



**Whitepaper**  
**Process Control System Security**

**Author: Max Rockliff**  
**Principal PCS Security Engineer**  
**PLEXAL GROUP**



## Contents

CHAPTER 1	INTRODUCTION .....	1
CHAPTER 2	WHAT IS SECURITY? .....	3
CHAPTER 3	WHAT IS THE EXPOSURE? .....	4
3.1	SUMMARY .....	5
CHAPTER 4	HOW DO WE MANAGE PCS SECURITY? .....	6
4.1	SCOPE .....	7
4.2	THREAT ANALYSIS .....	7
4.3	DESIGN REVIEW .....	8
4.4	RISK ASSESSMENT .....	8
4.4.1	CHOICE OF A RISK MODEL.....	8
4.4.2	DETERMINATION OF ACCEPTABLE RISK.....	9
4.4.3	DETERMINATION OF RESIDUAL RISK.....	9
4.4.4	IDENTIFICATION OF ADDITIONAL SECURITY CONTROLS.....	10
4.5	RISK MITIGATION.....	13
CHAPTER 5	ON-GOING PCS MANAGEMENT .....	14
5.1	OWNERSHIP AND RESPONSIBILITY.....	14
5.2	MANAGEMENT .....	15
5.2.1	SYSTEM AUDIT.....	15
5.2.2	THREAT AND RISK REVIEW.....	15
5.2.3	ON-GOING RISK MITIGATION.....	16
5.2.4	INCIDENT RESPONSE .....	16
5.2.5	BUSINESS CONTINUITY AND DISASTER RECOVERY .....	17
CHAPTER 6	SUMMARY .....	19
CHAPTER 7	AUTHOR BIOGRAPHY .....	20

## CHAPTER 1 INTRODUCTION

For many years process control system (PCS) environments have been operating with the “luxury” of isolation from the rest of the world in technical and physical terms. This was largely due to their proprietary nature and the corresponding specialised knowledge that was needed to work with them. System components were purchased as black boxes considering only their end-to-end function rather than being concerned with the devices’ interconnectivity with other systems.

Vendors have increasingly adopted standard technologies, operating systems and transmission protocols, such as Microsoft™ and TCP/IP in response to market pressures, which has brought greater versatility and connectivity potential. These changes have opened doors to improved productivity by providing easy remote connectivity and access across corporate infrastructure and the Internet. However, the use of non-proprietary operating systems has reduced the security of PCSs through the introduction of vulnerabilities already common to the greater IT community. This often makes the PCS environment an unfortunate, incidental victim and a greater potential target due to the extensive knowledge of such vulnerabilities.

Protection of networks is often achieved by installing firewalls at their external connection and relying on these firewalls to “keep out the bad guys”. This approach can result in a high level of trust in the perimeter security at the expense of internal security. While properly configured and maintained firewalls can offer strong protection, there have been incidents in which firewalls have been breached or bypassed, despite good management, providing the hacker or virus access to the less secure internal systems. Such reliance on the external perimeter security, with lesser or weak internal controls, is known as eggshell security: The egg has a hard outer shell, but is soft and vulnerable on the inside. A breach of the shell can quickly result in the destruction of the contents. This analogy follows for computer and PCS networks when little consideration is given to internal protection should the firewall be breached. A PCS that is reliant on the corporate firewall may be at greater risk, as PCS risk may be greater than that of the corporate network for which the firewall was designed.

The use of industry standard technologies has also seen a widening of options for maintenance and support to include not only the vendor, but corporate-IT as well. Previously, the proprietary nature of PCS technologies permitted Control Systems Engineers to focus on PCS operation and rely of the vendor for maintenance and support, confident that they were well versed in the needs and nuances of their PCS. Now in-house Corporate IT has many of the technical skills to provide support but may have limited experience with the critical operational requirements of a PCS. There are usually conflicting requirements between corporate IT-standards and the unique PCS operational requirements and constraints.

PCS security now needs the combined efforts of all three groups:

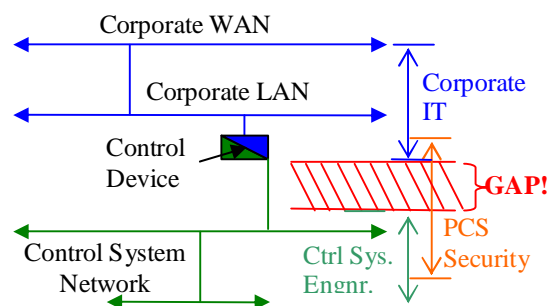
- The control systems group to manage all aspects of the PCS including security and ensure business operational requirements are met;
- The Corporate-IT group to provide detailed understanding of the business IT infrastructure, the experience to manage security on a day to day basis and ensure corporate business requirements are met; and
- The PCS vendors to provide the detailed understanding of the system itself and ensure technical requirements are met.

Recent widely publicised security breaches and virus/worm attacks have precipitated an air of fear and ill-conceived, over-reaction to perceived security shortcomings. Many companies and some countries are now introducing onerous security regulation on critical infrastructure, which may consequently impact the PCS. What is required is analysis of realistic scenarios in which *real* threats and risks are identified and effective controls are implemented to address *real business risks – and no more*. PCS security is just another business risk.

