electronics

Article

Survey on Application of Trusted Computing in Industrial Control Systems

Jing Bai [1], Xiao Zhang [2], Longyun Qi [3], Wei Liu [3], Xianfei Zhou [1], Yin Liu [3], Xiaoliang Lv [3], Boyan Sun [3], Binbin Duan [4], Siyuan Zhang [4] and Xin Che [4,*]

1 State Grid Beijing Electric Power Co., Ltd., Beijing 100031, China; baijing@bj.sgcc.com.cn (J.B.); zhouxianfei@bj.sgcc.com.cn (X.Z.)
2 State Grid Corporation of China, Beijing 100031, China; zhang-xiao@sgcc.com.cn
3 NARI Group Corporation/State Grid Electric Power Research Institute, Nanjing 210003, China; qilongyun@sgepri.sgcc.com.cn (L.Q.); liuwei5@sgepri.sgcc.com.cn (W.L.); liuyin@sgepri.sgcc.com.cn (Y.L.); lvxiaoliang@sgepri.sgcc.com.cn (X.L.); sunboyan@sgepri.sgcc.com.cn (B.S.)
4 State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China; 22060300@zju.edu.cn (B.D.); 22232109@zju.edu.cn (S.Z.)
* Correspondence: chexin@zju.edu.cn

Abstract: The Fourth Industrial Revolution, also known as Industrial 4.0, has greatly accelerated inter-connectivity and smart automation in industrial control systems (ICSs), which has introduced new challenges to their security. With the fast growth of the Internet of Things and the advent of 5G/6G, the collaboration of Artificial Intelligence (Al) and the Internet of Things (loT) in ICSs has also introduced lots of security issues as it highly relies on advanced communication and networking techniques. Frequent ICS security incidents have demonstrated that attackers have the ability to stealthily breach the current system defenses and cause catastrophic effects to ICSs. Thankfully, trusted computing technology, which has been a popular research topic in the field of information security in recent years, offers distinct advantages when applied to ICSs. In this paper, we first analyze the vulnerabilities of ICSs and the limitations of existing protection technologies. Then, we introduce the concept of trusted computing and present a security framework for ICSs based on Trusted Computing 3.0. Finally, we discuss potential future research directions.

Keywords: industrial control systems; trusted computing; security

Citation: Bai, J.; Zhang, X.; Qi, L.; Liu, W.; Zhou, X.; Liu, Y.; Lv, X.; Sun, B.; Duan, B.; Zhang, S.; et al. Survey on Application of Trusted Computing in Industrial Control Systems. *Electronics* **2023**, *12*, 4182. https://doi.org/10.3390/electronics12194182

Academic Editor: Stefano Scanzio

Received: 3 August 2023
Revised: 28 September 2023
Accepted: 29 September 2023
Published: 9 October 2023

1. Introduction

Industrial Control Systems (ICSs) are crucially important in key infrastructures, including energy, transportation, water conservation, and other critical areas. In the early stages, physical isolation has helped to ensure the security of ICSs, owing to the independence and relative closeness of the industrial network. However, with the rapid advancement of the Internet of Things and Artificial Intelligence [1,2], ICSs are now widely connected to the Internet, which has led to numerous potential security hazards [3]. In Table 1, we present a list of typical ICS security events that occurred between 2018 and 2022, along with their common characteristics including attack path, trusted networks, data protection, software verification, layer. Specifically, a trusted network refers to a network connection that has security features such as identity authentication and data encryption transmission. Examples of data protection measures include data encryption and isolated storage. Program verification is the process of ensuring that a program's integrity has not been compromised by malware. The level indicates the primary level of the ICS architecture where the attack is targeted, as attackers often do not limit their actions to a single level.

By analyzing the attack characteristics in Table 1, we can observe that the attackers frequently exploit vulnerabilities in operating systems (OS) and applications, or use phishing emails to inject malicious code and steal confidential data and gain access to internal

files. Ransomware attacks have become one of the most common types of security events. Attackers encrypt internal data and files through various paths, threatening the integrity of the system's static storage content. Examples of such events include Light S.A (2020), Delta Electronics (2022), and Expeditors International (2022). In other security events, attackers collect users' data to change device settings through cyber attacks, threatening the integrity of the system's dynamic running program. Examples of such events include the refrigeration control system in Scotland (2019), the Municipal water treatment system in the USA (2021), and others. While attackers initiate attacks across the network, their goal is not to destroy the network connection but to target confidential data and control programs. In a positive example, India's UHBVN power company was attacked in March 2018. Hackers stole and locked a significant amount of customer billing data, as in many other events. However, the stolen database was encrypted, ensuring the relevant data would not be disclosed. Additionally, the company had a database backup and could complete data recovery immediately, avoiding any business interruption or losses. Despite the lack of a trusted network connection, the company avoided loss through data protection, highlighting the value of data encryption and isolated storage.

Table 1. Typical ICSs Security Events.

Target	Attack Path	Trusted Networks	Data Protection	Software Verification	Level
Light S.A, a Brazilian power company, June, 2020 [4]	Ransomware	no	no	not involved	Enterprise resource
Delta Electronics, Taiwan, China, January, 2022 [5]	Ransomware	no	no	not involved	Production management
Expeditors International, February, 2022 [6]	Ransomware	no	no	not involved	Enterprise resource
Network of a power plant in the United States, March, 2018 [7]	Malware	no	no	not involved	Field control
Stadler, a Swiss railway locomotive manufacturer, May, 2020 [8]	Malware	no	no	not involved	Production management
Hoya, Japan's largest manufacturer of optical products, April, 2019 [9]	Network attack	no	no	not involved	Enterprise resource
Shell, March, 2021 [10]	The zero day vulnerabilities of the file transfer program	no	no	not involved	Production management
online store of Segway, January, 2022 [11]	Plug-in vulnerabilities	no	no	not involved	Enterprise resource
A power company in the western United States, September, 2019 [12]	A firewall firmware vulnerability	no	no	no	Enterprise resource
Refrigeration control system, Scotland, February, 2019 [13]	Remote anonymous login	no	no	no	Enterprise resource
Municipal water treatment system in alderma, Florida, USA, February, 2021 [14]	Remote anonymous login	no	no	no	Process monitoring
Uttar Haryana Bijli Vitran Nigam, an India's power company, March, 2018 [15]	Malware	no	yes	not involved	Production management

In ICSs, three types of information security protection methods are commonly used, i.e., industrial firewall, intrusion detection, and trusted computing. Industrial firewalls (IFWs) are designed to isolate different areas of industrial control networks by parsing and filtering data streams, making them resistant to attacks from external networks. Depending on their scope, IFWs can be classified into three categories, i.e., security inter-domain IFWs, field industrial control firewalls, and web application firewalls [16]. Note that the IFW techniques cannot handle internal attackers, and external attackers can still use network configuration and protocol vulnerabilities to intrude into ICSs and cause damage to the system.

Intrusion detection is a protective technology that identifies abnormal behaviors of internal or external networks by collecting and analyzing relevant information from ICS equipment and networks. This technology has gained much attention from both industry and academia, as seen in the host-based method proposed to detect and identify abnormalities in an oil refinery's distributed control system network [17]. It is important to note that intrusion detection systems based on abnormality may generate false alarms, potentially disrupting the production process and leading to unforeseen consequences.

