercise.

1.2. Digital Twins and Supply Chain

Digital twins include a physical and a virtual entity, which should have a similar state in the end of the realized twinning. The physical entity is measured or observed, and then realized as a virtual entity. The flow of information is similar: back from the virtual entity back to the real world [17]. The concept of the digital model might be more appropriate for our research, i.e., a system where data flow is not automatic [13]. However, the supply chain itself is not a single distinct entity, but a network of actors. Calling a digital representation of such an entity a digital twin is meaningful, as the concept itself is not well-defined.

The data flows in mirroring or twinning are presented in Figure 3, as suggested by Jones et al. [17]. Such real-time approaches are not quite feasible for cyber security situations, not least because of the often sensitive nature of the domain data. We discuss the actual solution in the result section of this paper.

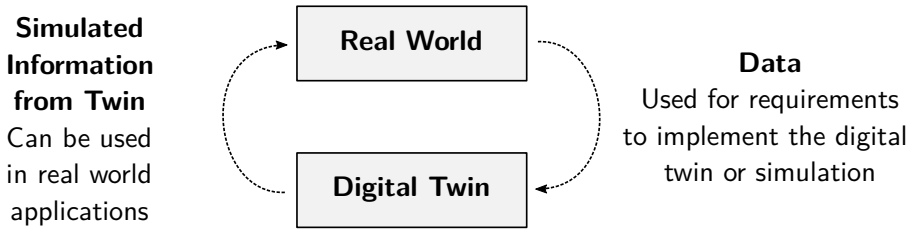

Figure 3. Theoretical dependencies between a real-world system and a digital twin.

The use of digital twins is somewhat implicit in cyber exercises. The concept for a supply chain digital twin has been discussed elsewhere, e.g., by Barykin et al. [18]. They conclude that such twins differ from twins of other—mainly physical—concepts, and that simulation, optimization, and data analytics are the main technologies needed for implementation, although there is no clarity about this in the literature they reviewed. Wang et al. propose a smart supply chain driven by digital twins and highlight a real-use case involving a retailer [19]. Marmolejo-Saucedo describes the design and development of digital twins for supply chains. The presented case study focuses on a pharmaceutical company, and includes simulations related to the supply chain [20]. In their review, Abideen et al. [21] emphasize the use of data analytics as the next step for digital twins in the supply chain and logistics.An review articleby Eckhart and Ekelhart [22] concludes that the concept of digital twins has possibilities beyond the few present uses. They also present a definition of the digital twin for cyber–physical systems, where real-time or historical data is used to build a replica with sufficient fidelity. Studies such as Alim et al. [23] have implemented digital twins with physical testbeds to mirror farmland canal systems. Enns and Suwanruji have created a simulation testbed that was used for supply chain modeling. The solution was based on network flows and featured a user interface [24]. The mentioned

studies illustrate the usefulness of digital twins in testbeds for various domains. However, little literature exists about actual implementations of such systems in the context of supply chains and cyber security.

1.3. Aims and Motivation

We aim to show that the digital twin can also be built to support cyber security concerns. Consequently, a digital twin of relevant parts of the food supply chain is described. This study aims to describe the implementation of the food production cyber arena, which meets the eight high-level requirements mentioned above. This digital representation facilitates the creation of a simulated supply chain for a cyber exercise aimed at organizations working in the domain of food production and processing. For example, food production companies could exercise their response to cyber attacks targeted at critical points in their processes. A cyber exercise in the food supply domain could include participants from a food processing factory. Staff members from departments such as management, communications, and operations could participate. The scenario includes a cyber attack to the factory, to which the participants should react. The resolution of the problem will provide resilience information to the departments. In this article, we describe the design of the digital twin for this purpose.

The following key questions in this study can be identified:

- RQ1: How can we develop a digital twin of the food supply chain for cyber exercises?
- RQ2: What kind of simulation concept fulfills the requirements of the food supplychain digital twin?

This article is structured in the following manner. After the introduction, the cyber range used in this study, the Realistic Global Cyber Environment (RGCE), is described in Section 2. Section 3 describes the proposed design, the design science approach used in this study, the requirements of the system, architecture, implementation, and simulation concerns. The results are discussed in Section 4, describing the use of digital twins in RGCE, and evaluating how the system fulfilled the requirements. Finally, Section 5 concludes the article.

