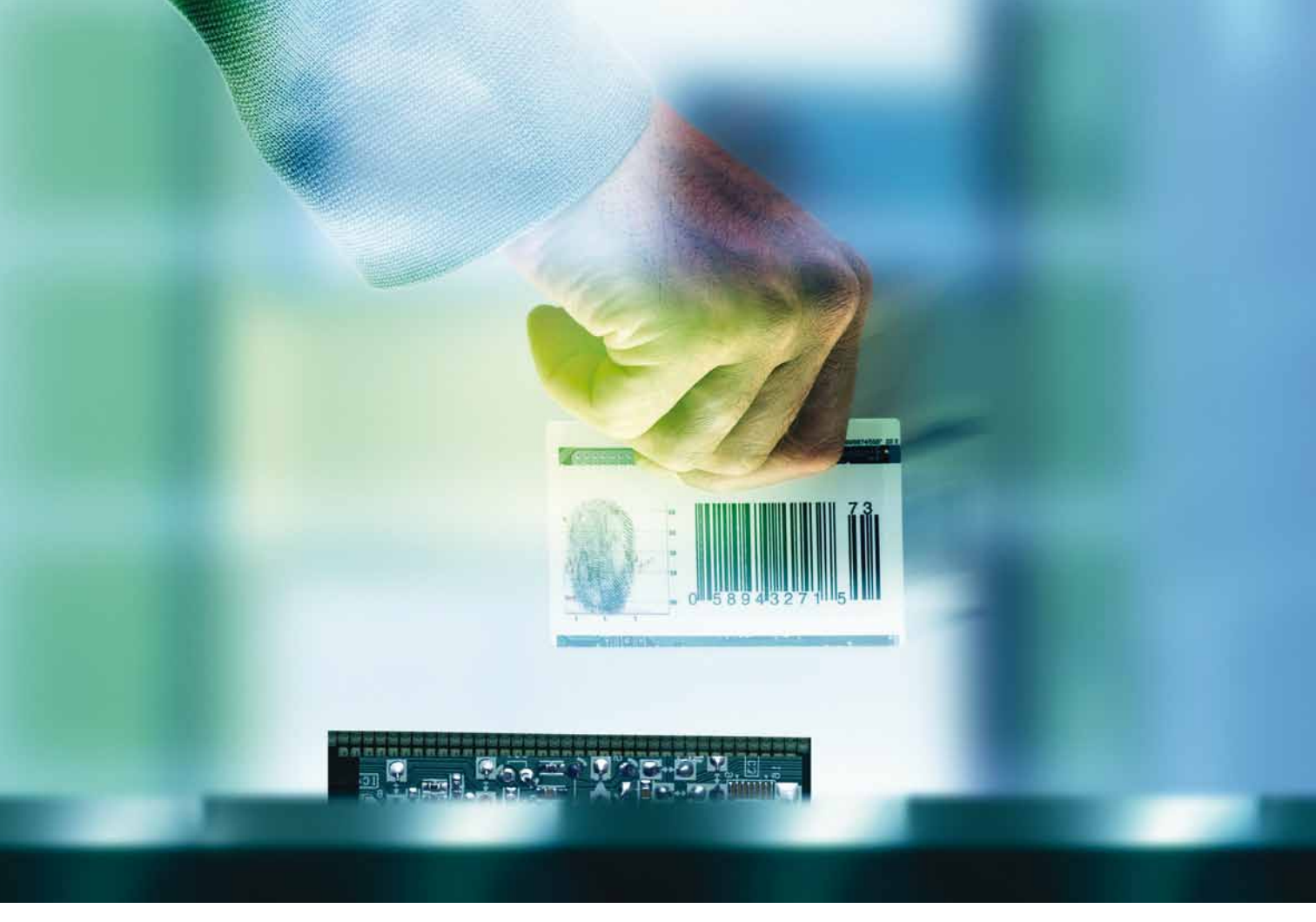
The National Infrastructure against Cybercrime (NICC) is the Dutch approach in fighting cybercrime. The NICC programme is a public-private partnership.

Process Control Security in the Cybercrime Information Exchange

NICC


73
0 5894327 1 5

Process Control Security in the
Cybercrime Information Exchange
NICC

Mark Frequin
Director-General Energy and Telecom at the Ministry of Economic Affairs

The continuity of our vital infrastructures and the security of many other production processes stands or falls with the (information) security of process control systems. Analyses and incidents have shown that this can be improved.
Before the risk to our society becomes too great, we must jointly and collectively tackle this security problem. I have entered into agreements in this respect with the CIO Platform Nederland.
The Cybercrime Information Exchange forms the link between the national and international public-private partnership activities in this area, and has produced this publication. It makes clear why the security level of production processes must be brought up to a high level and maintained there. Maintaining the security of process control systems requires an integrated approach to both information security and organizational and physical security. Awareness of this is vital, and a starting point for a joint approach. I therefore endorse the content of this publication.

Detecting, investigating and prosecuting cybercrime? Extremely important, but not really the solution for the problem. Prevention is better!

Introduction

Detecting, investigating and prosecuting cybercrime? Extremely important, but not really the solution for the problem. Prevention is better! The sectors that have joined the Cybercrime Information Exchange have accepted the challenge of ensuring the effectiveness of the (information) security of process control systems (PCS), including SCADA. This publication makes it clear why it is vital that organizations establish and maintain control over the security of the information and communication technology (ICT) in their process control environments.
It is also made clear why it is important that the desired security level for the process control systems within and outside the vital sectors is established and maintained, and why a common, united approach is important. 'United' in this case means uniting the strengths and knowledge in the public and private sectors of the PCS users and all others involved, such as manufacturers, suppliers, system integrators, service providers, governmental authorities, educational establishments and knowledge institutes.

