A framework of security and safety checking for internet-based control systems

Lili Yang*

Business School,
Loughborough University,
Loughborough, Leicestershire LE11 3TU, UK
Fax: (44) 1509-223961
E-mail: L.Yang@Lboro.ac.uk
*Corresponding author

S.H. Yang

Computer Science Department,
Loughborough University,
Loughborough, Leicestershire LE11 3TU, UK
Fax: (44) 1509-211586
E-mail: s.h.Yang@Lboro.ac.uk

Abstract: Internet-based control is a way of using the internet as a platform for remote monitoring and control operation. The obvious benefit is to enable remote monitoring and maintenance of process plants and to initiate global collaboration and data sharing between operators from geographically dispersed locations. However, connection to an open network and the use of universal technology present high safety and security risks to the new generations of control systems. Are we opening up our internet-enabled control systems for trouble since a number of malicious hackers continually attack web servers on the internet? The new type of control systems will never be accepted by industries if people do not have enough confidence in their safety and do not feel secure by using the system. This paper presents a framework of security and safety checking, used in the design of internet-based control systems. Based on the existing measures of physical and network securities, such as firewall and comprehensive user-authorised access control, the framework proposed in this paper focuses on the security of control commands transferred over the internet, responding actions to malicious attacks and system safety. An internet-based control system for a process rig is used as a case study to illustrate the implementation of the framework.

Keywords: hybrid data encryption; information and computer security; internet-based control; malicious attacks; safety.


Biographical notes: Lili Yang received a BSc degree in Instrument and Automation from the University of Petroleum, China, MSc degree in Information Technology from Loughborough University, and PhD in Computer Science from Derby University in the UK. She is a Lecturer in the Business
School at Loughborough University. She is a Member of the British Computer Society (MBCS) and a Chartered IT Professional (CITP). Her research interests focus on networking security and risk analysis, networked control and evolutionary computation. She was the best paper winner in the 16th International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (IEA/AIE-2003).

Shuang-Hua Yang received a BSc degree in Instrument and Automation and MSc degree in Process Control from the University of Petroleum, China in 1983 and 1986, respectively, and PhD in Intelligent Systems from Zhejiang University in 1991. He is a Senior Lecturer in Computer Science and the Director of the Networks and Control Research Group at Loughborough University. He is also an Overseas Professor in Central China Normal University and a Guest Professor in Huazhong University of Science and Technology. His research interests include wireless sensor networks, networked control, safety critical systems and real time software maintenance. He is a fellow of the Institute of Measurement and Control (FInstMC), the chairman of the East Midlands Section of InstMC and a Chartered Engineer (CEng) in the UK. He is a member of the editorial advisory board of the *Int. J. Information and Computer Security* and an Associate Editor of the *Int. J. Systems Science*.

1 Introduction

Internet-based control is becoming a new generation of control systems, in which the internet is used as a platform for global remote monitoring and control. An internet-based control system allows 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 a local process (Yang and Alty, 2002). A typical internet-based control system is illustrated in Figure 1 (Yang, Chen and Alty, 2003), in which the detailed control functions are implemented on the local side. Internet-based control on the remote side is invoked only when updating parameters, such as set-points. The new set of remote parameters is used as the input for the local control system until the next set of parameters is received. One of the advantages of this typical internet-based control system is the preservation of investment in legacy systems, such as scheduling internet-based control systems through existing distributed control systems and programming logic controllers. It also offers a high safety level because the local control system is working as its redundant system. Furthermore, it is likely not to be greatly affected by the internet time delays because the internet time delays are excluded from the close loop of the local control system.

Figure 1  The block diagram of the internet-based control (Yang, Chen and Alty, 2003)
Security and safety checking for internet-based control systems

The difference from normal remote control systems and/or distributed control systems is that the communication medium 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, Kato and Sekozawa, 2000; Shindo 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. The nature of remote control also increases the safety risk to the processes since there might not be any local operators around the processes. Therefore systematic safety and security checking in the design of internet-based control systems is essential in order to reduce the loss caused by the attacks. It will also provide the guidelines for the operators to efficiently respond the attacks.