Differently, Trusted Computing (TC) technology provides security functions, such as encryption, decryption, and authentication, based on a hardware chip known as the root of

trust. This technology ensures that information in the chip cannot be accessed by external software. TC is realized through cryptography, which provides confidentiality, and hash algorithms, which implement integrity measurement. The output of a hash algorithm will be different if the input is different. Therefore, if the measured object is tampered with, the output results will change, indicating that the object has been compromised. The root of trust measures the target program using the hash algorithm and compares the result with the benchmark value safely encrypted and stored in the root of trust. If they are different, the system startup is terminated, and an alarm is given. If they are the same, the integrity of the next program started by the system is verified. Thus, the integrity verification before the tampered program runs ensures the safety of the system operating environment. TC technology also verifies the integrity of running programs in real time to prevent anonymous or compromised programs from running. Hence, TC has the potential to improve the security of ICSs. The primary concern is that ICSs are a typical type of cyber-physical system. Introducing trusted computing can result in significant computation and storage costs that could impede the performance of the electronic system responsible for controlling the physical system. This, in turn, could cause severe damage to the system.

This paper analyzes the vulnerabilities of ICSs and the limitations of existing protection methods based on existing security incidents and research. It clarifies the necessity of establishing an active defense system based on TC. We then present two key points in TC. Based on this, we introduce an active defense security structure for ICSs that combines TC 3.0 with the typical architecture of ICSs.

The remainder of this paper is organized as follows. Section 2 presented the necessities of applying TC in ICSs. Section 4 provides the concepts of TC technology. The security structure for Industrial Control Systems based on TC 3.0 is provided in Section 5 following the potential research directions in Section 6. The conclusion is given in Section 7.

In addition, to assist readers in better understanding the abbreviations used in the text, some of the acronyms and their full names that appear in the text will be presented in Table 2.

Table 2. Acronyms and Their Full Name.

Acronym	Full Name
RTOS	Real-Time Operating System
BIOS	Basic Input Output System
NVM	Non-Volatile Memory
SMM	System Management Mode
TSS	TCG Software Stack
CNC	Computer Numerical Control
SCADA	Supervisory Control And Data Acquisition
SMM	Trusted Software Base

2. The Necessity of Applying TC

In this section, we conduct a detailed analysis of the vulnerabilities in ICSs and show existing security methods falling short of safeguarding ICSs. We then show the effectiveness of TC techniques in mitigating these issues.

Vulnerability Analysis of Industrial Control Systems

Figure 1 illustrates a typical ICS's architecture consisting of five layers separated by firewalls [18]. Usually, attackers infiltrate the enterprise layer from the internet and exploit vulnerabilities in devices to bypass the firewalls. Once access to the process monitoring layer is gained, the attacker can steal monitoring data or manipulate control instructions. In contrast to conventional IT systems where confidentiality is paramount, ICSs prioritize availability as the highest security property, followed by integrity and confidentiality. The controllers' normal operation guarantees the system's availability. PLCs, or Programmable Logic Controllers, boast a rugged design that surpasses that of microcontrollers, enabling

them to endure higher levels of heat and environmental stress. They offer a versatile platform for precisely defining and executing complex processes, ensuring the desired outcomes are consistently achieved. What further enhances their appeal is the user-friendly programming language they employ, which simplifies the configuration process, making it accessible even to those with limited programming experience. As a key part of ICSs, Programmable Logic Controllers (PLCs) vulnerabilities are analyzed in detail here. First, we analyze the communication protocols' vulnerability of PLCs. We are able to bypass the AutothinkV3.1.5 programming software and remotely control the Hollysys LE5106 PLC by starting, stopping, resetting, and cold resetting it. The success of these attacks can be attributed to the absence of identity authentication and data encryption in the PLC communication protocol. The existing work regarding these vulnerabilities and the conclusions are summarized as follows.

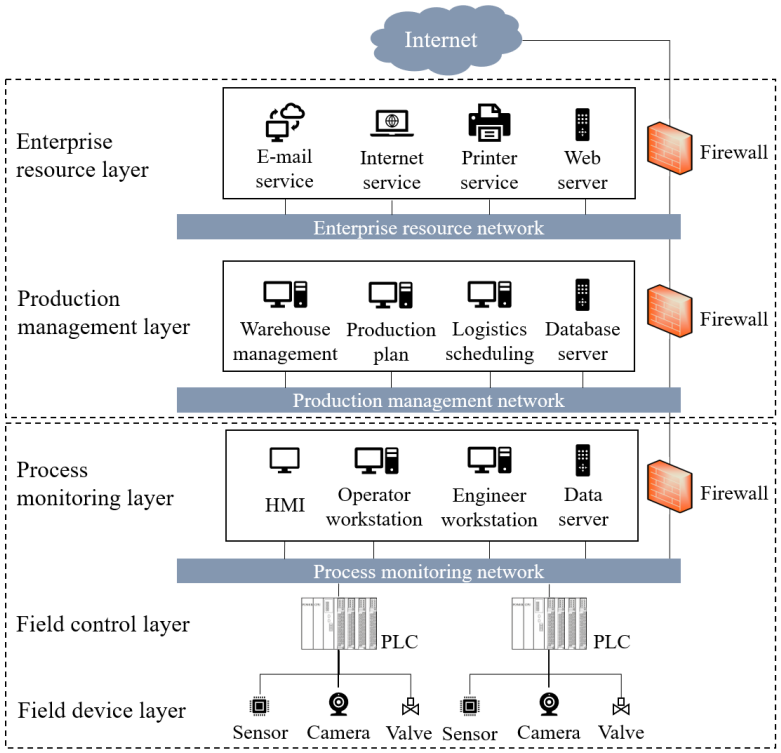

Figure 1. The typical architecture of industrial control systems.

- Several vulnerabilities in communication protocols have been identified. Langner et al. showed that the S7 protocol vulnerability can allow the injection of malicious code and termination of legitimate programs [19]. Meixell et al. identified the Modbus protocol vulnerability, which enables the construction of an IP-based control data packet that can tamper with control commands [20]. Tzokatziou et al. observed that there is no authentication process for communication objects in the PLC communication protocol [21]. This allows attackers to use CoDeSys to directly connect with the PLC, capture communication data packets, and send tampered control instructions to the PLC to start or stop it arbitrarily. Hui and McLaughlin indicated that the S7 protocol lacked authentication, leading to attacks on Siemens PLC. In addition, such vulnerabilities can also be used to implement replay attacks, MITM, and so on [22]. In the case of communication protocol vulnerabilities such as these, attackers typically begin by intercepting data packets exchanged between a Programmable Logic Controller (PLC) and other systems using packet capture software. These packets often lack encryption measures, which creates a vulnerability that can be exploited. Subsequently, attackers identify specific commands within these packets, such as start, pause, and execute commands, which have distinct syntax compared to the

protocol's heartbeat packets. Once the desired data packets are identified, attackers can accurately transmit these commands to the PLC controller from an engineer's machine. Since there is no need for authentication of the data packets, attackers can achieve their objectives without hindrance.

Conclusion 1: ICSs are unable to verify the legitimacy of communication object identities due to the lack of a secure and trusted network connection mechanism, as well as a trusted third-party-based identity authentication mechanism.

