SAFETY AND SECURITY CHECKING IN THE DESIGN OF INTERNET BASED CONTROL SYSTEMS

Lili Yang and Shuang-Hua Yang

Computer Science Department, Loughborough University, Loughborough, Leicestershire LE11 3TU UK

Abstract: Internet-based control is becoming new generations of control systems, in which the Internet is used as a platform for global remote monitoring and control. The obvious benefit is to enable global collaboration and data sharing between operators from geographically dispersed locations. However, connection to an open network and the use of universal technology presents new problems that did not exist with the conventional design and construction of control systems, such as safety and security. This paper presents the safety and security checking procedures used in the design of Internet based control systems. A process control case study is used to illustrate the checking procedures.

Keywords: control system design, process control, communication network, safety analysis, security.

1. INTRODUCTION

Nowadays the Internet is playing a very important role in different domains. During the previous years a lot of research (Yang et al., 2002, 2003; Overstreet and Tzes, 1999) has been done for trying to develop applications, which make it possible to supervise and control industrial processes using the Internet. Internet based control can be described as the whole of operations performed to control or monitor a system in the Internet environment. Internet-based control system allows the process data to be retrieved by a controller, operator, and engineer at a remote location. Control action issued in the remote location can be executed in the process. The difference from normal remote control system and/or distributed control system is that the communication media is the Internet rather than any other private media. The public Internet possesses security risk by its open environment nature. The remote operation extends the scope of the Internet based control system safety from the plant sites to the whole Internet community because there are some degrees of possibility that the local control system is falsified by outsiders through the Internet. The features of the public Internet must be considered in the design of Internet based control systems in order to prevent them from attacks by outside hackers. The existing technologies such as plant firewall, user authentication, communication path encryption, access log and format conversion (Furuya et al., 2000) might be able to make the Internet based control systems safer but never be able to stop the attacks from malicious hackers. Therefore systematic safety and security checking in the design of the Internet based control systems is essential in order to reduce the loss caused by the attacks and will provide the guidelines for the operators to efficiently response the attacks.

This paper will systematically consider the safety and security issues through the design phase and clarify all the scenarios of malicious hacker attacks. Actions to response the attacks will be suggested as the results of the safety and security analysis. The rest of the paper is organised as follows. Section 2 identifies

*Corresponding author: Dr S H Yang, Senior lecturer in Computer Science at Loughborough University, UK. Email: s.h.yang@lboro.ac.uk

the safety and security problems in the Internet based control systems. Section 3 describes all the possible targets for attack by malicious hackers. Section 4 presents a safety risk analysis procedure based on the principles of process plant HAZOP (HAZard and OPerability). Section 5 gives a case study to illustrate the safety and security checking. Section 6 is the conclusions.

2. SIMILARITY OF SAFETY AND SECURITY

The safety risk analysis process has the aim of specifying the safety requirements of the system. The security risk analysis identifies the potential security problems. There are some differences but more similarities between safety and security properties (Eames and Moffett, 1999). For example, in security the weaknesses in the system and dangers are called vulnerabilities and threats, in safety they are called failure mechanisms and hazards, but they can be considered to be alike. In security examples the countermeasures that need to be put in place to counter the risks are access controls, fire walls, etc., in safety they are redundancy, protective equipments, monitoring devices, etc. Rushby (1994) presented the nature of safety and security, in which the differences between the two were recognised, but also both groups subscribe to similar development techniques, i.e. safety and security techniques could be applicable to each other's domains. Security could benefit from fault tolerant approaches typically found in safety techniques, and that security system developers might benefit from a greater understanding of the hazard analysis methods used by safety engineers.

In general, safety, security and their associated risk analysis techniques are closely related. Both deal with risks and both result in constraints, which may be regarded as negative requirements. Both involve protective measures, and both produce requirements that are considered to be of the greatest importance. These similarities indicate that some of the techniques applicable to one field could also be applicable to the other.

