IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 12, 2019, accepted January 13, 2020, date of publication January 17, 2020, date of current version January 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2967453

Integrated Functional Safety and Security Diagnosis Mechanism of CPS Based on Blockchain

AI GU[1,2], ZHENYU YIN[1,2], CHUANYU CUI[3,4], AND YUE LI[1,2]

[1]School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, China
[2]Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168, China
[3]Institute of Metal Research, Chinese Academy of Sciences, Shenyang 110016, China
[4]School of Materials Science and Technology, University of Science and Technology of China, Hefei 230026, China

Corresponding author: Zhenyu Yin (congmy@163.com)

This work was supported in part by the National Key Research and Development Project under Grant 2017YFE0125300, and in part by the Science and Technology Program of Liaoning Province under Grant 2019JH2/10100019.

ABSTRACT This paper proposes a functional safety and information security protection mechanism based on blockchain technology. The design of the basic level and integration level blockchain structure of CPS distributed architecture and related functional safety and information security measures are introduced. An effective communication judgment mechanism based on functional safety error threshold is proposed, which is stored and judged by smart contract. And a refund transaction with a clock is proposed to ensure the effective execution of the functional safety error threshold mechanism. The article takes cyber physical machine tool system as an example to describe the SIL judgment method of CPS physical equipment and functional safety loop and combines SIL with fault diagnosis and risk protection. Finally, the rationality of our proposed mechanism is proved by information security, functional security, real-time and maintainability.

INDEX TERMS Blockchain, CPS, functional safety, smart contract.

NOMENCLATURE

A	collection of micro attack trees and meta attack trees
A_k	collection of known attack trees with a common end goal
TOP_OR_k	OR gate with n_k inputs and one output
g_k	attack target
MA_k	micro attack tree
MA	collection of micro attack trees
FT_k	fault tree
e_i	event
$e_{i\_subtree}$	subtree of fault tree
$Ma_{j\_success}$	the attack target of the attack tree successfully caused e_i to occur
λ	failure rate
λ_S	safety failure rate
λ_D	dangerous failure rate
λ_{DD}	dangerous detected failure rate
λ_{DU}	dangerous undetected failure rate
MRT	mean repair time
$MTTR$	mean time to repair
t_{CE}	system downtime
TI	test cycle
PFD_{avg}	average probability of dangerous failure on demand
PFH	average frequency of a dangerous failure per hour
β	common cause failure factor
SFF	safety failure fraction
Sc1	smart contract 1
μ	probability of failure per hour
TI	test time
o	output
I_A	input set A
I_B	input set B
C_A	functional safety threshold A
C_B	functional safety threshold B
t_b	buffer transaction
t_r	refund transaction
K	key
PrK	private key

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaochun Cheng.

PbK	public key
V_d	digital certificate for new enrollment device
V_b	signature of blockchain
K_s	symmetric key
DC	diagnostic coverage
e_{ron}	information security loopholes in CNC system

I. INTRODUCTION

The recent advances in our next generation of industry-Industry 4.0 puts a spotlight on cyber-physical systems [1]. The term cyber-physical systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities [2]. CPS, together with internet of things (IoT) and cloud computing, paves the way for the actualization of Industry 4.0 [3]. However, unlike IoT, after sensing the physical environment information, CPS can perform feedback operations through computing, communication, and control systems. On the basis of the industrial internet, CPS emphasizes on the physical world and the integration of operators, machines and things [4].

The goal of CPS is to provide a channel for the interaction between the physical world and the cyber word. But the natures of these two worlds vary so vastly that such interaction brings security and safety challenges. For example, CPS often monitors the dimensions of the part in the physical world in real time and feeds them to the cyber world to be calculated and analyzed to obtain the machining steps, which is then feed back to the numerical control systems in the physical world [5]. In this example, CPS can gather sensitive information about the dimensions of the parts as well as actuate changes to them. The lack of information security and functional safety will leak the confidential information of the parts, or even worse, produce unqualified products, causing devastating impacts on both the physical world and the cyber world. Many attacks on CPS have been reported [6], urging researchers to develop new techniques to defend CPS from various attacks and failures.

In this article, we explore the possibility of using blockchain technology to tackle the safety and security problem of CPS. The main concerns of this work are as follows: (1) Introducing blockchain technology to solve the problem of information security and functional safety protection of CPS; (2) Proposing a safety protection mechanism of CPS and different levels of zones Block-chain design; (3) Applying block-chain technology to the safety research of Cyber physical machine tool system (CPMTS).

II. RELATED WORKS

The researches on the safety of CPS can be traced back to 2008 [7], and are continually increasing ever since. Among the researches, Baheti and Gill [8] introduced the threats faced by CPS sensing layer, data transmission layer and application control layer. E K Wang *et al.* [9] and Ashibani and Mahmoud [10] abstracted the general workflow of the network physical system, objected to the content-aware security framework of the generic CPS system and raised some potential security issues. Choley *et al.* [11] pointed out that, due to the uniqueness of CPS, the traditional security strategies and methods are insufficient to meet the security challenges faced by CPS with different specification and different connection methods. Krishna K V [12] and Venkatasubramanian *et al.* [13] added the physical environment information gathered by the CPS sensors to the key negotiation and identity authentication technologies of CPS itself, utilized the fact that CPS can closely interact with the physical environment to its own advantage. However, the above works are directed to the separate protection and analysis of safety or security, which has been unable to meet the increasing security requirements of CPS [14].

According to IEC 61508 [15], functional safety is part of the overall safety relating to the equipment under control (EUC) and the EUC control system which depends on the correct functioning of the electrical/electronic/programmable electronic (E/E/PE) safety-related systems, other technology safety-related systems and external risk reduction facilities. Based on the suggestion of National Information Assurance Glossary, Committee on National Security Systems Instruction [16], information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

In recent years, many researchers have begun to propose specific processes or methods for achieving comprehensive analysis of functional safety and information security. These works are mainly considered form the following two aspects: (1) Functional safety and information security are similar in some respects and may even promote each other. Therefore, a integrated safety and security process in which functional safety and information security are comprehensively considered can effectively ensure safety and security and reduce costs at the same time; (2) Functional safety and information security are conflicting in some respects, and some technical measures may enhance one party, but at the same time weaken the other. Abdi *et al.* [17] concerned about the risk of security caused by information security attacks and proposed a new protection framework to ensure the safety of smart factories. Kim *et al.* [18] discussed the safety issues regarding train collisions caused by train safety signals and studied the vulnerability of CPS safety and security. Wang *et al.* [19] realized the optimization of safety systems and enhancement of security strategies by means of optimizing defensive resource allocation, their measurement increased the robustness of CPS. A detailed analysis work was reported by Wang *et al.* [20] to discuss the difference and connection between functional safety and information security, they also proposed the concept of security integration and integrated lifecycle model,

which gives a preliminary description of how to realize the security integration of intelligent manufacturing process. Śliwiński *et al.* [21] proposed a new approach to integrate safety and security assessment of industrial control system by means of process-and-procedure-based safety and security management. Compared with the traditional functional safety communication, the Safe-Sec safety communication method proposed by Song M *et al.* [22] only adjusted the data verification method to ensure the integrity and non-repudiation of the data. Wan *et al.* [23] proposed the implementation of information security in the industrial Ethernet security protocol stack based on Cortex-A8. Only device authentication, access control, and information encryption measures were adopted for common security problems, no relevant identification method for functional safety was adopted. Aimed at the feature that cyclic redundancy check only detects errors related to data integrity, Ding *et al.* [24] proposed a new extension method to quantify the residual error rate of functional safety communication of fieldbus, which provided new ideas for SIL verification of functional safety communication However, most of these processes or methods are researches on the level of risk analysis and security assessment, and have not really realized comprehensive analysis or provided systematic information security identification and protection ideas.

Blockchain security is a research area of information security and has been widely discussed. From P2P (point-to-point) networks to consensus mechanisms based on proof of work, all have contributed to the security of the native blockchain network. Liu *et al.* [25] pointed out that the architecture of the distributed system is more suitable for the user's requirements for the robustness and controllability of CPS system than the centralized architecture. Wang *et al.* [20] utilized blockchain technology to create a secure cloud storage framework with access control, where the data owner can set an effective access cycle for data usage. This implements a distributed access control scheme and effectively prevents the central authority from being attacked. Biswas and Muthukkumarasamy [26] proposed a security framework that integrates blockchain technology with smart devices to provide a secure communications platform for smart cities. Yin *et al.* [27] applied blockchain technology to M2M devices in CPS to increase the communication security. Zhang and Fan [28] proposed safety device diagnostic mechanism based on joint blockchain technology to achieve more effect, convenient and safety device maintenance. Blockchain technology has the characteristics of transparency, decentralization and high traceability, which will guarantee the functional safety research of CPS. Features such as high credibility, non-tamperability, and high encryption security are in line with current CPS information security protection research directions [29].

We believe that the integration of CPS and blockchain technology will provide new ideas and innovations for CPS's overall security research.