On the left-hand pages of this publication you will first find a description and explanation of PCS, followed by a selection of examples of the use of PCS in various different sectors. These pieces explain in a nutshell why the reliability of PCS is so important for Dutch society. It involves matters that concern you personally every day. In order to guarantee their reliability, we need to bring PCS information security under control together and maintain it. The necessity for doing this is illustrated by examples at the bottom of these pages describing incidents and threats that have actually occured.

Process control systems: the heart of many sectors

We use the term PCS to include everything that involves process control systems, including systems for Supervisory Control and Data Acquisition (SCADA), process control networks, PLC systems and their physical and organizational environments. This is often also called process automation (PA). PCS are used in many sectors for the automatic monitoring and control of essential physical processes. You can think, for example, about our energy supply, the drinking water supply (production, transport and distribution), water management processes, railway transport (points and signalling, for instance) and tunnel security systems.

PCS form the heart of production processes in refineries, the chemical industry and the food and drug industries. They are applied increasingly often in building and facilities management and access control systems in vital establishments such as telecommunications exchanges and computer centres.

There are differences between office automation and process automation when it comes to the requirements that the systems are expected to meet. While the first priority in office automation is often given to confidentiality, and only after that to availability and integrity, in process automation the first place is usually given to availability and integrity, with confidentiality as a lesser priority. This also results in differences in the security focus.

APRIL 2009

Jesse William McGraw (using the hacker identities GhostExodus and PhantomExodizzmo) penetrates a number of systems at the W.B. Carrell Memorial Clinic, a hospital in Dallas, Texas. He manages to gain access to the patient registration system and the process control systems that regulate heating, ventilation and other types of air treatment.

United against cybercrime

Private and public sector organizations are fighting together side-by-side in the National Infrastructure against Cybercrime in order to bring the level of cybersecurity within the vital sectors in the Netherlands up to the level desired. In this way, the National Infrastructure against Cybercrime (NICC) programme plays a facilitating, unifying and reinforcing role. By sharing knowledge and exchanging information, government and the business world gain access to sufficient information to be able to take good decisions themselves.

The Cybercrime Information Exchange is the beating heart of the NICC. The vital sectors form an important part of it. They have identified the information security of PCS as a cross-sector theme.
The information security of PCS is falling behind that found in normal office automation systems. The unwanted and undesirable manipulation of PCS is a growing threat. Together this has resulted in a risk that can and must no longer be ignored. PCS control physical processes. Their unwanted manipulation can lead to serious disruption of the vital infrastructure, which in turn has grave consequences for our economy, the environment and the lives of people and animals. For these reasons, the business community (as users and suppliers), government (as user, supervisor and catalyst), education and research must energetically tackle this risk together.

Safety and security underground

The GVB in Amsterdam and the RET in Rotterdam each carry hundreds of thousands of passengers by metro to their destinations each day. That requires reliable PCS for the energy management, power to drive the trains, and ensuring the safety and security of the railway tracks by using signals and points. PCS are also used to monitor the safety and security of passengers in the underground stations. Just think about the fire safety measures and emergency closure systems in the event of flooding.
Both public transport companies are looking at possibilities for introducing full automation to their metro systems, which would mean that train drivers would no longer be needed. It is planned to introduce this in Amsterdam on the East Line in 2014. In 2019, all metro trains must be able to run without drivers. For this reason it is essential to first ensure that the (information) security of the PCS that is to control and monitor all of this is and will continue working well.

JANUARY 2008

A young hacker learns how to manipulate the points in tram tracks in the Polish city of Lódz with a modified remote control device. Four trams are derailed and twelve passengers are wounded.

What is the risk?

Many ingredients combine together to increase the vulnerability of PCS. Here we list them together in four categories.

Risk factors of PCS technology

The (information) security of PCS often lags far behind that of office automation systems. The reasons for this can be to do with policy decisions, but can equally well have organizational, technological or economic origins. There are significant cultural differences in many organizations between the process automation and office automation departments.

Process automation has traditionally had a strong focus on high levels of availability, reliability, efficiency and safety. PCS technology has been slowly but steadily changing however. Special PCS hardware with supplier-specific applications and hardware was used in the past that was difficult to influence or manipulate from outside. This is now being increasingly often replaced by COTS (commercial-off-the-shelf) computer systems with open operating systems such as Windows or Linux, an Internet protocol suite and application programs (sometimes even open source SCADA software).

The periods typically used for writing off (non-Windows) PCS are long compared to office automation systems. PCS therefore have a long economic life when compared to the fast technological developments of ICT, and so are used for a long time. It is often difficult or inconvenient to add extra security measures to them.

Personnel and behavioural risk factors

Traditionally, process automation engineers have not been trained in (information) security. They are therefore unaware or scarcely aware that a task has been added to their job profile.

When process automation managers are already aware of security issues, they seldom find a listening ear amongst senior management because changes can cost a lot of money.

ICT departments used to see process automation as a collection of sensors, pumps, engines and valves, and not as information technology that must be secured.

Whenever process automation engineers and ICT people try to work together, a huge cultural difference becomes visible between the process management and control approach ('twenty-four hours a day, seven days a week') on the one hand, and the ICT approach of the office automation people ('just re-boot during the lunch break') on the other hand.