Then,vulnerabilities of the embedded OS operating of PLCs and the programming or monitoring software on the workstations can impact the system's availability, i.e.,

- Embedded OS vulnerabilities: Beresford et al. pointed out that x86 Linux vulnerabilities can be exploited to blast the shell and illegally connect to the Simatic PLC to obtain program permissions [23]. In addition, hackers can dump all data stored in the memory of VxWorks, which is the remote debugging port of the software used by various Siemens and Schneider's PLCs, and find all login passwords in the memory to bypass login verification [24]. In the case of such Embedded OS vulnerabilities, attackers can capture or construct their own authenticated data packets, subsequently establishing their own session with the PLC. Due to certain features in some monitoring software that allow the removal of memory protections, these memory protections can record packets returning to the PLC, allowing them to be replayed discreetly to disable the protection. Attackers can also alter the memory protection password on the PLC, effectively locking engineers out of their own devices.
- Engineering software vulnerabilities: In addition to using four zero-day vulnerabilities of Windows OS, two vulnerabilities in the process monitoring software WinCC (Windows Control Center) of the Siemens PLC are also exploited by Stuxnet [25]. The attack method was an internal connection by USB. As in [26], the attacker can remotely replace the firmware and shut down the PLC by exploiting the vulnerability of Unity Pro, the programming software of the Schneider series PLC. For this vulnerability, attackers can interact with the PLC using MODBUS [27] and FTP protocols to carry out firmware upgrades. When the attacker opts for the FTP protocol, the firmware can be downloaded via FTP Ethernet without the need for authentication for older firmware versions that are currently in operation. For some newer versions, Wireshark can be used to capture plaintext passwords and communication data during the login process. Upon successful login, remote upload and download can be achieved, allowing attackers to easily disrupt the PLC by replacing the firmware.

Conclusion 2: ICSs are unable to confirm whether the OS or industrial control software has been modified or not. This is due to a lack of remote verification mechanisms between managers, engineers, and software in the system, a lack of local verification mechanisms between different software in the same work area, and a lack of integrity measurement of the OS and industrial control software. These factors can lead to attacks launched by tampering with software files and codes.

Conclusion 3: The ICSs cannot effectively protect the key identity information, operation logs, and monitoring data stored in the server, as there is no secure isolated storage area of data and a lack of encryption and access control mechanisms for key files. The corresponding attacks can steal confidential information by using the above vulnerabilities.

The above analysis demonstrates the availability, integrity, and confidentiality of ICSs can be jeopardized and it is essential to deploy protection technologies accordingly, which are discussed in the following part.

3. Protection Technologies for Industrial Control Systems

To deal with the above ICSs' vulnerabilities, various security protection technologies are available for ICSs, including IFWs, IDSs, anti-virus software, and vulnerability scanning tools installed on computers [28]. One popular method is implementing IFWs on network boundaries, which provides some level of security for external network connections. IFWs offer identity identification and data leakage protection, but attackers can fabricate identity

or exploit network-accessible identity information to circumvent IFWs [29]. While IDSs can indirectly evaluate the integrity of ICS's vital resources and data by monitoring and filtering communication data, they lack software verification or data encryption mechanisms [30]. Additionally, as ICS security requirements continue to evolve, and attackers become more sophisticated, certain defects are exposed, i.e.,

- Self-checking defects: Integrated control systems are increasingly becoming more open, which poses a significant security risk. Due to the existing software architecture, it is easy for imperceptible malicious codes to be implanted in computer resources. Traditional methods of detecting malicious code through software are unreliable and cannot guarantee the security of the detection software itself. This includes most anti-virus software and intrusion detection systems (IDSs).
- Passivity: Defensive mechanisms, such as an IDS based on pattern matching or expert systems, are often deployed to detect known viruses, vulnerabilities, and attacks. However, these methods are limited in their ability to defend against emerging threats that fall outside their detection scope.
- Failure of internal protection: Protection technologies such as IFWs can be challenging to handle attacks from within the system. This is because they are typically deployed at the network layer to prevent unauthorized access from outside the system. Similarly, many IDSs deployed at the boundary layer are also limited in their ability to detect and prevent attacks originating from within the system.
- Hysteresis: Most anti-virus software and vulnerability scanning tools use prevention methods that involve capturing characteristic information of hacker attacks and virus intrusions and recording them in logs. However, these safeguards only take effect after security incidents have already occurred, and the attacker's objectives may have already been achieved.
- Reduction in availability: Protecting against new threats requires updating virus databases, filtering rules, and intrusion detection models. However, this can result in increased implementation costs and false positive rates for anti-virus software, IFWs, and IDSs. Moreover, increased runtime overhead can reduce the availability of ICSs. A prominent example is the Spectre and Meltdown vulnerabilities discovered in 2018. These CPU hardware vulnerabilities allowed attackers to gain unauthorized access to sensitive data. Due to the defects in the chip's underlying design, these vulnerabilities are complex and challenging to repair. Updating the repair patch may lead to system performance degradation or blue screen errors.

Given the aforementioned shortcomings, it is promising to shift protection methods from software-based to hardware-based, from passive to active, and from peripheral blocking to overall prevention. Unlike IFWs and IDSs, which are software-based, TC technology protects the key, verification algorithm, and database using the hardware root of trust [31,32]. This ensures they are not exposed to the workstation's OS or the PLC's RTOS, resulting in a small attack surface. TC technology ensures the security of the system operating environment by actively measuring system startup files, without needing to make corresponding responses based on the attack type. Additionally, the active measurement of running programs enables overall system protection from static files to dynamic programs. TC is a new hot topic in the field of network security and has garnered significant attention from academia and industry. It aims to address two critical issues [33]: (1) Which software is running on a remote computer? (Remote Attestation) (2) How to ensure that only a particular software stack can access a stored secret? (Sealed Memory).

Solving issue (1) ensures that only authorized software can run on the device, maintaining the security of the system's dynamic operation. The hash algorithm used by TC ensures that any modification to the software source code will result in different hash calculation results. This allows for the verification of bootloader, OS, and software executable files, enabling the detection of threats before abnormal software behavior occurs. Additionally, only programming and monitoring software on the white list is permitted to run, effectively

blocking malware operations. Conversely, when some IDSs trigger an alarm after detecting anomalous software behavior, the attack effect may have been created.

Solving issue (2) ensures that only authorized individuals can access the encrypted information stored, protecting the system's static storage. In TC, confidential data are encrypted via the root of trust, sealed with the authorized subject, and stored in the non-volatile memory of the root of trust. Since the encryption algorithm's key is derived from the endorsement key, which cannot be accessed outside the root of trust, key leakage is prevented. The NVM of the root of trust is isolated from the host, making it difficult to steal encrypted data through a compromised network or host. Even if the NVM is invaded, unauthorized subjects cannot access confidential data in the sealing mechanism. Without these protections, ransomware can easily steal confidential data in ICSs.

Deploying TC systems may increase startup time and runtime overhead, which may be more noticeable on ICS devices with limited computing resources. The cost of controllers and switches equipped with TC technology will also increase. However, the link between ICSs and networks is becoming increasingly close, which expands the attack surface and raises security requirements. Therefore, it is necessary to apply new and more effective protective measures. Additionally, the prolonged startup time on long-running ICS devices is acceptable, and the runtime overhead is gradually decreasing due to the study of functional clipping and lightweight deployment. With the maturity of production technology, the hardware cost will decrease, making large-scale application more feasible. Consequently, applying TC in ICSs has significant potential.

4. Trusted Computing Concepts

Trusted Computer System Evaluation Criteria (TCSEC) published by the US Department of Defense in 1985 was the first formal standard for computer system security evaluation [34]. The TCSEC's class C security level introduced the notion of a TC base (TCB), which is viewed as the foundation of information security. The TCSEC focuses on software reliability, which can be regarded as TC 1.0. AMD et al. announced the TC Group (TCG) in April 2003, which served as the industry standard for evolving published TCPA specifications [35]. The TCG presented the TPM for the first time and emphasized that hardware provides better protection than software [36], known as TC 2.0. However, the TPM was invoked by the computing components such as the OS and measured the system passively. In 2006, China established a special group on TC Cryptography to build norms and standards for TC, renamed the Chinese TC Union (CTCU) in 2008, and C. Shen et al. proposed TC 3.0 in 2016 [37]. Its main feature is the construction of a dual system architecture with separate computing and security components, leading to an active protection system.