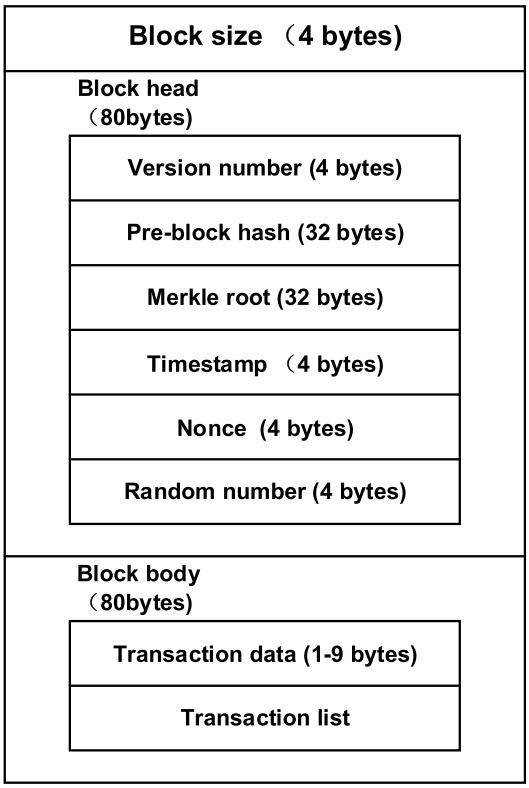

FIGURE 1. The structure of a block.

III. BLOCKCHAIN AND ANALYTICAL METHOD OF FUNCTIONAL SAFETY

A. THE CONCEPT AND ITS STRUCTURE

Blockchain is a chain structure that combines data blocks in chronological order. By maintaining this chain structure, this technology can maintain a continuously growing and non-tamperable data record [30]. As shown in Fig. 1, a block, the basic structural unit of a blockchain, consists of a block header containing metadata and a block body containing transaction data. A block header generally contains the hash value of this block, the hash value of the previous block, the timestamp, the nonce, a random number and the Merkle root that can quickly summarize all the transaction data. A block body mainly encapsulates the specific information regarding the transaction. In order to minimize the storage room, the specific information is stored in hash values.

Considering the blockchain as a state machine, each transaction is an attempt to change the state once, and each time the consensus generated block is the participant confirms the results of the state change caused by the transaction in the block. In terms of implementation, it is firstly assumed that there is a distributed data record ledger, where data can only be added but cannot be deleted. The basic structure of the ledger is a linear linked chain consisting of a series of blocks, as shown in Fig. 2, the successor block records the hash value of the leading block. New data to be added must be placed in a new block. The legitimacy of the newly added block can

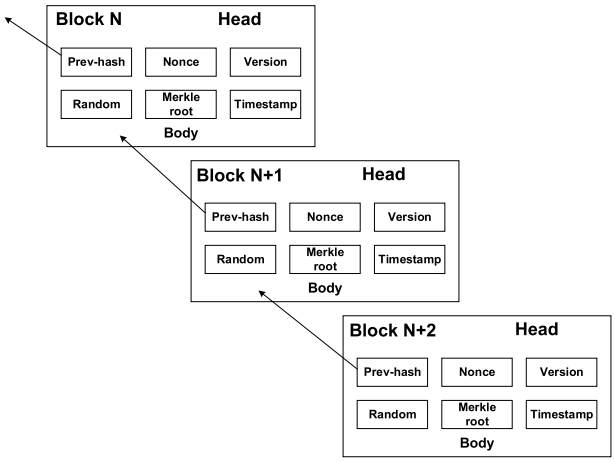

FIGURE 2. The structure of a blockchain.

TABLE 1. Safety integrity levels and interval probabilistic criteria for safety-related systems.

Safety integrity level (SIL)	PFD_{avg} interval criteria for systems operating in a low demand mode	PFH interval criteria for systems operating in a high demand or continuous mode
SIL4	$[10^{-5}, 10^{-4})$	$[10^{-9}, 10^{-8})$
SIL3	$[10^{-4}, 10^{-3})$	$[10^{-8}, 10^{-7})$
SIL2	$[10^{-3}, 10^{-2})$	$[10^{-7}, 10^{-6})$
SIL1	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

be quickly checked by quickly calculating the hash value. Any node can propose a new block, but a certain consensus mechanism must be used to agree on the final selected block.

To mitigate the physical node storage space shortage with increasing data in the blockchain, the nodes of the blockchain are divided into core nodes and light nodes. The complete blockchain data is stored in the core node, while the light node is only stored in the block data related to its own transaction, but the entire blockchain information can be obtained from the entire network at any time.

B. SAFETY INTEGRITY LEVELS OF THE PHYSICAL DEVICES

The digitization of the physical properties of CPS is not a problem that can be solved by blockchain. Only the digitized IoT data can use blockchain to enhance security. Therefore, the attributes of the physical devices are digitized into safety integrity levels (SIL) in this paper to enhance the safety level of CPS by fully utilizing the blockchain technology.

As listed in Table 1 [15], the safety integrity level (SIL) of a physical device is classified as such:

But, according to IEC 62061 [31], the SIL of that physical device is also limited by its maximum fault margin and safety failure score. See Chapter IV for specific analysis.

The functional safety basic standard IEC 61508 Appendix C gives the following methods for calculating the failure probability of the devices [32]: cause consequence

TABLE 2. [31] System structure constraint table.

SFF	DC		
	0	1	2
$< 60\%$	-	SIL1	SIL2
$60\% \sim < 90\%$	SIL1	SIL2	SIL3
$90\% \sim < 99\%$	SIL2	SIL3	SIL3
$> 99\%$	SIL3	SIL3	SIL3

analysis, fault tree analysis, Markov models, reliability block diagrams, simplified formula, etc., but the specific method selection and detailed calculation process are not introduced. Among these methods, Markov model has the highest precision, but the risk of the state transition matrix exponential explosion is too high; simplified formula possess the fastest calculation speed, but its precision is too low to meet the industrial needs; fault tree analysis is most suitable for weighting the dual requirements of computational complexity and accuracy of results. The attack tree [33] is the most commonly used method and attack example for describing information security attacks. Analogous to the fault tree analysis in system trustworthiness analysis, the attack tree model focuses on the security breach of the system and describes the set of times than can lead to system security failure. Therefore, the analyst can simulate all the attacks that a system may be subjected to and use the attack tree to analyze the security of the network system.

Compared with other methods, the advantages of the attack tree model are:

1) The tree structure allows the combination of the safety and security analysis methods to have the natural advantage of clear structure. The graphical method can more intuitively show the relationship between functional safety and information security.
2) The fault tree takes the safety event as the top event and can be further decomposed from it to find the connection with information security. The top-down structure can provide an overall threat identification and analysis that links functional safety with information security.
3) Fault trees and attack trees are mature analysis methods in the fields of functional safety and information security, respectively. There have been many research efforts to upgrade and expand them, providing a wide range of possibilities for further research in the future.

Some researchers have applied functional safety methods to the field of information security, which proves the demand to integrate functional safety and information security analysis methods. Winter *et al.* [34] adopted the hazard and operability analysis in the functional safety analysis method, and added information security analysis to the traditional hazard analysis of safety-critical systems. Schmittner *et al.* [35] used the failure mode and effect analysis model to unify functional safety and information security into a failure mode-consequence analysis model. Helmer *et al.* [36] used the fault tree to analyze the information security requirements of software intrusion and detection systems and demonstrated

the role of fault trees in the software design phase. Brooke and Paige [37] also proved that fault trees can be used not only for functional safety-critical systems, but also for the design of information safety-critical systems. However, these works are all applying the functional safety method to the field of information security. Here we explore the other way around by applying the information security method to the field of functional safety.

For attack trees, define $A = \{at_i\}$ as the set of all known micro-attack trees and meta-attack trees. The set of targets of these micro-attack trees and meta-attack trees is defined as

$$G = \{goal\ at, \forall at \in A\} \tag{1}$$

Without considering the direct physical damage, the fault tree and the attack tree are integrated and analyzed at the connection point of the "target of the attack tree" through the relationship of "the target of the attack tree being the basic event or intermediate event of the fault tree". To achieve this integration, define

$$A_k = \{at : goalat = g_k, g_k \in G, at \in A\} \tag{2}$$

where A_k represents the set of all known attack trees with a common end goal. In order to construct a new structure, a special logic gate TOP_{ORk} is defined. This logic gate is an OR gate with n_k inputs and one output satisfying the following conditions:

$$n_k = |A_k| : input_i TOP_{OR_k} = at_i \tag{3}$$

$$i = 1 \cdots n_k, outputTop_{OR_k} = g_k, \quad g_k \in G \tag{4}$$

The attack target g_k, OR gate TOP_{ORk}, and OR-related inputs are a structured micro-attack tree MA_K. A micro-attack tree includes all methods that can achieve its malicious goals.

Let MA be the set of all known micro-attack trees, then if and only if

$$\exists e_i \in EU_k : e_i = goalMA_j, \quad MA_j \in MA \tag{5}$$

the fault tree FT_k can be integrated with the information obtained from the attack tree. In other words, the fault tree can be integrated with a series of attack trees only when there is time when the target of the attack tree is the fault tree. In this way, the selected fault tree and micro-attack tree can be combined by the following steps:

1) The subtree $e_{i\_subtree}$ of the fault tree removed from the source of the event e_i is separated from the fault tree.

2) An OR gate with two inputs A and B (hereafter called a merge gate) is connected to the event e_i, which means that e_i is the output of this merge gate.

3) The micro-attack tree MA_k is connected to the input A of the merge gate. As mentioned above, we consider the ultimate goal of the attack tree as an event that occurs when the attack is successfully implemented. In this way, we have followed the rules for constructing fault trees, that is, the input and output of each logic gate should be an event.