2. Realistic Global Cyber Environment

The most recognized term for a technical cyber exercise environment is the cyber range. To understand the term cyber range, it can be associated with a shooting range where one can improve one's skills with firearms [25], or a driving range, where players can improve their golf swings. In a cyber range, one can train and improve their cyber security-related skills and tactics. There are, globally, a multitude of cyber ranges developed by governmental organizations, industries, universities, and research centers. The inaccuracy of the term cyber range is that it is used from the one-server testbed to enormous infrastructure mimicking global internet in organization environments.Because of this heterogeneity, Karjalainen and Kokkonen introduced the term cyber arena to describe those massive cyber environments which are implemented for the simulation of a total and complex cyber–physical system of systems [11].

One of the most valuable and critical assets of cyber security is the knowledge and skills (know-how) of the individuals. At the organizational level, the cyber know-how of the staff members forms the cyber resilience of the organization. Cyber exercise is an effective way to improve skills facing the stressful situation of a cyber attack. Cyber exercise is beneficial to the skills of individual people but also to the cyber security capability of the organization. During the exercise, organization's internal processes and co-operation interfaces with other organizations are trained during realistic scenarios in a realistic environment. To demonstrate the need for such environments, we refer to Finland's cyber security strategy, where measures to promote cyber security competence include, for example [26], *"Training programmes related to cyber and information security"*. The strategy also emphasizes the support provided *"by both national and international training and exercises"* [26]. Nationally, exercises are encouraged as well as *"digital security training*

in the public administration" to develop the personnel's skills, including those of businesses, stakeholders, and citizens [26].

The cyber arena used for this study is the RGCE, which is a fully functional live cyber arena. It performs in an isolated private cloud, a realistic digital globe with realistic organization environments, by combining virtualization techniques, physical devices, and business-specific systems. As a digital twin of that global entity, it offers possibilities not only for realistic trainings and exercises but also for research and development activities [16].

RGCE is isolated and fully controlled, so it allows usage of vulnerabilities and real attack vectors, which is a specific feature to be considered when implementing a digital twin for cyber exercises: how can we realistically mimic the systems that can be compromised during the cyber exercise?RGCE has been implemented since 2011 by various research and development projects. In the ongoing project *Food Chain Cyber Resilience*, critical food-production infrastructure is mimicked as a digital twin for cyber security exercises for food-production organizations [27]. The environment is implemented and hosted by the JYVSECTEC (Jyväskylä Security Technology) center for cyber security, artificial intelligence, and data analytics-focused research. The development and training center is hosted by the Institute of Information Technology at Jamk University of Applied Sciences.

3. Proposed Design

3.1. Design Science Approach

This study takes the design science approach. The approach focuses on the processes and especially the artifacts created in the processes. The two main tasks are to build and evaluate the artifact during the research. Consequently, the approach is suitable for information science research [28]. Design science closely resembles constructive research, where the goal is also to produce an artifact [29]. The presentation of such research varies, although some efforts have been made when considering software engineering and design science [30]. The process elements of design science can be summarized as follows [31]:

- Problem identification and motivation,
- Objectives of a solution,
- Design and development,
- Demonstration,
- Evaluation,
- Communication.

The goal of the design science process is to create a new artifact, which in this study is the digital twin model of the food supply chain. The objectives and design are described further in this section. The demonstration and evaluation of the system take place during the cyber exercises that use the digital twin, which are discussed in Section 4 of this article.

3.2. Requirements

The requirements were discovered from domain experts via interviews and group work. Both domain requirements and cyber exercise requirements need to be taken into account when creating a system for the cyber arena. The requirements considered the following categories: (i) Realistic enough to represent farms and factories. (ii) Factory system simulation at the level that cyber attacks could be used against the simulated machines. (iii) Scalable and flexible so that multiple copies of the target, e.g., farms, could be created effortlessly. (iv) Possibility to represent food shipments and storage. (v) Dynamic possibility to create recipes for food products.