In addition to these “untargeted” attacks, there have been several notable incidents due to SCADA system failure through hacker or virus activity, some examples of which are given below

- 1999:** Bellingham, USA – SCADA system failure causes gasoline pipeline leakage – 2 killed in resulting vapour explosion.
- 2000:** Maroochydore QLD sewage control systems hacked by disgruntled ex-employee releasing raw sewage into waterways.
- 2001:** California, USA - California Independent System Operator, operator of California’s power grid, detect hack of their computer systems.
- 2002:** Ohio, USA – Slammer worm disables safety monitoring system for 5hrs at Davis-Besse nuclear power plant.
- 2003:** Blaster worm linked to major US power grid blackout.

If security is managed objectively and rationally, mitigation appropriate to the business requirements can be easily implemented, maintained and demonstrated. PCS security need not be a burden and may be easily managed with minimal outlay. This paper attempts to demystify the hype and provide a clear and effective methodology to address the security of PCSs.



**Figure 1.1 - The PCS Security Gap**

## CHAPTER 2 WHAT IS SECURITY?

Security, according to the Merriam-Webster Online dictionary is “the quality or state of being secure – to be free from danger”. According to industry standards, it is defined as follows.

**Confidentiality** Ensuring that only authorised personnel are able to see information for which they are authorised.

**Integrity:** Ensuring the information provided by the system has not been modified, corrupted, destroyed or otherwise disrupted since its entry or creation and is free from error. I.e. the operator can have confidence in the information made available to them by the system.

**Availability** Ensuring that information (and systems) are available to those who need them, when they need them.

In addition, the following supplementary definitions are often incorporated.

**Authenticity:** The quality of being sure that an individual operating an authorised access account is the person to who that authority was granted. It also refers to the authenticity of the information – that it is original and is not a reproduction or fabrication.

**Access Control:** Being able to control the access to the various information available on a system to which a person has been authorised and authenticated.

These definitions apply equally to PCSs. PCS operators must generally ensure that information generated by the PCS is accurate and available only to authorised personnel, as it is often linked to the profitability and reputation of the organisation.

**PCS Confidentiality** has long been a concern, but Control Systems Engineers and developers have only ever needed minimal measures to ensure this, as it has often been inherent due to the proprietary, physically and electronically isolated nature of the traditional PCS.

**Integrity** of PCS information must also be assured so that it accurately represents the status and history of the process.

Facilitating these objectives is the supplementary security aspects of authenticity and access control as these are the mechanisms that control connectivity to the PCS and access to the various sources of information it provides or functions of which it is capable.

**Availability** is of particular interest to a PCS, as most such systems are required to work 24 hours a day, 7 days a week, all year long. Outages to part or all the PCS, may adversely affect the plant safety or business profitability. Even an outage of a low-criticality component may have an escalating adverse effect should the outage time extend without resolution.



All of these issues have typically been addressed appropriately and satisfactorily in the traditional PCS environment. However, the recent non-proprietary nature and trend to interconnect or integrate with corporate networks and other remote access networks, has resulted in a significant increase in the exposure and risk to the PCS environment.

### **CHAPTER 3      WHAT IS THE EXPOSURE?**

The security issues surrounding a traditional PCS were generally of little concern to the control systems engineer compared to the functional requirements, other than, perhaps, safety related issues. The systems were most often based on proprietary, purpose-built, operating systems and proprietary or industry unique network technologies and transmission protocols. In addition, the physical isolation of a typical PCS, usually confined to a production facility and not generally electronically connected to any other network systems (other than, perhaps, similar PCSs), resulted in inherent security, especially from external sources.

An attacker required physical access to the PCS and a strong technical knowledge to bring about any harm.

The industry pressure on PCS vendors to move to non-proprietary operating systems and network technologies did not, in isolation, impact the PCS security. However, the use of such systems has increased the number of people with sufficient skill to access the system and paved the way to connect with other computer network systems such as the corporate network, providing greater opportunity for unauthorised access. On the positive side, the ability to connect to the PCS for monitoring, optimisation and engineering purposes from the corporate network, especially remote to the facility, is attractive. All of this allows much greater scope for understanding and managing the business.

Some organisations maintain a strict isolation from other networks, but that may be short-lived and most are now connecting their PCSs to their corporate networks. Some organisations may enforce strict authorisation control, change management and work-authorisation processes for PCS management, but the potential for such functions to be compromised, or the PCS accessed, remotely by unauthorised personnel often remains available and unchecked. Worse, such activity may go undetected.

In this respect therefore, technology may be used to facilitate the adherence to correct procedures, but it should be noted that reliance on technology to enforce such procedures and access control absolutely is inherently flawed. All technology is limited, and can fail to effectively satisfy the control requirements due to inappropriate configuration or incorrect management. Through this, weaknesses in the security protection may be exposed to the wily attacker, or create opportunity for adverse impact from untargeted attacks such as computer viruses or worms.

It is possible, for example, that a well intentioned, corporate system administrator could unwittingly reconfigure a purpose-built PCS firewall while standardising all corporate firewalls, without knowledge or consideration of the particular security needs of the PCS.