4) The goal of the micro-attack tree MA_k is modified to "successfully attack and cause e_i to occur." In this way, we avoid the situation where the input and output of the merge gate are the same event.

5) The fault tree subtree $e_{i\_subtree}$ is used as the input B of the merge gate to complete the merge of the fault tree and the attack tree.

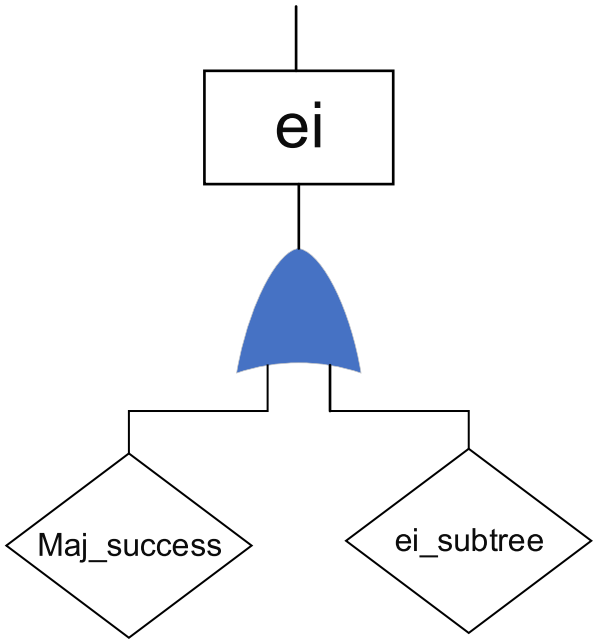

FIGURE 3. Safety and security analysis of CPS.

The formed functional safety information security extended fault tree is shown in Fig. 3. Among them, the micro-attack tree needs to be further transformed to complete a consistent format of the extended fault tree due to the different symbols.

The SIL of the underlying physical equipment of the CPS was calculated by FMEDA analysis, model in Fig. 3 and the reliability block diagram method. IEC 61508 and IEC 62061 provide the prerequisites for the calculation of failure probability of electronic, electrical and programmable electronic systems.

1) Within the lifespan of the system, the failure probability of the components of the control system is always on;

2) In the system, each processing channel (voting group) has the same failure probability and diagnostic coverage and is calculated separately. The total hardware failure rate of the system is a combination of safety failure rate and dangerous failure rate.

Taking CPMTS as an example, in the hardware design process of the numerical control system, the current hardware design mainly adopts a microprocessor-based 1oo1D structure or a dual-processor redundant cross-detection 1oo2D structure. The failure of the system mainly includes safety failure and dangerous failure. Because the 1oo1D system adopts a series structure, any module that produces a dangerous failure will cause the entire system to fail. According to IEC 61508 and IEC 62061, the 1oo1D system only needs

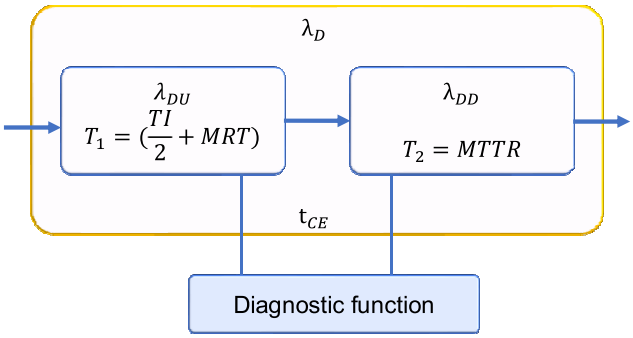

FIGURE 4. Reliability block diagram of 1oo1D.

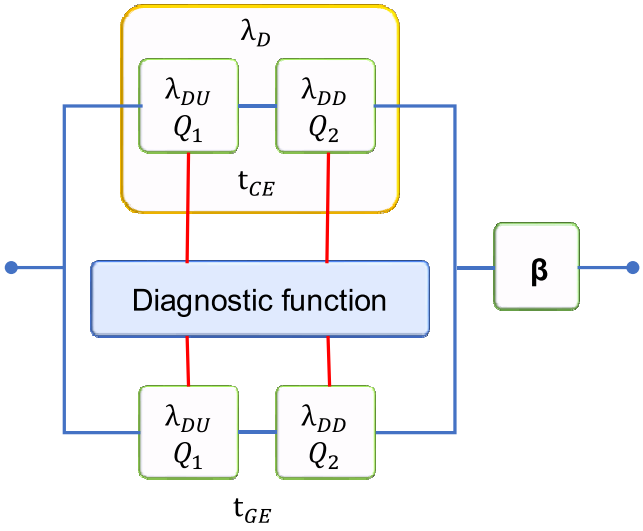

FIGURE 5. Reliability block diagram of 1oo2D.

to consider self-diagnosis and does not need to consider common cause failure. Its reliability block diagram is shown in Fig. 4:

The dangerous failure rate of this system can be expressed as:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \tag{6}$$

$MRT = MTTR$ is specified in IEC 61508, so

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{TI}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \tag{7}$$

$$PFD_{avg} = \lambda_{DD} \times MTTR + \frac{1}{2}\lambda_{DU} \times TI \tag{8}$$

Aiming at the dual-channel mutual detection structure existing in the hardware design of the numerical control system, and some specific models adopting dual-processor redundancy or a heterogeneous dual-channel mutual detection structure constructed by a processor + logic device, this structure can be abstracted into a 1oo2D structure. As shown in Fig. 5:

This structure includes two parallel channels. When a system failure is detected in any channel, the output status is output through the other channel through voting judgment. If the two channels detect a difference in execution results or detect a failure at the same time, then the system enters the safety protection state and the structural failure probability is approximately:

$$F(t) = [Q_1(t) + Q_2(t)][Q_3(t) + Q_4(t)] \tag{9}$$

$$t_{CE} = \frac{1}{2}\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{1}{2}\frac{\lambda_{DD}}{\lambda_D}MTTR \tag{10}$$

It can be seen that though the average stop time of each device is still the result obtained in the 1oo1D structure, the average stop time of the entire system is about half of the average stop time of each device. Both devices fail, and the entire system fails. Therefore, the average PFD of one device is calculated based on t_{CE}, and the other is calculated based on t_{GE}, so:

$$PFD_{avg} = 2\left(1 - e^{-\lambda_D t_{CE}}\right)\left(1 - e^{-\lambda_D t_{GE}}\right) \tag{11}$$

and according to IEC 61508, after considering the common cause failure, PDF_{avg} can be expressed by (12).

$$PFD_{avg} = 2[(1-\beta)\lambda_{DU} + (1-\beta)\lambda_{DD}]^2 t_{CE} t_{GE} + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \beta_D\lambda_{DD}MTTR \tag{12}$$

C. SIL OF FUNCTIONAL LOOPS

It should be noted that SIL is for a specific safety function. CPS safety-related systems often have multiple loops, each implementing a safety function, so a CPS with different functional loops has multiple SIL for different loops. According to IEC 61508 [32], the functional SIL are divided as follows:

When defining the SIL of a chain, distinguishing between the following two situations is necessary:

(1) For a separate module or chain, when one module fails, it will not affect other modules. In this case, the SIL of the chain is the value without parentheses in Table 3. If there are two independent modules A and B, which can switch between each other and their SIL is 2, the two modules will independently generate the same safety function, thus achieving SIL3;

(2) If the module or chain is not independent, when one module fails, it will affect other modules. In this case, the SIL of the new chain is equal to the highest SIL of the module in the parallel chain. If there are two SIL2 models or SIL1 and 2 models combined, similar failures cannot be ruled out, then the combined link SIL is 2. Therefore, the combination of the two SIL2 devices does not produce SIL3, because there may be a common cause failure. According to Gao [38], SILs of the loop circuits are listed in Table 3.

The specific analysis process is as follows:

1) Connection of the module;

2) Identify the modules related to the safety function;

3) Eliminate modules that are not related to safety functions;

4) Inductive individual chains;

5) Inductive parallel chains;

6) Change the structure of the block diagram.

TABLE 3. Sil of parallel links.

	1	2	3	4
1	2 (1)	3 (2)	4 (3)	4
2	3 (2)	3 (2)	4 (3)	4
3	4 (3)	4 (3)	4 (3)	4
4	4	4	4	4

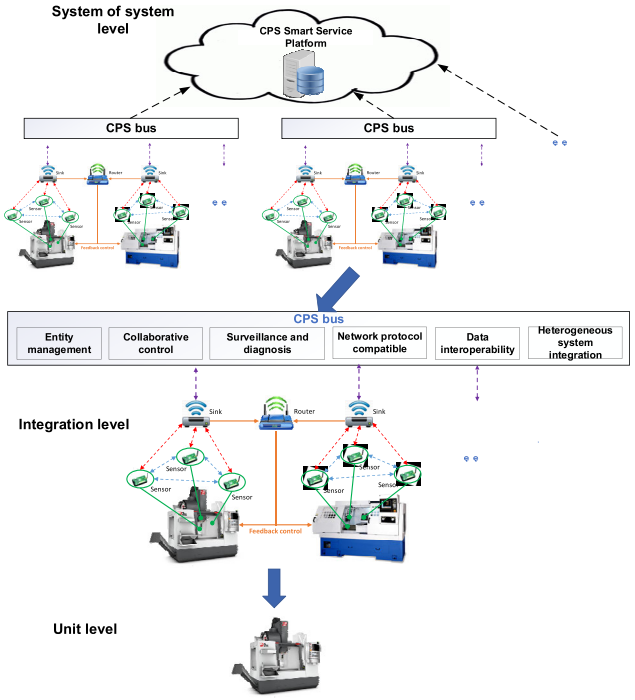

FIGURE 6. Distributed architecture of CPS.