This paper will systematically consider the safety and security issues through the design phase and clarify all the scenarios of malicious attacks. Actions to respond 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 the similarity of the safety and security problems in the internet-based control systems. Section 3 proposes a framework of stopping all the possible attacks from malicious hackers. Section 4 addresses how to secure the control commands, transferred over the internet through a hybrid data encryption algorithm. Section 5 presents a safety risk analysis, based on the principles of process plant HAZard and OPerability (HAZOP) (MOD, 1996; Chung, Yang and Edwards, 1999). Section 6 gives a case study to illustrate the procedures of safety and security checking. Section 7 is the conclusion.

2 Similarity of safety and security

The safety risk analysis 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 and dangers in a system are called vulnerabilities and threats, and in safety they are called failure mechanisms and hazards, but they can be considered to be alike. In security examples, the counter-measures that need to be put in place to counter the risks are access controls, firewalls and so on. 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 the 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 also could be applicable to the other.

In internet-based control systems the safety problems are caused by the authorised users because of the nature of the remote operation. Avoiding the failures caused by the authorised users can be achieved through safety analysis at the internet-level. The security problems are caused by the malicious attacks. Preventing attackers from accessing the internet-based control systems are assured by the measures of network security, physical security and data security such as firewall and data encryption. Adequate responding actions should be taken to prevent any fatal accidents from happening once these measures of security fail.

3 Security risks from malicious hackers

3.1 Framework of security checking

The internet router is obviously the first target of attack if any malicious hacker tries to get unauthorised access into a local control system (Shindo et al., 2000). Figure 2 shows a possible intruding path from breaking 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). 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. Actually Figure 2 gives four possible points at which the path from A1 to E5 might be cut off:

Figure 2  Framework of stopping possible malicious attacks
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 and purely relies on the measures of the available network security and physical security. There are rich literatures (Hamdi and Boudriga, 2005; Marin, 2005) in these areas, which are not investigated in this paper.

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 external network (Node B4) and allowing the control system to run isolated from the network. A virtual system on safe control will be discussed for this purpose.

Cutting the path between the Nodes C3 and D4 by using a safeguard to protect the process from an unexpected change in control parameters. The safeguard might be based on a simple threshold for a key-process parameter or a complex-control performance index.

Cutting the path between the Nodes D4 and E5 by activating a Safety Interlock Systems (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. The SIS has been widely used and independently implemented with the safety critical control systems (Yang et al., 2001).

3.2 What-If approach applied in the framework

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

The What-If approach was mainly used for safety checking. As described in Section 2, because of the similarity of safety and security the What-If approach can be employed for security checking according to the framework shown in Figure 1. Three scenarios generated in the security checking are summarised in Table 1. Three actions (Actions 1–3) must be taken to avoid the consequences occurring. In Scenario 1 firewall and password control have been broken by malicious attacks. The corresponding action (Action 1) is to disconnect the external link of the local control system with the internet.

In Scenario 2, 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 reduce the influence of the parameters change. The safeguard system might be designed to simply filter out the abnormal control action. Scenario 3 is that, if an abnormal process condition has been created by an attacker, a SIS will be activated to keep the process in a safer condition and wait for the intervention from a local operator. The details of three actions are described as follows.

**Action 1:** Disconnect the external link of the local control system with the internet if the intrusion goes through.

The plant will never be absolutely safe and secure if a remote user is allowed to directly access and make any change to the local control system. On the other hand, the plant will never be remotely controllable if a remote user is not allowed to access and justify the control system. Action 1 can be implemented through a virtual controller and a virtual
plant, which are introduced to act as a mediate between the remote user and the plant. Any authorised remote user can have direct access to the virtual system, but not to the real plant. The virtual system is designed to predict the behaviour of the real plant under the control action assigned by the remote user and therefore it can be used to check whether or not the control action from the remote user is doing any harm to the real plant. If the behaviour of the virtual plant under a certain remote control action is desirable this control action is applied to the real plant via a safeguard, otherwise the remote control action is rejected. Figure 3 illustrates the principle of the safe control mechanism described above.