Often, PCSs are a secondary victim to other attacks, such as computer viruses or worms. An example of this was experienced in the USA in late 2003, when the effect of the Blaster worm



was thought to have overloaded the power distribution SCADA system responsible for much of Washington State, causing widespread, extended power outages. Despite the existence of protection such as firewalls, the system became overloaded with extraneous network traffic, blocking the legitimate SCADA traffic.

The use of operating systems such as Microsoft Windows™ and Unix has introduced a range of exposures to the PCS environment, not experienced before (arguably less for Unix). The operating system is known to have vulnerabilities and these are used by computer virus authors and hackers alike to attack systems. Viruses are certainly a greater threat as they are more common, usually untargeted and indiscriminate in their attack and propagation.

In order to correct a discovered vulnerability, the vendor will typically release a patch or service pack update. Despite the release of these updates, it is generally unwise to simply apply them immediately to systems within a PCS. Such updates may require a system outage or have the potential to adversely impact the PCS functionality. Many PCS installations require scheduled outages and only with appropriate notice and authorisation (eg. 90+ day). Logistically, personnel to manage the upgrade and provide contingency support may not be available.

It is also possible that the upgrade may prevent the PCS applications from functioning or place the system in an unsupportable state as the vendor may not yet have certified the upgrade; a process that may take weeks.

To manage this situation and ensure on-going support and vendor-certified operation of the PCS, the control systems engineer must often delay such a security upgrade or approve its immediate implementation if the risk is deemed great enough. The former situation results in a time window during which the PCS will remain vulnerable and the latter introduces a risk of system failure as a result of the upgrade, which may not be immediately noticeable. Disconnection from the business network may no longer be a practical alternative to protecting the PCS.

### **3.1 SUMMARY**

To summarise, the adoption of non-proprietary operating systems and protocols has introduced many new security exposures, previously not of general concern to the PCS environment.

Due to the wide-spread, general purpose usage of the non-proprietary operating system, the PCS has become more vulnerable than it was in the traditional, proprietary environment. These vulnerabilities are far more widely known and exploited by virus authors and hackers. The associated need for increased management to eliminate published vulnerabilities along with the general impracticality and logistical issues of system outages and potential incompatibilities with the PCS application suites, further exposes the PCS to security breaches.

The increasing use of the TCP/IP network transmission protocol and the attractiveness to interconnect or integrate with corporate networks and provide other remote access, further exposes the PCS to external (to the PCS) attack, be it targeted or incidental.

## CHAPTER 4 HOW DO WE MANAGE PCS SECURITY?

The business risks associated with PCS security are fundamentally related to anything that may result in either a system outage, safety impact or any lost operational window. These risks can be in any area that constitutes the PCS environment, from physical security (central systems and control room access for example), people-related security issues (eg. policies, procedures, authorisation, training and culture), to electronic or IT-related security. The methodology to identify, evaluate, mitigate and manage the risks that your PCS faces is a multi-phased approach, each with a set of sub-processes.

1. **Threat Analysis:** The process of identifying all reasonable sources of threat, be they people, practice or systems (including other networks) that may be responsible or permit an attack on the PCS. The second step of threat analysis is to then determine the actions or events that the identified sources could perpetrate that would result in undesirable business impact.

2. **Design Review:** A detailed review of the PCS infrastructure, identifying all nodes (servers, workstations, PLCs, etc.), all network segments and associated protocols and technology, and all connection paths within the PCS and between the PCS and any external systems (including logical extensions such as remote control rooms). Individual nodes may be logically grouped together and considered as one for the purpose of risk analysis.

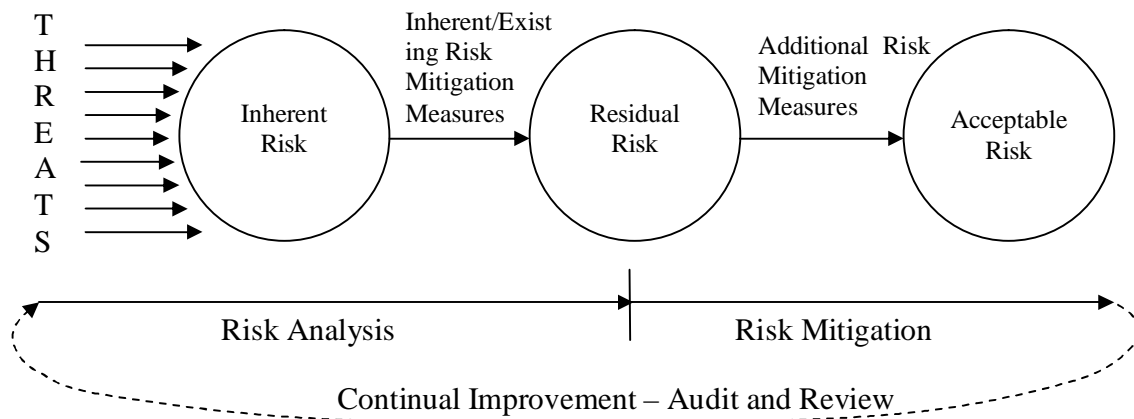
3. **Risk Assessment:** A two phase process. The first is to determine, without consideration of any existing protection, the acceptable level of risk associated with each node or major grouping. The second is to determine the perceived business risk associated with each of the identified threats on each of the identified nodes or node groups.