Root of Trust: The security functions provided by TC technology, including encryption, measurement, attestation, and isolated storage, can be guaranteed by the physical mechanism based on the hardware root of trust. According to the definition of the TCG [38], the root of trust is the TPM, a hardware structure shown in Figure 2. The RSA engine, SHA-1 engine, HMAC engine, random number generator, and key generation are used as the basis of confidentiality for the platform to provide the hardware components required for encryption, decryption, and hash calculation. The NVM and volatile memory are used to store keys, certificates, and internal data. During the production of each TPM, the manufacturer burns a randomly generated Endorsement Key (EK) into the chip. The EK is an RSA public–private key pair with a module length of 2048 bytes. The private key is stored inside the TPM and will never be exposed outside the TPM. Meanwhile, the EK is used to generate the attestation identity key (AIK), the storage root key (SRK), and other keys. Therefore, the EK, as the permanent identity certificate of the TPM, ensures the security of each TPM itself. Only well-designed software interfaces exist in addition to the physical link between the TPM and the host. When encryption is needed, the user acquires the index value of the newly derived key through the appropriate interface in the system.

As a result, no keys are exposed outside of the TPM. This is the secure data encryption mechanism based on the TPM.

Regarding data-isolated storage, the system can only access the NVM and the volatile memory through particular interfaces. The authorized subject information is used to seal the encrypted data from the system. This means that the data can only be accessed if both the identity and key are valid. Accessible data includes user-stored information, hash computation results, logs, and so on.

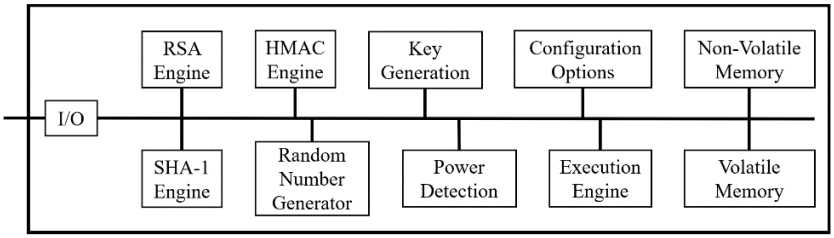

Figure 2. The structure of Trusted Platform Module (TPM).

Chain of Trust: TC technology ensures the overall protection of a system by measuring the integrity of the OS loader, OS, and applications in a chain of trust. This chain of trust extends trust throughout the entire computer platform, based on the root of trust. The TCG trusted PC's chain of trust is depicted in Figure 3. The root of trust comprises the TPM and BIOS boot block. From the BIOS boot block to the OS loader, OS, and applications, a chain of trust is formed. Each level measures the next level, and each level trusts the next level, thereby guaranteeing the integrity of platform resources. Due to limited TPM storage space, the measurement extension method is adopted, which connects and hashes the old measurement value with the new measurement value to prevent tampering with the old value. The measurement value is recorded and stored in the TPM, while the detailed information of the measurement object and the measurement results are stored in the disk as a log. These records confirm each other to prevent tampering. When the access object makes an inquiry, the TPM provides a report that includes hash values and logs to evaluate the trusted state of the TPM. Note that to ensure the report's security, encryption, digital signature, and authentication must be used for platform remote certification.

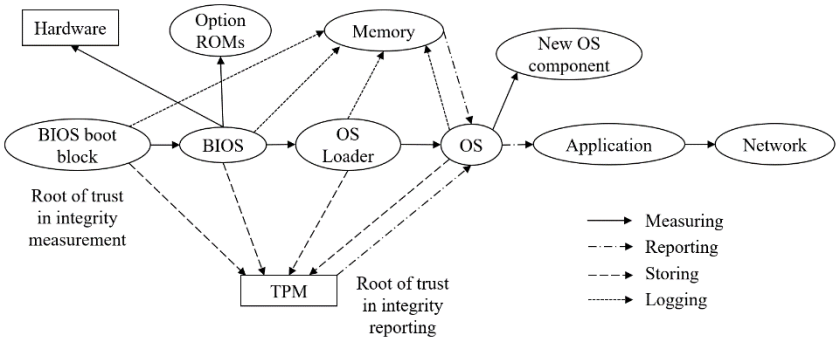

Figure 3. The chain of trust of TC group trusted PC.

Trusted Execution Environment: A Trusted Execution Environment (TEE) is a specific implementation of Trusted Computing, and it is a secure isolation environment typically present in the hardware or operating system of computing devices. In the TEE, the software realm is divided into two environments. A trusted environment, where both code and data are considered trustworthy to ensure the secure execution of code and data, and an untrusted environment. These two environments coexist within the same computer system and are physically separated through hardware mechanisms [39]. Intel SGX is one of the most widely used TEEs. It enables applications to establish a secure container in which sensitive information is inaccessible to untrusted entities, typically referred to as

a secure enclave. The secure enclave is a protected area within the application's address space, providing confidentiality and integrity even in the presence of privileged malicious software [40].

Trusted Computing 3.0: In TC 3.0, a Trusted Platform Control Module (TPCM) is used to replace the TPM, which realizes active measurement and further completes the chain of trust. Actually, TC represented by the TCG still realizes passive measurement by calling an external TPM chip via the main program. Using the BIOS as part of the root of trust makes it hard to check the BIOS's security. Therefore, C. Shen's team has proposed a "host + trusted" dual node active immune TC architecture [41], as shown in Figure 4. The computational component and the trusted component are logically distinct. To achieve system trust, the trusted component actively monitors the computational component. In addition, China's TC technology is geared toward network security and the establishment of highly trusted networks, marking TC enter the 3.0 era.

As the root of trust, the TPCM integrates trusted measurement, trusted storage, and trusted reporting. It includes the hardware layer, basic software layer, and functional component layer, as shown in Figure 5. The hardware layer contains the CPU, memory, controller, and interfaces, providing the fundamental operating environment. The basic software layer contains firmware and the OS core, which accomplish internal resource scheduling, job management, and interface driving. Trusted measurement, strategy base management, the Trusted Software Base (TSB) interface, and other components are included in the functional component layer. It performs hash computation, cryptography operations, trusted policy acquisition, and other functions. Based on the powerful software and hardware functions, the TPCM can start before the computational component to accomplish comprehensive and real-time measurement.

However, achieving full maturity and widespread application of the TPCM currently presents some disparities compared to the TPM. Firstly, the TPCM constitutes a more comprehensive security framework, necessitating the design and development of entirely new, universally applicable foundational hardware and software components. Additionally, in scenarios with stringent security requirements demanding the construction of a complete chain of trust, no trusted component, whether it be the control chip, dual-fusion motherboard, trusted software, or trusted connections, can be omitted. This could potentially result in higher costs.

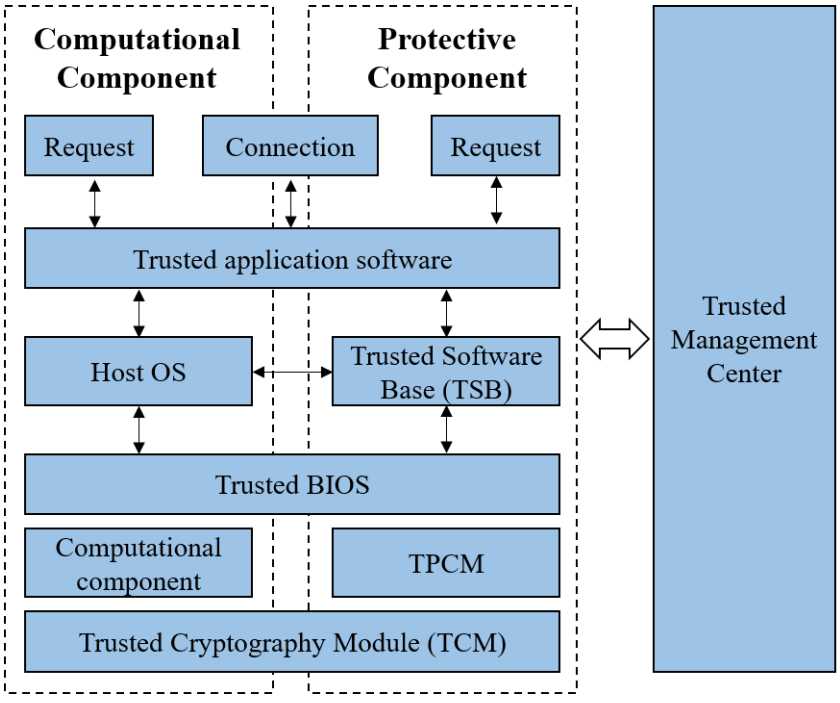

Figure 4. Dual architecture supported by TC 3.0.

