International Journal of Automation and Computing 12(6), December 2015, 567-578
DOI: 10.1007/s11633-015-0923-9

Cyber-physical System Security for Networked Industrial Processes

Shuang Huang[1,2] Chun-Jie Zhou[1,2] Shuang-Hua Yang[3] Yuan-Qing Qin[1,2]

[1]School of Automation, Huazhong University of Science and Technology, Wuhan 430074, China

[2]Key Laboratory of Ministry of Education for Image Processing and Intelligent Control, Wuhan 430074, China

[3]Department of Computer Science, Loughborough University, Leicestershire, UK

Abstract: Cyber-physical systems (CPSs) are integrations of networks, computation and physical processes, where embedded computing devices continually sense, monitor, and control the physical processes through networks. Networked industrial processes combining internet, real-time computer control systems and industrial processes together are typical CPSs. With the increasingly frequent cyber-attack, security issues have gradually become key problems for CPSs. In this paper, a cyber-physical system security protection approach for networked industrial processes, i.e., industrial CPSs, is proposed. In this approach, attacks are handled layer by layer from general information technology (IT) security protection, to active protection, then to intrusion tolerance and physical security protection. The intrusion tolerance implemented in real-time control systems is the most critical layer because the real time control system directly affects the physical layer. This novel intrusion tolerance scheme with a closed loop defense framework takes into account the special requirements of industrial CPSs. To illustrate the effectiveness of the CPS security protection approach, a networked water level control system is described as a case study in the architecture analysis and design language (AADL) environment. Simulation results show that 3 types of injected attacks can be quickly defended by using the proposed protection approach.

Keywords: Critical infrastructures, cyber-physical systems (CPSs), information security, system and architecture design, intrusion tolerance.

1 Introduction

Cyber-physical systems (CPSs) are integrations of networks, computation and physical processes, where embedded computing devices continually sense, monitor, and control the physical processes through networks, usually with closed loops in which physical processes affect computations and vice versa[1]. Modern networked industrial processes and critical infrastructures, such as water treatment[2], transportation[3], and chemical plants[4], are typical industrial CPSs[5].

In the past few years, industrial control systems have implemented special and proprietary communication networks to ensure the isolation of monitoring and control functions from external networks[6, 7]. Designers typically built control systems with fault-tolerant techniques with special attention to disaster recovery[8, 9], but ignored security protection. It was assumed that the system is protected because it is not accessible from external networks[10]. However, nowaday, industrial CPSs combine components of the cyber world and the physical layer together to achieve a common goal[11]. The physical processes are usually controlled/monitored over a network through embedded computer systems, where the physical layer affects the cyber system and vice-versa[12, 13]. While the cyber world provides remote monitoring and control functions, it also brings potential cyber-security problems[14, 15]. The cyber-security issues are crucial for the industrial CPSs because the entities within the systems not only interact with each other but also interact with the physical environment. Cyber-security guarantee of the industrial CPS must be designed according to the hierarchical structure of the system, and all levels of cyber-security must be taken into account[16]. However, many industrial control systems do not have their built-in security functionalities, and the cyber-security solutions in the information technology (IT) domain are not suitable for industrial CPSs because of the different goals and assumptions concerning the protection[17, 18]. Therefore, it is necessary to develop a flexible and resilient cyber-security protection approach to guarantee the cyber-security of the industrial CPS.

In this paper, a multi-layer cyber-security protection architecture with flexible structure and resilient intelligence for industrial CPSs is proposed, which can help us to make cyber-security strategies for industrial CPSs. In the architecture, the real time (RT) control layer security is the most critical layer and is quite different from those of other layers, because controllers are connected to physical devices directly and the decisions of controllers have an immediate impact on the physical layer. The intrusion tolerance protection with a closed loop defense framework is built to guarantee the control layer security, which takes into account the domain features of the industrial control system.

Regular paper
Manuscript received April 18, 2014; accepted August 1, 2014
This work was partially supported by Natural Science Foundation of China (Nos. 61272204 and 61433006) and the Fundamental Research Funds for the Central Universities, China (No. 2013ZZGH006).
Recommended by Associate Editor Hong-Nian Yu

To evaluate the efficiency of the cyber-security protection architecture, a networked water level control system is investigated as a case study. A cyber-security verification platform based on the ocarina architecture analysis and design language (AADL) tool suite[19] is established for the networked water level control system to analyze the process of cyber-security protection approach.

The paper is organized as follows. Section 2 analyzes the cyber-security issues of the industrial CPS. In Section 3, a multi-layer cyber-security architecture for the industrial CPS is proposed. The detail of the intrusion tolerance scheme with a closed loop defense framework for the RT control layer is given in Section 4. Then, Section 5 presents a networked water level control system as a case study based on the ocarina AADL tool suite to evaluate the cyber-security protection approach. Section 6 makes a conclusion.

2 Security analysis of industrial CPSs

Historically, industrial control systems were either physically isolated or connected to other systems only through the proprietary hardware and communications. The security issue was not critical. However, currently, the industrial CPSs, which are the main form of industrial control systems, are rapidly evolving: from proprietary to standard protocols, and from isolation to interconnection with corporate business networks. Consequently, the security issues of industrial CPS are urgently required to be resolved. Fig. 1 shows a general hierarchical architecture of an industrial CPS.

According to the confidentiality, integrity, availability (CIA) triad model[20], the security goals of general information technology (IT) systems are confidentiality, integrity, and availability, where confidentiality is considered as the most important one. However, these security goals can be prioritized differently in the industrial control environment. A major disaster might happen when a system component such as a controller is unavailable, which could cause serious injury to the people or widespread damage to the environment. Thus, security in these systems is primarily concerned with maintaining the 24/7 availability of all system components and controlled plants. Fig. 2 illustrates the security goals and their priorities in the industrial CPS and the IT domain.