In Internet based control systems the safety problems are caused by the authorized users because of the nature of the remote operation. Avoiding the failures caused by the authorized users can be achieved through safety analysis at the Internet level. The security problems are caused by the malicious hacker's attacks. Preventing attackers from accessing the Internet based control systems are assured by network security measures.

3. SECURITY RISKS FROM MALICIOUS HACKERS

The Internet router is obviously the first target of attack if any malicious hacker tries to get unauthorized access into the local control system. Based on the research by Shindo et al. (2000), Fig. 1 shows a possible intruding path from breaching the Firewall (node A1) to causing a fatal accident (node E5) through intruding into the Intranet (node A2), intruding into the control system (node B2), altering control parameters (node C3), and causing abnormal process conditions (node D4). In Fig. 1 intrusion takes time from left to right and increases the degree of risk from bottom to top. Cutting off the path at any point, which starts at the node A1 and ends at the node E5, will prevent the fatal accident from happening. In fact Fig. 1 gives four possible points at which the path from A1 to E5 might be cut:

- Cutting the path between the nodes A2 and B2 by detecting and shutting out the intrusion into the Intranet (nodes A3 and A4). This way has a minimum risk to the process.
- Cutting the path between the nodes B2 and C3 by detecting the intrusion into the local control system (node B3), cutting off the link with the network (node B4), and allowing the control system to run isolated from the network.
- Cutting the path between the nodes C3 and D4 by using the safe guard to protect the process from an unexpected change in control parameters.
- Cutting the path between the nodes D4 and E5 by activating the safety interlock system (SIS) to trigger the normal shutdown procedure. This is the last protection before causing a fatal accident and has a maximal loss to the process.

4. SAFETY RISK ANALYSIS

Authorized remote users and the failures in the components of Internet based control systems can cause safety risks as well. A comprehensive safety risk analysis is required in order to identify all potential hazards and preventing them from occurring. The hazard analysis framework for computer-controlled plants proposed in our previous research (Chung et al., 1999; Yang and Chung, 2001; Chung and Yang, 2003; Treseler et al., 2001) can be extended to safety checking for Internet-based controlled plants. A Process Control Event Diagram (PCED) was used in the hazard analysis framework. A PCED is an abstract and qualitative model of the communication between process, controller and operator. The advantage of this representation is that connections between process variables and the control logic can be visualized in a very simple and descriptive manner. Due to its simplicity, PCEDs can be understood by people from different engineering domains and they can provide the basis on which a Hazard and Operability (HAZOP) discussion can take place. Treseler et al. (2001) gave a formal definition of the original PCEDs. Chung and Yang (2003) described the transformation from the formal description of the PCED into a symbolic model checking representation and carried out safety checking.