Risk factors of the PCS environment

The process automation environment is becoming increasingly open. Market developments have meant that organizations are sometimes required to provide details from their PCS to third parties via the Internet. It is also handy for employees who have to deal with faults to be able to access the PCS from home. And suppliers of turnkey systems want to be able to implement changes remotely.

Reliable drinking water

PCS have become indispensable in the extraction, purification and distribution of our drinking water. These processes have been greatly improved by their use. The arrival of PCS has enabled consumption prognoses to be used in the management of the production process for example. This in turn allows for much more constant and regular production, leading to significant improvements in efficiency and product quality. The production process data is also available much faster. Water supply companies can therefore react to it faster; in most cases even automatically. The continuity of the water supply and water quality are secured effectively through PCS.

The importance of reliable PCS is therefore evident. In the event of a PCS failure, the water companies will often be able to fall back on the old methods of supplying water. But that is certainly not a simple matter, and would have serious consequences for effectiveness, efficiency and organization.

FEBRUARY 2008

A PCS failure in the pumping station in Epe leads to an uncontrolled increase in pressure in the drinking water pipe system. Pipes burst in seven places. The supply of drinking water in Epe, Oene and Zuuk has to be cut off for several hours.

PCS designers, PCS suppliers and system integrators are more focused on the development of new possibilities than they are on the development of systems that are inherently more secure. This has been brought about in part by client demand. A change in this respect can already be seen however, both on the demand and the supply side.

External (criminal) risk factors

In terms of threats, we have observed an increasing interest in, and knowledge about, PCS/SCADA in hackers' circles. External links between PCS networks and the outside world, combined with the poor resistance of PCS protocols to incorrect communications reports, substantially increase the possibility of a PCS failure caused by a Trojan or a hacker.

Apart from this, malware can penetrate a PCS infrastructure both deliberately and unintentionally. In either case the resulting damage can be significant.

Continuous gas pressure

Gasunie supplies natural gas to all of the Netherlands and parts of Northwest Europe. A disruption to the gas supply has immediate consequences for society. Gasunie wants to prevent disruptions as far as possible and, failing that, to limit their consequences. Flexibility has therefore been designed and built into the supply network.
The PCS that conrol the transport of gas have been implemented in duplicate. The switchover between them is tested regularly. To prevent any mistakes, changes to the systems are also carefully checked and tested.
The network environment of the PCS is separated from the office environments. The robustness of its defence against undesired and undesirable access by people and malicious software is also periodically tested. Well-trained and risk-aware employees ensure that Gasunie can execute its gas transport tasks in a high quality and reliable manner. Their effectiveness must be continuous, even if an unforeseen mistake should occur.

NOVEMBER 2001

A part of the Province of Zeeland is delivered with gas with an extremely high percentage of nitrogen. The cause: one of the PCS in the Delta gas mixing station in Borssele works incorrectly due to the installation of the wrong PCS software. Around 26,000 families have to sit in the cold and are unable to cook for up to three days. The house-to-house reconnection to the gas supply calls for a large-scale deployment of police, fire brigade and gas breakdown staff from all over the country.

Finger on the pulse

How secure or insecure is the way we go about implementing PCS (information) security? The Dutch drinking water sector asked itself this question in 2007. A quick-scan benchmark revealed a number of sector-wide weak points. Striking differences in security levels between the various drinking water companies also came to light.

The drinking water sector has developed good practices in order to tackle these weak points. In order to also help companies and authorities outside the Netherlands and to receive useful feedback, these good practices have been translated into English and made available internationally. Third parties are working on translations into Italian, French and Japanese.

The energy sector has used the same benchmarking approach. Sector-wide points requiring improvement were found there too. A comparison of the two sectors reveals some interesting similarities and differences. Almost all companies in both sectors use the Code for Information Security (ISO/IEC 27002:2005) for their office automation. Most companies in both sectors also apply this Code as the guiding principles for the security of their process automation. The greatest differences between the sectors are found in areas of policy, for example whether or not they have a specific policy for the PCS environment.

Dry feet

Many people in the Netherlands live a number of metres below the level of the sea or nearby rivers. We sleep peacefully nevertheless. We have confidence in our public water authorities that maintain the dikes, pumps, locks, sluices, dams and other waterworks. The management and control of the water levels in the polders and ditches, 24 hours a day and the whole year through, is increasingly performed using PCS. The measurement of water levels and the control of pumps and dams are often conducted remotely, sometimes via GSM/GPRS or even via the Internet.
The huge sea barriers, such as the Oosterschelde and Maeslandt storm surge barriers and the sea lock complexes, also keep our feet and infrastructure dry. Rijkswaterstaat, the governmental agency whose responsibilities include water management, controls them with PCS. In threatening situations, based on expected winds and tides, the closure of the sea barriers is fully automatic.

MARCH 2000

As a result of human operator error, the wrong lock gate opens in the sea locks at Delfzijl. Due to the strong current that is created, the lock gates then cannot be closed. Canals run empty, boats and houseboats all the way into the city of Groningen become stranded for a number of days, and shipping is also halted for days.

Areas of concern for both sectors include the lack of guarantees for the PCS information security provided through audits (legislation on annual accounts even requires this) and the way in which access to the PCS environment is arranged for the maintenance technicians of third party organizations.
The benchmark has demonstrated its value in practice.
It has enabled the identification of a number of collective points requiring attention, and indicated points to individual companies that represent particular shortcomings.
An agenda has been established for addressing these points for the Water-ISAC and the Energy-ISAC in the Cybercrime Information Exchange.

