

# Critical Infrastructure Protection – do you care?

TNO Defence, Security and Safety



Eric Luijff, Principal Consultant

Clingendael Centre for Strategic Studies

- Eric Luijff MSc. Principal Consultant Information Operations & Critical Infrastructure Protection
- TNO Defence, Security and Safety [www.tno.nl](http://www.tno.nl)
- Clingendael Centre for Strategic Studies ([www.ccss.nl](http://www.ccss.nl))

C(I)IP and process control 2

## Agenda

- Critical (information) infrastructures**
  - vital for lives, economy, ecology, and society
- Security and Process Control Systems**
  - SCADA (in)security
- Consequences for the Process Industry**
- The Next Step**
- Questions**

C(I)IP and process control 3

## Critical Infrastructures (CIs)

- Defined by EU (COM(2004)702 Final) as**
  - physical and information technology facilities, networks, services and assets
  - if disrupted or destroyed seriously impact on health, safety, security or economic well-being or effective functioning of governments
- Our earlier Dutch definition is (almost) alike**
  - cause dramatic impact upon economy and/or ecology
  - cause loss of lives of people and animals
  - seriously affect functioning of government and democracy
  - seriously affect public confidence
- CIs increasingly dependent on ICT**
  - increasingly intertwined and interdependent

C(I)IP and process control 4

## Dutch example: 11 critical sectors 31 critical products and services

No.	Sector	Product or service
1	Energy	Electricity
2		Natural gas
3		Oil
4	Telecommunications	Fixed telecommunication networks services
5		Mobile telecommunication services
6		Radio communication and navigation
7		Satellite communication Incl. GPS
8		Broadcast services
9		Internet access
10		Postal and courier services
11	Drinking water	Drinking water supply
12	Food	Food supply and food safety
13	Health	Health care
14	Financial	Financial services and financial infrastructure (private)
15		Financial transfer services (government)

C(I)IP and process control 5

## Dutch example: 11 critical sectors 31 critical products and services

16	Retaining and managing surface water	Management of water quality
17		Retaining and managing water quantity
18	Public Order and Safety	Maintaining public order
19		Maintaining public safety
20	Legal order	Administration of justice and detention
21		Law enforcement
22	Public administration	Diplomacy
23		Information provision by the government
24		Armed Forces / Defence
25		Public administration
26	Transport	Road transport
27		Rail transport
28		Air transport
29		Inland navigation
30		Ocean shipping
31		Pipelines

C(I)IP and process control 6





## Process Control Systems and CI's

- **Energy sector**
  - electrical power generation, transmission, distribution
  - natural gas production, processing, transport and distribution
- **Drinking water** production, transport, distribution
- **Water management** pumps, locks, sluices, sewage processing
- **Rail system**
- **Transport of chemicals, oil, gas, etc.**
- **Health sector** (medicines; nuclides; ...)
- **Chemical and nuclear plants**
  - if process out of bounds, it draws upon the other CI's !



C(I)IP and process control

13

## Safeguarding the Process Industry

The need is clear .. but what is the current status?

Process Control Systems e.g. SCADA / PLC / EMS / DCS



C(I)IP and process control

14

## Process Control Systems – the trend

- **Towards Commercial-off-the-Shelf (COTS)**
  - from process automation to computer controlled
  - from proprietary software to public protocols
  - systems increasingly based on COTS platforms and operating systems (e.g. Windows, VxWorks, QNX, OS-9)
  - Programmable Logic Controllers start to have TCP/IP engine on board
- **Operations**
  - downsize and cut operating costs
  - convergence of networks & connections to external networks
    - billing, management information
    - information exchange with system and market operators
  - tunnel connections over the Internet
  - outsourced and remote maintenance



C(I)IP and process control

15

## Threats and Vulnerabilities

- **Threats**
  - against continuity (availability) and integrity of process
  - unauthorised changed settings with operations safety impact and altered metering data
- **Vulnerabilities**
  - two groups: general ICT and PCSs specific



C(I)IP and process control

16

## Vulnerabilities due to 'general ICT'



C(I)IP and process control

17

## General ICT environment of PCSs

- **Users in general lack proper security awareness**
  - no precautions, no/late patching
  - dangerous way of operating
  - easy to lure into traps (social engineering)
  - maintenance has unprotected laptops with all keys, location information,...
- **Low COTS software quality**
  - same type of vulnerabilities over and over again
  - no incentive for quality improvement as costs are with end-user
  - COTS: 48 new vulnerabilities / week, 70% easy to exploit



C(I)IP and process control

18

## General ICT environment of PCSs

- 'Bioterrorism in Cyberspace' (viruses; worms; Trojans)
  - monocultures: world-wide pandemonium in less than 30 minutes
  - payloads still proof-of-concept rather than havoc
  - Internet "health" prediction: infection likely within 20 min unprotected
- **Process control connected to Internet?**
  - Slammer took down nuclear power plant's safety monitoring system (2003)
  - Blaster blocked power transport control network (2003)



C(II)P and process control

19

## General ICT environment of PCSs

- **Hacking**
  - visibility is 'low impact' Cyber-graffiti, real threat concealed
  - wide-spread and increasingly sophisticated toolsets
  - (Distributed) Denial-of-Service attacks
- **KEMA reported on power utility incidents**
  - 100-150 intrusion attempts/day, 17 serious intrusions
  - 2 DoS events
  - 3 loss of control events
- **Process control connected to public network?**
  - wireless?
  - shared network assets?
  - modem lines?