3.3. Architecture and Implementation

Figure 4 illustrates the setup of the food supply chain simulation. The basis for the simulation was mainly implemented using the Node.js runtime environment. Each service is simulated using the Node.js application that provided the needed interfaces. The various services run on virtual machines in containers on the virtual machine platform of the cyber arena. The services communicate via the (virtual) network, sending the simulated control

messages and simulated material flow using TCP/IP. Messages are passed using REST APIs or mock-ups of protocols such as Modbus. Such messages are usually formatted as JSON using schemas specific to the scenario. Storage is presented with a simple PostgreSQL database solution, which can increase and decrease the amount of material as needed by the scenario or as requested by the simulation. The raw materials and products passed from apparatus to another are simulated using the Bull queue system for the Redis in-memory cache. Figure 5 also shows the relation of the technologies to the simulation.

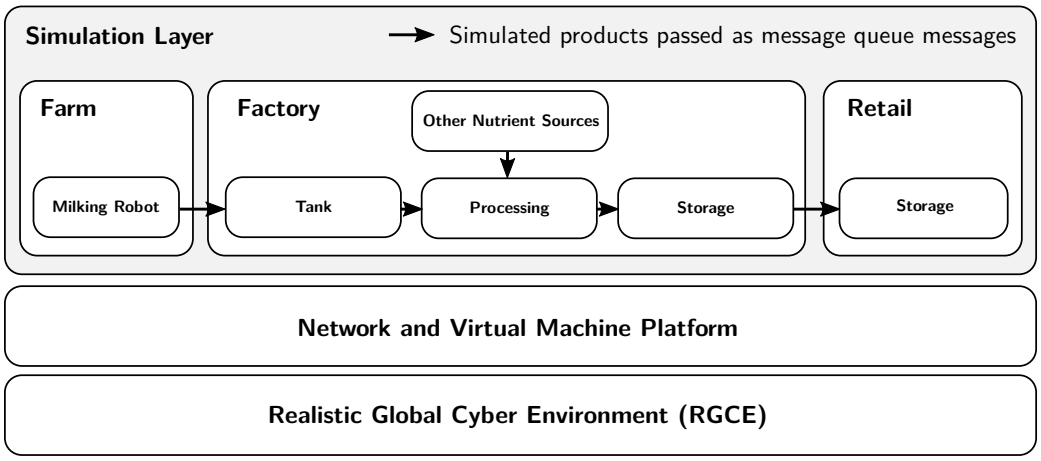

Figure 4. Food supply chain simulation building blocks.

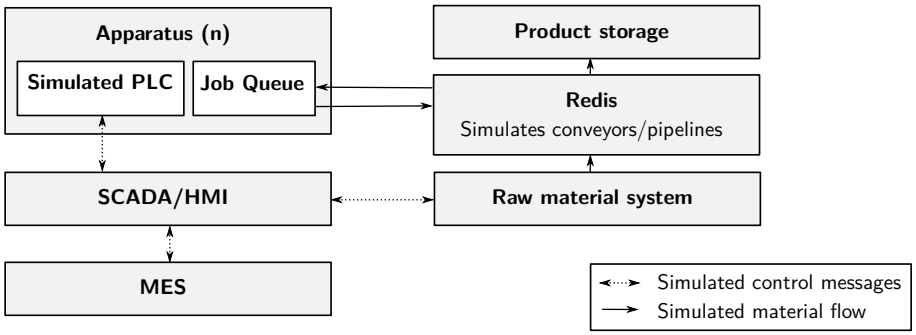

Figure 5. Apparatus schematic.

3.4. Simulation

The simulated factory in the cyber exercise is created so that malicious actors can use cyber attacks against the factory. Each of the parts described below can be targeted as required by the exercise scenario.

The supply chain itself is modeled using two basic elements: apparatus and messages. The apparatus represents the various machines and storage in the supply chain. Apparatus can represent, for example, milking robots, food-processing machines, and packaging machines. The messages are passed from one apparatus to another. These messages contain the relevant domain information (e.g., a message could contain the amount of milk in liters), and metadata (such as the measurement unit).

The simulated factory has the following parts created as Node.js services. As with many industrial applications, a supervisory control and data acquisition (SCADA) unit controls the programmable logic controllers (PLC). Both SCADA and PLCs are built for the exercise scenario. The SCADA system is used via a human machine interface (HMI), which enables humans to give commands via, for example, a web interface. While SCADA controls the machinery's PLCs, the manufacturing execution system (MES) controls the production process itself. Therefore, the production plan dictated by MES will be followed

by SCADA, which commands the individual apparatuses. For exercise purposes, each of these can have bespoke user interfaces created for the exercise scenario.