Continuous transhipment

Goods are transferred from seagoing ships to the quayside and vice versa in the Dutch ports. The integration of PCS with back-office ICT is playng an ever greater role in this process. At the European Container Terminal (ECT) in Rotterdam, sea containers are lifted out of ships by crane fully automatically, twenty-four hours a day, seven days a week. Computer-controlled trucks (Automated Guided Vehicles, or AGVs) drive independently across the terminal, carrying the containers to their storage location and loading them onto train wagons or trailers for immediate further transportation.
PCS give the AGVs the order to drive to the storage or handling location. They monitor the position and status of the vehicles and regulate the right of way and priority between one AGV and another. PCS ensure a rapid transhipment of the sea containers so that a container ship can leave the Port of Rotterdam again within a maximum of 24 hours.

MAY 2004

The PCS network of RailCorp in Australia becomes a victim of the Sasser worm. In a wide area around Sydney a day later, 80% of the trains can no longer be allowed to run as the safety system has been rendered unreliable. 50,000 passengers are faced with very long delays.

Insight into incidents

The security risk, or the combination of vulnerability, threat and potential effect, is ensuring that the subject of PCS (information) security is appearing increasingly frequently on the agenda of policy makers, nationally and internationally. Quite reasonably, they are asking about the urgency and extent of the problem. It is a question that is not easy to answer.

To obtain insight into the risk for Dutch society, the TNO and KEMA were jointly commissioned by the Ministry of Economic Affairs in 2006 to map out the PCS (information) security problem. Were security incidents occurring and, if so, what was their (potential) impact? Public sources in fact only reveal PCS (information) security problems in the United States and Australia. Incidents are often made public there either because it is legally required to report them or because they are revealed through published accounts of court proceedings.

Non-public sources actually reveal that PCS (information) security incidents also ocur in Europe and in the Netherlands. Sometimes they reach the press, often then described as a 'technical fault' or 'problems of an as yet unknown origin'. Most PCS incidents are kept quiet. A lack of formalized reporting lines means that they are often even not revealed to senior management.


DVE

Public and private sector organizations share information about incidents such as these within the cross-sector consultations of the Cybercrime Information Exchange. Despite this, the nature and extent of the unwanted and undesirable manipulation of PCS in the Netherlands remains unclear, as it does in other countries. In order to gain countrywide insight and to learn from incidents experienced by others, the Cybercrime Information Exchange started a registry of PCS incidents as a test. GOVCERT.NL has taken responsibility for the hosting of this incident database. Organizations can participate voluntarily in the test. All participants have full access to the information.

Safely under lock and key

The Custodial Institutions Agency (Dienst Justitiële Inrichtingen, or DJI) executes punishments and freedom-depriving measures on behalf of the Ministry of Justice. The DJI has 19,000 employees in more than a hundred prison establishments and custodial houses, forensic psychiatric centres and detention and deportation centres, spread throughout the Netherlands. Each year around 80,000 people are accommodated in these institutions for shorter and longer periods. The DJI also processes a stream of visitors to them each day. PCS continuously monitor and regulate the safety and security of more than a hundred thousand people. Systems for building and facility management, safety and security ensure that DJI employees can work safely and that detainees remain safely and securely under lock and key. Integrated PCS regulate fire safety, emergency power supplies, air conditioning, cameras, gate barriers and remotely operated locks. The fire at Schiphol Airport demonstrated how important these systems are for ensuring the safety of detainees and DJI employees.

MAY 2009

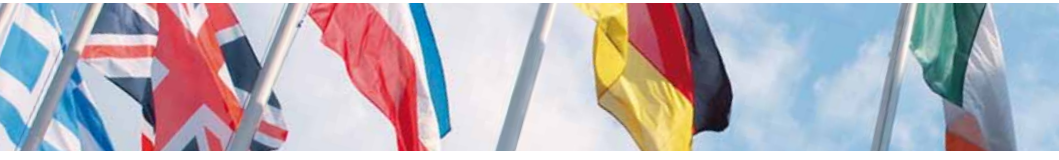
A failure in the safety system of De Geerhorst prison in Sittard leads to a commotion. It appears as if a person is sitting on the prison roof. A cordon consisting of a helicopter and police vehicles is placed around the prison, but further investigation reveals that all prisoners are accounted for.

International problem

It is becoming more and more apparent that PCS (information) security is lagging behind that of office automation internationally, and that an increasing risk has been created. In the United States, hearings have been held on the subject in Congress. The GAO, the US national audit office, has issued critical reports on the problem. The Department of Homeland Security has started R&D programmes designed to produce improvements in PCS security. Work is also being done internationally on the documentation of good practices and the development of new standards for PCS (information) security.

The crux of the matter is that the challenges are being tackled jointly by the government (as user, legislator for special sectors and supervisor), PCS users, manufacturers, system integrators, suppliers and knowledge, educational and research institutes.

The Netherlands is faced with a choice: sit still and wait for standards and technical improvements to be fully developed, or proactively tackle the problems in an international context. The parties participating in the National Infrastructure against Cybercrime have chosen the latter strategy. They are developing initiatives on a national level, but fine-tuning them on an international basis. The NICC plays an active part in the European SCADA and Control Systems Information Exchange (EuroSCSIE) and the Meridian Process Control Security Information Exchange (MPCSIE). An international group of PCS users have united together within the Plant Security working group of the WIB (International Instrument Users' Association) in order to work towards increasing the level of PCS security in their organizations.



