NOVEMBER 2016

Fact sheet: Process Control System and Network Security

Definition Process Control System and Network [1]

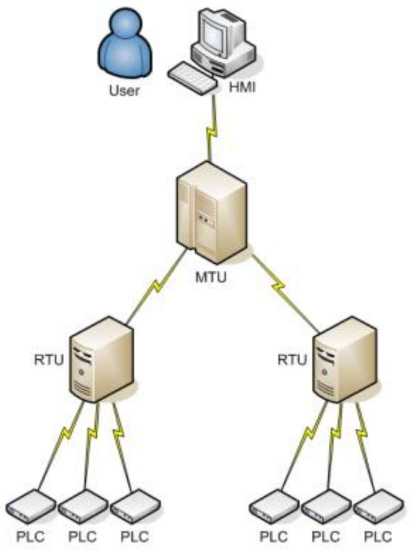
Process Control Networks (PCNs) are networks that mostly consist of real-time industrial process control systems (PCSs) used to centrally monitor and (over the local network) control remote or local industrial equipment such as motors, valves, pumps, relays, etc. Process Control Systems are also referred to as Supervisory Control and Data Acquisition (SCADA) systems or Distributed Control Systems (DCS).

General setup of a PCN [3]

A PCN usually consists of the following subsystems:

- A human-machine interface or HMI is the apparatus or device which presents process data to a human operator, and through this, the human operator monitors and controls the process;
- A supervisory (computer) system (Master Terminal Unit or MTU), gathering (acquiring) data on the process and sending commands (control) to the process;
- Remote terminal units (RTUs) connecting to sensors in the process, converting sensor signals to digital data and sending digital data to the supervisory system;
- Programmable Logic Controllers (PLCs) used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs;
- Communication infrastructure connecting the supervisory system (MTU) to the remote terminal units; and
- Various process and analytical instrumentation.

The user has access to the Human Machine Interface. That interface is connected to the Master Terminal Unit. The MTU is the heart of the PCN and controls the Remote Terminal Units. Those Remote Terminal Units can monitor and control the Programmable Logic Controllers. These PLCs will be connected to various sensors and actuators.



In general a large industrial production plant will harbor a number of production facilities including the PCNs to monitor and control these facilities. Dependent on geographical spread they interconnect by means of LAN/WAN to central monitoring and control facilities and enterprise networks.

Developments in PCN

Just like ordinary office IT infrastructure, PCNs follow(ed) the common development steps:

1. monolithic 'one purpose' computing using proprietary technologies;
2. distributed 'LAN-based' computing;
3. fully networked approach interconnecting (mixing) proprietary systems with standard protocols including internet connection.

The move from proprietary technologies to more standardized and open solutions together with the increased number of connections between PCNs and office networks and the Internet has made them more vulnerable to cyber-attacks. As many PCNs use legacy operating systems and/or are not actively patched, the vulnerability for cyber-attacks is increased. Examples of malware focusing on PCNs are Stuxnet [7] and Duqu [8].

Misconceptions regarding PCNs

- PCNs have the benefit of security through obscurity and the use of specialized protocols and proprietary interfaces;
- PCNs require specialized knowledge, making them difficult for network intruders to access and control;
- PCNs resides on a physically separate, standalone network;
- Connections between PCN and other corporate networks are protected by strong access controls; and
- PCNs are secure because they are disconnected from the Internet.

Typical properties of PCNs [2]

- Hacking of or security breaches in PCNs will affect many aspects of the physical world around us, impact is not limited to financial statements or financial losses;
- The level of (information) security of the PCN is often significantly lower than of the office automation;
- Traditionally, the process engineer is trained in process control and continuity, not in (information) security;
- The IT used in PCN's is increasingly based on open standards;
- PCNs tend to have no anti-malware software, intrusion detection systems (IDS) and firewalls when not directly connected to the internet;
- On the threat side (in circles of hackers) a growing interest in and knowledge about PCS / SCADA are developing; and
- IT audits supporting the financial statement audits do regularly not scope PCNs in.