The apparatus are the various machines in the factory. There can be many apparatus, since a food-production process could require multiple sequential or parallel steps. A simulated apparatus contains a PLC, which runs programs as instructed by SCADA, and a job queue, which requests raw materials from conveyors and sends products to conveyors.

The raw material system (RMS) contains various tanks, from which the SCADA system can make requests. There could be a tank for each type of ingredient which can be arbitrarily created for the exercise scenario. The virtual raw material is then conveyed to the apparatuses, which require ingredients to create the products. Redis simulates the conveyors and pipelines in the factory. Product storage is the end point for the products.

The apparatus schematic is shown in Figure 5. Here, all simulated control messages and simulated material flow are passed via TCP/IP at the exercise infrastructure level.

4. Results and Discussion

4.1. Digital Twins in RGCE

The RGCE can be considered as one comprehensive digital twin of the global internet, consisting of several interconnected digital twins. As a basis, there is the RGCE's internet, consisting of several realistic functions and services: for example, BGP routing and realistic structure with public IP addresses, or global PKI infrastructure for certificates. The RGCE includes a wide range of internet public services, such as news sites, social media, and discussion forums. The other layer of the digital twins in the RGCE are the specific organization environments. There is a wide range of organization environments implemented for the RGCE: financial organization, electricity companies, and healthcare-related organizations, to name a few examples. As in the real world, there are interrelated connections between those different elements and, for example, a cyber attack against an electricity company may cause cascade effects to other elements. Similarly, attacks against some crucial software may cause effects on another organization, or if the other organization offers services to another, those might be interrupted because of the cyber attack, which allows training for co-operation between organizations [16].

In this study, the digital twin of the food-production value chain is modeled. It consists of several organizational elements connected digitally which are dependent on those previously implemented services. These parts of the food production value chain are, for example, smart farming, food-production companies, and retail chains. For example, if there is a cyber attack against a refrigeration unit of the food-production organization, it affects other elements, and that same unit with the same vulnerability can also be used in retail.

During the implementation of those digital twins, there is a lot of co-operation between the real actors of the industry sectors. By that co-operation, the requirements for the implementation can be gathered to ensure that the implemented digital twins are, from the cyber security training and exercise point of view, as realistic as possible.

The schematic idea behind every digital twin in the RGCE is presented in Figure 6. The requirements describing processes and structures related to the domain are passed from the real world. The feedback to the real world after an exercise concerns organizational practices and processes.

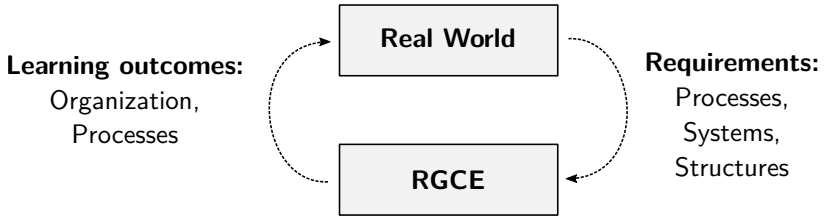

Figure 6. Digital representations in RGCE.

4.2. Evaluation

The implemented digital twin of the food production value chain was tested during the pilot cyber security exercise on 28–29 March 2023. Participants of the exercise varied from governmental organizations to the private sector, including direct participants of food production (for example, smart farming, food production, and retail chains) but also companies that offer services for food production (for example, internet service operators or manufacturers of special hardware) [27,32].

The requirements for the system are presented in the previous Section 3.2. Table 1 compares the requirements with the implemented solution. In the following sections, the requirements are evaluated individually, based on the cyber exercise where the system was used as part of the cyber arena.

Table 1. Solutions that were implemented to satisfy the requirements.

Requirement	Solution
Realism of the environment	Realistic products and descriptions, realistic supply chain components
Factory system as cyber attack target	Open to vulnerabilities, identifiable inconsistencies
Scalability	Each apparatus running on dedicated virtual instance
Representation of food shipments and storage	JSON descriptions and Redis pipeline
Dynamic food recipes	Versatile JSON descriptions

4.2.1. Realism of the Environment

The realism of the environment was achieved with the use of realistic products and product descriptions. The sufficient representation of the food supply chain was achieved so that the participants could recognize and understand the simulated supply chain. The visual presentation of the various views was also a concern. The ultimate evaluation for this is how well the system was received by the participants of the cyber exercise.