Table 1  General What-If reviews in terms of the framework

<table>
<thead>
<tr>
<th>If</th>
<th>What</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario 1: Firewall and password control are broken.</td>
<td>Attackers obtain the access to the control system</td>
<td>Action 1: Disconnect the external link of the local control system with the internet if the intrusion is detected</td>
</tr>
<tr>
<td>Scenario 2: Attackers have modified control parameters</td>
<td>Disturbances have been introduced into the process</td>
<td>Action 2: A safeguard system filters out any abnormal change to the local control system</td>
</tr>
<tr>
<td>Scenario 3: Attackers have created safety critical conditions</td>
<td>A fatal accident might be happening</td>
<td>Action 3: An emergency SIS is required to be automatically activated</td>
</tr>
</tbody>
</table>

Figure 3  Safe control through a virtual system

Action 2: A safeguard system filters out any abnormal change to the local control system.

Various control performance assessment methods can be used in a safeguard to check whether or not the control action from the remote user is doing any harm to the real plant. Being simpler than the ordinary control performance assessment the virtual process output under the control action assigned by the remote controller is used in the safeguard to calculate the integral of absolute error and mean squared error.

1 Integral of Absolute Error (IAE): over a period of time the integral of absolute deviation between the set-point and the measurement. It can be employed to assess the control performance during set-point change. For the process with disturbances, this value increases monotonically with time.
191

\[ IAE = \sum_{k=k_0}^{k_f} |e_k| \]  

(1)

where \( e_k \) is the difference between the samples of the set-point and the output at the instant \( k \). \( k_0 \) and \( k_f \) are the starting and ending instants of the samples.

2 Mean Squared Error (MSE): the integral of the squared difference between the set-point and the measurement divided by the time interval.

\[ I_{MSE} = \frac{1}{f} \sum_{k=k_0}^{k_f} e_k^2 \]  

(2)

where \( f \) denotes the number of the calculated data.

If \( IAE < \lambda \) or \( I_{MSE} < \lambda \) then it shows the control action from the remote controller is acceptable, where \( \lambda \) is the maximum tolerant index, which is set according to the experience, otherwise the control action received from the remote controller is suspectable.

**Action 3:** A SIS is activated.

A SIS, which is sometimes called an emergency shutdown system (AIChE/CCPS, 1993), is one of the most important protective measurements in process plants, which provides automatic actions to correct an abnormal plant event, which has not been controlled by basic control systems and manual interventions. A SIS is only needed on those rare occasions when normal process controls are inadequate to keep the process within acceptable bounds. A SIS must be designed independently with normal control systems and serve as their last backup system.

**4 Data security**

The above framework of stopping possible malicious attacks presents four layers of protecting internet-based control systems from malicious attacks. The first layer is the standard firewall protection, which uses password control to allow only authorised users to enter the control system. The second to fourth layers are the protection measures of responding to the possible intrusion by employing a virtual system, safeguard and SIS in order to stop the happening of fatal accidents. Data security is the measure of protecting control commands from changing by malicious hackers on the way of transferring from the remote site to the local site over the internet. Data security for internet-based control systems must be secure enough and satisfy the real-time requirements as well. In this section a two-stage hybrid data encryption algorithm is investigated. In the setup stage the RSA Rivest-Shamir-Adleman (RSA) algorithm (DI Management, 2005) is used to establish the communication link by generating a RSA public key and a RSA private key and securely transferring an Advanced Encryption Standard (AES) cipher. The RSA algorithm uses a public key to encrypt the AES cipher and uses a private key to decrypt it. The second stage is data exchange, in which the AES (Daemen and Rijmen, 1999) is used to regularly encrypt/decrypt the real-time control commands using the transferred AES cipher. All of the steps in the AES data encryption are simple matrix operations,
which make the AES suitable for real-time data encryption/decryption. This combination has been compared with a similar combination of the AES and the Secure Sockets Layer (SSL) (Netscape, 1996), in which the AES is used to encrypt the real-time data and the SSL to transfer the AES cipher. The detail is given as follows.