Top 10 PCN risks [1]

- Insufficient knowledge with the IT auditor of specific characteristics of the PCN, because each PCN is custom build;
- Not taking into account risks, consequences and impact of a malfunctioning PCN for the physical world around us;
- Inadequate policies, procedures and culture governing control system security.
- Poorly designed PCNs that fail to incorporate IT security as integral component of its design, i.e. compartmentalize communication connectivity, fail to employ sufficient 'defense-in-depth' mechanisms, fail to restrict 'trusted access' to the control system network, that rely on 'security through obscurity' as a security mechanism;
- Badly configured operating systems and embedded devices that allow unused features and functions to be exploited (e.g. commonly known attack vectors like 'buffer overflow'); untimely (or impossible) implementation of software and firmware patches; inadequate or impossible testing of patches prior to implementation;
- Use of inappropriate or inadequately secured wireless communication;
- Use of non-dedicated communication channels for command and control and non-deterministic communication such as Internet-based PCNs. A lack of adequate authentication of control system communication-protocol traffic;
- Lack of mechanisms to detect and restrict administrative or (vendor) maintenance access to control system components; inadequate identification and control of modems installed to facilitate remote access; poor password standards and maintenance practices; limited use of VPN configurations in control system networks;
- Lack of quick and easy tools to detect and report on anomalous or inappropriate activity among the volumes of appropriate control system traffic;
- Dual use of critical control system low-bandwidth network paths for non-critical traffic or unauthorized traffic;
- Lack of appropriate change management or change control on control system software and patches.

Summarizing: The main risks are; lack of security awareness, procedures and implementation of these procedures to make security an integral aspect of the design and operating of PCNs. Given the fact that PCNs support critical infrastructure like waste water plants, chemical processing plants, (nuclear) energy production plants, the consequences of cyber terrorism may be very serious.

The good news is: Most of the vulnerabilities, risks and countermeasures can be addressed by using IT security approaches also used in office automation.

Aspects to take into account when auditing Process Control Networks [4]

Organizational aspects

- Approved and committed (information) security policies, sufficiently designed security organization and procedures in place;
- Security agreements and policies with peer sites or with suppliers;
- Sufficient coordination on security requirements between users and suppliers;
- Appropriate SoD, adequate change and patch management; and
- Incident response planning.

Human Factor:

- Instigate sense of security, foster awareness and knowledge of security, security culture ("Can this happen to us?"), avoid the (mis)perception that information is difficult to obtain and to understand (obscurity);
- Focus not only on safety but also security;
- Elaborate on the connection between the continuity and the security aspect;
- Be aware of security vs. functionality trade-off; and
- Prepare for diminishing knowledge of legacy and unused (emergency) systems ('de-skilling').

Hardware and software

- Install update patches regularly per a standard patch process which includes testing;
- Avoid configuration and implementation errors (like unnecessary web-enabling or other 'features'), avoid unsecure or clear text protocols;
- Strong user authentication, enforced principle of least privilege, limited guest and group accounts;
- Good password practices: No standard or shared passwords, no hard-coded or scripted passwords and access keys; and
- No unnecessary connectivity (USB, PDA, Bluetooth, wireless).

Infrastructure

- Secure (e.g. compartmentalize) interconnectivity between industrial control systems and the enterprise network;
- Strengthen use and usefulness of firewalls, intrusion detection systems (IDS), VPN or DMZ-network segments;
- Limit external connections (remote access, extranets and dial-in/out modems); and
- Avoid rogue devices.

Further recommendations for the IT Auditor

- Perform a risk assessment; make use of well-known and accepted frameworks for risk assessment and expand these with specialized frameworks for the security of PCNs and SCADA systems [6];
- Further fill in these frameworks with the desired specific controls taking into account the organizational aspects, the human factor, infrastructure as well as hard and software; and
- Assess the control and security measures in place at various physical locations (head quarters, branches, monitoring and control rooms, production plant facilities).

Key documentation and website links

[1] Process Control Network Security Comparing frameworks to mitigate the specific threats to Process Control Networks - ir. S. Peerlkamp and M. Nieuwenhuis - March 2012. http://www.jbisa.nl/download/?id=16249370

[2] Process Control Security in het informatieknooppunt Cybercrime nicc

https://www.cpni.nl/publications/PCS_brochure-NL.pdf

[3] SCADA http://en.wikipedia.org/wiki/SCADA

[4] ISACA Journal Online - Security of Industrial Control Systems; What to look for / Erwin van der Zwan, 2010 http://www.isaca.org/Journal/Past-Issues/2010/Volume-4/Pages/JOnline-Security-of-Industrial-Control-Systems.aspx

[5] SANS - Security for Critical Infrastructure SCADA Systems

http://www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644

[6] NIST - Industrial Control System Security NIST SP 800-82, NIST Industrial Control System Cyber Security Workshop 24 September 2010

http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Sept2010-Workshop/NIST_ICS_workshop_Sep2010_SP800-82_briefing_Abrams.pdf and related Guide to Industrial Control Systems (ICS) Security

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

[7] Stuxnet http://en.wikipedia.org/wiki/Stuxnet

[8] Duqu http://en.wikipedia.org/wiki/Duqu