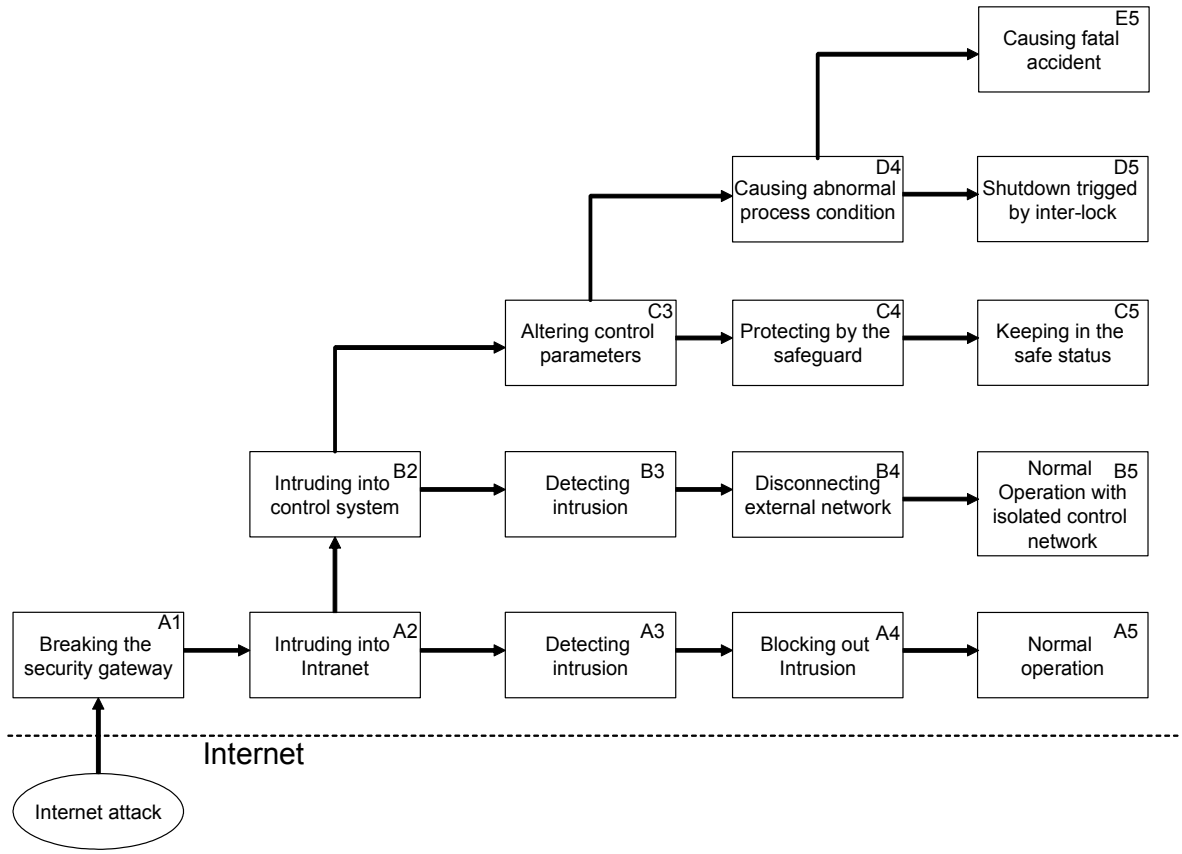

Fig. 1. Possible attacking targets from malicious hackers

A modified PCED is adopted in this study for the safety risk analysis of Internet-based controlled plants. An example of a modified PCED is shown in Fig. 2. The PCED illustrates the interaction between nodes, which are arranged on six different layers (from the top to the bottom layer: Web client, Web-based System, Internet, Local Computer, Sensor/Actuator, Process). The nodes represent the components involved in the system (e.g., sensors, actuators, control algorithms), and an edge between two nodes stands for the propagation of a signal. Using our formal description of the PCED the modified PCED can be described as a quadruple:

$$PCED = (Lay, Nod, Edg, Act) \quad (1)$$

In which *Lay* denotes an ordered set of symbols *Web Client (Wc), Web-based System (Wbs), Internet (Int), Local Computer (Comp), Sensor/Actuator (S/A), and Process (Proc)* that represent the six layers. Assigned to these layers are several different types of nodes. The set of nodes is formed by:

$$Nod = (Nod_{Wc}, Nod_{Wbs}, Nod_{Int}, Nod_{Comp}, Nod_{S/A}, Nod_{Proc}) \quad (2)$$

The set $Edg = \{e_1, \ldots, e_{nedg}\}$ denotes a finite set of *edges*. The set *Act* is a finite ordered set of signal processing *actions* given as a combination of nodes and edges. The order of actions α_j in the set $Act = \{\alpha_1, \ldots, \alpha_{nact}\}$ corresponds to the horizontal order with which the nodes involved are arranged in the PCED from left to right. In this study we follow the HAZOP principle and apply various deviations into the PCED for each action α_j in order to identify the potential safety identification purpose.