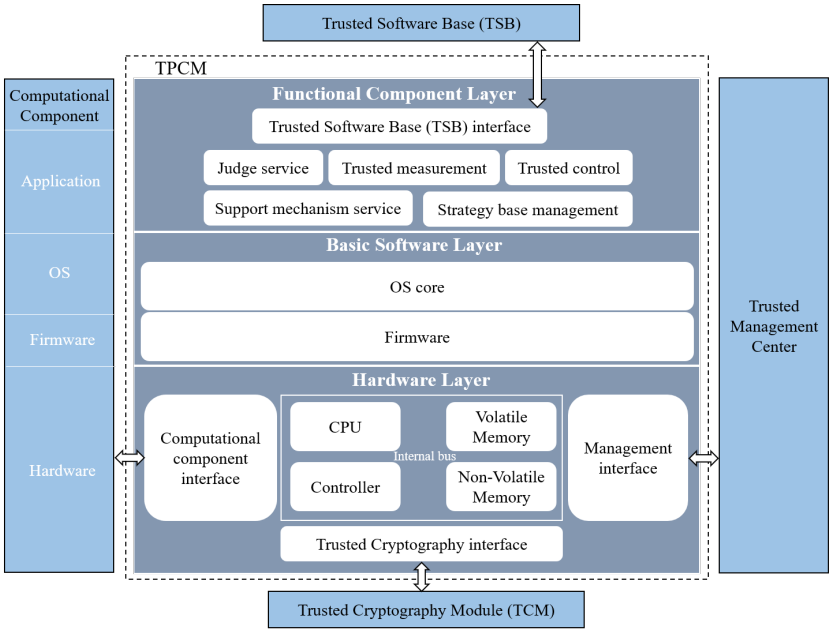

Figure 5. The function and interface framework of TPCM.

5. Secure Framework for Industrial Control Systems Based on TC 3.0

An active defense security structure for ICSs based on TC 3.0 technology is proposed as shown in Figure 6. It broadens and universalizes the security immune model for the power monitoring system [42]. The structure consists of four parts: TC environment, trusted area boundary, trusted communication network, and trusted management center.

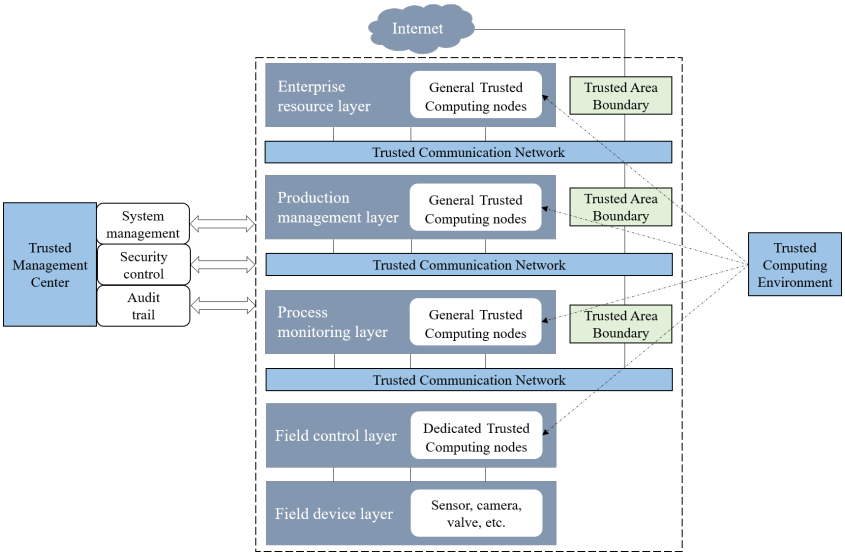

Figure 6. An active defense security structure for industrial control systems.

5.1. Trusted Computing Environment

A TC environment consists of TC nodes. TC nodes are formed by deploying trusted components on computational components in ICSs. In a TC environment, the integrity of all software is verified in real time, and confidential data is encrypted and isolated in TPCM. For new devices, the TPCM can be directly embedded into the motherboard to form a trusted motherboard or the TPCM function can be realized by using a new CPU internal security chip or IP core, e.g., the Feiteng CPU [43]. For old devices, TPCM can be connected through the PCIe interface of the motherboard or the USB to support TC. A general computing node, such as a workstation or a server, may be easily converted into a

TC node. The current focus of the existing studies is on deploying the root of trust in real-world industrial scenarios. The key challenge is determining how to implement dynamic software verification without compromising system availability, which is especially critical in ICSs. Liu et al. developed a dynamic measuring technique that uses SMM mode and TCM to check the integrity of a computing terminal without rebooting it [44]. This design satisfied the real operation requirements of the power system's computers. However, in order for this design to work, the hardware manufacturer must adjust the motherboard design stage. Wu et al. investigated a TC platform for a power monitoring system, including the TC platform of host computers and field control devices [45]. It is more difficult to install trustworthy computing resources on dedicated computing nodes such as PLC. These devices are exclusive to ICSs with limited system resources. Additionally, there are issues below.

- The TPCM OS core does not correspond to the PLC Real-Time OS (RTOS). Zhang et al. proposed the RE-TPM and RE-TSS, which were all operating in kernel mode in VxWorks, to match the low-power and real-time requirements of VxWorks [46]. The average percentage of time savings was 65.81%. Xu et al. built a trusted real-time platform based on dual kernel architecture. It runs RTOS in a trustworthy virtualization environment [47]. In the platform, TVP implemented by SW-TPM worked as the host OS, and Xenomai worked as the guest OS.
- Different root of trust's hardware interface. Tu et al. enhanced the security of CNC machines through trusted communication monitoring and control modules and realized a TC environment [48]. Because it is difficult for CNC equipment to install TPCM and TSB directly. Shang et al. designed a trusted PLC product by combining the embedded platform chip ZYNQ, a CPLD coprocessor, and a TPM chip, which supported a variety of security functions and was highly available and reliable [49].
- Integrity verification of control programs. To protect the control program integrity of PLCs, Shang et al. incorporated a hybrid remote attestation mechanism with a physics-based model [50]. Typically, the TPM was chosen as a trust anchor for the prover, providing a secure isolated environment for creating attestation reports. Wang et al. proposed a dynamic integrity measurement scheme for the software of smart meters based on TC and software traces [51].

Although there have been some practical studies, to comply with the notion of TC 3.0, it is necessary to study from four aspects: the integration of hardware TPCM, the matching of OS, the integrity verification of business software, and the creation and verification of prototype.

