PLATFORM FOR CYBERSECURITY
CPNI.NL

# Security of legacy process control systems

*moving towards secure process control systems*

Cybersecurity a public-private integrated approach

# Content




**CPNI.NL**
Version 1.0 (February 15, 2012)



**Authors:**
Maarten Oosterink, CPNI.NL
Review and input:
Aad Dekker, Alliander
Paul Hendriks, Essent
Lhoussain Lhassani, Stedin
Mirsad Murtic, Yokogawa
Joost Roldaan, Heineken
Renny ter Veer, Waterleidingmaatschappij Drenthe
Martin Visser, Waternet
Wil Weterings, Schiphol Groep
Bart de Wijs, ABB

Auke Huistra, CPNI.NL
Eric Luiijf, TNO/CPNI.NL

# Executive summary



This white paper describes solutions which organisations may use to improve the security of their legacy process control systems. When we refer to a legacy system, we generally refer to old methodologies, technologies, computer systems or applications which are still in use, despite the fact that new technologies or more efficient methods are available.

Legacy systems are characterised by the fact that for some reasons they cannot be adequately secured in the regular way against new threats regarding availability, integrity and confidentiality. Examples are: missing or incomplete support from the supplier and  a lack of security updates. Another reason may be the loss of (the required amount of) knowledge and expertise within the organisation, for instance, because of staff turnover.

It is essential to be familiar with the organisation's particular environment. With regards to this, it is important to know which process control systems are used in the organisation, how critical these are to the continuity of the business processes and which vulnerabilities these systems contain.

This white paper discusses several possible (mitigating or corrective) measures to protect legacy process control systems against undesirable effects on availability, integrity and confidentiality of information in these systems or the processes which are controlled by them. There is no generic answer. Each situation and every organisation has its own vulnerabilities and ways to take care of them, to prevent the occurrence of incidents or to minimise the risk of consequential loss.

A unique mix of measures applies to each situation. These measures should be the result of a risk assessment, in which a well-considered choice has to be made based on the risk of a specific threat occurring, the impact this will have and the costs or investments required to decrease or remove this risk.

The threats process control systems are exposed to and the risk of a threat being exploited is subject to change. It is recommended to use existing Information and Communication Technology (ICT) procedures or audit mechanisms during regular evaluation of implemented measures.

# Definitions



In this document we will use the following definition for legacy process control systems (also referred to as legacy systems from here on) with regards to their security:

Legacy systems are systems which cannot be secured completely by regular measures and technologies and therefore pose a larger risk to the continuity, integrity and confidentiality of the controlled process(es).

Examples of reasons to characterise systems as legacy systems are:

- Missing (partial) support by supplier/vendor or lack of spare parts.
- Declining knowledge and expertise about systems on the market or in the own organisation.
- Insufficient security against physical or logical threats from the environment.

With security, we refer to the protection against undesirable effects on availability, integrity and confidentiality of the systems and the processes they control.

# Objectives

The objective of this white paper is to provide a number of mitigating and corrective measures to increase the security of legacy process control systems and to discuss these measures briefly. A secondary objective is to give management and other decision makers of organisations dealing with legacy systems guidance in their decision making process where it handles the protection of these legacy systems.

# Core



Practically every organisation using process control systems will encounter critical legacy systems and missing knowledge or documentation about those systems. There may also be systems which people do not dare to change because they fear possible consequences.

This is one of the reasons why regular methods and techniques to protect (information) systems are not (fully) applicable to legacy systems.

The result is that a specific set of measures needs to be selected for these systems. These do not always have to be special or expensive. For most systems, a collection of measures can be determined using a company-wide approach, selected from a set of potential building blocks.

Examples are:

- Regular installation of security updates (patches)
- Creating and announcing policy for using removable media
- Regular backups
- Having tenable support contracts
- Availability of good logical access control (strong passwords)

One crucial point: although systems are often referred to as 'legacy' because of their age, this does not always have to result in an increased security risk. Not every system needs regular updates and a well-tested backup will provide a safety net for old systems as well. With regard to a process control system without network connections or USB ports, less drastic measures can be implemented.

It is not solely the suppliers' responsibility when support for and knowledge about operational systems fades out. Often enough, reorganisations or natural staff turnover results in knowledge disappearing from within the organisation itself too. A lack of documentation may play a part in this. This applies mostly to systems which seldom require attention, which is often the case for process control systems. The damage is already done long before one knows it.

The set of building blocks which constitutes security for legacy systems is essentially not different from those used in traditional ICT systems. Just like in ICT environments, it is common practice to select and implement measures based on well-considered risk factors. These should be the result of a risk assessment, in which the chance of a specific threat occurring is balanced against the possible impact and the costs or investments required to decrease or remove this risk.

More information on risk analysis and process control security is available through the CPNI good practice guide entitled, 'Understanding the business risk'.
*(source: Centre for Protection of National Infrastructure UK)*

Let us not forget that a risk assessment is a snapshot in time. New threats arise on a daily basis. This may affect the way systems need to be secured to maintain an acceptable level of risk. It is essential that these threats are analysed as often as practically possible and that changes are made when necessary. It is recommended to use (existing) ICT procedures or audit mechanisms for this purpose.