The second step requires examination of the potential, unmitigated (i.e. nothing stopping the undesirable event) impact, considering the effect of any inherent security capability and existing security controls, and then determining the existing perceived residual risk level. Inherent security capability may be such things as proprietary systems or protocols, the number of layers above that would need to be penetrated first, etc.

Due to the specific IT nature and the need for an in-depth understanding of the business and operational impact of each node on the PCS, this should generally be a collaborative effort, involving control systems, business and IT representation.

4. **Risk Mitigation:** Again this is a two-step phase. The first step entails identifying any additional controls, including possible restructuring of the PCS, new policies and procedures, etc. that would be needed to reduce any unacceptable risks (i.e. those residual risks that are greater than the agreed acceptable risk level), then to formalise the new system design. It is important that formal agreement is obtained for the design from all stakeholders.

Finally the design can enter the implementation phase. Following the implementation, it is advised that some sort of audit or post implementation review be carried out to ensure that the implementation correctly meets the operational design specification and objectives in mitigating the risks.



**Figure 4.1 - Risk Analysis and Mitigation Process**

#### 4.1 SCOPE

It is important to point out that the scope of the threat and ensuing risk assessment should be clearly determined and agreed by all management and stakeholders. For example, physical security may be excluded as this might be governed by a separate facility security management plan. It is important that the particular security needs of any excluded aspects are consistently and adequately controlled by other management regimes so that PCS business security outcomes are indeed satisfied. This may be completed as a separate exercise. The scope of the threat sources and actions will need to be agreed also.

#### 4.2 THREAT ANALYSIS

The first phase is the threat analysis, which, unlike risk analysis, is just identifying the threat sources (i.e. from where or whom a threat comes) and the threat actions (the activity that could result in system loss and not related to the likelihood of the impact). All threats need to be identified as if there were no control barriers, inherent or additional to mitigate the potential impact. In this process, all threats are identified, even if the feeling is that the existing infrastructure or procedures, or easily implemented controls would be deemed to reduce the risk to an acceptable level. Control Systems Engineers need to determine what real threats exist, even if they are considered low likelihood or already mitigated. Identified threats should be reasonable and not extremely unlikely to occur. However, care should be taken to ensure that the threats chosen are appropriate to the business.

For ease of analysis, the identified threats should be categorised and grouped to reduce the effort and generalise the result. Such categories as malware (computer viruses, worms or other malicious software) and unauthorised access (internal, external, from personnel with some form of authorised access and those without any), may be used to:

- a) bundle the threats into groups to ease the risk assessment; and
- b) generalise the risk assessment to a degree so that other threats may be included later.

If, during this process a threat is deemed to be unworthy of attention, yet falls within a particular category, the mitigating circumstances should be documented within the threat analysis.

### **4.3 DESIGN REVIEW**

The overall existing design of the PCS under review needs to be fully identified, including any temporary installations, modifications or work-arounds. This usually entails comparing any existing design specifications with the actual PCS installation and interviewing technical stakeholders. This is to ensure that all nodes and links, be they servers, workstations, communications equipment or network infrastructure are correctly and clearly identified. In a sense, this is a verification process to bring the design specifications up to date.

This step in the risk analysis process is critical to ensure that all nodes and entry, exit and interconnection paths between other parts of the PCS are clearly understood

### **4.4 RISK ASSESSMENT**

Once all the threats have been identified and agreed, then a risk assessment may be completed. Risk assessment involves identifying the potential, unmitigated loss due to system failure or attack in conjunction with the likelihood of such a failure or attack being successful. The potential impact is the worst reasonable undesirable outcome assuming the failure or attack event has occurred.

At this stage it is useful to ignore any inherent security capability or existing security controls and determine an unmitigated risk level. Following this, identify all the inherent security protection and existing security controls afforded to the system to arrive at the residual (or actual existing) risk level.

This approach aids in identifying if any inherent or existing controls are critical to the risk mitigation and therefore may need to be checked in the on-going management and threat and risk reviews.

This requires four steps as follows.

1. Choice of a risk model
2. Determination of acceptable risk levels
3. Determination of residual risk levels
4. Identification of appropriate additional security controls to reduce any unacceptable risks to the identified acceptable level.

#### **4.4.1 CHOICE OF A RISK MODEL**

The choice of a risk model, primarily being the various levels of risk, usually from insignificant to catastrophic, is important in order to be able to measure your relative risks in a consistent manner. It is best to define your risk model in line with your organisation's risk model if one exists. This will ensure that the risks identified and quantified are consistent with and justifiable against your organisation's fundamental business mission and business risk profile. This



approach avoids the possibility that any perceived risk is not confined to the particular experiences and preferences of the Control Systems Engineers or other stakeholders involved.

If a an organisational risk model is not available, then following guidelines outlined in such standards as AS-NZS 4360, is recommended as this will provide a process consistent with industry best practice. Essentially the risk model chosen should rank risks in four or five levels, using such definitions as low, medium, high, catastrophic. The risk may be evaluated in several categories, such as (potential) financial loss ranges, facility loss, human impact or environmental impact and some industries have metrics for this type of categorisation.