5.2. Trusted Area Boundary

The trusted area boundary is in charge of controlling data flow into and out of the TC environment. According to the trusted management center's security policy, it performs trusted measurement and security inspection on data to shield illegal data. Although it functions similarly to IFWs, identity authentication, and data encryption are added. This section of the study has a small number of participants, which overlaps with the research of a TC environment and trusted communication network. Yuan et al. proposed cryptographic technology to ensure the confidentiality of communication sessions between the field control layer and the process monitoring layer to ensure the reliable transmission and source of data [52]. The authors of [53] designed a trusted access model for the intelligent substation terminals, which implanted the TC platform into the terminal equipment of the smart substation to provide it with the trusted password module and TSB. In addition, it realized the trust guarantee of the whole process of terminal access to the intelligent substation.

5.3. Trusted Communication Network

The TC resources are deployed on network nodes to realize the trusted communication network. It realizes identity authentication and access control mechanism based on node credibility. It is able to isolate malicious nodes and report abnormal information to

the audit server of the trusted management center. The additional security mechanism will lengthen communication time and also have an impact on the system's real-time performance and availability. The present framework still exists in theory, so it is still a long way from being applied in practice. Okhravi et al. first proposed a trusted process control network (TPCN) architecture, which applied trusted network architecture to process control architectures [54]. The TPCN contains identity authentication, access device status evaluation, and other functions. In the TPCN, the Identity Authentication Server verifies the trustworthiness of devices by utilizing TPM chips to validate the signatures of critical device components and assess their status. Devices that pass this authentication process are considered trustworthy. The 'access device status' functionality is accomplished through the Terminal Security Assessment Server. When a new device seeks to join the TPCN, the Security Assessment Server retrieves client attributes from the Network Access Device. These attributes typically include information such as the operating system version, applied patches, or virus signature versions. These data are then used to evaluate the compliance of the client device. Hence, the TPCN can eliminate the problem of firewall bypass, and prohibit malicious users or untrusted devices from accessing the network. The work in [55] proposed a trust evaluation model which took the abnormal behaviors of nodes, historical trust information, and trust information of neighbor nodes into comprehensive consideration. It provided a method for balancing the security and availability of an ICS's trusted network connection. Yuan et al. built a trusted network system of electric power system SCADA through four lines of defense: establishment, monitoring, audit, and self-healing [56]. This is a theoretical overall defense scheme, the security of which was verified by the attack mechanism of Stuxnet. The authors of [57] proposed an Industrial Internet Platform (IIP) security scheme based on TC technology. It extended the chain of trust from physical devices to virtualization software and network-connected edge devices, which is the first time that TC 3.0 has been introduced into the industrial communication network.

5.4. Trusted Management Center

The trusted management center is primarily in charge of providing trusted policies and analyzing audits. The trusted components carry out certain security behaviors in accordance with the trusted policies. It lowers the cost of deployment and the impact on applications. Specifically, it includes a system management module, security control module, and audit trail module. The system management module manages system resources such as identity information, trusted measurement strategy, benchmark database, and emergency strategy to provide basic security support. The security control module generates the security policy according to the actual business requirements of ICSs, transmits it to the TC environment, trusted area boundary, and trusted communication network as the basis of access control, and transmits the exception log to the audit trail module. The audit trail module stores and executes the audit strategy, classifies and marks the malicious behavior of the whole system, and provides the basis for implementing the emergency strategy.

Wang et al. cooperatively deployed the TC platform, trusted data protection mechanism, and trusted network in the field equipment layer, production monitoring layer, and enterprise management layer of ICSs [58]. The analysis showed that compared with the old protection scheme, this scheme had great advantages in dealing with internal attacks, efficiency, and integrity protection. The three trusted mechanisms in this design were not controlled uniformly without the trusted management center. Therefore, it is not common. The authors of [59] gave the specific location of deploying TC platforms, access control, and the trusted network server in typical ICSs. Abnormal information was reported to the audit server, which was the prototype of the trusted management center. Tao et al. proposed a TC 3.0 prevention and control system for nuclear power ICSs, and simply analyzed the construction of TC nodes [60]. They also evaluated the performance of the protection system through attack tests, system startup time tests, and operation cost tests. Wang et al. designed the security immune model of a power monitoring system based

on TC 3.0, which consists of a TC environment, trusted communication network, trusted area boundary, and trusted management center [42]. However, only the field control layer and process monitoring layer were considered, and no simulation experiment was carried out [61].

5.5. Security Analysis

For typical attacks, we provide the following security analysis of the introduced active immune protection scheme based on a trusted mechanism.

- Mitigation of unknown threats: We employ Trusted Computing 3.0's dual-system protection architecture to prevent system infiltration and monitor the system state in real time. Access control policies, encryption, and credibility-based mechanisms isolate malicious nodes, providing early warnings of attacks. The scheme ensures system inaccessibility, information protection, data integrity, and defense against malicious attacks, effectively mitigating unknown threats.
- Information leakage: Attackers collect vital information and intercept critical data. Core data access control employs virtual protection to ensure trusted user access, blocking unauthorized users and diverting risky access to a protected domain. Key instructions use encryption and credible authentication during transmission to deter forgery and participation by unauthorized users.
- Unauthorized access: This common attack, often utilizing backdoors or malicious code, seeks unauthorized control, data manipulation, and dangerous commands. Our trusted operational mechanism, rooted in an access control strategy, prevents unauthorized users and processes, thwarts unauthorized access to critical data, and prevents forgery of control commands. Unauthorized access is thus blocked.

To delve deeper into the enhanced protective capabilities inherent in our proposed framework, we will now provide a detailed analysis. Our framework is designed to leverage the resource capacities existing at various levels within industrial control systems, implementing a range of protective measures across these different tiers. Within the Field Device Layer, with the indispensable support of the Trusted Computing Module (TCM), we ensure the provision of encryption, decryption, and signature functionalities during the startup and operational phases of field devices. This deployment establishes a trusted and isolated virtual domain, rendering it highly effective in thwarting unauthorized access attempts.

At the Process Monitoring Layer, our framework relies on sophisticated access control methods. When access requests to sensitive data are detected, our system employs pre-configured access control policies within the Trusted Management Center to validate the identity and role of the requesting processes. Furthermore, it identifies and verifies access behaviors, guaranteeing the security of sensitive data access. This comprehensive approach ensures the overall security of the system, including the integrity of data and control flows.

At the Production Management Layer and Enterprise Resource Layer, the framework actively isolates potential threats and malicious nodes to safeguard the integrity and availability of the peripheral network. Simultaneously, the implementation of the Trusted Communication Network facilitates secure information transfer between different levels, thereby ensuring the security of critical command transmissions.

Our framework's collaborative operation encompasses the foundational platform environment, dynamic runtime environment, and dynamic behavioral aspects. This collective effort is instrumental in enabling Industrial Control Systems (ICS) to operate securely and reliably on a trusted platform.

6. Future Research Directions

Based on the analysis above, it is evident that trusted computing has the potential to significantly enhance the security of industrial control systems, particularly in the context of the industrial internet. However, it is important to note that the field is still in its infancy

and requires further research to fully leverage the benefits of trusted computing in ICSs. To this end, a future study could focus on the following aspects.