Switch off, lights out

In the Netherlands we can be confident in our energy supply. We do not realize that the provision of electricity is a complex process, comprising generation (nuclear, coal-fired, gas-fired and hydro-electric power stations, wind parks and solar cell centres), switching and transformer stations and transmission lines. The boundaries of this distributed high voltage machine run from the Arctic Cape via the UK and the Iberian Peninsula through Morocco, Italy, Greece and the Eastern European countries to the Baltic States. In time this will be extended through to Vladivostok and there will be a closed ring around the Mediterranean Sea. The process works, despite it consisting of many components that are managed and controlled by a large number of organizations, often with conflicting commercial interests.
PCS monitor, manage and control the generation of electricity. By regulating the rotational velocity of the generators, the generation is brought into balance with the electricity that is purchased and used (the load).
PCS also monitor the voltage and the frequency in the network, the transfer of capacity via transmission lines and transformers, the reactive capacity, and very much more.
When major variances occur, the load from large companies is automatically disconnected. If this is insufficient to maintain the system in balance, the lights will also go out in private households.

JANUARY 2003

The PCS network of First Energy's Davis Besse nuclear power plant in Ohio becomes infected with the SQL Slammer worm. The worm penetrates the PCS network via a call-in connection and infects the system that renders the security parameters. This system is out of use for five hours. The central processing computer is also unusable for six hours. The nuclear plant itself is fortunately undergoing maintenance at the time.

Manufacturers and suppliers

PCS manufacturers and the suppliers of PCS services (from design and application development to turnkey-project-development and maintenance) play a major role in PCS security. They not only ensure that the software provides security options. With the advice they provide and through their way of working, they can raise their clients' PCS security to a higher level. They can offer 'hardening' of the underlying control system in their quotations and proposals for example. Or they can make proactive agreements from the supply side about 'information-secure' ways of working through their maintenance personnel.

PCS users and providers in America have jointly drawn up a Cyber Security Procurement Language for Control Systems (CSPL). This catalogue detailing security requirements for PCS is a first step towards the development of a professional, joint approach to PCS (information) security. In several countries, including the Netherlands, work is currently going on to disseminate, and where necessary improve, this CSPL. The Plant Security working group in the WIB has already taken the initiative itself to draw up Process Control Domain Security Requirements for Vendors, with Shell as one of the pioneers in this respect. A connection for this is being sought with the development of the SP-99 standard for PCS. This will open up the possibility of PCS certification with respect to information security.

Baggage to Timbuktu

The baggage handling systems at Amsterdam Airport Schiphol process between 130,000 and 160,000 pieces of baggage every day. These high quality systems ensure that your baggage arrives with you at the same time in Timbuktu and that the baggage of passengers on their way to other parts of the world does not end up in Timbuktu.
From their headquarters coordination room, airport and KLM coordinators keep a close eye on the baggage process, twenty-four hours a day, seven days a week. They do this via a SCADA IM (Installation Management) package that has been specifically designed for the baggage handling process. Should a deviation occur in a system or parameter, a coordinator can immediately intervene via the IM.
An example is the loading of a sorting conveyor belt, the final point in the baggage system where the baggage from each flight is sorted out. If the baggage is not taken off in time, the conveyor belt becomes over full. When a predetermined density of baggage is reached on the belt, the IM raises the alarm and the coordinator intervenes.

APRIL 2008

A software fault in the baggage handling system in the newly-opened Heathrow Terminal 5 leads to weeks of baggage processing chaos. More than 28,000 suitcases are incorrectly sorted. British Airways cancels more than four hundred flights. Enormous quantities of cases are transported using extra cargo flights to other European airports to use their baggage systems to ensure they eventually arrive at the correct destinations. The loss is estimated to be 50 million dollars.

The challenge

CIOs of major companies and governmental organizations have discussed the PCS risk with the Director-General Energy and Telecom in a Round Table. The conclusion: no single party in the field is yet able themselves to guarantee PCS (information) security. PA environments are complex, and dependencies are increasing because of the increasing level of automation in the PCS. The threats are diverse and extremely variable. The boundaries of organizations are becoming more and more diffuse, whereby a growing number of activities are being farmed out to turnkey organizations, outsourcing partners, PCS suppliers and other subcontracted parties. It is only through a joint approach being taken by all those involved that a high enough level of PCS (information) security can be achieved in the Netherlands and also guaranteed in the future. The Round Table participants have committed themselves to arriving at a national approach in order to bring PCS (information) security in the Netherlands up to the right level and maintaining it there. A number of parties in the National Infrastructure against Cybercrime have accepted the challenge of taking the initiative to arrive at a 'National Roadmap to secure Process Control Systems'. This will detail the physical, personnel and ICT measures that will have to be taken in order to keep PCS secure. Active participants include the WIB, several sectors from the Cybercrime Information Exchange, suppliers, knowledge institutes, universities, the CIO Platform Nederland and the government.