It is the mix of measures that needs to make the difference. Measures need to be selected according to the 'defence-in-depth' principle, meaning one specific vulnerability will be covered by more than one measure. More information about this can be found in the good practice guide from the US Department of Homeland Security, 'Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies' *(source: Department of Homeland Security US).*

The most common protective and corrective measures for legacy process control systems will be discussed briefly in this white paper. However, providing a full overview is impossible.

# Measures



### Replacement or upgrade

From the point of view of an information security officer, replacing a legacy system is often a logical option. However, security has competition from aspects such as the cost and time accompanying migration. A risk assessment should be the deciding factor. When the risk is transparent and measures have been defined, an unacceptable residual risk may still remain. This may drive an accelerated replacement or upgrade of the legacy system.

### Hardening

Hardening refers to stripping a system to its essentials. For computer systems and network components, this means removing parts or applications which are not required. This reduces the number of potential vulnerabilities to a minimum and may involve disabling an unused network connection or deactivating a built-in web server. In Windows systems, this could be removing unnecessary applications like Windows Media Player. In UNIX systems, one could consider removing or disabling unnecessary services like X11 or the Telnet daemon. Information about safe configuration of ICT systems is available from the National Security Agency (NSA) website *(source: National Security Agency US)*. Also check with suppliers whether they already provide specific services or solutions that provide hardening.

### Physical marking and access restriction

In a lot of systems, logical security measures, such as setting passwords or restricting user rights, may be circumvented when physical access to the system is obtained. This will mostly involve malicious intent. Physical access may only be prevented by isolating vulnerable systems. Place them behind lock and key, but do remember that some keys have (too) many copies going around.

The human factor may unintentionally cause problems as well. People involved often do not realise the consequences of their actions on specific (vulnerable) systems. Marking systems as vulnerable or critical may be – simple as it is – an effective measure. Such a warning could be a physical marking, but it can also be applied using login banners. Clear instructions on the risk involved in using a system costs little, but could prevent incidents.

### Limiting user rights and logical access

In many (old) systems, no distinction is made between user types, like administrators or users who only need to look up specific values. Previous decisions not to make any distinction (for good or bad reasons) may now have aggravating consequences, especially when systems are network connected or when using portable media. Modern malware, like viruses and Trojans, is able to spread across systems and networks incredibly fast, usually by leveraging unnecessary elevated user account rights. Allocating new user account rights according to the 'least privilege' principle may prevent rapid replication. This involves checking which provisions this system offers. It could even be that unused system capabilities in differentiating user account rights are available.

Use of a generic or too simple password may result in people unintentionally using a vulnerable system. Far-reaching integration in existing authentication environments like an Active Directory may result in people having unnecessary access to a system, thus forming a (conscious or unwitting) threat to these systems.

### Passwords

Access to systems, or certain functionality within systems, is often protected by passwords. It is advisable to use personal user accounts with passwords that are difficult to guess whenever possible. Additionally, it makes sense to have a policy for changing passwords regularly. This will, for instance, prevent that accounts which were allocated to multiple users may still be accessed by people who no longer need them. There is no unambiguous answer regarding the required password complexity or the frequency of changing passwords. This depends on a lot of factors, like other security measures present including physical security or social control, and the potential damage in case of abuse.

### Network segregation and firewalls

It is not just users who may directly have a negative impact on legacy systems. Older systems in particular can sometimes demonstrate an unpredictable response to network traffic. Even what would be considered regular traffic in office environments could have an undesirable effect on process control systems. Moving these systems to a separate section of the network may solve this, preferably combined with the use of firewalls. Particularly for vulnerable systems, the market offers also specialised firewalls which enable their secure use in the existing network environment.

### Spare parts in stock

For systems which have been labelled 'end-of-life' by the supplier, or for those which the supplier cannot get spare parts on-site (in time) for different reasons, it might be wise to keep spare parts and the necessary documentation in stock yourself. Because parts have a limited life cycle, the risk of failure increases with older systems. The extent to which suppliers are able to replace these parts seems inversely proportional to the age of the systems. This may be because of a shortage of parts, but also because their employees may not be familiar enough with the old systems. Arrangements can be made with suppliers about keeping spare parts on consignment. It is also possible to purchase these yourselves and keep them in stock. Also consider documenting required configuration data and procedures.

### Virtualisation

Virtualisation has become very popular in ICT. At first sight, innovative developments and legacy systems seem like an odd couple. Still, virtualisation offers a lot of opportunities here. So-called 'physical to virtual' (P2V) solutions enable us to 'copy' physical (IT) systems to virtual systems and thus to modern virtual environments. This prevents dependency on old hardware that is hard to replace. It also provides opportunities for backup (snapshots) and restore, increasing the availability. Some suppliers offer solutions for

current systems, but virtualisation may also be a viable solution for older, no longer supported systems as a way to increase their availability.