- Trusted terminal products. Terminal devices are popular targets for attackers because they are a crucial element of the field control layer. At the moment, there is a scarcity of mature trusted terminal solutions based on self-controllable hardware root of trust. On devices with limited computer resources, they may perform the trusted measurement, encryption, and decryption, as well as remote authentication. Moreover, terminal devices are deployed in large quantities in ICSs, so it is necessary to reduce the cost of trusted terminal products.
- Flexible deployment. The addition of a large number of trusted computer resources will inevitably affect the availability of ICSs. One future direction might be to minimize the deployment of security mechanisms based on security requirements, particularly on devices with limited computing resources such as gateways, controllers, and terminals.
- Simulation analysis of complete protection systems. The research of the existing protection system either stays in the theoretical stage or only simulates and analyzes the startup and operation of the TC environment. The simulation environment of the trusted area boundary trusted communication network and trusted management center needs to be established to analyze the security, efficiency, and availability of the whole design.
- Trade-off between high cyber security and high physical system performance. Industrial Control Systems represent quintessential cyber-physical systems, demanding real-time, dependable, and secure feedback control. However, the deployment of trusted computing in the lower control layer, such as PLC devices, can introduce delays or potential faults due to the resource-intensive nature of trusted computing, which may compromise other system capabilities. Thus, we must meticulously weigh the trade-off between robust cybersecurity and optimal physical system performance.

7. Conclusions

This paper analyzed the necessity of applying Trusted Computing techniques in ICSs, investigated related works thoroughly, and pointed out the potential research directions. Note that many studies remain in the theoretical design stage without considering real-world production scenarios and equipment requirements. Therefore, there is a need for further research to bridge the gap between theoretical design and practical implementation. Moreover, it is essential to consider the equipment requirements and limitations of the systems in which the TC models are being deployed. This will help to ensure that the proposed models can be easily integrated into existing systems and provide maximum benefit without disrupting system functionality or performance. Ultimately, by addressing these issues, we can advance the development of TC environments and promote their widespread adoption in various industrial applications.

Author Contributions: Conceptualization, J.B.; methodology, X.Z. (Xiao Zhang) and L.Q.; software, W.L.; validation, X.Z. (Xianfei Zhou); formal analysis, Y.L.; investigation, X.L.; resources, B.S.; data curation, B.D.; Writing – original draft, S.Z.; Writing – review and editing, X.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Science and Technology Program of SGCC (5108-202240041A-1-1-ZN).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study. Written informed consent has been obtained from the patient(s) to publish this paper.

Data Availability Statement: Data sharing not applicable.

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.

References

1. He, S.; Shi, K.; Liu, C.; Guo, B.; Chen, J.; Shi, Z. Collaborative sensing in Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 1435–1474. [CrossRef]
2. Xing, F.; He, S.; Leung, V.C.M.; Yin, H. Energy efficiency optimization for rate-splitting multiple access-based indoor visible light communication networks. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 1706–1720. [CrossRef]
3. Zhao, C.; He, J.; Cheng, P.; Chen, J. Analysis of consensus-based distributed economic dispatch under stealthy attacks. *IEEE Trans. Ind. Electron.* **2016**, *64*, 5107–5117. [CrossRef]
4. Arghire, L. SECURITYWEEK . Available online: https://www.securityweek.com/ransomware-operators-demand-14-million-power-company/ (accessed on 5 September 2023).
5. The Stack. Available online: https://www.thestack.technology/delta-electronics-ransomware-attack/ (accessed on 5 September 2023).
6. Expeditors. Available online: https://investor.expeditors.com/press-releases/2022/02-21-2022-032617120 (accessed on 5 September 2023).
7. Perlroth, N.; Sanger, D.E. The New York Times. Available online: https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html (accessed on 5 September 2023).
8. Arghire, L. SECURITYWEEK. Available online: https://www.securityweek.com/railway-vehicle-maker-stadler-hit-malware-attack/ (accessed on 5 September 2023).
9. The Japan Times. Available online: https://www.japantimes.co.jp/news/2021/04/22/business/corporate-business/hoya-hack-ransomware/ (accessed on 5 September 2023).
10. Securitynewspaper. Available online: https://www.securitynewspaper.com/2021/03/22/zero-day-vulnerability-in-file-transfer-platform-leads-to-a-data-breach-in-shell/ (accessed on 5 September 2023).
11. Threat Intelligence Team. Malwarebytes. Available online: https://www.malwarebytes.com/blog/threat-intelligence/2022/01/segway-store-compromised-with-magecart-skimmer (accessed on 5 September 2023).
12. Cimpanu, C. ZDNET. Available online: https://www.zdnet.com/article/cyber-security-incident-at-us-power-grid-entity-linked-to-unpatched-firewalls/ (accessed on 5 September 2023).
13. Kovacs, E. Securityweek. Available online: https://www.securityweek.com/refrigeration-systems-used-supermarkets-hospitals-left-exposed-online/ (accessed on 5 September 2023).
14. Vera, A. CNN. Available online: https://www.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html (accessed on 5 September 2023).
15. Panchkula. The Indian Express. Available online: https://indianexpress.com/article/cities/chandigarh/cyber-attack-hits-haryanas-power-discoms-billing-data-5115191/ (accessed on 5 September 2023).
16. Wu, Y.; Hu, X. Industrial Internet security protection based on an industrial firewall. In Proceedings of the 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 28–30 June 2021; pp. 239–247.
17. Kim, K.H.; Kwak, B.I.; Han, M.L.; Kim, H.K. Intrusion detection and identification using tree-based machine learning algorithms on DCS network in the oil refinery. *IEEE Trans. Power Syst.* **2022**, *37*, 4673–4682. [CrossRef]
18. Dehlaghi-Ghadim, A.; Balador, A.; Moghadam, M.H.; Hansson, H.; Conti, M. ICSSIM—A framework for building industrial control systems security testbeds. *Comput. Ind.* **2023**, *148*, 103906. [CrossRef]
19. Langner, R. A Time Bomb with Fourteen Bytes. 2011. Available online: http://www.1angner.com/en/2011/07/21/a-time-bomb-with-fourteen-bytes/ (accessed on 5 September 2023).
20. Meixell, B.; Forner, E. Out of control: Demonstrating SCADA exploitation. *Black Hat USA* **2013**, *1*, 1–7.
21. Tzokatziou, G.; Maglaras, L.; Janicke, H. Insecure by design: Using human interface devices to exploit SCADA systems. In Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research, British Computer Society, Leicester, UK, 17–18 September 2015; pp. 103–106.
22. Hui, H.; McLaughlin, K. Investigating current plc security issues regarding siemens s7 communications and TIA portal. In Proceedings of the 5th International Symposium for ICS and SCADA Cyber Security Research 2018, Hamburg, Germany, 29–30 August 2018.
23. Beresford, D. Exploiting Siemens Simatic S7 PLCs. *Black Hat USA* **2011**, *16*, 723–733.
24. Kimon. Uncover VxWorks-Directly Hit Security Weakness of the Internet of Things. Available online: http://chuansong.me/n/1864339 (accessed on 1 November 2015).
25. Edwards, M. An analysis of a cyberattack on a nuclear plant: The Stuxnet worm. In *Critical Infrastructure Protection*; IOS Press: Amsterdam, The Netherlands, 2014; Volume 116, p. 59.
26. Z-One. Reveal Schneider PLC Ethernet Module Back Door Account. Available online: http://plcscan.org/blog/2014/06/schneider-electric-quantum-ethernet-module-hard-coded-credentials/ (accessed on 12 June 2014).
27. Li, X.; Meng, F.; Zheng, X. Automatic Control System of Sluice Based on PLC, MCGS and MODBUS Communication. In Proceedings of the 2021 7th Annual International Conference on Network and Information Systems for Computers (ICNISC), Guiyang, China, 23–25 July 2021; pp. 716–720.