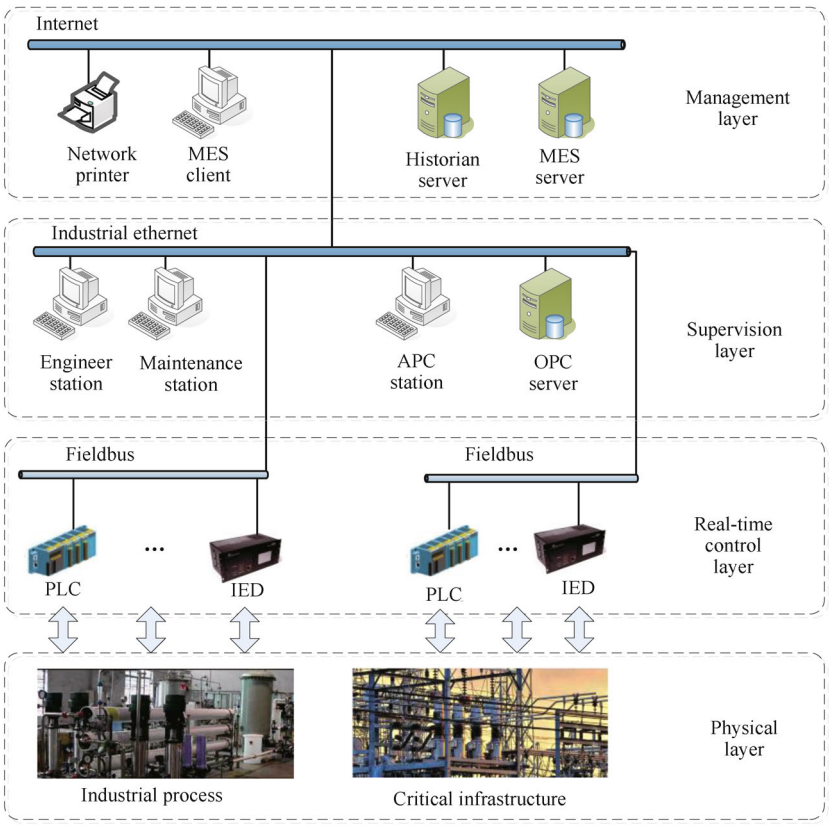


Fig. 1 General architecture of industrial CPS

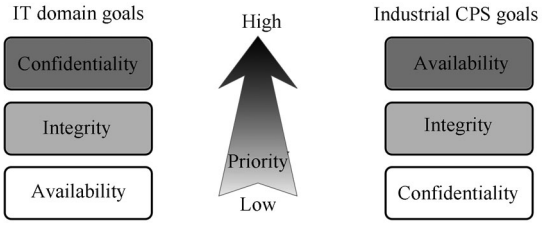


Fig. 2 Comparison of different security goals in industrial CPS and IT domain

The types of attacks are different in different layers, as the layer′s functions and communication protocols are usually not the same. Firstly, at the management layer, the general communication protocol is the transmission control protocol/interent protocol (TCP/IP). Attacks occuring at this layer are the same as those in the IT domain. Secondly, at the supervision layer, industrial ethernet is widely used, such as PROFINET, POWERLINK. The functions of this layer are: configuring control system parameters and monitoring the overall health of control systems. The main attacks are deception attacks and denial of service (DoS) attacks[21, 22]. During the deception attack, the right information is manipulated. To launch a deception attack, adversaries can send inaccurate information to system operators, make unauthorized changes to programmed instruction in local processors or change alarm thresholds or disable them[23]. The DoS attacks at this layer include exhaustion, collision, flooding attacks, etc. To launch a DoS attack, the adversary can jam the communication channels to affect the availability directly. Thirdly, at the RT control layer, there are many types of communication protocols, such as PROFIBUS, controller area network (CAN), RS485, and industrial Ethernet. The main types of attacks are response injection attack and command injection attack[24]. These two types of attack correspond to the deception attack which sends false information to controllers or actuators, and the false information can include: an incorrect measurement, the incorrect time when the measurement is taken, or the incorrect sender identification number (ID). Last but not the least, at the physical layer, the security issues consist of direct attacks and indirect attacks. The direct attack is launched by physical contact while the indirect attack is from the RT control layer as others layers cannot directly access physical layer[24].

3 Multi-layer cyber-security protection architecture

With the development of the network attack technologies, cyber threats become more difficult to be resisted by using a single defense technology[25, 26]. In order to achieve a balanced strategy between risk and accessibility, a multi-layer cyber-security protection architecture is proposed here. As shown in Fig. 1, an industrial CPS can be divided into 4 layers: management layer, supervision layer, RT control layer, and physical layer. Accordingly, the cyber-security protection architecture is composed of 4 layers of security defense: IT security, Active protection, Intrusion tolerance and physical security, as shown in Fig. 3. The RT control layer, which is the most vulnerabile, is protected by the intrusion tolerance sheme.

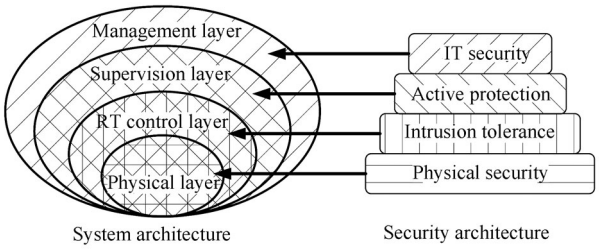


Fig. 3 Multi-layer security protection for industrial CPS

3.1 IT security

At the management layer, entities exchange the information through the Internet, and the functions of layer include: historical data storage, data management, and some other office tasks. Thus, the security requirement of this layer is similar to that of an IT system. However, specific details of the security might be different. At this layer, industrial firewall is the main method of security protection.

The industrial firewall is an inter-network connection device that restricts the data communication traffic between two connected networks in the industrial environment[16]. Typically, firewalls are used to define zone borders with rules to restrict the ports to be accessable. Industrial firewall can be configured to block all inbound network traffics except those which are explicitly required to maintain day to day operations. For instance, the industrial firewall can be configured to recognize and allow only traffic belonging to certain industrial protocols (e.g., PROFINET and ETHERCAT). If the local industrial network uses only POWERLINK, the industrial firewall can be set-up to allow only the POWERLINK traffic.

3.2 Active protection

At the supervision layer, the communication protocols, which are generally industrial protocols, are different from TCP/IP protocols. Thus, the cyber-security defense in this layer should not only be achieved by just adopting the security solutions in the IT domain, but also should instead be implemented according to the application characteristics. To protect the cyber-security of the supervision layer, an active protection line of defense can be built, which is implemented through access control (AC).

Access control regulates what a user/device can do and what the programs are allowed to execute on behalf of the user/device[27]. At this layer, access control is composed of identification and authentication control, operations and function block control. Identification and authentication control (a simple access control mechanism) is the process by which the system authenticates the identity of a user/device, which can prevent the unauthorized users or

devices from accessing the stations. Furthermore, the objectives of the access control can include function blocks and operations.

3.3 Intrusion tolerance

At the RT control layer, the cyber-security issue is quite different from that in the IT system. The physical devices are connected to the controllers. In other words, the controllers′ behaviors directly affect the physical layer, and the feedback information about the physical layer also affects the controller decision. The cyber-security strategy of the RT control layer must ensure that the plant can continue operating safely even when cyber-attacks do occur. Thus, the cyber-security control should have the strong adaptability, and the intrusion tolerance concept is used to build the cyber-security line of defense at this layer. An intrusion tolerance scheme with a closed loop for RT control layer is proposed, and more detail will be presented in Section 4.