IV. PROPOSED SAFETY AND SECURITY DIAGNOSIS MECHANISM

A. BLOCKCHAIN BASED CPS ARCHITECTURE

As an emerging technology for decentralization, the distributed architecture adopted by the blockchain can provide new ideas for CPS layout optimization. The storage and processing of conventional CPS data is centralized, which makes the entire system must be integrated. We use a distributed architecture, and its decentralized database can transfer information without going through the center, which can save costs while improving security. The distributed architecture consists of three levels, as shown in Fig. 6:

(1) Unit level. It is the smallest indivisible unit of cyber physical system. Through the physical hardware (such as transmission bearings, robot arms, motors, etc.), self-embedded software system and communication modules, it forms a basic closed loop containing the automatic flow of ''perception-analysis-decision-execution'' data. A smart component, an industrial robot or an intelligent machine tool may be the smallest unit of a CPS. In addition to this, the CPS at the cell level can also interact with the outside world.

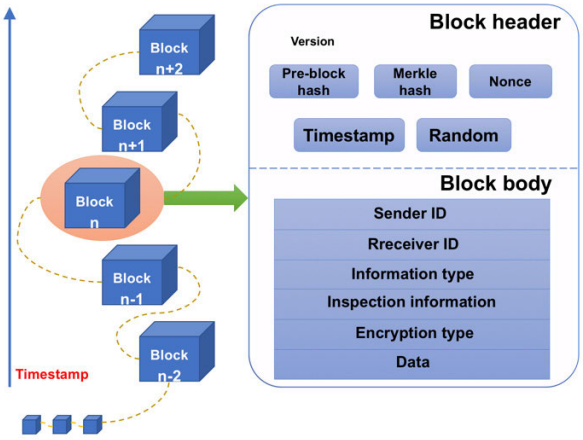

FIGURE 7. The structure of basic level blockchain.

(2) Integration level. Based on the unit-level CPS, the integrated CPS can realize the coordinated deployment of system-level CPS through the introduction of the industrial network. At this level, the integrated system-level CPS of multiple cell-level CPS and non-CPS cell devices, such as a robotic arm or a smart assembly line. The integrated level CPS mainly emphasizes the interconnection between components. On this basis, it focuses on real-time and dynamic information control of different components, realizes the coordination and unification of cyber space and physical space, and requires the unified management of integrated computing system, perception system, control system and network system.

(3) System of system level. System of system (SoS) level SoS is interconnected by multiple integrated levels of CPS, such as the integration of multiple production lines or multiple factories into a shop-level CPS or a smart factory. The SoS level covers the vastest physical space, the most complex information space networking and the most realistic perceptual data. Based on data services, SoS level also provides services such as resource management and operational optimization.

B. BLOCKCHAIN DESIGN AND SAFETY PROTECTION FOR CPS FUNCTIONAL SAFETY

1) BLOCKCHAIN DESIGN AT THE BASE LEVEL

The CPS of the basic level is used as the underlying support of the entire architecture and is mainly used to realize the connection between blocks, the storage of basic level data, and related information query. It has the following features:

1 Basic perception of CPS physical components, data storage and transmission functions;

2 Standardization function of data;

3 Save the information of the data transmission between the CPS of each base level and the transmission records.

The block structure of the base level is shown in Fig. 7. The blocks in this layer mainly store the data in the interconnection process between devices, and the functional safety of

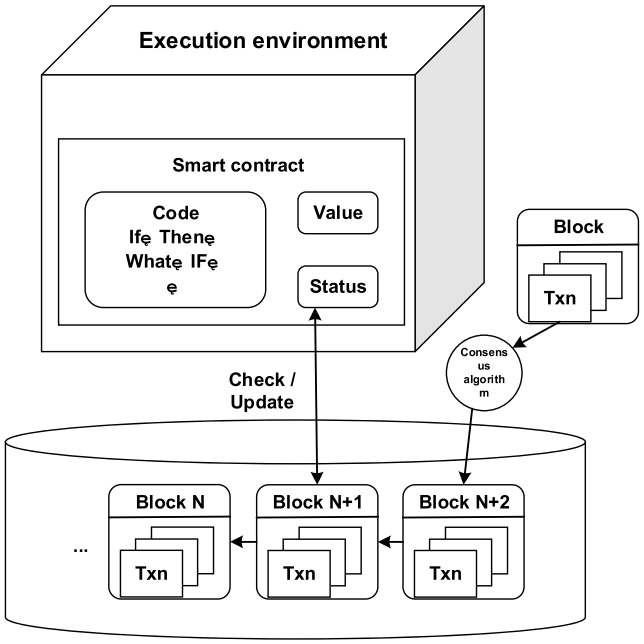

FIGURE 8. The operating mechanism between smart contracts and blocks.

the communication between the nodes is guaranteed by the effective communication of the nodes. On the wrong data, on the one hand, the entire system communication cannot be terminated due to an error in the communication, which makes the system very sensitive and adversely affects normal use, on the other hand, errors in system communication cannot be ignored, which makes it possible to operate the system in a dangerous state. Therefore, a judgment processing mechanism of an error threshold is needed to analyze the current error to determine whether the current system is operating in a normally controllable stable state.

The correct use of the functional safety error threshold mechanism first requires reliable erroneous data judgment. The key to the erroneous data judgment is the CRC check. The CRC32 algorithm is used in this design, and it is considered that CRC32 can reliably detect the error of the communication data frame [39]. Smart contracts are unique in blockchains. When a certain time, condition or special situation occurs, the contract will be triggered automatically, and the system will automatically perform the corresponding operation without human intervention [40]. As shown in Fig. 8, the smart contract Sc1 is used to perform the judgment of the block function security threshold. When an error is detected by the CRC32 check, Sc1 will increase the functional safety threshold of the block by m. Each successful communication will decrement the functional safety threshold by one. That is to say, every time a communication error occurs, m correct communication is required to offset the error. When the value of the functional safety threshold is gradually accumulated and cannot be cancelled, when the preset threshold n is reached, the node will be marked and send a report to the remaining nodes, stop the communication, and feedback the node information to the supplier for repair or replacement. When used, the numerical values of m and n are determined by the designer according to the actual situation.

We learned from the clock mechanism of Bitcoin to set a clock for the transaction between the block and the smart contract. The transaction with the set clock will not be sent to the network until the clock expires. The node receiving the transaction is responsible for storing the transaction locally and not publishing the transaction to the network until the clock expires. The clock mechanism not only guarantees the timeliness of transactions between the block and the smart contract, but also can ensure that the object of the node cannot be confined to one or several single nodes The communication between the block and the smart contract uses 2-of-2 multi-output signature to effectively block malicious attacks, so that functional safety and information security are guaranteed. The algorithm is as follows:

01: Block sends a set of input I_B to Sc1, which contains a functional safety threshold of C_B.

02: Sc1 selects its own input set I_A, which contains a functional safety threshold of C_A.

03: Sc1 creates a transaction $t_b\{[I_A, I_B], [o = C_A + C_B \rightarrow (A, B)]\}$

04: Sc1 creates a transaction with a clock $t_r\{[o], [C_A \rightarrow A, C_B \rightarrow B]\}$

05: Sc1 sends t_b and t_r to Block

06: Block signs two transactions t_b and t_r and sends them to Sc1

07: Sc1 signs t_s and broadcasts it to the blockchain network t_b is bugger transaction, the purpose of which is to lock the functional safety threshold in the communication process to the shared account. When t_b is signed and published to the network, if a participant is unable to fulfill the agreement, the multi-signature output of the transaction will not be used. In order to avoid this, we created a refund transaction with a clock t_r. If the agreed transaction is not successful before the clock expires (i.e. the functional safety threshold exceeds the system set threshold n), the transaction t_r will send a return-to-zero signal to the unfinished transaction, and the functional safety threshold is set to zero to restart the superimposed data. Increasing the effective time clock design enables more objective and fair communication effectiveness. For t_b, the transaction includes the inputs I_A and I_B of both parties to the transaction, which requires signatures from both parties. For t_r, its input o will use a single-signed output. The combination of multi-signature and single signature improves the efficiency of the algorithm while ensuring that functional safety is not affected by information security factors.

2) BLOCKCHAIN DESIGN AT THE Integration LEVEL

The structure of the integration level block is shown in Fig. 9. The integration level CPS is not a simple superposition and aggregation of the CPS at the base level, but a deep integration of the CPS at each base level. It is where the CPS of the newly accessed base layer is audited and authenticated, the data

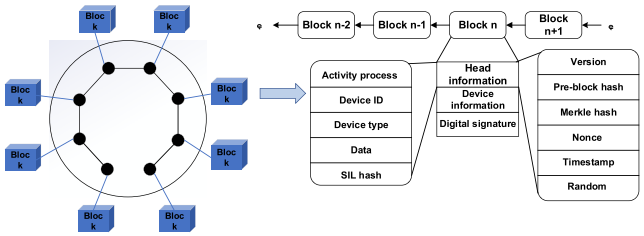

FIGURE 9. The structure of integration level blockchain.