Due to Internet environment constraints even authorized remote users may cause failures in the process without any improper operation. Therefore, we need to identify what can go wrong and consider what consequence may result. An efficient, systematic way of finding potential risks is to introduce possible deviations from the design intent, i.e. scenarios, node by node in the PCED on the basis of the use of "guidewords" which are words or phrases expressing specific types of deviation. In conventional HAZOP the common guidewords are *no, more, less, part of,* and *other than.* Based on the UK Ministry of Defence safety checking guidance (MOD, 1996) three more guidewords should be used for control systems: *reverse, early, late*. The other three guidewords are added in our research: *before, after, as well as.* The possible attributes of control systems are *data/control flow, data rate, data value, event, action, timing of event or action, repetition time, and response time*. The guidewords that are applicable to Internet based process control systems are interpreted in Table 1. Deviation from normal behaviour of the control systems is considered for each action α_j in the PCED. Causes, corresponding consequences and correcting actions can be proposed by a team of experts. Potential hazards or safety critical events can then be identified. The procedure of the hazard analysis will be illustrated in the following case study.

Table 1 Attributes, guidewords and interpretations for Internet based control systems

Attribute	Guide Word	Interpretation
Data /control flow	No	No information flow
	More	More data is passed than expected
	Part of	Information passed is incomplete
	Reverse	Information flow is in a wrong direction
	Other than	Information is complete, but incorrect
	Early	Information flow before it was intended
	Late	Information flow after it was required
Data rate	More	Data rate is too high
	Less	Data rate is too low
Data value	More	Data value is too high
	Less	Data value is too low
Event	No	Event does not happen
	As well as	Another event takes places as well
	Other than	An unexpected event occurred instead
Action	No	No action takes place
	As well as	Additional actions take place
	Part of	Incomplete action is performed
	Other than	Incorrect action takes place
Timing of event or action	No	Event/action never takes place
	Early	Event/action takes place before expected
	Late	Event/action takes place after expected
	Before	Happens before another expected event
	After	Happens after another expected event
Repetition time	No	Output is not updated
	More	Time between outputs is longer than required
	Less	Time between outputs is less than required
	Other than	Time between outputs is variable
Response time	No	Never happens
	More	Time is longer than expected
	Less	Time is shorter than expected
	Other than	Time is variable

5. CASE STUDY

To illustrate how well the safety and security checking procedures can be applied, a water tank teaching rig in our Internet control laboratory is used as an example. An Internet-based dual-loop control system for the water tank is implemented and introduced in our other publication. This section only focuses on the safety and security checking.

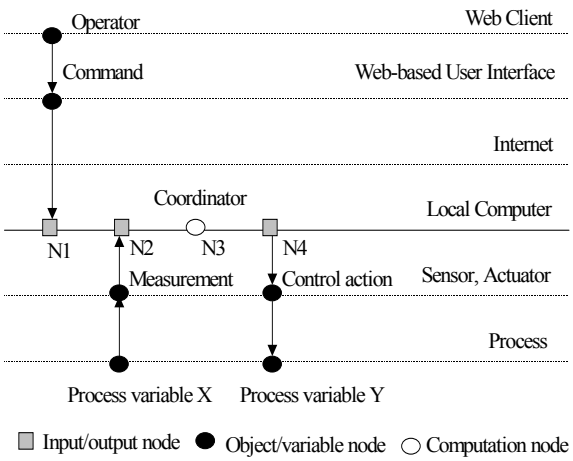

Fig. 2. Modified Process Control Event Diagram

5.1 System Architecture

The experimental system layout is shown in Fig. 3. The control target is to maintain the liquid level of the water tank at a desired value. The tank is filled by the inlet flow controlled by a hand valve and is emptied into a drainage tank through a connection pipe and a pump. The outlet flow is controlled by a local control system, a PID controller, to maintain the liquid level of the tank at a desired value. The remote control system is designed to remotely adjust the set-point of the local control system. The DAQ instrument is used to gather the liquid level signal from and send a control command to the water tank. The remote control system is connected with the Internet through a BT broadband with 56K bandwidth.