### Backup and restore

Creating backups of legacy systems on a regular basis is important, just like it should be for all systems. Depending on the system concerned, this could be a full copy of the operating system and applications, or a dump of the application code from a programmable logic controller (PLC). For a legacy system it is advisable to create a backup with every change. Even more important than the backup itself is testing whether a backup can actually be restored when necessary. One could, for instance, make arrangements about this with the 3rd party service supplier. An additional advantage is that administrators or operators already know what to do whenever it is really necessary, saving valuable time in restoring operations. Such a test is also a good opportunity to document configurations and procedures and assess them on their correctness.

### Reinstallation

Some systems have been configured (or badly documented) in such a way that integrity is at stake when regular security measures like antivirus software or hardening are applied. In these cases, reinstalling such a system could offer a solution. Such an action could be combined with an attempt to start using more recent or current hardware. One could, for instance, look at the possibility of installing an application which the supplier only supports under Windows 2000 onto a more recent Windows version. Also consider a combination of possibilities, e.g., by applying virtualisation. This allows a legacy application to be installed to a clean Windows 95 operating system that acts as a virtual machine in a Windows 2003 server environment, running on up-to-date hardware. Mind you, most of the time reinstallation is a costly exercise and there is always a chance of failure. Still, it can be a viable option in particular situations.

### Documentation and organisation

When lack of documentation is observed, people all too often do not take time to create documentation in hindsight. This means the partial knowledge employees have gained while servicing the system still is not secured. The absence of clear policies or guidelines for managing the system or system documentation is one of the reasons for this. An example of a guideline for ensuring system documentation is being created and updated is defining a maintenance process. Such a process may prescribe to update documentation.

The quality of system management often depends on personal skills and views of individuals. This is not judicious with critical systems. This dependency may be removed by deploying clear instructions, designating responsibilities and monitoring the abidance to guidelines.

### Awareness and training

Information security completely depends on the awareness of the people involved. This also applies to legacy systems. People who are aware of the additional risk factors involved in particular

systems will handle them more carefully. This may inadvertently prevent harmful actions. Proper training of employees is the most important way to create awareness. Consider, for example, the use of mandatory e-learning before granting access to process control systems or specific legacy systems.

# In conclusion



In theory, there is not a whole lot of difference between the security of legacy process control systems and current (ICT) systems. The security of information systems, including process control systems, starts with a risk assessment. In this risk assessment, the risk factors are examined. These are weighed by using the formula: risk = probability times consequence. Based on this, we can consider accepting the risk or taking additional measures.

Looking at legacy systems, decisions from the past may haunt us today. Sometimes it is sensible to go to the root of the problem, for instance, by reinstalling the system from scratch. This may prevent problems with unnecessarily elevated user rights and often solves instability issues caused by uncontrolled installation of extra software.

Usually other less costly measures suffice. These may be technical, like a redesign of the network where the legacy systems are connected to or implementing firewalls. But it may also be procedural, e.g., by implementing a mandatory training for the use of legacy systems.

As usual, protecting legacy systems starts with reducing the risk of undesirable effects on the availability or integrity of these systems or the processes controlled by these systems. There are a number of effective measures available to reduce this risk.

Hardening minimises the number of vulnerabilities of the system. Training, or a warning in the form of an explicit label, makes users aware of the specific risk of using these legacy systems.

Completely removing risks to the availability or integrity of systems is often impossible. A tested backup and trained administrators will reduce the damage created by disruptions. Good and tested procedures, documentation and recording configuration data are essential. Also consider a safe and, in case of an emergency, accessible location to store backups. As a complementary corrective measure it may be wise to keep your own stock of spare parts or complete (if possible for installed and configured) redundant systems.

**Additional information**

Available sources and online documents offering additional information about this topic:

Good Practice Guidelines, from CPNI UK:

http://www.cpni.gov.uk/advice/infosec/business-systems/scada/

Standards & References, conveyed by Control Systems Security Program from the American Department of Homeland Security:

http://www.us-cert.gov/control_systems/csstandards.html

Guide to Industrial Control Systems (ICS) Security, from NIST, USA:

http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

SP99, Industrial Automation and Control Systems Security, from International Society of Automation, USA:

http://www.isa.org/mstemplate.cfm?section=home&template=/TaggedPage/getStandards.cfm&MicrositeID=988&CommitteeID=6821

# Relevant literature



References

UK Centre for Protection of National Infrastructure
PROCESS CONTROL AND SCADA SECURITY: GUIDE 1. UNDERSTAND THE BUSINESS RISK. Retrieved 19 July 2011, from CPNI.gov.uk:

http://www.cpni.gov.uk/documents/publications/2008/2008024-gpg_scada_business_risk.pdf

Department of Homeland Security VS. Recomended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Retrieved July 19, 2011, from Control Systems Security Program:

http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

National Security Agency. Security Configuration Guides. Retrieved July 12, 2011, from National Security Agency:

http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml

**CPNI.NL | TNO**
Mail address
P.O. Box 96864
2509 JG  The Hague

Visiting address
Oude Waalsdorperweg 63
2597 AK  The Hague

P (+31) 88 866 38 61
E info@cpni.nl
I www.cpni.nl