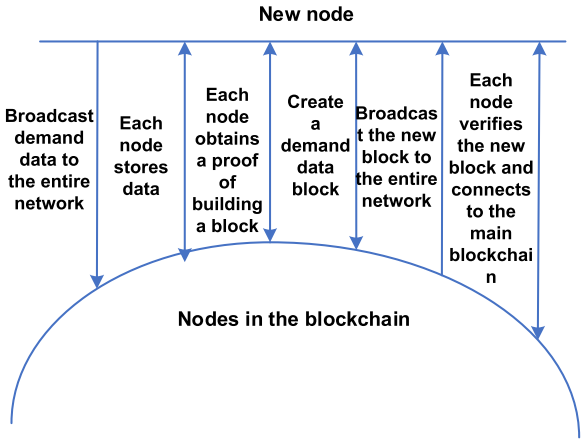

FIGURE 10. The formation process of a new block.

format is unified, the data conversion rules are established, and the traces of device connections are recorded. In addition, the integrated level CPS features interoperability, plug and play, edge gateway, data interoperability, collaborative control, monitoring and diagnostics.

The ciphertext of the process is used to mark the production process involved in the CPS of the integrated layer set and the scope of the base level CPS included. Device identification information, device type and device signature are used to implement data consistency and audit management of new devices. The main data of the transmission is mainly used to solve the problems of underlying data acquisition and heterogeneous data standardization. The key part of data consistency implementation is digital signature. In the architecture designed in this paper, once the new device is added, it means that the data it transmits is trusted. So, when the new physical device is connected to the existing integration level CPS, a rigorous review is required. In the architecture designed in this paper, new devices need to be authenticated for their components and overall functional safety before accessing the blockchain network. Registration is only possible after the certification has been passed. The new device is only registered on the blockchain by its ID, as shown in Fig. 10. In this phase, the ID and symmetric key K are embedded in each node, where K is used for data privacy protection during transmission, shared by the CPS node and its attribute application. In addition, the new device uses the SHA256 algorithm [41] to calculate the private key PrK from the random number, and then uses the algorithm such as Secp256K1 [42] to generate the public key PbK. Pbk is associated with its ID and is open to the public, while PrK is confidential. The new device is sent to the blockchain for registration with the digital certificate V_d and Pbk tagged with its own identity. The blockchain records the device's signature and returns its own signature V_b. In order to reduce the complexity of the authentication process, the blockchain uses the symmetric key K_S and transmits it back to the device node after being encrypted by the public key, and the device node verifies whether the blockchain is valid. When the two-way authentication is successful, the device can participate in the CPS of the integration level, and its data is also considered to be trusted.

The SIL verification is performed before the new device accesses the CPS. Only the physical device that meets the requirements for the SIL value can access the CPS. We use the SIL evaluation process of CPMTS to describe how the SIL of complex physical equipment is determined. In the process of safety integrity assessment of a system, the system can be divided according to functions, software and hardware structures, etc., and then the system safety integrity assessment is performed around the system hardware and software submodules, and finally the safety integrity of the overall system evaluation result. The overall safety and integrity of the CNC system is determined by the minimum values of system software and hardware SIL. Taking the LT-B10 CNC system as an example, the hardware functional safety of CPMTS is evaluated. We use failure mode, impact, and diagnostic analysis FMEDA to quantify the failure parameters of the device hardware circuit, and based on this, apply a probability assessment model suitable for exponential distribution: based on the extended fault tree reliability block diagram method for device hardware Model the safety assessment and determine the hardware SIL of the device.

According to the functional characteristics of the LT-B10 CNC device, the structure can be divided into four main functional modules: base plate, power module, display board, and core board. The four modules form a series structure in function, which is a typical 1oo1D structure.

Taking the base plate module as an example, provided by the manufacture, the FMEDA forms including the device name, label, function, failure mode, failure impact, importance, and various failure data are sorted according to function classification, and the sub-units of the base plate module are more detailed: such as the control unit, power supply unit, NCSF bus unit, USB unit, LCD screen unit, BOOT selector switch failure data, as shown in Table 4. Bring into the formula (13) and (14), you can get the percentage of dangerous failures and the diagnostic coverage DC of each module sub-unit on the base plate.

$$DC = \sum \frac{\lambda_{DD}}{\lambda_D} \tag{13}$$

$$SFF = \left(\sum \lambda_s + \sum \lambda_{DD}\right) \Big/ \left(\lambda_S + \lambda_D\right) \tag{14}$$

According to Table 5, FMEDA analysis were performed on the power supply module, core board module, and display module of the device.

TABLE 4. FMEDA analysis of base plate.

Unit	Sub-unit	λ_{DD}	λ_{DU}	Dangerous failure percentage	DC
base plate	control unit	69.53	495.57	0.3925505	0.12304
	power unit	58.28	459.60	0.3640551	0.11254
	NCSF unit	0	191.49	0.1516808	0
	USB unit	0	79.36	0.0628592	0
	LCD unit	10	25.84	0.0206391	0.27904
	boot select switch	0	10.59	0.0138094	0

TABLE 5. FMEDA summary.

	(1E-9/h)					
Modular	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	DC	SFF
base plate	0	1885.44	137.81	1262.432	9.84%	61.58%
display plate	0	348.47	0	958.845	0.00%	26.66%
core plate	0	614.86	244.33	905.094	21.26%	48.70%
power	0	125.6	28.86	93.953	23.50%	62.18%

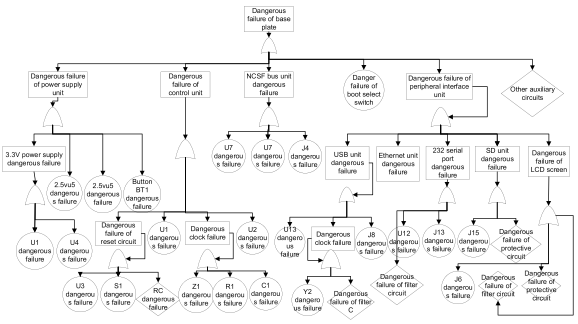

FIGURE 11. Fault tree model of base plate.

According to Chapter III, the fault tree model and the attack tree model of CPMTS can be illustrated as Fig. 11 and Fig. 12, respectively. The attackers can access CPMTS by scanning the operator's data communication or removable storage media. The scan found vulnerabilities ($e_{ro1}, e_{ro2}, e_{ro3}$) in the CNC system and obtained user permissions After entering the core network of CPMTS, and then re-flashing the ECU system firmware by reverse engineering, the attackers can enter the firmware to set the bus data values, tamper with

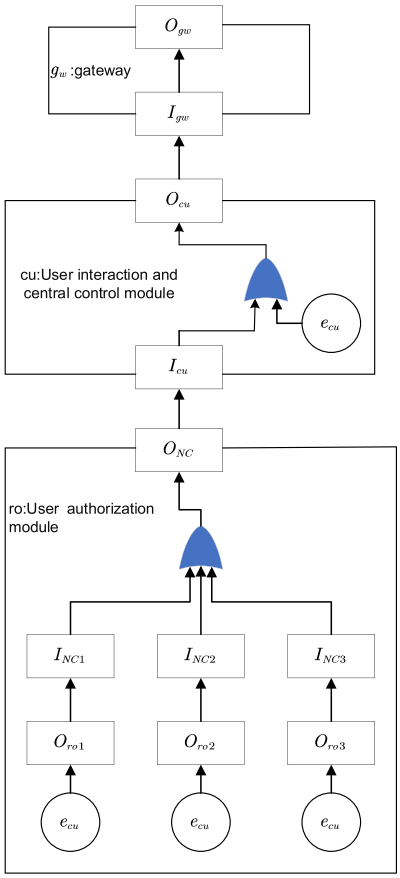

FIGURE 12. Attack tree of CPMTS.

the bus data, send error control instructions to the physical process, or send error data to the control center.

The attack tree is mainly combined with the failed branch of the Ethernet unit in the peripheral interface unit of the base plate. The fault tree-attack tree model is as follows:

Combined with the failure data of the backplane module in the FMEDA summary table analyzed earlier, we can get:

$$\begin{aligned} PFD_{avg} &= \frac{1}{TI}\int_0^{TI}(\lambda_{DD}\times MTTR+\lambda_{DU}\times t)\,dt \\ &= \lambda_{DD}\times MTTR+\frac{1}{2}\lambda_{DU}\times TI \\ &= 137.8104\times 10^{-9}\times 8 \\ &\quad +\frac{1}{2}\times 1262.432\times 10^{-9}\times 8760 \\ &= 5.531\times 10^{-3} \end{aligned} \tag{15}$$

Taking that the TI functional test time is 8760 h and MTTR average maintenance time is 8 h for the above calculations, we can get:

$$\begin{aligned} PFH &= PFD/TI \\ &= 1.106\times 10^{-2}\div 8760 \\ &= 1.263\times 10^{-6} \end{aligned} \tag{16}$$

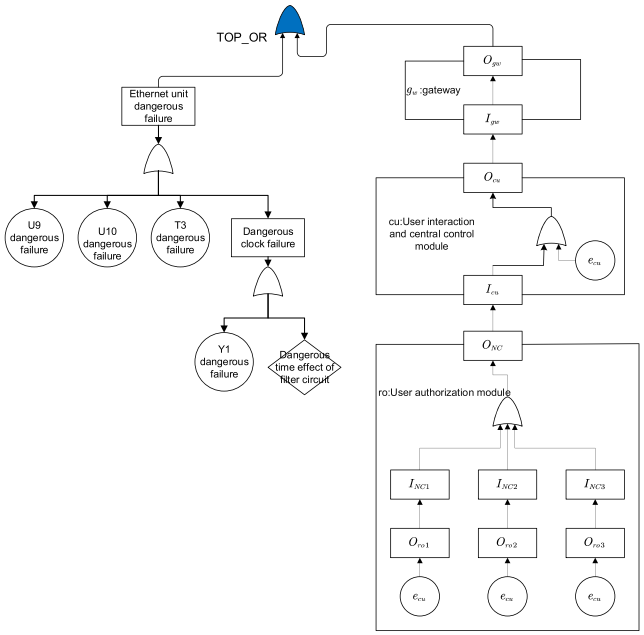

FIGURE 13. Fault tree-attack tree of base plate (part).