More with milk

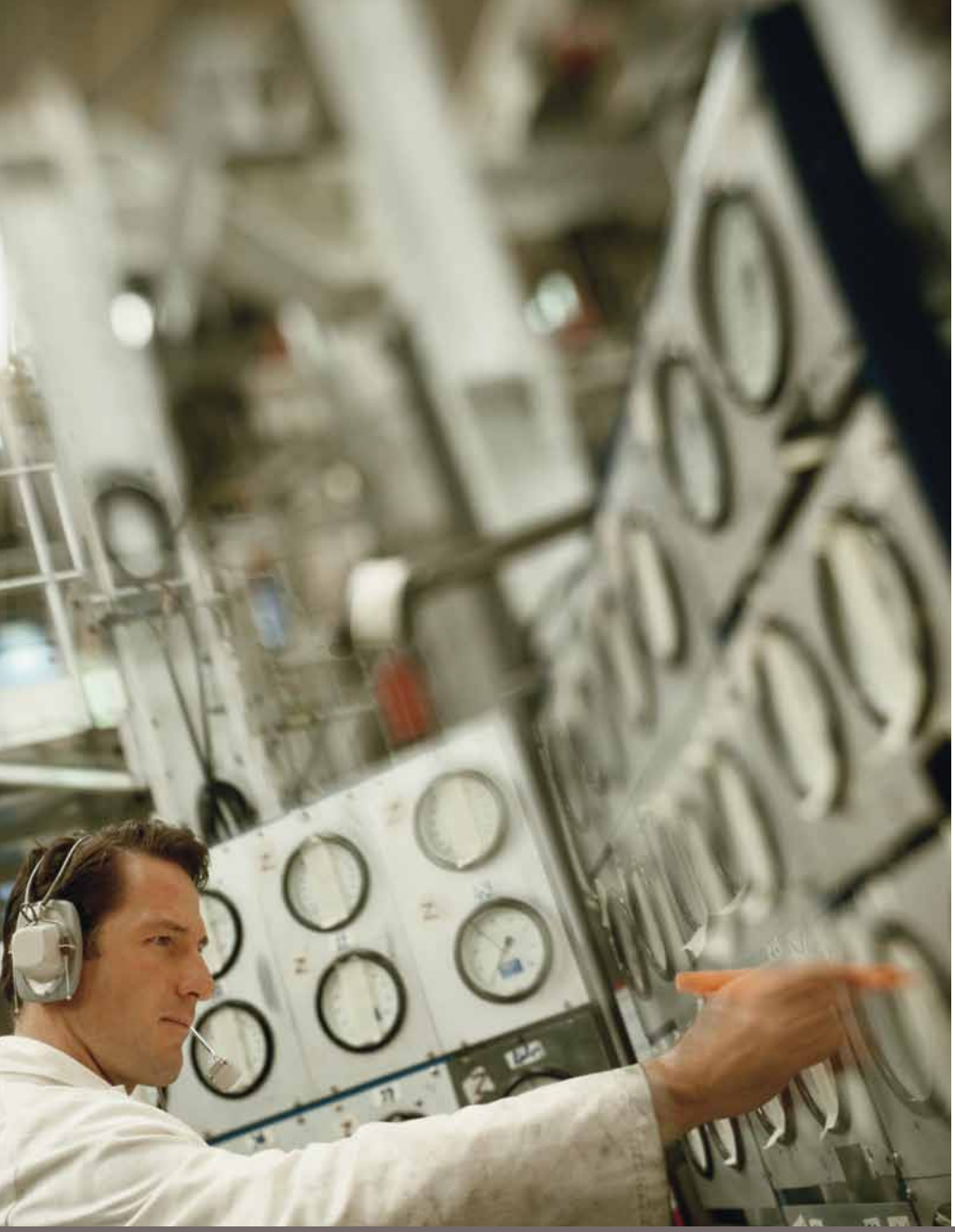
A healthy glass of milk does not automatically make you think of PCS. But in modern dairy farms it is not the farmer or the farmer's wife themselves but PCS that monitor the health of the cows, regulate the milking automatically and ensure that the milk is safely kept at the right temperature.
PCS control and monitor the processing of the raw milk into a wide range of milk products in the dairy or milk plant.
In this way, the quality of all the different end products is guaranteed.
At the end of the processing stage it is PCS that take care of the filling of the cartons and other containers with milk, buttermilk, custard, cream and yoghurt, often mixed with flavourings, additives or pieces of fruit. The next step is the automatic stacking of the end products on pallets.

A hacker knows how to penetrate the facilities management system of a computer centre in a large European bank. He or she manipulates the air conditioning settings, causing all the servers to stop working through overheating.

Towards a National Roadmap

The first steps towards a National Roadmap to secure Process Control Systems have been taken. The inspirational examples from the United States are extremely appropriate for use in the situation in the Netherlands. There it has been experienced, for example, that there are only differences in emphasis to be seen between the individual sectoral roadmaps. For this reason, a cross-sector approach has been chosen in the Netherlands: a single National Roadmap. The human factor plays a key role in this. Efforts have been made to maintain a balance in de Roadmap between the organizational and technical aspects on the one hand and factors concerning human behaviour on the other. The security measures taken can be physical, personnel-related and organizational as well as those concerning ICT. The initiative for the Roadmap was presented in a workshop attended by all parties during the NICC's third Process Control Security Event, 'Control IT!' The vision has been discussed and the objectives have been determined. The point of departure of the Roadmap is a shared vision that has provisionally been defined as follows:

'Within ten years, the protective layers for the PCS that control critical processes will be designed, implemented and maintained. This will be established in accordance with the risk identified. The objective in this respect is that there will be no loss of critical functions during and after a cyber-incident.'



The Roadmap focuses on secure PCS use during the entire PCS life cycle. Manufacturers, suppliers, service providers, the government, educational establishments, knowledge institutes and international partner organizations support this. In close collaboration, these parties have translated the vision into the following objectives:

1. To ensure a permanent high level of awareness
2. To measure and determine security posture and level
3. To develop and integrate protective measures
4. To detect intrusions and implement response strategies
5. To sustain security improvements
6. To ensure PCS are 'secure by design'

These objectives are elaborated in the Roadmap in action-oriented terms at strategic and tactical levels in milestones for the short-term, or 'quick wins', (up to one year), medium-term (to 3 years) and long-term (to 10 years). Tasks, roles and responsibilities are described in SMART (specific, measurable, acceptable, realistic, time-bound) terms.