4.1 Hybrid algorithm, based on advanced encryption standard and rivest-shamir-adleman

The principle of this hybrid algorithm, based on the AES and RSA is shown in Figure 4. In the setup stage the RSA public and private keys are generated by the key generator on the receiver side, and then the RSA public key is sent to the sender side. The generated AES cipher on the sender side is encrypted using the received RSA public key and then sent to the receiver side and decrypted using the RSA private key. In the data exchange stage the real-time data is encrypted/decrypted using the AES algorithm and the transferred AES cipher.

Figure 4 Hybrid algorithm based on the AES and RSA algorithms

In the process of the RSA encryption, the private key is saved in the receiver and the public key is transmitted to the sender at the same time. The RSA algorithm adopts the public key to encrypt the AES cipher and the private key to decrypt it. It is impossible to determine the private key from the public key. Owing to the private key never being transported, the security of the AES cipher transferred by the RSA algorithm is apparently much higher than that of the AES algorithm. The security of the RSA algorithm comes from the computational difficulty of factoring large numbers, and costs much more time for encryption/decryption data than the AES one. In contrast, the AES algorithm encrypts real-time data only using simple matrix operations and has a high rate of encryption/decryption. The hybrid real-time data encryption/decryption algorithm shown in Figure 4 might absorb the advantages of AES and RSA algorithms and avoids their disadvantages.

In order to evaluate the hybrid encryption algorithm, the time delays of the AES, RSA and their hybrid encryption/decryption algorithms are compared in a similar network environment. The total time delay is composed of three parts: the data encryption time, the encrypted data network transmission time and the data decryption time. If the network environment and the processing power are similar, the total time delay will depend on the data encryption/decryption time delays. Figure 5 shows that the total time delay of the
hybrid algorithm is close to that of the AES and is much shorter than that of the RSA. Furthermore, since the AES cipher of the hybrid algorithm is encrypted by the RSA, it is much hard to be deciphered. Therefore, the hybrid algorithm is securer than the AES.

Figure 5  Comparison of the end-to-end latency of AES and RSA

4.2 Hybrid algorithm, based on Advanced Encryption Standard and Secure Sockets Layer

Similarly, the AES and SSL can be combined together to secure the control commands transferred over the internet for internet-based control systems. In the new combination the RSA is replaced by the SSL for transferring the AES cipher. The way of using the AES is the same as the one in the combination of the AES and RSA. The SSL in this hybrid algorithm involves the authentication on both the sender and receiver sides. The AES algorithm and this hybrid algorithm are implemented and compared. The experimental results are illustrated in Figure 6, which shows that this hybrid algorithm and the AES algorithm have a similar end-to-end latency, but the hybrid algorithm can prevent unauthorised access to the network. The result of the SSL is not shown in Figure 6 since it is only for TCP socket, and not for UDP.

Figure 6  Comparison of end-to-end latency of AES and SSL
4.3 Discussion of the experimental results

The experimental results are summarised in Table 2. The average end-to-end latency indicates the normal operation period. The maximum and minimum latencies illustrate the existence of the unpredictability of the internet transmission. The advantages and disadvantages of the four possible data encryption/decryption algorithms are also summarised. As shown in Table 2, the end-to-end latency of two hybrid algorithms is close to that of the AES algorithm and much shorter than the RSA algorithm, and the lower average latencies of the two hybrid algorithms, 288.94 and 255.47, indicate that they are suitable for securing control commands, transferred over the internet for internet-based control systems. Considering the two hybrid algorithms, the one using the AES and SSL algorithms can prevent unauthorised access to the network and bring lower latency as well. But it can’t ensure the AES cipher and cipher-text simultaneously. Both of them use the AES algorithm to encrypt/decrypt the AES cipher and are equally suitable for real-time applications.