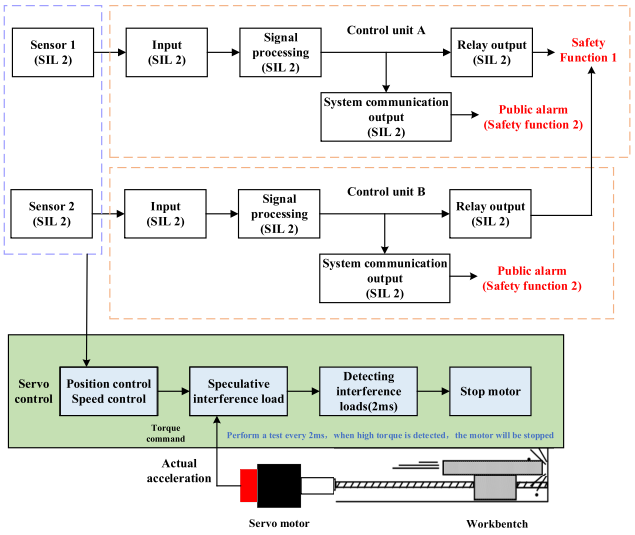

FIGURE 14. The safety alarm system of CPMTS.

The failure data of the CNC system and other components are as follows:

Comparing between Table 6 and Table 1, we can obtain the SIL of the numerical control equipment and each component and store it in a block.

In addition to the first step of verification when the device is connected to the CPS, the SIL can also provide protection for the physical device as a judgment condition when the physical device is running. We still use CPMTS as an example to discuss. The entire security alarm system is shown in Fig. 14.

For the safety problem of the mechanical abnormality during the automatic machining of the machine tool of CPMTS,

TABLE 6. Failure probability table.

	PFD	PFD_{avg}	PFH
base plate	1.106×10^{-2}	5.531×10^{-3}	1.262×10^{-6}
display plate	8.399×10^{-3}	4.199×10^{-3}	9.588×10^{-7}
core plate	7.931×10^{-3}	3.966×10^{-3}	9.053×10^{-7}
power	8.233×10^{-4}	4.117×10^{-4}	9.397×10^{-8}
CNC	2.919×10^{-2}	1.459×10^{-2}	3.33×10^{-6}

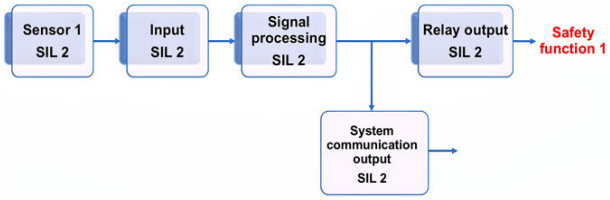

FIGURE 15. Identify the modules related to the safety function.

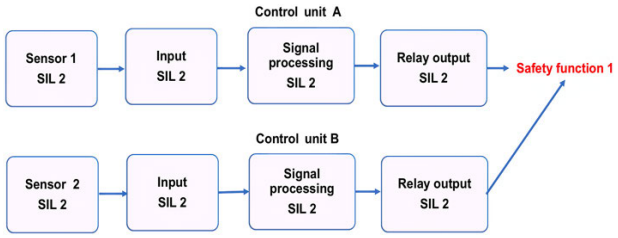

FIGURE 16. Eliminate modules that are not related to safety functions.

the measuring unit is constituted by the speed and acceleration sensor to detect the running state. Assume that the safety system consists of one measurement unit (including two sensors), two control units (including two input modules, two signal processing modules), two system communication output alarm modules, two relay output modules and a common alarm unit (including the system communication input module, the signal processing module and the relay output module) is composed, and assuming that the SIL of each module is 2, according to the introduction, the safety alarm function SIL is determined as follows:

The safety alarm system as shown in Fig. 10 has two security functions, namely:

Safety function 1: Each control unit triggers its own relay output, and both relay outputs can perform unified safety function. The SIL determination of safety function 1 is shown in Fig. 15 – Fig. 18.

Safety function 2: The control unit transmits the alarm signal to the public alarm unit. The SIL determination of the safety function 2 is shown in Fig. 19 – Fig. 23.

According to the final operation mode of the safety function SIL and CMPTS, corresponding protective measures are taken. For example, the servo axis of CPMTS will take the operation of stopping immediately at the current

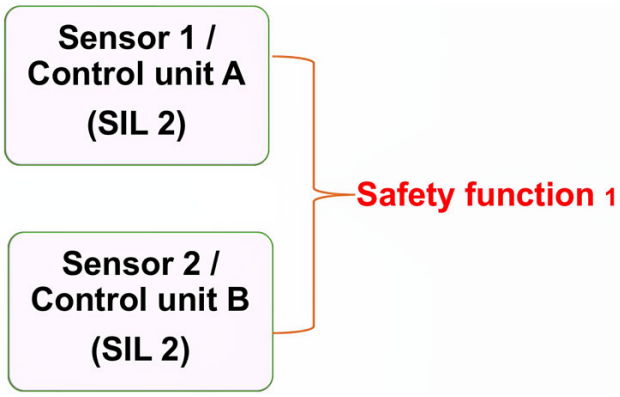

FIGURE 17. Inductive individual chains.

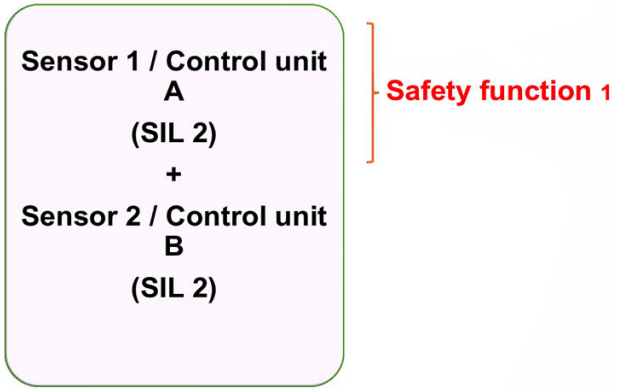

FIGURE 18. Inductive parallel chains.

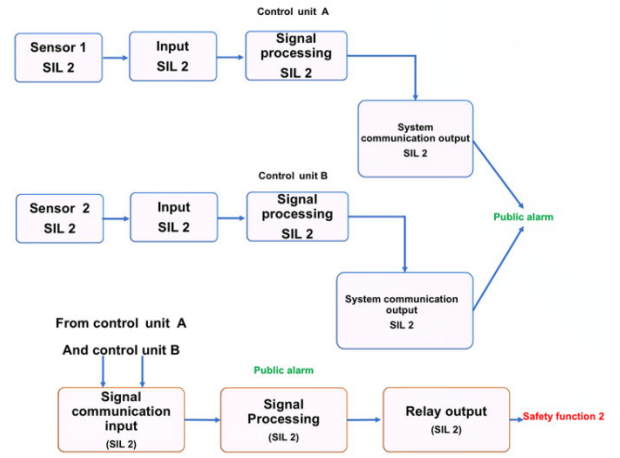

FIGURE 19. Eliminate modules that are not related to safety functions.

position or specifying the amount of return according to different SIL.

3) BLOCKCHAIN DESIGN AT THE SoS LEVEL

This level packs the system level block data within different organizations to form a higher level blockchain. This blockchain is used to implement higher-level data query and record and requires coordination between different organizations. Because the application scenarios involved are limited, this article does not consider it.

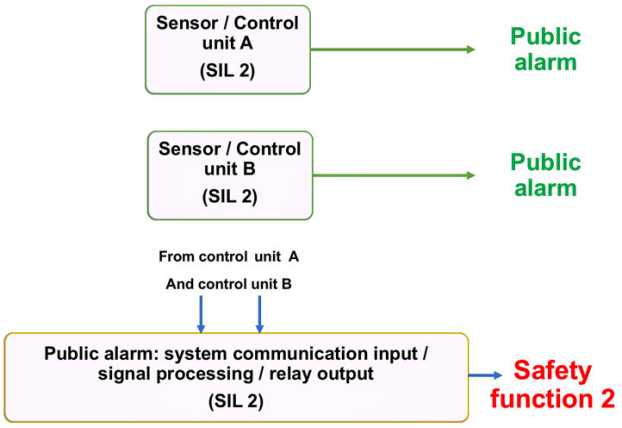

FIGURE 20. Inductive individual chains (the first loop).