Cyber-controlled cracking

In our ports and in other locations in the Netherlands are large petrochemical complexes with crackers and many kilometres of transport pipelines. Crackers process chemical raw materials such as naphtha, butane, ethylene and other oil products. Long carbon chains are broken down so that lighter fractions are produced by the cracker after distillation: (poly)ethylene and other aromatics that are used in nearby factories for the production of complex carbon chemical products.
PCS are the eyes and ears of the process operators in the (petro)chemical industry. Working safely is the number one priority. All process parameters are monitored, and where necessary regulated and readjusted, from central control rooms so that intermediary and end products are the right quality. The process is designed to be fail-safe. This does not prevent the occasional appearance of large flames above the burn-off tower and unpleasant odours escaping however, should the control of the process get out of hand. Unauthorized manipulation of the controlled processes must always be prevented. Nevertheless, hackers have been known to penetrate the PCS that control petrochemical installations such as these.

MAY 2008

Between May 8th and June 29th 2008, after his dismissal by Pacific Energy Resources, where he had worked as a PCS software manager, Mario Azar manipulates the settings of the leak detection system of oil pipelines between oil platforms and the coast.

Over the years, companies and the government have undertaken all the activities required and taken measures to raise PCS security to a higher level. These are being integrated into the Roadmap as far as possible. Examples include the organization of Red/Blue team training courses (in collaboration with the US Department of Homeland Security), international collaboration, the implementation and adaptation of the Cyber Security Procurement Language, the drawing up of 'Process Control Domain Security Requirements for Vendors', the development of standards, the registration of PCS incidents and (inter)national Process Control Security Events.

Clear waste water

Municipalities and water authorities are responsible for the transport and treatment of our waste water. More than 100,000 kilometres of sewage pipelines and 368 sewage water treatment installations are used for this. The treatment capacity of just one of these installations can be as much as that required to serve a million residents. To a great degree this continuous process is automated. With increasingly complex process steps and regulations, operations and controls being conducted remotely, and outsourcing, dependence on PCS reliability is only growing still further. Should the waste water chain malfunction, there would be grave consequences for the environment and public health.

NOVEMBER 2007

In Nokia, Finland, a connection between a waste water pipeline and a drinking water pipeline is opened in order to flush out and clean the waste water pipes. A difference in pressure causes waste water to flow back into the drinking water. 12,500 residents suffer stomach and intestinal complaints. Hundreds of people have to be admitted to hospital, and three patients die as a result of the contaminated drinking water. It takes several months to restore safety and security to the drinking water system.

Pulling out all the stops together

The examples in this publication make it crystal clear why guaranteeing the availability and reliability of essential products and services is so important. Not only for our society as a whole, but also for individual citizens. It has also been demonstrated that no single party can tackle this challenge alone and bring it to a successful conclusion. Collaboration is vital!

Keeping an eye on bridges

Rijkswaterstaat, the Directorate-General for Public Works and Water Management, manages the national road and waterway systems. More and more bridges, sluices, locks and tunnels are operated and controlled remotely using PCS. Problems in and failures with these operations and controls lead to major tailbacks, traffic jams, obstructions, many hold-ups, unsafe situations, other kinds of nuisance, and sometimes damage to the environment. What should we think if a bridge unexpectedly remains open during the rush hour, as once happened with the bridge forming part of the A4 near Leiderdorp?
Road users also demonstrate unforeseen behaviour: they ignore a stoplight or barrier. If this goes wrong and cars fall from the bridge, it becomes front-page news. The safe opening and closing of a bridge while being fully aware of the situation at that moment is therefore crucial for Rijkswaterstaat. PCS help with the flow of traffic and safety.

DECEMBER 2006

Since its opening in December 2006, the Dublin Port tunnel has had to be closed more than twenty times for hours at a time as a result of SCADA failures. The tunnel ensures that heavy goods vehicles travelling between the port and the surrounding motorways can avoid the centre of the city and its residential areas. The result of every tunnel closure is enormous traffic chaos and significant environmental damage.