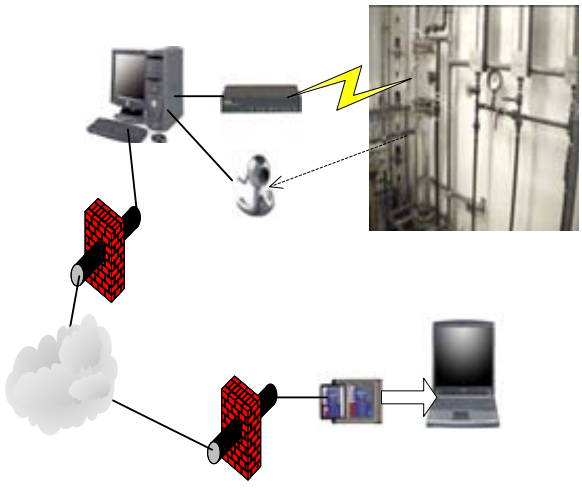

Fig. 3. Physical layout of the Internet-based control system

According to the security and safety risk analysis given in the sections 3 and 4, the control system protection is composed of three layers. The first layer is the standard firewall protection, which uses password control to allow authorised users to enter the control system. The second layer relies on the

encoding and decoding mechanisms to protect the data exchange between the local control system and the remote control system. The encoding and decoding algorithms are associated with the user's IDs. The third layer is based on the inherent system safe design such as the safety interlock system (SIS).

5.2 Security Checking

The What-If approach is basically a communication exercise and asks what-if questions of the systems or processes. Information is presented, discussed, analysed and recorded. Specifically the potential risks are identified and determined if adequate design measures have been taken to prevent an accident from happening.

Table 2 Partial What-If reviews for the water tank control system

If	What	Actions
Firewall and password control are broken.	Attackers obtain the access to the control system.	Disconnect the external link of the local control system with the Internet if the intrusion is detected.
The attackers have modified control parameters.	Disturbances have been introduced into the process.	The safeguard system filters out any abnormal change to the local control system.
The attackers have created safety critical conditions.	A fatal accident might be happening.	The emergency safety interlock system is required to be automatically activated.

The What-If approach was mainly used for safety checking. As described in the section 2, because of the similarity of safety and security the What-If approach can be employed for security checking according to the possible attacking targets shown in Fig. 1. Three scenarios about the security checking are summarized in Table 2. Various actions must be taken to avoid the consequences occurring. For example, if a malicious attacker changed the control parameters the control system will not work properly. The corresponding action is to trigger a safeguard system to stop the influence of the parameter change. The safeguard system might be designed to simply filter out the abnormal control action. Another example, if an abnormal process condition has been created by an attacker, the safety interlock system (SIS) will be activated to keep the process in a safer condition and wait for the intervention from a local operator.

5.3 Safety Checking

If replacing the process variable X with the liquid level, the process variable Y with the opening of the outlet valve, and the computation node N3 with the PID control algorithm, the PCED shown in Fig. 2 then exactly describes the control logic for the water tank case study. Following the principles of HAZOP, deviations from a normal behaviour can be introduced for each action in the PCED by using the guidewords in Table 1. For example, the deviation for the action *receiving a signal from a remote site* (Node N1 in Fig. 2), would be *fail to receive a signal from a remote site*. The consequence of this deviation is that the set-point of the local PID controller is not available or a BAD value. If no measure was taken for this consequence the local PID controller will be not able to work properly, which may lead to the liquid level of the water tank changing dramatically. Similarly, deviations for other actions in the PCED will need to be considered. Table 3 summaries deviations, corresponding causes, and consequences for the water tank shown in Fig. 3. Actions in Table 3 must be taken in order to prevent the consequences from happening.