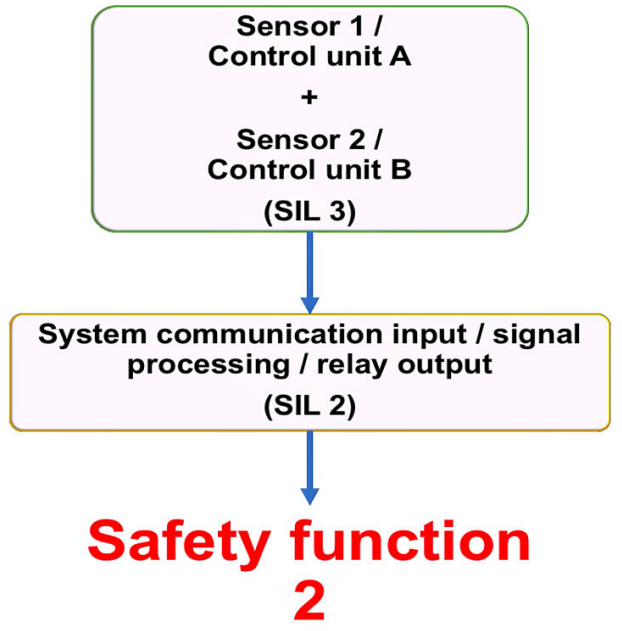

FIGURE 21. Inductive parallel chains (the first loop).

V. SAFETY ANALYSIS AND DISCUSSION

The significance of CPS is to network physical devices and to embed and connect computing and communication units onto physical systems or processes. This makes the requirements of CPS add safety based on traditional confidentiality, availability, and integrity. The safety of our proposed safety mechanism is discussed from four aspects:

1) Confidentiality. The blockchain mainly uses address randomization, information encryption and state channels to ensure the confidentiality of information. CPS generates a large amount of data in the process of sensing, computing and service. The safety mechanism proposed by us fully utilizes the principle of confidentiality of the blockchain. The content of data and transactions is encrypted by asymmetric key in the process of transmission and storage. It effectively

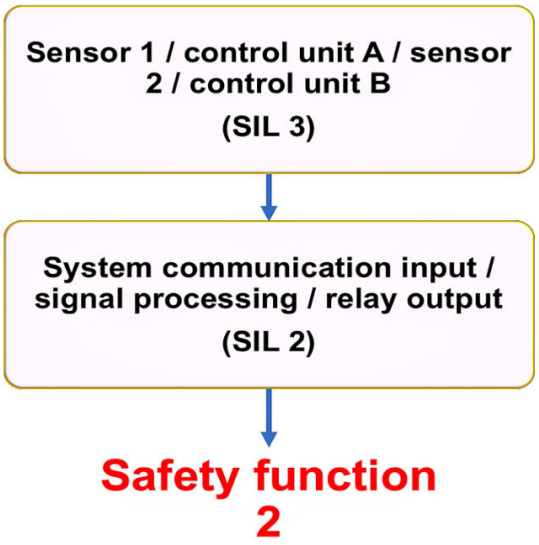

FIGURE 22. Change the structure of the block diagram (the first loop).

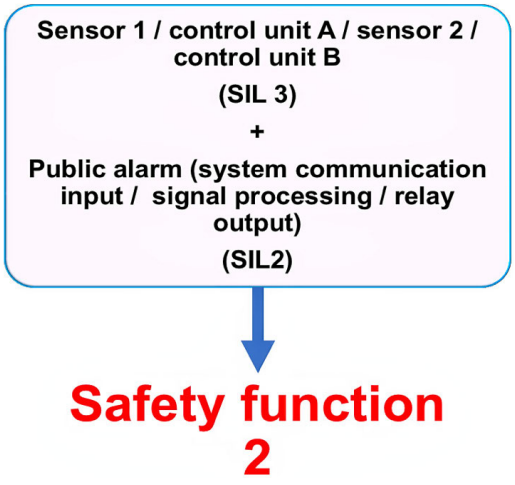

FIGURE 23. Inductive individual chains (the second loop)–ended.

prevents the risk of important data being acquired after the information is hijacked, thereby protecting the privacy of the user and the transmission of the perceived data and the calculated data. In the process of block authentication, because the transmission environment is relatively secure, we transmit it back to the device node with a symmetric key with relatively low complexity. Our proposed safety mechanism effectively reduces the complexity of the authentication process while ensuring the confidentiality of CPS information.

2) Availability. The distributed architecture adopted by the blockchain provides a new idea for CPS layout optimization. The blockchain has multiple backup ledgers, and the ledgers are stored on the distributed nodes. The cryptographic algorithm is used to store the data in the block, such as the hash algorithm (Fig. 24), except that the length of the fixed text data can be saved as a fixed-length hash value can also identify data tampering due to large changes in the hash value

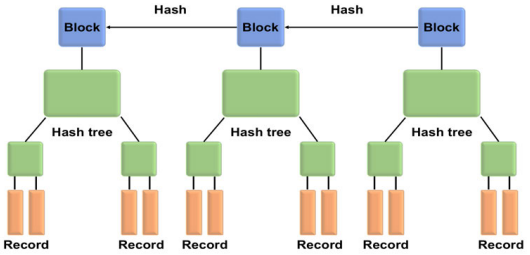

FIGURE 24. Hash algorithm in blockchain.

as the text data changes. In the blockchain network, the joining and exiting of nodes are carried out in a trusted environment. Since the entire environment is transparent and open, no node can deceive other nodes, and manipulation or loss of one individual account does not affect the system.

3) Integrity. CPS must ensure the long-term operation of the system is safe and reliable, the industrial control process is continuous and highly available, which poses huge challenges to the requirements of data integrity. Under our mechanism, physical entities wanting to access CPS need to first perform functional safety authentication and need to register in the blockchain. This makes the safety and reliability of CPS guaranteed. At the same time, the access of the nodes requires the mutual authentication of all the blocks, which can ensure the authenticity of the data. The blockchain defines the hash value and timestamp of the previous block due to the header. Once the transaction information in the block changes, the pre-hash of the post block will change, which makes the block chain impossible to tamper with, thus the integrity of the data can be well protected. At the same time, the signatures, Consensus, data chaining and timestamps that determine the identity of the two parties constitute a complete distributed ledger chain, each of which is protected by cryptographic principles. Our proposed mechanism protects information and data integrity in an important way.

4) Safety. Due to the large increase in the number of entities and the size of the network, the information security and functional safety boundaries of the system are gradually blurred. From the perspective of the risk evolution path, the differences and similarities between the two have the possibility of combining. Fig. 25 shows the evolution path of the two accidents and their relationship with the environment and the system. The main difference in forming the evolution path is the different starting points. The evolution paths after a failure or attack are similar. The protection mechanism proposed in this paper uses smart contracts to allow users who do not trust each other to complete the transaction without the need of third-party trusted intermediary or authority to ensure the security of communication between CPS devices, and to use

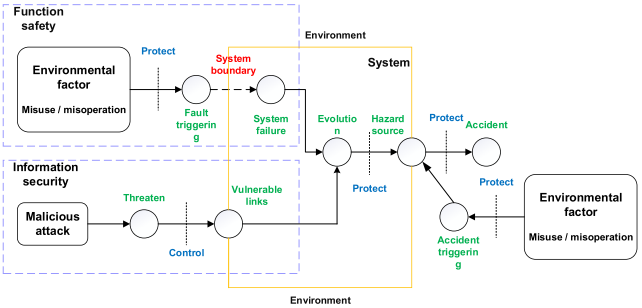

FIGURE 25. Comparison of evolution paths of safety accidents and security accidents.

blockchain technology for information security. The effective protection ensures that the data related to functional safety is not affected by information security attacks, and the communication security is guaranteed to the greatest extent. We store the ID, image, sound, environmental data, location data, and CPS device ID and SIL information generated by the sensor network through the blockchain. For the functional safety protection of CPS equipment, the data integrity of the blockchain can guarantee the prediction and identification of risks and faults. Traceability can provide important clues for subsequent protection measures when risks occur.

In addition to the above safety and security features, our mechanism can also guarantee the real-time and the maintainability of CPS.

Real-time performance is an important requirement of CPS [39]. The industry needs CPS to track the running status of physical entities in real time. We use smart contracts to make judgments about functional safety error communication thresholds. We designed an effective communication time to eliminate redundancy without sacrificing privacy or control. In the process of interworking between blockchain and smart contract, two transaction modes are designed. Different ways of multi-signature and single signature are adopted according to different degrees of confidentiality, which greatly improves the efficiency of the algorithm.

Maintainability. The header block and the timestamp contained in the header of the blockchain can be used to connect the blocks in a chronological chain pattern. This makes the order of historical information fixed and impossible to change. When the CPS receives the risk and fault alarm and makes protective measures such as emergency stop, the repairer can rely on the query historical information to effectively maintain or replace the machine. At the same time, mutual communication records between nodes can also assist in querying faulty nodes and nodes that may have problems. Applying blockchain technology to CPS security protection can effectively improve the maintainability of CPS.