It is important to agree and define in the scope just what categories of risk are being analysed and which ones are not, and possibly why (eg. covered in other safety plans etc.).

An alternative to defining specific metrics for each level of risk, is to apply a more qualitative approach where risk levels are agreed based on a consensus (among stakeholders) of perceived risk. These are still categorised such as low, medium or high, but the assignment of risk is subjective. This method is arguably easier and relies heavily on the knowledge and experience of the stakeholders. The quantified, objective method discussed earlier, is most appropriate when using a corporate risk model, as the impact ranges are then consistent with all corporate risks.

#### **4.4.2 DETERMINATION OF ACCEPTABLE RISK**

This requires an assignment of a minimum risk level that would be acceptable within the chosen risk model. This may be on a node (or group) by node basis, with each having its own acceptable risk or simply to identify a normalised acceptable risk level, such as “low”.

One possible method is to define the risk model as low, medium, high, catastrophic (for example) and then to assert that a low risk is acceptable, a medium risk is marginally acceptable, depending on the cost effectiveness or practicality of any additional controls required to reduce it to a low, and anything high or catastrophic is unacceptable.

#### **4.4.3 DETERMINATION OF RESIDUAL RISK**

Once the acceptable risk for each node (or group) has been agreed, each node (or group) should be examined to identify the unmitigated risk. This is the business risk, calculated on outside factors without consideration of any internal, inherent security capability or existing security controls. I.e., the risk should only be calculated based on the potential impact and the likelihood of an undesirable event actually occurring and not considering what protection the system affords itself. The value of this step is to facilitate the determination of the effectiveness and criticality of any inherent capability or existing security controls. For instance; an unmitigated risk may be high, due to a high impact and significant likelihood of an incursion occurring. However, the inherent capability and existing controls may reduce the risk to a residual level of low. This would indicate that the inherent capability and/or existing controls are essential in maintaining that residual risk levels and steps must be taken to ensure that they continue to be effective should there be a change in technology or system design.

Once the unmitigated risk has been determined then the effect of any inherent protection afforded by the system technology or design (i.e. without additional components) and existing control measures (i.e. those protection devices, and usage procedures that control access to the node) may be taken into account to calculate the residual risk.

#### **4.4.4 IDENTIFICATION OF ADDITIONAL SECURITY CONTROLS**

For all nodes (or groups) with a residual risk greater than the acceptable risk, additional security controls must be designed. There are several methods of achieving this as follows and one or more methods may be chosen depending on the perceived weakness or vulnerability of the system.

- Bolster the security robustness of the node (or group), itself
- Provide additional protection around the node,
- Redesign the infrastructure to provide greater inherent protection.
- Implement policies and procedures.

##### **Bolster the Security of the Node.**

Where a node is found to be vulnerable in its own right, it may be possible to apply upgrades or software/firmware patches, additional configuration, or to choose an alternate, more robust, device, to reduce the risk level. This may have to be coupled with both additional procedures to ensure on-going currency and additional protection around the node to accommodate any delays in the implementation of said upgrades or patches, to provide adequate risk reduction.

This process may also include the disabling of non-essential functions and services on a node to minimise the opportunities for attack. Non-essential services often provide a path through which a wily hacker may quietly break in, as compromise of these services can often go unnoticed if they neither perform nor affect any visible function in the normal operation of the PCS.

##### **Provide Additional Protection Around the Node.**

When a node cannot be further protected within itself, or when there must exist a window of vulnerability between an upgrade or patch becoming available and being able to install that upgrade or patch, additional protection around the node (or group) can be implemented. Such additional protection could include one or more of the following.

- Connection Filtration.

Additional filtration of connections to reduce the exposure of the device – exposing only those functions, facilities and application ports required for essential operation. Like disabling non-essential services, this mechanism further limits the points of possible attack. This may be achieved through the use of devices such as routers (using access control lists) and firewalls (using firewall rules). Such filtration may be extended to limit connection to the node (or group) to only authorised nodes, using such features as MAC (Media Access Control – typically the unique address or manufacture provided number allocated to a network interface card) and IP

addresses. While this is not impervious it does provide easily implemented control using inexpensive routers. Firewalls can provide more sophisticated control.

- Authentication:

Additional authentication may be implemented (eg. through the use of firewalls), to require the connecting user or their workstation (not as secure) to authenticate to the connection gateway, be it a firewall or other device (certain routers may incorporate user authentication for example).

User authentication is by far the best method as it allows an authorised user to connect from any permissible network location and provides greater security than authentication of a workstation that may be left unattended and used by an unauthorised person.

Note: in this instance, authentication only provides assurance that the person attempting to connect is using the authentication factors that were assigned to an authorised person. The stronger the authentication, the more confidence one can have in the identity of the individual as the authorised person.

The authentication may also provide a high degree of filtration through the implementation of virtual private networks, or secured (through authentication and encryption) paths from an accessing workstation to a PCS node or section.

- Access Control

Access control, also known as security by design controls the authorised user's access and functional privilege once authenticated and connected. Access control is especially effective when coupled with strong authentication: The authentication provides the confidence that the person is who they say they are and the access control limits what they can do once on the system.