3.4 Physical security

In the physical layer, many industrial processes and critical infrastructures, which are directly contacted with the RT control layer and interconnected with each other by material flow, are the final goal of the attacks. To protect the industrial processes and critical infrastructures from attacks, the physical security protection line can be built through a safety instrumented system (SIS).

An SIS is a distinct, reliable system used to protect a process against a catastrophic release of toxic, flammable, or explosive chemicals[28]. The function of the SIS is to monitor the process for potentially dangerous conditions (process demands), and to take action when the process needs protection. It is composed of sensors, logic solvers, and final control elements for the purpose of taking a process to a safe state or trigger the normal shutdown procedure, when predetermined conditions are violated.

4 Intrusion tolerance scheme with a closed loop for RT control layer

The RT control layer of an industrial CPS has the following domain characteristics: 1) directly connected with the physical layer; 2) real-time requirement. The tight coupling between the RT control layer and the physical layer means that attackers can affect critical infrastructures in the physical layer through the RT control layer, which may result in death or serious injury of people. Thus, cyber-security defense at the RT control layer is the critical part of the industrial CPS security protection architecture and must be implemented with consideration of resilience. The real-time requirement is one of the basic requirements for the industrial process control. The cyber-security defense must be constructed with consideration of the real-time requirement.

Considering the above points, an intrusion tolerance scheme with a closed loop defense framework is proposed to defense cyber-security for the RT control layer. The main idea of this approach is combining intrusion tolerance concept and model based approach at the software level to build the critical defense layer of industrial CPS security. The process of the proposed intrusion tolerance scheme consists of 4 stages: intrusion detection, cyber-security impact assessment, security strategy decision, and intrusion response, which form a closed loop defense framework as shown in Fig. 4.

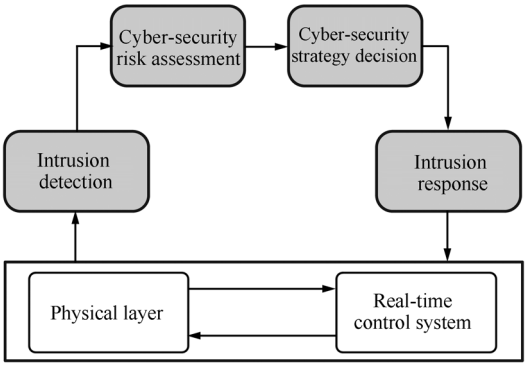


Fig. 4 Intrusion tolerance scheme with a closed loop

4.1 Intrusion detection

Intrusion detection techniques in general can be classified into two types: signature-based intrusion detection and anomaly based intrusion detection[29]. Industrial CPS systems usually have a relatively fixed structure and predictable behaviors, and they are also operating in resource constrained environments and achieve real-time/deterministic performance. Anomaly detection technique is used during the intrusion detection phase in intrusion tolerance as the aim of the anomaly intrusion detection is to detect the occurrence of the intrusion rather than the attacker itself.

There are two challenges to be addressed in the anomaly detection: 1) constructing a normal model; 2) reducing false alarms, which occur because of the error of the normal model. In the paper, a multi-model approach from our prior work[30] is used to model the normal system. The general knowledge of CPSs can be divided into 3 parts: communication engineering knowledge, software engineering knowledge, and control engineering knowledge. Thus, the multiple models are built in multiple domains: communication engineering, software engineering and control engineering, and contain the following models: communication models, task models, resource models, control data flow models and critical states of physical system.

4.2 Cyber-security impact assessment

The purpose of the cyber-security impact assessment is to identify threats and the consequences of successful attacks so that security managers can prioritize security defense resources[17]. The cyber-security impact assessment can be achieved by the following three steps: asset identification and classification, asset quantization, and dynamic

assessment. The first two can be completed off-line while dynamic assessment must be accomplished online.

To evaluate the security impact level of the industrial CPS, the assets can be decomposed into small portions according to the system structure model. The asset identification and classification aims to present the assets properties which can be used to indicate the status of the asset, and classify the assets according to their properties. Because of the relatively fixed structure of the industrial CPS, the analytic hierarchy process (AHP) method can be employed to list the system assets and their properties. The quantification of assets for an industrial CPS is a complex task because of the existence of various security properties. In this paper, AHP method is used to build a hierarchical quantitative model of security impact assessment[31]. Fig. 5 shows the security impact assessment based on AHP. The impact weights ω_{ij} of the components and properties are defined off-line during the quantification phase according to expertise.

Along with the system operation, the security status of the system is dynamic. Thus, security impact assessment for an industrial CPS should be executed online and periodically. The total system impact value can be calculated as the weighted sums of the individual impact components. The impact value of a meta-component which cannot be further decomposed can be calculated as the weighted sums of all properties impact values. And the impact value of the meta-component property can be defined as the attack status. For a component, the impact value can be calculated as

$$impact = \sum_{i=1}^{m} \omega_i \times impact_i \tag{1}$$

where m is the number of the subcomponents in the component, $impact_i (i = 1, \cdots, m)$ is the impact value of the i-th subcomponent, and $\omega_i (i = 1, \cdots, m)$ is the impact weight. With different applications, the weighting factors can be adjusted according to security requirement of components in the target system. The $impact_i$ can be further calculated in the same way as shown in (1) by substituting the components with meta-components. The impact of a meta-component can be obtained from each property impact. The attack status of each property can be either 1 if it is attacked or 0 if it is not attacked.

4.3 Dynamic game for determining cyber-security protection strategy

Security is about trade-offs and nothing is absolute secure[32]. Security services are supported by security mechanisms, such as encryption service is implemented with rivest shamir adlemen (RSA) algorithm, Rivest cipher 4 (RC4) algorithm, or data encrypt standard (DES) algorithm. And the implementation of security mechanisms has an adverse effect upon the performance of the industrial CPS. Thus, the decision process of security protection strategy is a dynamic game, which aims to seek a most suitable security protection strategy to achieve multi-goals.