Table 2 Comparison of the experimental results

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>Average latency (ms)</th>
<th>Maximum latency (ms)</th>
<th>Minimum latency (ms)</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>1003.46</td>
<td>1250</td>
<td>978</td>
<td>Cipher more safety</td>
<td>High latency</td>
</tr>
<tr>
<td>AES</td>
<td>249.57</td>
<td>446</td>
<td>227</td>
<td>Low latency</td>
<td>Cipher not secure enough</td>
</tr>
<tr>
<td>Combination of AES and RSA</td>
<td>288.94</td>
<td>544</td>
<td>270</td>
<td>Cipher securer; low latency; AES cipher and cipher-text synchronous</td>
<td>No authentication</td>
</tr>
<tr>
<td>Combination of AES and SSL</td>
<td>255.47</td>
<td>284</td>
<td>236</td>
<td>Cipher securer; low latency; access by authentication</td>
<td>Cannot ensure AES cipher and cipher-text synchronous</td>
</tr>
</tbody>
</table>

5 Safety risk analysis

Authorised 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 the previous research (Chung, Yang and Edwards, 1999; Yang, Tan and He, 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 visualised 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 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, based on the symbolic model checking approach.

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 Figure 7. 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 user interface, 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:

$$PCED = (Lay, Nod, Edg, Act)$$

in which $Lay$ denotes an ordered set of symbols Web Client (Wc), Web-based user interface (Wbi), 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:

$$Nod = (Nod_{Wc}, Nod_{Wbi}, Nod_{Int}, Nod_{Comp}, Nod_{S/A}, Nod_{Proc})$$

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 $a_j$ in the set $Act = \{a_1, \ldots, a_{nact}\}$ corresponds to the horizontal order with which the nodes involved are arranged in the PCED from left to right. In this study, the HAZOP principle is followed and various deviations are applied into the PCED for each action $a_j$ in order to systematically identify the potential safety risks.

**Figure 7** Modified process control event diagram

![Modified process control event diagram](image)

Due to the nature of remote operation and internet environment constraints even authorised remote users may cause failures in the process without any improper operation. Therefore, it is necessary 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 the conventional HAZOP (AICHE/CCPS, 1993) 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. Further three guidewords have been added in this work: 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 summarised and interpreted in Table 3. Deviations from normal behaviours of the control systems are considered for each action $a_j$ 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 applying the hazard analysis will be illustrated in the following case study.

Table 3  Attributes, guidewords and interpretations for internet-based control systems

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

6.1 Internet-based control system design

To illustrate how well the safety and security checking procedures can be applied, an experimental water tank rig in our Networks & Control laboratory at Loughborough University is used as a case study. The experimental system layout is shown in Figure 8. The control objective is to maintain the liquid level of the water tank at a desired value. The tank is filled by the inlet flow and is emptied into a drainage tank through a connection pipe and a pump. The inlet flow is controlled by a local Proportional Integral Derivative (PID) controller to maintain the liquid level of the tank at a desired value. The remote controller is designed to adjust the set-point of the local controller from a remote site. The Data AcQuisition (DAQ) instrument is used to gather the liquid level signal from and send a control command to the water tank. The remote controller is connected with the internet through a British Telecommunication (BT) broadband with the 56K bandwidth.

![Figure 8 Physical layout of the internet-based control system](image)

6.2 Measures of security

Guided by the framework of stopping possible malicious attacks, shown in Figure 2 the following measures have been taken in the design of the above internet-based control system:

- Firewall and access control in place. As seen in Figure 8 a firewall is designed to stop any unauthorised access to the local control system. Password control is also in place in the remote control system. Only registered users can view the remote control interface and have access to the internet-based control system.