After the exercise, feedback was collected from the participants in order to further develop the cyber arena and the exercise concept. As a motivation for this goal, it seemed that nearly all of the BT and WT members would participate in an exercise again.Feedback also included ideas and requirements for future development. In general, it can be said that the pilot exercise was a success, and the participants were satisfied with the technical implementation. Furthermore, the pilot exercise was arranged to identify possible deficiencies and future implementation topics. After a thorough analysis of the feedback and the next version of the implementation, there will be the first full version of the food production cyber range as a digital twin for training and exercise usage.

Figure 7 shows the view in the SCADA/HMI (see also Figure 5) This view indicates the production status of three production lines. The name of the line and the current product are mentioned on the left. The completion percentage of the production line for the batch is indicated on the right.

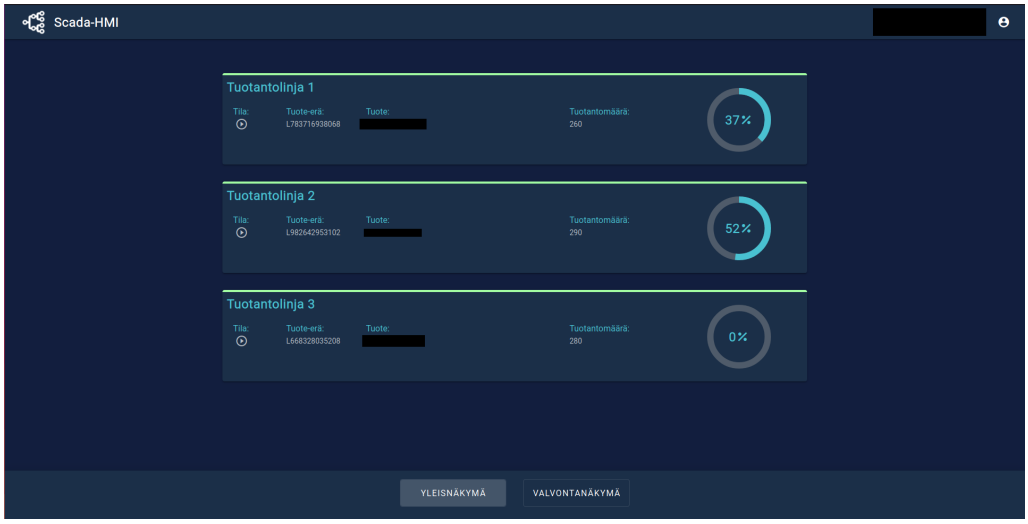

Figure 7. Production-line view in the user interface.

4.2.2. Factory System as Cyber Attack Target

The system was used during a cyber exercise. This demonstrates that it was at a mature enough level to provide cyber attack targets for the exercise scenario. The use of the system also shows that its functioning could be disturbed in a meaningful way, so that the participants could detect the attack, react, and defend the critical infrastructure. By leaving the system open to simulated cyber attacks, the red team could create threat scenarios during the exercise. The participants were able to detect the consequences and inconsistencies in the information. Figure 8 shows an interface to follow the production process. Interruptions in the graphs and logs could indicate cyber attacks. Either the organizing white team or the defending blue team could use such an interface to monitor the processes.

Figure 8. Apparatus monitoring.

4.2.3. Scalability

Running all apparatuses on one virtual machine was not feasible because a realistic representation of the food supply chain contains many production lines and many machines. Consequently, each apparatus runs on its own virtual instance, so that new apparatus can be spawned and killed from the simulation as needed by the exercise scenario. This way, only the capacity of the virtual machine platform limits the size of the simulated manufacturing plants. Figure 9 shows the user interface to inspect a certain production line, where each

block is one apparatus in the line and there are seven in total in this line. This illustrates how crucial it is to have a scalable number of apparatus. A full supply chain simulation includes several production lines.

Figure 9. Apparatus in a production line.