A cyber-security protection strategy is a combination of security services which can be achieved by various security mechanisms. A hierarchical game process is proposed here to achieve a most suitable security protection strategy. The combination of security services is the result of the security game between the attack and defense. The security mechanisms, which support the security services, are the results of the security game between security and performance (sometimes including cost). Fig. 6 shows the decision-making process of the security protection strategy which is a two-step process: Firstly, build the attack-defense

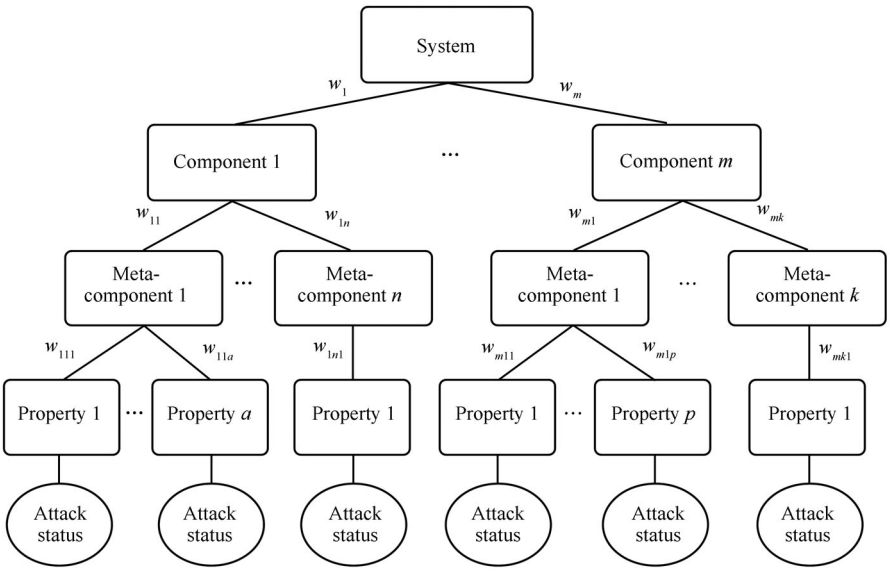


Fig. 5 Security impact assessment based on AHP

trees (ADTrees) model[33] and generate the combination of security services. Secondly, build a security-performance game (SPG) model[34] and generate the security protection mechanisms.

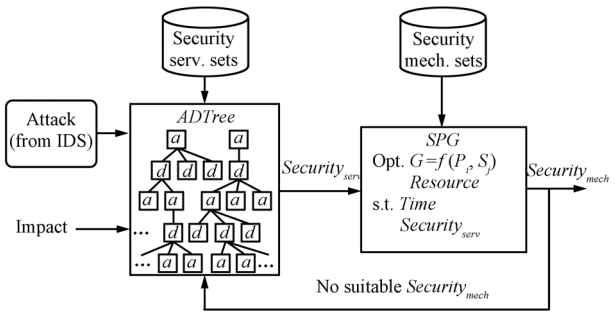


Fig. 6 Decision-making process of the security protection strategy

In the attack and defense context, the attacker aims to bypass the security protection mechanisms and to avoid being caught and being able to achieve attack goals (damage the system, filch secret information, or take over the control of a physical device), while the defender aims to protect the system as much as possible. The attackers and defenders make decisions on their strategies (a and d in Fig. 6) respectively. The ADTrees are built with consideration of the interactions between the attackers and the defenders. The security services are optimized by playing a two-player, non-cooperative, finite strategic game based on the ADTrees. The inputs in this phase include the result of the security impact assessment and the attack detected by IDS.

In the SPG model, performance metric (P_i in Fig. 6) is given through control mechanism, such as integral of absolute error (IAE), while security metric (S_j in Fig. 6) is quantified by several discrete levels, such as low, medium, and high. After the security services are determined, the security protection mechanisms implementing these security services could be achieved based on the security protection mechanismsets. For example, during the game process, the data encryption (a security service) is determined to resist the attack. However, which encryption algorithm (security protection mechanism) should be used to implement the data encrypted? To decide the specific security protection mechanism ($Security_{mech}$ in Fig. 6), we must take comprehensive consideration of the influence of security protection mechanisms on the security, and performance of industrial CPS. During the SPG process, the result of the attack-defense game, i.e. security service ($Security_{serv}$ in Fig. 6), can be regarded as an input, while the resource and time requirements of the specific application can be regarded as the boundary condition. If no suitable security protection mechanisms could be found to support the security services, the security services need to be modified by reconsidering the ADTrees. For example, the security service is downgraded for a non-critical task if necessary.

4.4 Real-time intrusion response

Industrial CPSs are usually operating in real-time and with constrained resources. Cyber-security stratigies should be implemented with consideration of these constraints. The essence of the real-time intrusion response in intrusion tolerance is a system dynamic reconfiguration, which is a three-step process: 1) task deployment at the system level; 2) message broadcast over the network; 3) task reconfiguration at the node level.

The real-time intrusion response interprets the cyber-security strategy from dynamic game module to determine the new deployment of system tasks. And it determines which nodes should be reconfigured and how to reconfigure according to the original deployment of system tasks. During the message broadcast phase, the tasks (including the running tasks and other tasks) in the system are allocated task numbers, and all operations of each task are also allocated operating codes (e.g., establish, destroy, suspend, activates). This way, the reconfiguration message can be represented as ⟨node ID, task number, operation code⟩, which can greatly reduce the traffic caused by real-time intrusion response and diminish the effect on the real-time messages. At the node level, the reconfigured task of a node is known to interpret the reconfiguration message. And the nodes reconfigure the tasks according to the task number and the corresponding operation code.

5 Case study

In this section, a networked water level control system (NWLCS) with the proposed hierarchical security architecture is studied. As mentioned in Section 3.1, the security defense at the management layer is similar to that in the IT domain, and there are rich literatures on these issues[35]. Therefore, this case study is focused on the other 3 layers below the management layer. Simulations of the NWLCS was carried out in the AADL environment which is a modeling language that supports early and repeated analysis of a system architecture with critical aspects.

5.1 Networked water level control system

The NWLCS, shown in Fig. 7, is composed of 3 layers: supervision layer, RT control layer and physical system. The physical system contains a storage tank, a water level sensor (WLS), and a pump to transfer water into the tank that raises the water level by the speed of 2% per millisecond. The water in the tank is sequentially heated and the water level decreases by 0.2% per millisecond. The RT control layer consists of a controller, a sensor, an actuator and a CAN bus. The controller attempts to maintain the water level of the water tank between H (setpoint value of high level) and L (setpoint value of low level) by turning on and off the water pump, and in the simulation, $H = 60\%$, $L = 40\%$. The upper and lower safety bounds of water level are $SH = 90\%$ and $SL = 10\%$, which should not be surpassed, otherwise safety accidents will happen. The