6. CONCLUSIONS

Without question, the design of Internet based control systems is currently an important topic in the process control community. There are many opinions as to the properties such new kind of systems should possess, and the techniques that should be used to develop them. Two such properties are safety and security. This paper explored risk analysis within the safety and security domains. The safety risk analysis aims to identify the potential hazards in the system. The security risk analysis focuses on finding a way to stop malicious attacks from outside and to prevent loss as early as possible. The similarity of safety and security has been identified and the risk analysis methods can be applied to each other. For the security risk analysis this paper pointed out four possible protections to stop the malicious attacks. The detail of the security risk analysis is given in terms of the IF-What method, which is mainly used for safety risk analysis. The safety risk analysis is based on our previous work for computer-controlled plants. A modified PCED is proposed for the Internet based control systems and the actions, which must be taken, are produced through the modified PCED based HAZOP analysis in order to ensure the safety of the Internet based control systems. A case study illustrates the procedures of applying the security and safety checking in a process plant.

REFERENCES

Chung, P. W. H and S. H. Yang (2003). Safety Analysis of Process Plant Control Systems Based

on Model Checking, The Journal of Safety & Reliability, **23**, 19-34.

Chung, P. W. H, S. H. Yang, and D. W. Edwards (1999). Hazard Identification in Batch and Continuous Computer-Controlled Plants. *Industrial & Eng. Chem. Research*, **38**, 4359-4371.

Eames, D. P. and J. Moffett (1999). The integration of safety and security requirements. *Lecture Notes in Computer Science*, **1698**, 468-480.

Furuya, M., H. Kato, and T. Sekozawa (2000). Secure web-based monitoring and control system. *The 26th Annual Conference of The IEEE Industrial Electronics Society*, **2**, 2443-2448. Nagoya, Japan.

Ministry of Defence (MOD) (1996). Hazop studies on systems containing programmable electronics, Part 2: general Application Guidance. Interim Defence Standard, Glasgow.

Overstreet, J. W. and A. Tzes (1999). An Internet-based real-time control engineering laboratory. *IEEE Control Systems Magazine*, **19**, 320-326.

Rushby, J. (1994). Critical properties: survey and taxonomy. *Reliability Engineering and System Safety*, **43**, 182-219.

Shindo, A., H. Yamazaki, A. Toki, R. Maeshima, I. Koshijima, and T. Umeda (2000). An approach to potential risk analysis of networked chemical plants. *Computers & Chemical Engineering*. **24**, 721-727.

Treseler, H., O. Stursberg, P. W. H. Chung, and S. H. Yang (2001). An Open Software Architecture for the Verification of Industrial Controllers. *Journal of Universal Computer Science*, **7**, 37-53.

Yang, S. H. and J. L. Alty (2002). Development of a Distributed Simulator for Control Experiments through the Internet. *Future Generation Computer Systems*, **18**, 595-611.

Yang, S. H., O. Stursberg, P. W. H. Chung, and S. Kowalewski (2001). Automatic Safety Analysis of Computer-controlled Plants. *Computers and Chem. Eng.*, **25**, 913-922.

Yang, S. H., X. Chen, and J. L. Alty (2003). Design issues and implementation of Internet-based process control systems. *Control Engineering Practice*, 11, 709-720.

Table 3 Partial HAZOP analysis results for the water tank control system

HAZOP item	Attribute	Guide word	Deviation	Causes	Consequences	Actions
N1	data flow	no	no signal from the remote site	Internet congestion, Internet time delay, Internet connection broken.	Set-point is the BAD value. The local PID controller will not work properly.	The previous set-point value is adopted if the current set-point is the BAD value.
N2	data flow	no	no signal from the liquid level sensor	The liquid level sensor is out of order.	The liquid level signal in the BAD value. The local controller will not work properly	Install a duplicate sensor.
N4	data flow	no	no signal to the outlet valve	The communication between the local computer and the outlet valve is broken.	The outlet valve is left uncontrollable.	Regularly checking the RS232 cable.
N1	data value	more other than	set-point incorrect	The remote operator made an error or the remote system failed.	The signal to the outlet valve is changed according to this incorrect set-point.	Adding a safety locking system to stop the mistake from the remote site propagating into the local control system.