4.2.4. Representation of Food Shipments and Storage

Representing food shipments was one of the core features for demonstrating the food supply chain. As described in Section 3.4, the raw material system and product storage services represent the storage. Food shipments were simulated, and the representations of raw material and food product shipments were handled internally as JSON messages. The relevant information was included in the shipment messages. Listing 1 provides an example of the representations of the raw materials in the system. Each shipment has an ID number and metrics describing its properties relevant to the food supply chain use case.

Listing 1. JSON representation of raw material.

```
{
      "id": "283d61bf-fafd-465a-a525-ca43b27c4cbe",
      "amount": 359,
      "batchId": "7552b60a-6413-4d2d-82b5-e3d2255ae4b6",
      "metrics": {
            "temperature": 5,
            "acidValue": 2.2132,
            "somaticCells": 344558
      },
      "type": "milk"
}
```

4.2.5. Dynamic Food Recipes

There was also a need to represent the products in detail, so that cyber attacks in the production line could cause changes in the composition of the products. The label and content descriptions of the products were sufficient to enable the tracking of product contents during the cyber exercise. In a cyber attack scenario, the description on the label could be erroneous due to manufacturing deficiency. A shortened example of the basic structure of food product representations is shown in Listing 2.

Listing 2. A shortened example of JSON representation of food products.

```
{
      "label": {
         "ean": "1234567890",
         "name": "Rye bread product X",
         "lotId": "L077007126630",
         "price": {
           "vat": {
                 "rate": 12,
                 "class": 3
            },
            "value": 1.50,
            "currency": "\euro",
            "priceUnit": ""
          },
       },
       "content": {
           "properties": {
              "nutrients": [
                 {
                    "name": "Energy",
                    "value": "1213 kJ / 290 kcal"
                 },
                 {
                     "name": "Carbohydrate",
                     "value": "50 g"
                 },
              ]
           },
           "batchAmount": 0.200
       }
    }
 }
```

5. Conclusions

This article presented a way to design a digital twin to represent supply chains for cyber exercises. The development of a digital twin of a food supply chain for cyber exercises (RQ1) could be achieved with standard web technologies. The design of a food supply chain digital twin uses generic apparatus services to simulate various production machines. In addition, the raw material system and the end storage can be simulated with databases and queues. Standard web technologies are sufficient to build the services required by a digital twin for cyber exercises. Accordingly, the developed simulation concept for the food supply chain (RQ2) followed a web service architecture. The use of simulated parts of the food supply chain actors, such as MES and SCADA, facilitates the immersiveness of the exercise. In addition, the scalable apparatus architecture makes it feasible to create new scenarios and extend the existing ones, depending on the domain needs.

Digital modeling and twinning can be seen as valuable tools for exercises. When building digital twins, a restricted domain and application area, e.g., cyber security, serve to constrain the complexity of the system. However, the evaluation of such constructs could be difficult because of the specifics of the domain. The realistic nature of the scenario is essential to cyber exercises. The simulated products were dynamically created as a process which enabled unusual events during the exercise. Cyber attacks against such targets are sensible for the attackers (RT) and for the exercise, because the consequences affect a realistic process.

The main limitation of this study is that the system was built for one specific cyber range, the RGCE. The solutions used in this cyber range could be idiosyncratic to it, and adaptability to other environments might be inconvenient. Secondly, as this is the first iteration of this kind of digital twin approach, the design and development process of future digital twins might reveal better technical practices in the implementation.

The use of digital twins of domain systems as part of cyber exercises improves the immersiveness by simulating real supply chains. This way, the participants can exercise in

a realistic environment which mirrors the systems and processes in their ordinary work. Implementing the digital twin requires a modular design with appropriate messaging simulating the real-world counterparts. Further research includes detailed validation by analyzing the conducted cyber exercises. The generalizability of the solution could also be studied.

Author Contributions: Conceptualization, M.P., K.-E.R., K.P., E.J. and T.K. (Teemu Kontio); methodology, M.P., K.-E.R., K.P., E.J. and T.K. (Teemu Kontio); software, M.P., K.-E.R., K.P., E.J. and T.K. (Teemu Kontio); investigation, T.S. and T.K. (Tero Kokkonen); resources, T.K. (Tero Kokkonen); writing—original draft preparation, T.S. and T.K. (Tero Kokkonen); writing—review and editing, T.S., T.K. (Tero Kokkonen) and M.P.; visualization, M.P. and T.S.; supervision, T.K. (Tero Kokkonen); project administration, T.K. (Teemu Kontio) and T.S.; funding acquisition, T.K. (Tero Kokkonen). All authors have read and agreed to the published version of the manuscript.