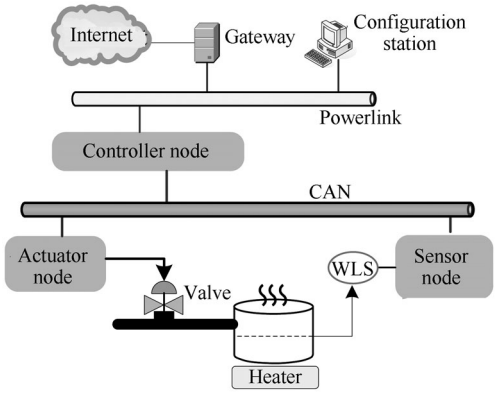
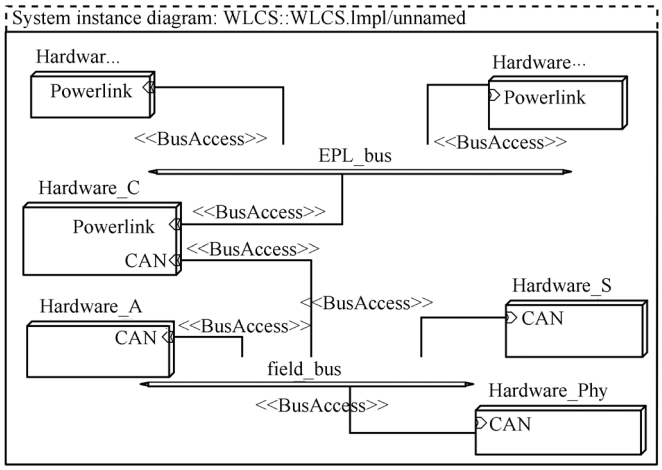


Fig. 7 System architecture of the NWLCS

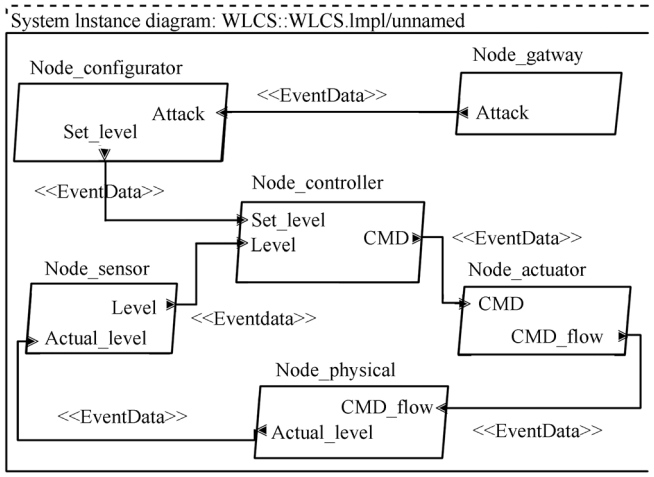
supervision layer consists of a configuration station, a gateway and a POWERLINK network. The configuration station allows an operator to manually turn the pump on and off and set the H and L water level values. The gateway is also connected to the Internet. In the simulation, the Internet is not considered, and attacks are launched at the gateway.

5.2 Simulation in the AADL environment

AADL allows the modelling of software components as well as execution platform components. Ocarina[17] can automatically generate the framework code from the AADL models. This code is then compiled with the AADL runtime and functional source code to create executable binaries. The AADL run-time provides execution services specific to the AADL generated code. With the help of the ocarina AADL tool suite, the simulation system architecture is given in Fig. 8. As sown in Fig. 8 (a), the hardware components of the simulation system contain 2 communication networks and 6 processors which are used as the gateway, configuration station, controller, actuator, sensor and physical system, respectively. In Fig. 8(b), the software of the simulation system contains 6 processes which correspond to the 6 processors accordingly.



(a) Hardware components



(b) Software components

Fig. 8 Simulation system architecture of the NWLCS in AADL

The security defense is constructed layer by layer. 1) At the supervision layer, active protection is built by access control. The access control is deployed on the gateway to control the access from the Internet, which is not the focus in this simulation. The data detection runs on the configuration station, and the detection rule can be represented as "$\langle (H < SH)\ \&\ (L > SL)\rangle$". 2) At the RT control layer, the intrusion tolerance is distributed, and deployed on the controller node, actuator node and sensor node. The security impact assessment and security strategy decision are implemented on the controller node, while intrusion detection and intrusion response are implemented on the controller node, sensor node, and actuator node. 3) At the physical plant, only the physical protection, also called safeguard, is used due to the simple structure of the physical system in this case, which is implemented in the physical system by mechanical devices. When the safeguard is activated, the command for other nodes will be discarded, and the water pump is controlled by the safeguard. The protection rules are represented as follows: a) If water level $> SH$, then turn off water pump; b) If water level $< SL$, then turn on the water pump.

To illustrate the efficiency of the proposed security defense architecture, attacks are simulated in C source code on the gateway, and the simulated attacks for the layers are listed in Table 1. All attacks simulated are at $t = 300$ ms.

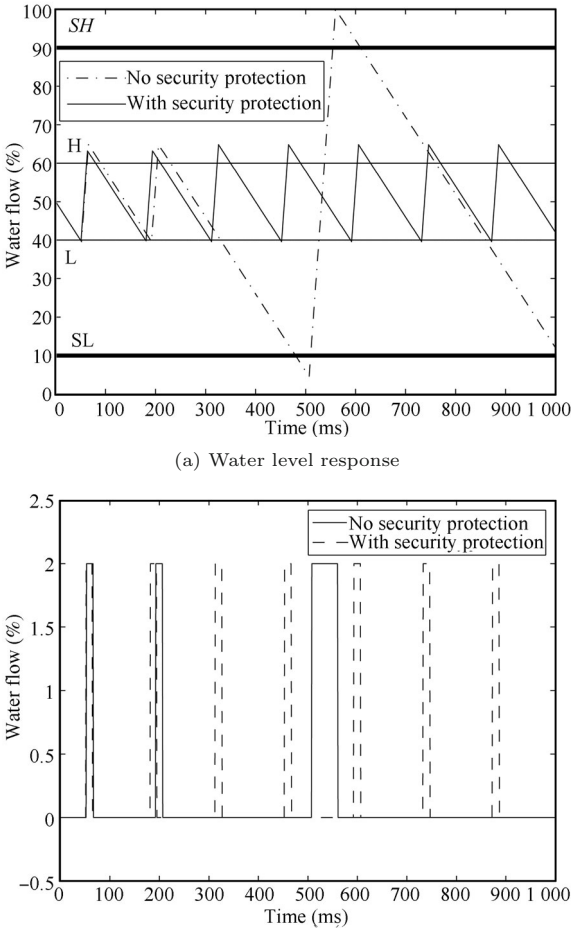
Table 1 Simulated attacks for the NWLCS

Scenario	Attack type	Attack description
1	Setting a fault setpoint	H =95%, L=5%
2	Setting a fault water level	Water level = 15%
3	Setting a fault command	Water flow = 0.0

5.3 Simulation results

In order to facilitate to efficiency analysis of security defense, the configuration of the NWLCS is given as follows: the dangerous point is $\langle SH = 90\%, SL = 10\%\rangle$, and the setpoint is $\langle H = 60\%, L = 40\%\rangle$. When the water pump turns on, water flow is 2.0%. When the water pump turns off, water flow is 0. And the bang-bang control methods is used here. When the water level is lower than L, the the water pump turns on. When the water level is higher than H, the the water pump turns off.