Appendices

Standards and Good Practices

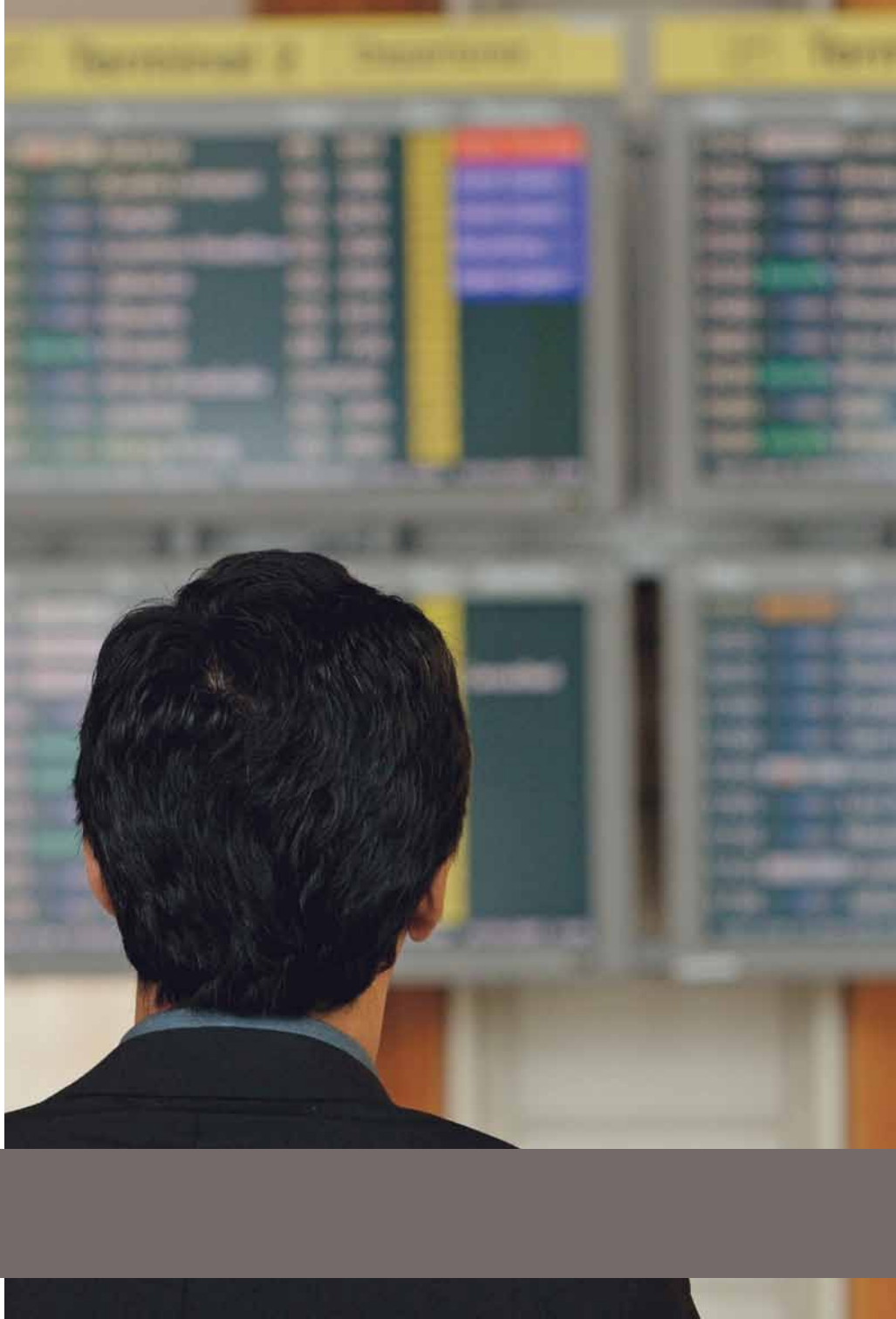
- SCADA Good Practices for the Dutch Drinking Water Sector, TNO DV 2008 C096, March 2008.
- A collection of SCADA Good Practices, including a firewall guide, provided by the Centre for the Protection of National Infrastructure (CPNI), http://www.cpni.gov.uk/Products/guidelines.aspx
- 21 steps to improve the security of SCADA networks, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf
- ISO/IEC 27001:2005, Information Technology – Security Techniques - Information Security Management Systems – requirements.
- ISO/IEC 27002:2005, Information Technology – Code of Practice for Information Security Management.
- NIST Special Publication SP 800-53 – Appendix I: security controls for Industrial Control Systems.
- NIST Special Publication SP 800-82 (draft) Guide to Industrial Control Systems (ICS) Security.
- Cyber Security Procurement Language for Control Systems (INL).
- Establishing an Industrial Automation and Control Systems Security Program, ANSI/ISA-99.02.01-2009 (draft IEC 62443-2-1).
- Operating an Industrial Automation and Control Systems Security Program, ANSI/ISA-99.02.02-2009 (draft IEC 62443-3-1).

Background information

- H.A.M. Luiijf and R. Lassche, SCADA (in)security - a role for the government?, TNO/KEMA report, April 2006 (in Dutch).
- Control Systems Security Program, DHS and US-CERT, http://www.us-cert.gov/control_systems - including the Cyber Security Procurement Language for Control Systems and other items.
- US Guide to Inspections of Computerized Systems in the Food Processing Industry, USFDA, http://www.fda.gov/ICECI/Inspections/InspectionGuides/ucm074955.htm

Research and development

- European Workshop on Industrial Computer Systems Reliability, Safety and Security, http://www.ewics.org
- Crutial – Critical Utility Infrastructure Resilience, http://crutial.cesiricerca.it
- IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems, http://www.irriis.org
- GRID – Cyber-vulnerabilities of electricity networks, http://grid.jrc.it



Programme

Annemarie Zielstra (ICTU)
programme manager

Auke Huistra
Information Exchange project manager

Eric Luiijf
NICC expert pool (SCADA/PCS)

The NICC programme is an ICTU programme, commissioned by the Ministry of Economic Affairs. The motto of the ICTU is: helping governmental organizations to perform better with ICT. ICTU combines knowledge and skills in the area of ICT and government. ICTU executes a wide variety of projects on behalf of and with governmental organizations. In this way policy is translated into concrete projects for the government. More information can be found at www.ictu.nl.

Colophon

Editing
NICC
Eric Luiijf (NICC expert pool)

Editors
Tekstbureau De Nieuwe Koekoek, Utrecht

Text by
Brabant Water / Gasunie / Schiphol Airport /
Rijkswaterstaat / Shell / Waternet / Witteveen & Bos

In cooperation with
Paul Bloemen, Gasunie / Jules Vos,Shell /
Martin Visser, Waternet

Design
OSAGE / communicatie en ontwerp, Utrecht

Photography
Marcel Rozenberg, Schiedam

Print
OBT / TD Sprintmaildata, Schiedam

November 2009

NICC | ICTU

Visiting address
Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postal address
P.O. Box 84011
2508 AA The Hague
The Netherlands
T +31 70 888 7946
nicc@ictu.nl
www.samentegencybercrime.nl