28. Jormanainen, J.; Mengotti, E.; Soeiro, T.B.; Bianda, E.; Baumann, D.; Friedli, T.; Heinemann, A.; Vulli, A.; Ingman, J. High humidity, high temperature and high voltage reverse bias-a relevant test for industrial applications. In Proceedings of the PCIM Europe 2018; International Exhibition and Conference for Power Electronics, Intelligent Motion, Renewable Energy and Energy Management, VDE, Nuremberg, Germany, 5–7 June 2018.
29. Neupane, K.; Haddad, R.; Chen, L. Next generation firewall for network security: A survey. In Proceedings of the SoutheastCon 2018, IEEE, St. Petersburg, FL, USA, 19–22 April 2018.
30. Alamleh, A.; Albahri, O.S.; Zaidan, A.A.; Alamoodi, A.H.; Albahri, A.S.; Zaidan, B.B.; Qahtan, S.; Ismail, A.R.; Malik, R.Q.; Baqer, M.J.; et al. Multi-attribute decision-making for intrusion detection systems: A systematic review. *Int. J. Inf. Technol. Decis. Mak.* **2023**, *22*, 589–636. [CrossRef]
31. Rajski, J.; Trawka, M.; Tyszer, J.; Wlodarczak, B. A Lightweight True Random Number Generator for Root of Trust Applications. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2023**, *42*, 2815–2825. [CrossRef]
32. Guo, X.; Xue, Y.; Feng, T.; Jiang, Y.; Yan, Y. Simulation Implementation and Verification of a Security Framework for ICS Based on SPD. *Autom. Control Comput. Sci.* **2023**, *57*, 37–47.
33. Kauer, B. OSLO: Improving the security of trusted computing. *Usenix Secur. Symp.* **2007**, *24*, 173.
34. Latham, D.C. *Department of Defense Trusted Computer System Evaluation Criteria*; Department of Defense: Washington, DC, USA, 1986.
35. Sumrall, N.; Novoa, M. Trusted computing group (TCG) and the TPM 1.2 specification. In *Intel Developer Forum*; Intel: Santa Clara, CA, USA, 2003; Volume 32.
36. Berger, B. Trusted computing group history. *Inf. Secur. Tech. Rep.* **2005**, *10*, 59–62. [CrossRef]
37. Shen, C.; Zhang, D.; Liu, J.; Ye, H.; Qiu, S. The strategy of TC 3.0: A revolutionary evolution in trusted computing. *Strateg. Study CAE* **2016**, *18*, 53–57.
38. TPM Main Specification Level 2 Version 1.2, Revision 116, Trusted Computing Group. 2003. Available online: http://www.trustedcomputinggroup.org (accessed on 5 September 2023) .
39. Hosam, O.; BinYuan, F. A Comprehensive Analysis of Trusted Execution Environments. In Proceedings of the 2022 8th International Conference on Information Technology Trends (ITT), Dubai, United Arab Emirates, 25–26 May 2022; pp. 61–66. [CrossRef]
40. Victor Costan and Srinivas Devadas, Intel Sgx Explained. Available online: https://eprint.iacr.org/2016/086 (accessed on 6 September 2023)
41. Shen, C. Building cyber security defense by trusted computing 3.0. *Inf. Commun. Technol.* **2017**, *3*, 290–298.
42. Tao, W.; Wu, J.; Liang, Z.; Jiang, Z. Trusted security immune model of power monitoring system. *J. Phys. Conf. Ser.* **2021**, *1744*, 022115. [CrossRef]
43. Sun, Y.; Hong, Y.; Wang, Y. An active immune protection design for industrial control system based on trust root of TPCM. *Inf. Technol. Netw. Secur.* **2021**, *40*, 14–18.
44. Liu, R.; Niu, D. Application research of trusted computing platform in electric power information system. In Proceedings of the 2010 IEEE International Conference on Networking and Digital Society, Wenzhou, China, 30–31 May 2010; Volume 1, pp. 212–215.
45. Wu, J.; Tao, W.; Lai, Y.; Qin, Z. Industrial control trusted computing platform for power monitoring system. *J. Phys. Conf. Ser.* **2021**, *1744*, 022114. [CrossRef]
46. Zhang, F. Research on trusted computing technology for embedded real-time operation system. In Proceedings of the 13th National Conference on Embedded System Technology, Beijing, China, 10–11 October 2015; Springer: Singapore, 2015; pp. 133–138.
47. Xu, M.; Gao, X.; Gao, Y.; Zhang, F. Real-time trusted computing technology for Xenomai. In Proceedings of the Chinese Conference on Trusted Computing and Information Security, Changsha, China, 14–17 September 2017; Springer: Singapore, 2017; pp. 87–96.
48. Tu, S.; Liu, G.; Lin, Q.; Lin, L.; Sun, Z. Security framework based on trusted computing for industrial control systems of CNC machines. *Int. J. Perform. Eng.* **2017**, *13*, 1336. [CrossRef]
49. Shang, W.; Zhang, X.; Chen, X.; Liu, X.; Chen, C.; Wang, X. The research and application of trusted startup of embedded TPM. In Proceedings of the 2020 IEEE 39th Chinese Control Conference (CCC), Shenyang, China, 27–29 July 2020; pp. 7669–7676.
50. Salehi, M.; Bayat-Sarmadi, S. PLCDefender: Improving remote attestation techniques for PLCs using physical model. *IEEE Internet Things J.* **2020**, *8*, 7372–7379. [CrossRef]
51. Wang, B.; Zheng, T.; Zhang, S. Dynamic integrity measurement scheme of smart meter based on trusted computing. *Inf. Syst. Signal Process. J.* **2019**, *4*, 7–12.
52. Tao, Y.; Hu, W.; Li, S. Construction of Integrated Protection System for Industrial Control System Based on Trusted Computing. 2021 International Conference on Intelligent Computing, Automation and Applications (ICAA), Nanjing, China, 2021; pp. 850-853.
53. Chen, L.; Yang, T.; Li, G.; Liu, X.; Lu, N.; Cheng, K.; Xin, X. Application of trusted computing technology in active defense of smart substation. *J. Phys. Conf. Ser.* **2021**, *2108*, 012065. [CrossRef]
54. Okhravi, H.; Nicol, D.M. Application of trusted network technology to industrial control networks. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 84–94. [CrossRef]
55. Zhang, Q.; Qu, J.; Wang, L. Study of wireless network information trust evaluation model in industrial control system. In Proceedings of the 2014 IEEE Fourth International Conference on Instrumentation and Measurement, Computer, Communication and Control, Harbin, China, 18–20 September 2014; pp. 473–477.

56. Yuan, M.; Chen, X.; Wang, Y.; Ding, H. A trusted power system network in electrical industry. In Proceedings of the 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 26–29 June 2017; pp. 636–643.
57. Fan, P.; Zhang, W.; Zhou, H.; Li, Y.; Jiang, H. A security scheme for industrial Internet platform based on trusted computing technology. In Proceedings of the 2021 IEEE International Conference on Computer Engineering and Artificial Intelligence (ICCEAI), Shanghai, China, 27–29 August 2021; pp. 32–37.
58. Wang, J.; Liu, J.; Yang, S.; Zhang, M. Integrated trusted protection technologies for industrial control systems. In Proceedings of the 2016 IEEE 18th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Republic of Korea, 31 January–3 February 2016; pp. 70–75.
59. Yang, W.; Tao, H.; Liu, W.; Wang, J.; Wei, X.; Wang, H.; Huang, H. An active defense architecture for industrial control system based on trusted computing 3.0. In Proceedings of the 2020 IEEE Chinese Automation Congress (CAC), Shanghai, China, 6–8 November 2020; pp. 2080–2085.
60. Wang, Y.; Cui, G.; Zhang, L.; Li, H. Research on application of trusted computing 3.0 in industrial control system of nuclear power plant. In Proceedings of the 2020 IEEE 12th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, 12–15 June 2020; pp. 297–301.
61. Wang, J.; Zhang, Z.; Wang, M. A trust management method against abnormal behavior of industrial control networks under active defense architecture. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2549–2572. [CrossRef]