Funding: This research and the APC were funded by the Regional Council of Central Finland/Council of Tampere Region with fund of Leverage from the EU, European Regional Development Fund (ERDF) and Recovery Assistance for Cohesion and the Territories of Europe (REACT-EU) Instrument as part of the European Union's response to the COVID-19 pandemic, as part of the Food Chain Cyber Resilience project of Jamk University of Applied Sciences Institute of Information Technology (grant number A77620).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Acknowledgments: The authors would like to thank project manager Elina Suni for assistance with project data and Tuula Kotikoski for proofreading the manuscript.

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

References

1. Bourlakis, M.A.; Weightman, P.W.H. Introduction to the UK Food Supply Chain. In *Food Supply Chain Management*; Bourlakis, M.A., Weightman, P.W.H., Eds.; Blackwell: Oxford, UK, 2004; Chapter 1, pp. 1–10.
2. Manning, L.; Soon, J.M. Building strategic resilience in the food supply chain. *Br. Food J.* **2016**, *118*, 1477–1493. [CrossRef]
3. Davis, K.F.; Downs, S.; Gephart, J.A. Towards food supply chain resilience to environmental shocks. *Nat. Food* **2021**, *2*, 54–65. [CrossRef] [PubMed]
4. Hobbs, J.E. Food supply chain resilience and the COVID-19 pandemic: What have we learned? *Can. J. Agric. Econ. Can. D'Agroecon.* **2021**, *69*, 189–196. [CrossRef]
5. Urciuoli, L.; Männistö, T.; Hintsa, J.; Khan, T. Supply chain cyber security — Potential threats. *Inf. Secur. Int. J.* **2013**, *29*, 51–68. [CrossRef]
6. Li, C.; Liu, Q.; Zhou, P.; Huang, H. Optimal innovation investment: The role of subsidy schemes and supply chain channel power structure. *Comput. Ind. Eng.* **2021**, *157*, 107291. [CrossRef]
7. Zhai, Y.; Bu, C.; Zhou, P. Effects of channel power structures on pricing and service provision decisions in a supply chain: A perspective of demand disruptions. *Comput. Ind. Eng.* **2022**, *173*, 108715. [CrossRef]
8. Stock, J.R. The US Food Supply Chain. In *Food Supply Chain Management*; Bourlakis, M.A., Weightman, P.W.H., Eds.; Blackwell: Oxford, UK, 2004; Chapter 14, pp. 211–220.
9. Alatalo, J.; Sipola, T.; Kokkonen, T. Food Supply Chain Cyber Threats: A Scoping Review. In Proceedings of the WorldCist'23—11th World Conference on Information Systems and Technologies, Pisa, Italy, 4–6 April 2023; *in press*.
10. Kokkonen, T.; Päijänen, J.; Sipola, T. Multi-National Cyber Security Exercise, Case Flagship 2. In Proceedings of the 14th International Conference on Education Technology and Computers (ICETC 2022), Barcelona, Spain, 28–30 October 2022; p. 7. [CrossRef]
11. Karjalainen, M.; Kokkonen, T. Comprehensive Cyber Arena; The Next Generation Cyber Range. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020; pp. 11–16. [CrossRef]
12. VanDerHorn, E.; Mahadevan, S. Digital Twin: Generalization, characterization and implementation. *Decis. Support Syst.* **2021**, *145*, 113524. [CrossRef]
13. Fuller, A.; Fan, Z.; Day, C.; Barlow, C. Digital Twin: Enabling Technologies, Challenges and Open Research. *IEEE Access* **2020**, *8*, 108952–108971. [CrossRef]