Technologies are becoming available that permit coupling of filtration, authentication and levels of access control, by applying filters that only permit transmission of permits commands and responses. However, this is complicated and difficult to establish.

- Compartmentalisation

Compartmentalisation is a security technique which essentially isolates one section of a system from the others permitting it to be accessed and operate independently from any other. This technique is very useful in PCSs to, say, isolate the control systems from the monitoring systems. Such isolation of safeguarding systems has usually been done traditionally, but arguably with slightly different motivations.

The purpose of compartmentalisation is as follows.

- a) Provide independent operation of one part of a PCS from any other,
- b) Strictly control all entry points to the section (usually only one),
- c) Facilitate disconnection from all other parts of the PCS and any external system without impact to the primary function of the particular section.

- **Electronic Isolation**

In some instances, it may be deemed necessary to block connectivity to a node (or group) from any remote node, either forcing work to be executed directly at the node, or by incorporating some type of physical or logical switching device that isolates the required node(s) when access is not required. This should be implemented with a robust change management and work authorisation system to prevent unauthorised access and the connection being left active after use.

- **Business System Isolation**

Often, PCSs are made accessible to devices on the corporate, business computer network for reasons discussed earlier. The critical operational nature of a control system may call for some form of isolation from the larger corporate network. This should be examined at two levels.

1. Isolation from the corporate network using techniques such as filtration and authentication as described previously.
2. Independence of PCS local area network infrastructure

Independence of the local area network involves ensuring that no network connection device, such as an ethernet switch, is shared by both the PCS devices and devices on the corporate network. While these devices may be logically segmented to affect electronic isolation, the PCS may still be adversely impacted through an event on the corporate network, such as device overload, thereby preventing the PCS devices from communicating effectively. Sharing of such devices also hampers isolation from the corporate network as physical intervention (unplugging cables) would be required.

- **Intrusion Detection**

All too often security measures are put in place and rigorously audited to ensure that they are doing what they're supposed to, but often this is the only practice. The intrusion prevention afforded by the security controls can be complemented with an effective intrusion detection system.

Intrusion prevention systems are just devices that make it harder to perpetrate an attack, but may not actually be effective. Intrusion detection provides that additional level of monitoring to check if the security controls have been breached. This is not unlike bank vaults which are rated based on the time expected to take in penetrating their protection. A bank will implement intrusion detection systems in the form of systems such as motion detection and closed circuit television, in order to raise an alarm should security barriers be breached, thereby permitting them to respond appropriately and within a time deemed sufficient to prevent full penetration and damage or loss.

Similar systems are available for computer systems, although they are not without problems. These systems may raise false-positives and alarms, or false-negatives where undesirable activity may go undetected.

Intrusion detection may be as simple as defining all communications devices to log appropriate events and review those logs regularly, although this can be time consuming and possibly of little value. Identifying unauthorised traffic on a network, access to a server or identifying a hack signature in amongst pages of system logs may be quite difficult. There are a variety of intrusion

detection packages available on the market, some which only notify you should certain critical files change, others that monitor the live network traffic, others that monitor the system log events of servers and others that provide various combinations of these. Depending on the extent of a particular implementation, these systems can become quite expensive to buy and maintain.

It may also not be essential or necessary, or practical to implement intrusion detection on all parts of the PCS, so careful consideration of the optimum location for and types of intrusion detection should be undertaken during the design phase.

### **System Redesign**

In some cases the most effective method of mitigating risks may be to redesign the PCS architecture to better protect the critical components or sections. This is usually not a wholesale redesign, merely a refinement of the existing design. Such a design should be defined to maximise the security effectiveness and to minimise any disruption to the function or on-going operation.

System redesign may be required when planning to implement compartmentalisation, especially if the PCS currently combines all components in a single network infrastructure.

### **Implement Policies and Procedures**

This control measure is usually essential as relying on technology alone is inherently flawed. Technology is prone to poor or inadequate design, failure or misconfiguration or becoming superseded. As such, it can only be relied upon to *facilitate* proper use, not protect absolutely.

Policies and procedures can be developed and disseminated to PCS users, so that they are aware of the expectations and limitations of normal operation and the consequences of a breach, and the correct procedures for operating, maintaining and managing the PCS.

Policies should be developed consistently with any existing business security policies and should state clearly and succinctly what the business drivers and objectives are and the various standards and general practices that are to be adopted. A policy may also define high-level ownership and roles and responsibilities.

The procedures are simply the steps that are to be carried out to execute a particular function or operation on any part of the PCS. One of the most important procedures is a Change Control Process that should define all the steps required to initiate, develop, test, approve and execute (including reversal or recovery) and modification to the PCS.

## **4.5 RISK MITIGATION**

This is the last phase of the risk analysis and is simply the development and approval of the formal design incorporating the identified control measures and ultimately, its implementation.

The design needs to be approved to ensure that the designers and stakeholders all agree that what is proposed achieves the recommendations of the risk assessment and that the particular implementation is effective in mitigating the identified residual risks to the required acceptable level. Stakeholders must also ensure that the design doesn't compromise any operational



requirements. It may be useful to review the risk assessment phase at the completion of the design phase and evaluate the projected residual risks, not only for those nodes being mitigated, but also to ensure that a design change has not increased risk elsewhere in the PCS.