Scenario 1. Security defense for setpoint attack at the supervise layer. The simulation results with setpoint attack are shown in Fig. 9. The setpoint is modified to $\langle H$ =95%, L=5%$\rangle$ at $t = 300$ ms. But the water level and flow have not been affected immediately, because the water level is within allowed limits. At $t = 330$ ms, the water level is lower than 40%, but the setpoint L is tampered as $L = 5\%$. Thus, the water pump doesn$'$t turn on, and the water level continues to drop. From $t = 480$ ms, the controller output is abnormal, which is exceeding the lower safety bound (SL). But in the NWLCS with security protection, by the detection rules $\langle (H < SH)\&(L > SL)\rangle$, this type of attack can be readily detected, and with the help of the IDR in configuration station, the setpoint is recovered to $\langle H = 60\%, L = 40\%\rangle$, and the water level and water flow accord with those of normal operations.



(a) Water level response

(b) Water flow

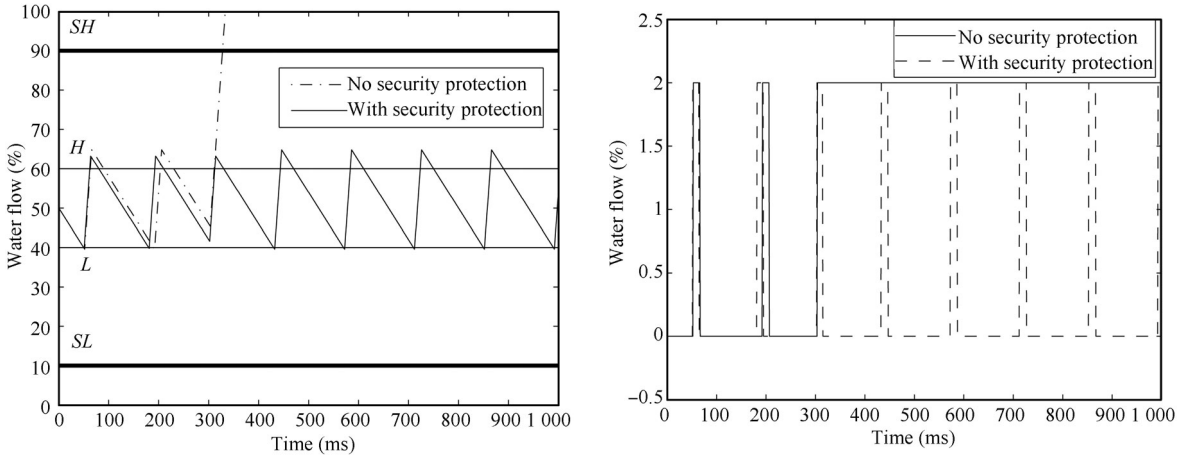
Fig. 9 Simulation results with setpoint attack

Scenario 2. Security defense for response injection attack at the RT control layer. In this scenario, a response injection attack is injected at $t = 300$ ms. As shown in Fig. 10, at $t = 303$ ms, the water pump turns on due to the false sensor response (water level = 15%, which is smaller than L), while the actual water level is 45.4% that is lager than L. Consequently, the water level goes up until the water brims over the tank. But in the WNCS with security protection, with the intrusion tolerance with closed loop, the 4 phases of response injection attack tolerance are shown in Fig. 11. Phase 1: At $t = 301$ ms, the intrusion detection module detects that the sensor data has changed which is an abnormal event. Phase 2 and phase 3: Security impact level is HH (top high risk), and the security strategy decision module decides that the alternative encryption is used for sensor data. Phase 4: The security strategy is implemented, and the sensor data is restored.

Scenario 3. Security defense for command injection attack at the physical layer. At $t = 300$ ms, the value of water flow is tampered to zero. Fig. 12 shows that the water level has not been affected immediately by the command injec-

tion attack, this is because the correct value of water flow is actually zero. At $t = 331$ ms, the value of water level is 39.8% which is less than L. But because of the command injection attack, the value of water flow to be sent to the actuator is also zero, not the correct value from the controller. In other words, the actuator is controlled by the attacker. Obviously, the water level would go down eventually until to zero. But in the WNCS with security protection, with the physical security, system can be kept in the safe status (being maintained between SL and 50%). Step 1. At $t = 480$ ms, the water level (10%) reaches to SL, and the safeguard is called for to turn on the water pump. Step 2. At $t = 503$ ms, the water level (51.4%) exceeds 50%, and the safeguard is released. The water level is maintained between 50% and SL level, as shown in Fig. 12 (a). And the water flow is shown in Fig. 12 (b).

In the simulations, three typical types of attacks are considered. The setpoint attack in the simulation is implemented by tampering the configuration data, and the change of the data is big. The response injection attack at the RT control layer must be detected and recovered through all the modules of intrusion tolerance. Although the response of the control system is also affected certainly, the system becomes normal after a little short with the intrusion tolerance scheme. The command injection attack at the physical layer greatly affects the response of the control system, but the aim of the physical security is to prevent an incident. In this respect, the physical security is very sufficient.