- A virtual system is employed in the local site. The virtual system is composed of a PID control algorithm and a plant model. Any control commands received from the remote control system are first applied to the virtual system. The control performance index IAE shown in Equation. (1) is calculated in the virtual system to justify if the control commands are potentially doing any harm. If there is no harm, the control commands are passed to the safeguard, otherwise, they are dropped in the virtual system.
A safeguard is installed in the local control system. For the set-point received from the remote site, about 99% is set as a simple threshold. Any valid set-point must be less than or equal to this threshold, otherwise the received set-point is omitted.

An emergency shutdown system is running independently with the local control system. About 99% is set as the threshold of the liquid level. Once the liquid level reaches the threshold, the inlet pump is shut off immediately, and therefore the overflow of the water tank never takes place.

All the control commands and parameters from the remote control system are encrypted before they are transferred over the internet and decrypted after received by the local control system using the hybrid algorithm of the AES and RSA. Figures 5 and 6 were the experimental results of the transmission latency for the remote set-point of the water tank.

### 6.3 Safety checking

If replacing the process variable $X$ with the liquid level, the process variable $Y$ with the opening of the inlet valve, and the computation Node N3 with the PID control algorithm, the PCED shown in Figure 7 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 3. For example, the deviation for the action ‘receiving a signal from a remote site’ (Node N1 in Figure 7), 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 not be 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 need to be considered. Table 4 summaries deviations and corresponding causes and consequences for the water tank. Actions in Table 4 must be taken in order to prevent these consequences from happening.

### 7 Conclusion

There is no doubt that 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 that these 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 explores a framework of safety and security checking for internet-based control systems. The security risk checking focuses on finding a way to stop malicious attacks from outside and to prevent loss as early as possible. Four possible protections to stop the malicious attacks are identified in the proposed general framework. After identifying the similarity of safety and security of the What-If method, which is mainly used for the safety risk analysis, it is applied to the security risk analysis. Three actions of stopping the malicious attacks at different layers are proposed in terms of the What-If method. The transferring of control commands over the internet for internet-based control systems is secured by a hybrid data encryption/decryption algorithm, which might be the combination of the ASE
and RSA or the ASE and SSL. The comparisons of these combinations with individual encryption/decryption algorithms are experimentally verified. The safety risk checking aims to identify the potential hazards in the control system. A modified PCED is proposed for the internet-based control systems and the actions, which must be taken in order to ensure the safety of the internet-based control systems, are derived through the modified PCED-based HAZOP analysis. The case study illustrates the procedures of applying the security and safety checking in the design of the internet-based control system for the experimental water tank rig.

Table 4 Partial HAZOP analysis results for the water tank control system

<table>
<thead>
<tr>
<th>HAZOP item</th>
<th>Attribute</th>
<th>Guide word</th>
<th>Deviation</th>
<th>Causes</th>
<th>Consequences</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>N1</td>
<td>Data flow</td>
<td>No</td>
<td>No signal from the remote site</td>
<td>Internet congestion, internet time delay, internet connection broken</td>
<td>Setpoint is the BAD value. The local PID controller will not work properly</td>
<td>The previous set-point value is adopted if the current set-point is the BAD value</td>
</tr>
<tr>
<td>N2</td>
<td>Data flow</td>
<td>No</td>
<td>No signal from the liquid level sensor</td>
<td>The liquid level sensor is out of order</td>
<td>The liquid level signal in the BAD value. The local controller will not work properly</td>
<td>Install a duplicate sensor</td>
</tr>
<tr>
<td>N4</td>
<td>Data flow</td>
<td>No</td>
<td>No signal to the outlet valve</td>
<td>The communication between the local computer and the outlet valve is broken</td>
<td>The outlet valve is left uncontrollable</td>
<td>Regularly checking the RS232 cable</td>
</tr>
<tr>
<td>N1</td>
<td>Data value</td>
<td>More other than set-point incorrect</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

References