14. Kokkonen, T.; Puuska, S. Blue Team Communication and Reporting for Enhancing Situational Awareness from White Team Perspective in Cyber Security Exercises. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*; Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 277–288.
15. Seker, E.; Ozbenli, H.H. The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. In Proceedings of the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, UK, 11–12 June 2018; pp. 1–9. [CrossRef]
16. Jamk University of Applied Sciences, Institute of Information Technology/JYVSECTEC. Realistic Global Cyber Environment (RGCE). Available online: https://www.jyvsectec.fi/rgce (accessed on 21 March 2023).
17. Jones, D.; Snider, C.; Nassehi, A.; Yon, J.; Hicks, B. Characterising the Digital Twin: A systematic literature review. *CIRP J. Manuf. Sci. Technol.* **2020**, *29*, 36–52. [CrossRef]
18. Barykin, S.Y.; Bochkarev, A.A.; Kalinina, O.V.; Yadykin, V.K. Concept for a Supply Chain Digital Twin. *Int. J. Math. Eng. Manag. Sci.* **2020**, *5*, 1498–1515. [CrossRef]
19. Wang, L.; Deng, T.; Shen, Z.J.M.; Hu, H.; Qi, Y. Digital twin-driven smart supply chain. *Front. Eng. Manag.* **2022**, *9*, 56–70. [CrossRef]
20. Marmolejo-Saucedo, J.A. Design and Development of Digital Twins: A Case Study in Supply Chains. *Mob. Networks Appl.* **2020**, *25*, 2141–2160. [CrossRef]
21. Abideen, A.Z.; Sundram, V.P.K.; Pyeman, J.; Othman, A.K.; Sorooshian, S. Digital Twin Integrated Reinforced Learning in Supply Chain and Logistics. *Logistics* **2021**, *5*, 84. [CrossRef]
22. Eckhart, M.; Ekelhart, A., Digital twins for cyber-physical systems security: State of the art and outlook. In *Security and Quality in Cyber-Physical Systems Engineering*; Biffl, S., Eckhart, M., Lüder, A., Weippl, E., Eds.; Springer: Cham, Switzerland, 2019; pp. 383–412. [CrossRef]
23. Alim, M.E.; Wright, S.R.; Morris, T.H. A Laboratory-Scale Canal SCADA System Testbed for Cybersecurity Research. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; pp. 348–354. [CrossRef]
24. Enns, S.T.; Suwanruji, P. A simulation test bed for production and supply chain modeling. In Proceedings of the 2003 Winter Simulation Conference, New Orleans, LA, USA, 7–10 December 2003; Volume 2, pp. 1174–1182. [CrossRef]
25. Tian, Z.; Cui, Y.; An, L.; Su, S.; Yin, X.; Yin, L.; Cui, X. A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus. *IEEE Access* **2018**, *6*, 35355–35364. [CrossRef]
26. Secretariat of the Security Committee. *Finland's Cyber Security Strategy, Government Resolution 3.10.2019*; Secretariat of the Security Committee: Helsinki, Finland, 2019, ISBN 978-951-663-055-0. Available online: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf (accessed on 14 June 2023).
27. Jamk University of Applied Sciences, Institute of Information Technology/JYVSECTEC. Food Chain Cyber Resilience. Available online: https://jyvsectec.fi/2021/09/food-chain-cyber-resilience/ (accessed on 21 March 2023).
28. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design Science in Information Systems Research. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]
29. Piirainen, K.A.; Gonzalez, R.A. Constructive Synergy in Design Science Research: A Comparative Analysis of Design Science Research and the Constructive Research Approach. *Liiketal. Aikakauskirja* **2013**, *62*, 206–234.
30. Engström, E.; Storey, M.A.; Runeson, P.; Höst, M.; Baldassarre, M.T. How software engineering research aligns with design science: A review. *Empir. Softw. Eng.* **2020**, *25*, 2630–2660. [CrossRef]
31. Peffers, K.; Tuunanen, T.; Gengler, C.E.; Rossi, M.; Hui, W.; Virtanen, V.; Bragge, J. The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. In *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology*; Claremont Graduate University: Claremont, CA, USA, 2006; pp. 83–106.
32. Jamk University of Applied Sciences, Institute of Information Technology/JYVSECTEC. Elintarvikeketjun Kyberturvallisuuden Pilottiharjoitus-Pilot Cyber Exercise for Food Production Value Chain. Available online: https://www.jamk.fi/fi/tapahtuma/elintarvikeketjun-kyberturvallisuuden-pilottiharjoitus (accessed on 21 April 2023).