VI. CONCLUSION

With the development and integration of technology, CPS is gradually interconnected with the public network. In addition to its widespread use of common physical equipment and communication protocols, a large number of defects and risks have emerged. This paper proposes a safety and security protection mechanism based on blockchain technology, proposes a distributed architecture of CPS, and designs the blockchain structure corresponding to each level of the architecture. Before the physical device accesses the CPS, it first authenticates its SIL and stores its SIL in the corresponding block to assist in fault diagnosis and risk protection during the operation of the device. Taking CPMTS as an example, we introduce the calculation method of physical equipment SIL and the determination method of safety function loop SIL. In the process of establishing a new device block, we use an encryption method combining asymmetric key and symmetric key to reduce the complexity of the authentication process. For the interworking between devices, we propose a fault threshold mechanism to ensure functional safety and information security in the communication process. We use smart contract technology to store and judge functional safety thresholds. We draw on the clock mechanism of Bitcoin and propose a refund transaction mode with clock to make the judgment of functional safety error threshold more objective and accurate. Transaction authentication is performed by means of a single signature and a multi-signature hybrid. This hybrid signature method is more efficient than the conventional multi-signature transaction method. Analysis of security, real-time and reliability proves that our proposed mechanism can meet the safety and security requirements of CPS. In future work, we will optimize the algorithm for functional safety thresholds and optimize the computational overhead of the entire protection mechanism and improve its scalability.

ACKNOWLEDGMENT

(Ai Gu and Zhenyu Yin contributed equally to this work.)

REFERENCES

[1] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015.
[2] H. Mo, N. S. Wagle, and M. Zuba, "Cyber-physical systems," *ACM Mag. Students*, vol. 20, no. 3, pp. 8–9, 2014.
[3] H. S. Kang, J. Y. Lee, S. Choi, H. Kim, J. H. Park, J. Y. Son, B. H. Kim, and S. D. Noh, "Smart manufacturing: Past research, present findings, and future directions," *Int. J. Precis. Eng. Manuf.-Green Tech.*, vol. 3, no. 1, pp. 111–128, Jan. 2016.
[4] M. Zhan, J. Wu, H. Wen, and P. Zhang, "A novel error correction mechanism for energy-efficient cyber-physical systems in smart building," *IEEE Access*, vol. 6, pp. 39037–39045, 2018, doi: 10.1109/access.2018.2854794.
[5] K. M. Alam and A. El Saddik, "C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems," *IEEE Access*, vol. 5, pp. 2050–2062, 2017.
[6] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.
[7] Y. Tang, H. Wang, K. Guo, Y. Xiao, and T. Chi, "Relevant feedback based accurate and intelligent retrieval on capturing user intention for personalized websites," *IEEE Access*, vol. 6, pp. 24239–24248, 2018.

[8] R. Baheti and H. Gill, "Cyber-Physical Systems," *Impact Control Technol.*, vol. 12, no. 1, pp. 161–166, 2011.

[9] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Security issues and challenges for cyber physical system," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun. Int. Conf. Cyber, Phys. Social Comput.*, Dec. 2010.

[10] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Comput. Secur.*, vol. 68, pp. 81–97, Jul. 2017.

[11] J.-Y. Choley, F. Mhenni, N. Nguyen, and A. Baklouti, "Topology-based safety analysis for safety critical CPS," *Procedia Comput. Sci.*, vol. 95, pp. 32–39, Jan. 2016.

[12] K. K. Venkatasubramanian, "Security solutions for cyber-physical systems," in *User-Driven Healthcare: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2009.

[13] K. K. Venkatasubramanian, S. Nabar, S. K. S. Gupta, and R. Poovendran, "Cyber physical security solutions for pervasive health monitoring systems," in *User-Driven Healthcare: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2012.

[14] D. Dinculeană and X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," *Appl. Sci.*, vol. 9, no. 5, p. 848, Feb. 2019, doi: 10.3390/app9050848.

[15] *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Parts 1*, Standard IEC 61508-1:2010, IEC, 2010.

[16] National Information Assurance Glossary, Standard CNSS Instruction 4009, Committee on National Security Systems, Apr. 2010.

[17] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Preserving physical safety under cyber attacks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6285–6300, Aug. 2019.

[18] S. Kim, Y. Won, I.-H. Park, Y. Eun, and K.-J. Park, "Cyber-physical vulnerability analysis of communication-based train control," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6353–6362, Aug. 2019, doi: 10.1109/jiot.2019.2919066.

[19] W. Wang, F. Di Maio, and E. Zio, "Adversarial risk analysis to allocate optimal defense resources for protecting cyber–physical systems from cyber attacks," *Risk Anal.*, vol. 39, no. 12, pp. 2766–2785, Dec. 2019, doi: 10.1111/risa.13382.

[20] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019, doi: 10.1109/access.2019.2929205.

[21] M. M Śliwiński, E. Piesik, and J. Piesik, "Integrated functional safety and cyber security analysis," *IFAC-PapersOnLine*, vol. 51, no. 24, pp. 1263–1270, 2018, doi: 10.1016/j.ifacol.2018.09.572.

[22] M. Song, T. R. Wang, K. D. Xu, Z. J. Yang, and K. Wang, "Study on the safe-sec safety communication approach for control system," *Process Autom. Instrum.*, vol. 34, no. 11, pp. 30–33, 2013, doi: 10.16086/j.cnki.issn1000-0380.2013.11.013.

[23] Y. P. Wan, S. Huang, Y. Qin, and C. Zhou, "Development of industrial Ethernet security protocol stack based on cortex-A8," *Comput. Eng. Des.*, vol. 34, no. 6, pp. 1941–1945, 2013, doi: 10.16208/j.issn1000-7024.2013.06.064.

[24] L. Ding, H. Wang, A. Xu, and S. Li, "New considerations for SIL verification of functional safety fieldbus communication," *J. Loss Prevention Process Industries*, vol. 43, pp. 488–502, Sep. 2016, doi: 10.1016/j.jlp.2016.07.013.

[25] J. Liu, D. W. Su, K. J. Qian, F. Shi, and L. W. Wang, "A method of distributed state estimation in dispatch central based on ripe data and topology model of substation," *Adv. Mater. Res.*, vols. 732–733, pp. 1283–1287, Aug. 2013.

[26] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun.; IEEE 14th Int. Conf. Smart City; IEEE 2nd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2016.

[27] S. Yin, J. Bao, Y. Zhang, and X. Huang, "M2M security technology of CPS based on blockchains," *Symmetry*, vol. 9, no. 9, p. 193, Sep. 2017, doi: 10.3390/sym9090193.

[28] X. Zhang and M. Fan, "Blockchain-based secure equipment diagnosis mechanism of smart grid," *IEEE Access*, vol. 6, pp. 66165–66177, 2018, doi: 10.1109/access.2018.2856807.

[29] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," *IEEE Access*, vol. 6, pp. 32910–32924, 2018.

[30] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[31] *Safety of Machinery-Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems*, Standard IEC 62061:2015, IEC, 2015.

[32] Y. Khalil, "New statistical formulations for determination of qualification test plans of safety instrumented systems (SIS) subject to low/high operational demands," *Rel. Eng. Syst. Saf.*, vol. 189, pp. 196–209, Sep. 2019, doi: 10.1016/j.ress.2019.04.033.

[33] S.-W. Choi, "Establishment of extended model for determining and evaluating ASIL in the ISO 26262 automotive functional safety system," *J. Korean Inst. Plant Eng.*, (in Korean), vol. 22, no. 2, pp. 39–55, 2017. [Online]. Available: https://KJD:ART002242276

[34] R. Winther, O.-A. Johnsen, and B. A. Gran, "Security assessments of safety critical systems using HAZOPs," in *Computer Safety, Reliability, and Security*, U. Voges, Ed. Berlin, Germany: Springer, 2001, pp. 14–24.

[35] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," in *Computer Safety, Reliability, and Security*, A. Bondavalli F. Di Giandomenico, Eds. Cham, Switzerland: Springer, 2014, pp. 310–325.

[36] G. Helmer, J. Wong, M. Slagell, V. Honavar, L. Miller, and R. Lutz, "A software fault tree approach to requirements analysis of an intrusion detection system," *Requirements Eng.*, vol. 7, no. 4, pp. 207–220, Dec. 2002, doi: 10.1007/s007660200016.

[37] P. J. Brooke and R. F. Paige, "Fault trees for security system design and analysis," *Comput. Secur.*, vol. 22, no. 3, pp. 256–264, Apr. 2003, doi: 10.1016/s0167-4048(03)00313-4.

[38] S. C. Gao, "Design of safety instrumented function loop & SIL certification," *Autom. Petro-Chem. Ind.*, vol. 53, no. 4, pp. 8–13, 2017, doi: 10.3969/j.issn.1007-7324.2017.04.003.

[39] T. Li, Z. Liu, J. Li, C. Jia, and K.-C. Li, "CDPS: A cryptographic data publishing system," *J. Comput. Syst. Sci.*, vol. 89, pp. 80–91, Nov. 2017, doi: 10.1016/j.jcss.2016.12.004.

[40] C. Xu, Z. Z. Han, Q. Y. Wang, G. F. Zhao, and S. Yu, "Modelling the impact of interference on the energy efficiency of WLANs," *Concurr. Comput.-Pract. Exper.*, vol. 31, no. 17, Sep. 2019, Art no. e5217, doi: 10.1002/cpe.5217.

[41] P. Yin, Q. Huang, P. Shi, and X. Cai, "Blockchain based large data security identity authenticating method, involves accessing private key by data node, and blocking big data node from accessing asset network when public key in digital fingerprint not matches private key," CN Patent 109 743 167 A, Appl. CN 109 743 167 A, and CN 10 011 189, Jan. 7, 2019, [Online]. Available: https://DIIDW:201944967M

[42] S. Fan, W. Wang, and Q. Cheng, "Attacking OpenSSL implementation of ECDSA with a few signatures," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, 2016, pp. 1505–1515.