(a) Water level response

(b) Water flow

Fig. 10 Simulation results with response injection attack

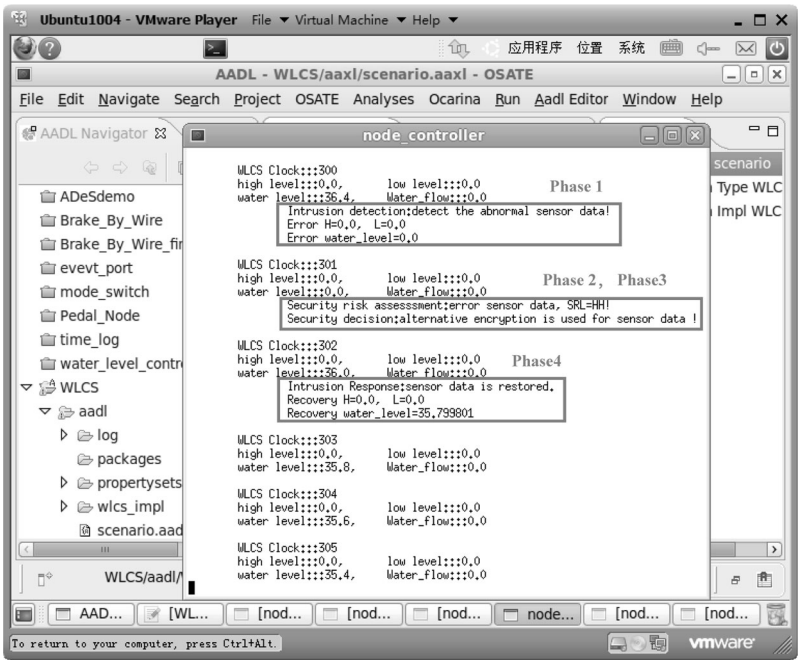
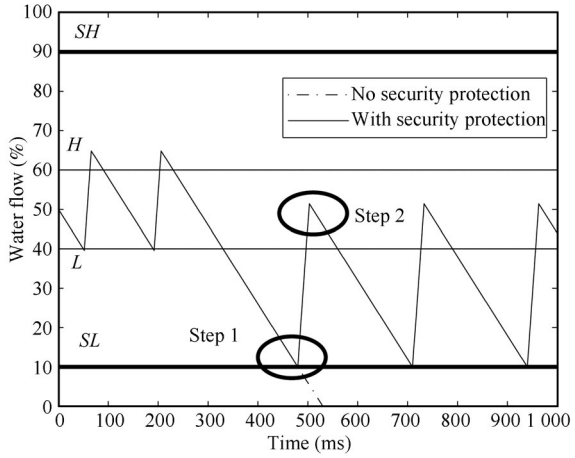
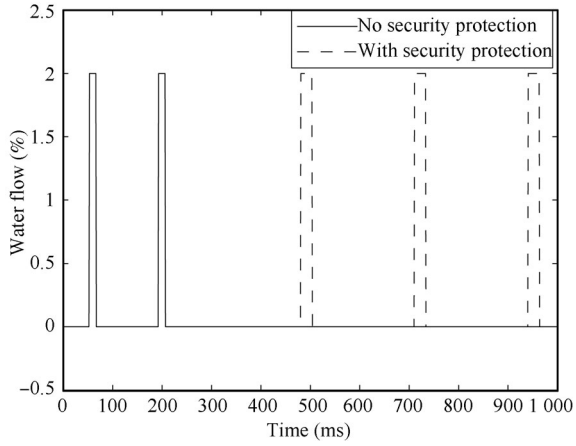


Fig. 11 Process of intrusion tolerance



(a) Water level response



(b) Water flow

Fig. 12 Simulation results with command injection attack

6 Conclusions

Cyber-security protection issue is the bottleneck for widely applied industrial CPSs. In this paper, a multi-layer cyber-security protection architecture with flexible structure and resilient intelligence for industrial cyber-physical systems has been proposed to facilitate the realization of security defense according to industrial CPSs architecture. With consideration of the features of industrial CPSs, the cyber-security protection architecture is composed of 4 layers: general IT security, active protection, intrusion tolerance and physical security. The intrusion tolerance scheme with a closed loop is the most important part which consists of 4 phases that are intrusion detection, security impact assessment, security strategy decision, and intrusion response. The intrusion tolerance is employed to protect the real-time control layer which is the core part of industrial CPSs. During the intrusion detection phase, the model based approach is used to detect abnormal events, security impact assessment is implemented with the help of a hierarchical quantitative model. Security strategy is decided through 2 dynamic game processes, and the intrusion response carries out self-reconfiguration for the RT control system, self-learning for the whitelist model, and self-updating for the active protection to achieve the resilient security. The simulation results of the networked water level control system based on the ocarina AADL tool platform illustrate the efficiency of the proposed cyber-security defense approach.

The proposed cyber-security protection architecture is derived from the general architecture of industrial CPS. Therefore, it is expected to be applicable to a wide range of industrial CPSs such as chemical plants, water supply systems. Furthermore, most of the critical infrastructures such as smart grids are connected through various communication technologies and share similar features with networked industrial processes. It is reasonable to expect that the proposed cyber-security protection approach is also applicable to those networked critical infrastructures if a proper modification is made at the real-time control layer and physical protection layer.

To further develop the cyber-physical system security protection methodology , future work could include: 1) further optimizing real-time performance and resource usage of the suggested approach; 2) exploring a broader set of applications for cyber-physical system security protection, such as the WNS, the advanced metering infrastructure (AMI); 3) further developing the proposed cyber-physical system security protection framework based on practical results.

References

[1] E. A. Lee. Cyber physical systems: Design challenges. In *Proceedings of the 11th International Symposium on Object Oriented Real-time Distributed Computing*, IEEE, Orlando, USA, pp. 363–369, 2008.

[2] L. J. Zhao, Y. T. Chai, D. C. Yuan. Selective ensemble extreme learning machine modeling of effluent quality in wastewater treatment plants. *International Journal of Automation and Computing*, vol. 9, no. 6, pp. 627–633, 2012.

[3] M. Y. Zhao, J. Walker, C. C. Wang. Challenges and opportunities for securing intelligent transportation system. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 96–105, 2013.

[4] Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, I. Koshijima. Safety securing approach against cyber-attacks for process control system. *Computers and Chemical Engineering*, vol. 57, pp. 181–186, 2013.

[5] M. Cheminod, L. Durante, A. Valenzano. Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, 2013.

[6] J. Lopez, C. Alcaraz, R. Roman. Smart control of operational threats in control substations. *Computers and Security*, vol. 38, pp. 14–27, 2013.

[7] N. X. Xiong, A. V. Vasilakos, L. T. Yang, E. Hossain. An adaptive and predictive approach for autonomic multirate multicast networks. *ACM Transactions on Autonomous and Adaptive Systems*, vol. 6, no. 3, Article number 22, 2011.

[8] U. Altinisik, M. Yildirim. A new fault tolerant control approach for the three-tank system using data mining. *Computers and Electrical Engineering*, vol. 38, no. 6, pp. 1627–1635, 2012.

[9] Y. Y. Zhang, J. L. Zhang, X. Y. Luo, X. P. Guan. Sensor/actuator faults detection for networked control systems via predictive control. *International Journal of Automation and Computing*, vol. 10, no. 3, pp. 173–180, 2013.

[10] D. J. Fergus. Industrial Control System Security Current Trends & Risk Mitigation, Technical Report. Intekras, Inc., Sterling, USA, 2009.

[11] C. J. Zhou, H. Chen, Y. Q. Qin, Y. F. Shi, G. C. Yu. Self-organization of reconfigurable protocol stack for networked control systems. *International Journal of Automation and Computing*, vol. 8, no. 2, pp. 221–235, 2011.

[12] W. Young, N. G. Leveson. An integrated approach to safety and security based on systems theory. *Communications of the ACM*, vol. 57, no. 2, pp. 31–35, 2014.

[13] H. Zhang, P. Cheng, L. Shi, J. M. Chen. Optimal Denial-of-Service attack scheduling against linear quadratic Gaussian control. In *Proceedings of the American Control Conference*, IEEE, Portland, USA, pp. 3996–4001, 2014.

[14] L. J. Wells, J. A. Camelio, C. B. Williams, J. White. Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, vol. 2, no. 2, pp. 74–77, 2014.