Implementation is relatively straight forward, but may require resources from both the control systems and IT disciplines.

Once implemented, a post implementation review, or audit, should be conducted to ensure that the new PCS implementation and its associated policies and procedures have been implemented according to the design and that the new design is, in fact, effectively mitigating the risks to the PCS as intended.

## **CHAPTER 5 ON-GOING PCS MANAGEMENT**

There are two aspects of the on-going management of security of the PCS:

1. Ownership and Responsibility,
2. Audit and Review.

### **5.1 OWNERSHIP AND RESPONSIBILITY**

The ownership or accountability for the PCS should rest with the group within the organisation that is fully accountable for the business outcomes and possesses complete knowledge of the functionality, dependencies and sensitivities of the PCS. In most cases this is clearly the Control Systems discipline group. However, with the adoption of non-proprietary operating systems and network technologies, the Control Systems group are becoming reliant on the corporate IT support groups.

This reliance introduces an exposure, as discussed earlier in this document, due to potential inexperience and lack of awareness of the critical operational nature of a PCS, by corporate-IT. IT groups generally aspire to standardise servers, workstations and network devices to reduce complexity and support costs. These general corporate standards may not be strictly (perhaps even at all) practical in the PCS environment. It is also, often the case that there are different operational requirements, methodologies and policies between the Control Systems and corporate-IT groups.

To facilitate clear delineation between the PCS and corporate business network devices, it may be that additional procedures and authentication methods need to be implemented to ensure administration and maintenance of the PCS independent to the corporate network. This would prevent undesirable events such as unscheduled outages of the PCS due to emergency upgrades or undesirable activity (e.g. virus attack) on the corporate network, which may well be able to absorb such an outage as the risk would be assessed differently. It would also protect against other events such as misconfiguration of the PCS devices by a well-intentioned system administrator during routine maintenance of the corporate systems.



Due to their historic independence from corporate IT (vendors typically provided total system support) Control Systems Engineers can be wary and possibly lack confidence in their own knowledge and abilities in the IT discipline. Care should be taken to develop a harmonious relationship with corporate IT so that both parties are fully aware of the overall accountability, the sensitivity and criticality of the PCS and, most importantly, the specific roles and responsibilities, authorities and individual technical and administrative limitations.

## **5.2 MANAGEMENT**

There are five major activities that should be carried out in the on-going management of PCS security.

1. System Audit - Compliance
2. Threat and Risk Review
3. On-Going Risk Mitigation.
4. Incident Response
5. Business Continuity and Disaster Recovery

### **5.2.1 SYSTEM AUDIT**

Regular security audits should be conducted on the PCS to ensure that all controls are properly implemented, fully functional as designed, and continuing to mitigate the associated risks effectively. Audits should cover all controls including policy and procedure awareness and adherence, as well as the proper implementation of any technical controls.

Any deficiencies found in the implementation of the controls should initiate remedial action. Any deficiency found in the effectiveness to mitigate risk should initiate a threat and risk review.

Such compliance review is essential to good security. Implementing security controls only to proceed in good faith that these controls are and will continue to be effective in preventing security breaches is ineffective security management. On-going compliance review is the only way to ensure that your systems and the operators are adhering to the prescribed standards and that those standards remain effective in preventing security breaches through known and future exploits.

While periodic audits are strongly advised, more frequent reviews and checks should also be conducted in the interim, perhaps through prescribed regular maintenance tasks.

### **5.2.2 THREAT AND RISK REVIEW**

The threat and risk analysis performed in the original risk analysis process should be reviewed for appropriateness on a periodic basis. It should also be reviewed in the event of any of the following:

- Audit deficiency in effectiveness of particular controls;
- Major system design changes, including implementation of any additional or replacement (alternate) equipment, system upgrades, and technology changes;

- Changes in perceived corporate threat;
- Actual incidents including internal and other organisation's control systems.

The threats and risk review should follow the same process as defined for the initial risk assessment and while that does call for complete and detailed examination of the threats, unmitigated and residual risks, it can be expected that most will remain the same. That said, it is essential to perform a complete, holistic review to ensure that the total security of the PCS is maintained within business requirements.

### **5.2.3 ON-GOING RISK MITIGATION**

The initial risk evaluation and mitigation process will only ever be a snapshot in time of the risks that face your business at a particular moment in your organisation's life. It is likely that as time proceeds, new risks will become evident as new vulnerabilities are discovered and incidents occur in the industry to challenge the perceived risk levels established previously. It is for this reason, and through the process of regular threat and risk analysis, taking into account changes in the security capabilities of the PCS as a result of market disclosures, actual incidents and escalating threats (increasing the likelihood of an undesirable event), that on-going risk mitigation is essential.