[15] Z. J. Le, N. X. Xiong, B. Yang, Y. Z. Zhou. SC-OA: A secure and efficient scheme for origin authentication of interdomain routing in cloud computing networks. In *Proceedings of International Parallel & Distributed Processing Symposium*, IEEE, Anchorage, USA, pp. 243–254, 2011.

[16] Y. B. Wang, M. C. Vuran, S. Goddard. Cyber-physical systems in industrial process control. *ACM SIGBED Review*, vol. 5, no. 1, Article number 12, 2008.

[17] Q. Y. Zhu, C. Rieger, T. Basar. A hierarchical security architecture for cyber-physical systems. In *Proceedings of the 4th International Symposium on Resilient Control Systems*, IEEE, Boise, USA, pp. 15–20, 2011.

[18] Y. Z. Zhou, Y. X. Zhang, H. Liu, N. X. Xiong, A. V. Vasilakos. A bare-metal and asymmetric partitioning approach to client virtualization. *IEEE Transactions on Services Computing*, vol. 7, no. 1, pp. 40–53, 2014.

[19] J. Hugues, B. Zalila, L. Pautet, F. Kordon. From the prototype to the final embedded system using the ocarina AADL tool suite. *ACM Transactions in Embedded Computing Systems*, vol. 7, no. 4, Article number 42, 2008.

[20] T. Baars, M. Spruit. Designing a secure cloud architecture: The SeCA model. *International Journal of Information Security and Privacy*, vol. 6, no. 1, pp. 14–32, 2012.

[21] M. Krotofil, A. A. Cárdenas. Resilience of process control systems to cyber-physical attacks. In *Proceedings of the 18th Nordic Conference, NordSec 2013, Lecture Notes in Computer Science*, Springer, Ilulissat, Greenland, pp. 166–182, 2013.

[22] H. Zhang, P. Cheng, L. Shi, J. M. Chen. Optimal DoS attack policy against remote state estimation. In *Proceedings of the 52nd Annual Conference on Decision and Control*, IEEE, Firenze, Italy, pp. 5444–5449, 2013.

[23] B. Genge, C. Siaterlis. Physical process resilience-aware network design for SCADA systems. *Computers and Electrical Engineering*, vol. 40, no. 1, pp. 142–157, 2014.

[24] Y. L. Huang, A. A. Cárdenas, S. Amin, Z. S. Lin, H. Y. Tsai, S. Sastry. Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection*, vol. 2, no. 3, pp. 73–83, 2009.

[25] S. H. Yang. *Internet-based Control Systems*, London, UK: Springer, pp. 131–145, 2011.

[26] Y. Z. Zhou, Y. X. Zhang, H. Liu, N. X. Xiong, A. V. Vasilakos. A bare-metal and asymmetric partitioning approach to client virtualization. *IEEE Transactions on Services Computing*, vol. 7, no. 1, pp. 40–53, 2014.

[27] K. Gill, S. H. Yang, W. L. Wang. Secure remote access to home automation networks. *IET Information Security*, vol. 7, no. 2, pp. 118–125, 2013.

[28] Functional safety: Safety instrumented systems for the process industry sector, IEC Standard 61511, 2003.

[29] W. Xiong, H. P. Hu, N. X. Xiong, L. T. Yang, W. C. Peng, X. F. Wang, Y. Z. Ou. Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications. *Information Sciences*, vol. 258, pp. 403–415, 2014.

[30] M. Y. Yang, X. F. Huang, S. Huang, C. J. Zhou. Multiple models based detection of transient faults for networked control system. *Applied Mechanics and Materials*, vol. 373–375, pp. 1369–1373, 2013.

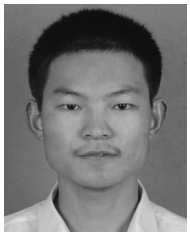
[31] F. Sha, H. Q. Zhou. The information security risk assessment based on AHP and fuzzy comprehensive evaluation. In *Proceedings of the 3rd International Conference on Communication Software and Networks*, Xi′an, China, pp. 124–128, 2011.

[32] R. Sandhu. Good-enough security: Toward a pragmatic business-driven discipline. *IEEE Internet Computing*, vol. 7, no. 1, pp. 66–68, 2003.

[33] B. Kordy, S. Mauw, S. Radomirović, P. Schweitzer. Attack-defense trees. *Journal of Logic and Computation*, vol. 24, no. 1, pp. 55–87, 2014.

[34] W. T. Zeng, M. Y. Chow. Modeling and optimizing the performance-security tradeoff on D-NCS using the coevolutionary paradigm. *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 394–402, 2013.

[35] T. Xie, X. Qin, A. Sung, M. Lin, L. T. Yang. Real-time scheduling with quality of security constraints. *International Journal of High Performance Computing and Networking*, vol. 4, no. 3–4, pp. 188–197, 2013.



Shuang Huang received the B. Sc. degree in automation from Huazhong University of Science and Technology, China in 2009. He is currently a Ph. D. degree candidate in control science and control engineering at School of Automation, Huazhong University of Science and Technology, China.

His research interests include industrial communication and industrial control system with special focus on security.

E-mail: huangshuang@hust.edu.cn

ORCID iD: 0000-0002-9851-2447

Chun-Jie Zhou received the M. Sc. and Ph. D. degrees in control theory and control engineering from Huazhong University of Science and Technology, China in 1991 and 2001, respectively. He is currently a professor in Department of Control Science and Engineering at Huazhong University of Science and Technology, China.

His research interests include industrial communication, artificial intelligent, theory and application of networked control system.

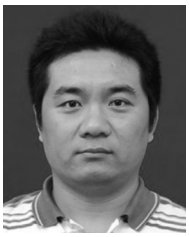
E-mail: cjiezhou@hust.edu.cn (Corresponding author)

ORCID iD: 0000-0001-5291-5841

Shuang-Hua Yang received the B. Sc. degree in instrument and automation and the M. Sc. degree in process control from the University of Petroleum, China in 1983 and 1986, respectively, and the Ph. D. degree in intelligent systems from Zhejiang University, China in 1991. He is currently a professor of networks and control and the director of the Networks, Communications and Control Systems Research Division at Loughborough University, U.K. He is the fellow of the Institute of Measurement and Control and a chartered engineer in the UK.

His research interests include wireless sensor networks, networked control, safety critical systems, and real-time software maintenance.

E-mail: S.H.Yang@lboro.ac.uk



Yuan-Qing Qin received the M. Sc. and Ph. D. degrees in control theory and control engineering from Huazhong University of Science and Technology, China in 2003 and 2007, respectively. He is currently a lecturer in Department of Control Science and Engineering, Huazhong University of Science and Technology, China.

His research interests include networked cotnrol system, artificial intelligent, and machine vision.

E-mail: yuan_qing@163.com