Terrorist activities of recent years have permanently altered the perceptions of security control necessity and effectiveness for two major reasons: The first is the perceived actual threat to the business and the second is the political theatre in which that business operates. For example, many US organisations responsible for what is defined as US National Critical Infrastructure (these definitions may vary from country to country) are now required to demonstrably comply with minimum security standards. The Enron collapse of 2003, has introduced legislation in the US that requires certain security measures to be taken over the protection and integrity of information. These regulations are now spilling over into countries such as Australia, especially with companies with a US-based parent company and areas that are affected by international regulation such as harbour security.

### **5.2.4 INCIDENT RESPONSE**

It is vital that any security plan incorporate an incident response. Security control can be achieved through a combination of protection and recovery, both of which contribute to the prevention of the perceived potential outcome of an undesirable event.

Security may be dealt with in general through take, treat, transfer or terminate. Taking a risk is accepting the outcome based on unavailability or the impracticality of effective mitigation. Treating the risk is what we are endeavouring to do to secure the PCS in the most part and that is to apply appropriate controls considered to acceptably mitigate the risk. Transferring the risk is the process of passing on the liability of the risk (the estimated potential loss or damage) to a 3<sup>rd</sup> party, be it through insurance or a contractor. However, in the case of the PCS, which usually forms the basis for the organisation's production and therefore profitability, transference is not always possible other than through protection of lost income. Termination is the process of pulling out of (or not initiating) a particular business activity due to an unavoidable and



unacceptable risk. This may apply to certain aspects of the PCS through not permitting certain technologies or practices.

The process of treating or implementing control measures to prevent an incident may not always be sufficient to adequately mitigate the risk. Also, some risks may need to be taken and therefore neither the likelihood or potential loss or damage is reduced. In these cases and to a lesser extent with any risk, incident response and system recovery is the only method available to adequately mitigate the risk. Appropriate response can serve to prevent or reduce a potentially undesirable outcome (an example of this would be first-aid at the site of motor vehicle collision that may reduce the likelihood of permanent disability or death of a victim).

An incident response process should be created in such a way that it can be applied to any foreseeable incident. It should provide for the establishment of an incident response team, ensuring that necessary resources are always available and that the logistical issues are properly managed. The process should also incorporate communication plans to report to both senior management and those affected by the incident of the progress likely recovery. Communications to the media may also need to be incorporated if the incident has public exposure.

The incident response plan should also provide latitude to vary the process within certain bounds during an incident, should impasses be reached or predetermined procedures prove inappropriate.

Incident response should not just be considered to be a process to stop a breach and recover from any damage that may have occurred. The possibility that some information may need to be captured in a reliable and secure fashion should it be called upon as evidence in a court case against a perpetrator should be incorporated. This would require a forensic process for gathering, securing and analysing the information or evidence such that it can reliably presented in a criminal or civil court or corporate disciplinary hearing. Computer forensics is a specialised field and no attempt to address it in detail will be presented in this paper.

A post-incident review should be conducted immediately following an incident to determine if there were any failings in the process and where improvement may be made.

### **5.2.5 BUSINESS CONTINUITY AND DISASTER RECOVERY**

Disaster recovery is defined as recovery of a system following total or partial loss due to a disaster event and usually considers such events as acts of God or major events outside the realms of the PCS such as fire, flood, earthquake or explosion. In such a disaster there is often far more at stake and higher priorities than recovering the PCS, but it is possible that a minor disastrous event, perhaps due to a major security breach, may occur that only affects the PCS, such as a fire in the main control room. Even in a more wide-reaching disaster, it is likely that the PCS will need to be recovered at some stage.

The essential aim of developing a disaster recovery plan is to agree on how long the business can go without the affected functions of the PCS, what process can be established to provide business continuity of essential services and then to define a plan that will be able to re-establish the affected PCS within the required time.



All disaster plans should be regularly rehearsed (much as companies rehearse fire-drills) to ensure that everyone involved knows exactly what to do, that all necessary resources are readily available and that the recovered system is able to function as expected.

## **CHAPTER 6      SUMMARY**

Information and IT security and PCS security is largely a given in today's business world. The risks faced by the business through the PCS can no longer be dealt with in isolation and the matter of PCS security must now be accepted as a real and significant business risk. Total or partial failure of a PCS can conceivably result in significant loss and in some extreme cases, perhaps even catastrophic impact.

The evolution of the PCS technologies, extended functionality and scattering of roles and responsibilities away from the core control systems discipline, has introduced many new risks, never before having been of issue to the control system environment. Therefore PCS security is now a real and significant challenge for business, no longer restricted to the technical confines.

System risk analysis is a task that should be undertaken by all large and small PCS and SCADA operators to ensure that their perceived risks are appropriately mitigated and that the organisation can then demonstrate due diligence in the event of an undesirable incident.



## **CHAPTER 7      AUTHOR BIOGRAPHY**

### **Max Rockliff (B.E. (Electronics))**

Max is the Principal PCS Security Engineer for Plexal Group. Prior to this he was the Information Security Coordinator for Woodside Energy Ltd. where he became involved in the risk assessment and implementation effective security control for process control systems. He has over 20 years experience in the IT industry covering a wide variety of technologies and holding various positions including senior systems analyst, team leader, section manager and project manager.

Max has a bachelor's degree in Engineer (Electronics) from the University of Western Australia and is currently completing a Masters of Internet Security at Curtin University in the School of Business.