Created by Telian/ICT

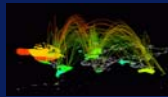


C(II)P and process control

20

## General ICT environment of PCSs

- **Internet as transport for process monitoring & control?**
  - lacks transparency of
    - organisational responsibilities and technical infrastructure
    - dependability infrastructure and continuity of base-services like DNS?
  - dependability and reliability not guaranteed
    - market instability / market failure
    - risk for (near) real-time and critical applications
  - Internet has some resilience, but major single-points-of-failure exist

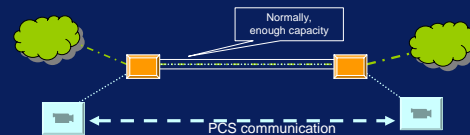


C(II)P and process control

21

## General ICT environment of PCSs (1)

- **Process monitoring & control on shared network?**
  - Virtual LANs (VLAN) / network sharing seem to be cost-effective
  - essential network elements have COTS vulnerabilities – universal failure

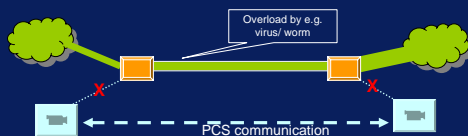


C(II)P and process control

22

## General ICT environment of PCSs (2)

- **Process monitoring & control on shared network?**
  - Virtual LANs (VLAN) / network sharing seem to be cost-effective
  - essential network elements have COTS vulnerabilities – universal failure
  - overload of link share equipment due to virus/worm blocks PCS link
    - happened in e.g. a power control network in the USA



C(II)P and process control

23

## Electronic Environment of ICT

- **Upcoming risk of electro-magnetic disturbances**
  - new tools for criminals, activists, terrorists
- **GPS jamming**
  - blueprint of jammers in hacker magazine, Internet, ..
  - GPS is essential part of many CII's and CI's
    - precise timing in control system areas ..
- **High-power microwaves**
  - commercially built for governments
  - ...?



Unsuspect HPM-case



C(II)P and process control

24

## Vulnerabilities specific to PCSs



## PCS network architecture

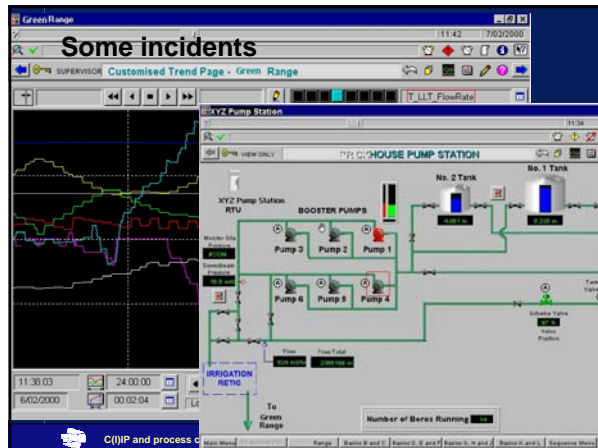
- **Current security based on flawed assumptions**
  - protocols are proprietary
  - protocols are not (well) known to hackers
  - stand-alone: network is completely detached from other networks
    - shared, billing, administration, remote maintenance ...
  - no one is interested in hacking process control networks
- **No one is really interested in security posture**
  - backdoors and illegal connections appear
  - temporary security shortcuts forgotten
  - unregistered modems connected to network nuclear power plant
  - no security in remote control
    - substation capture within five minutes...

## PCS protocols & access control issues

- **Control information in clear text**
- **Specific control protocols have exploitable flaws**
  - implementations not hardened against network threats
    - some implementations fail when scanned
    - ping-of-death like failures / denial-of-service by crafted packages
    - SNMP activated, but no password change/turn off option in PLC
- **Authentication of users and systems**
  - speedy accessibility of devices (safety) trade-off versus security
  - password change difficult in a 24\*7 operations environment
  - passwords not up to standards
  - single rather than mutual authentication

## PCS security management

- **Security patching**
  - requires going off-line - difficult to do in a 24\*7 operational environment
  - consequences of new software version for continuity?
  - consequence: no or late patching (if at all)
- **Legacy**
  - networks contain old legacy equipment (by the thousands)
    - limited processing power and small memory; small bandwidths (e.g. Intel 8088's from 1978)
  - real-time means no time for security (e.g. encryption) in the stack
- **Specific security devices/options**
  - COTS firewalls not adapted to specific process control protocols
  - Secure RTU options not used (signed, encrypted messages)



## PCSs unprotected @ Internet

- **Roosevelt Dam incident USA (1998)**
- **Energy distribution systems NL, NO, SP, UK, US ..**
  - 95% network capacity of a energy operator in the US went to hacker
- **Waste water system**
  - Brisbane (Australia) system manipulated by Vitek Boden
  - "As thousands use electronic payment over the Internet, water management process control can be done over Internet as well" (system manager in NL!)
- **Industrial plant**
  - reverse-osmose process semiconductor manufacturing shut down by hacker
- **Gas processing**
  - main control panel GazProm taken over by hackers
  - sabotage of plant to disrupt distribution services (European example)

## YOUR NEXT STEP :

### Safeguarding

C(I)IP and process control 31

## Requires balanced approach

C(I)IP and process control 32

### Safeguarding

- Have an enterprise-wide security vision
- Develop security policy
  - understand difference between critical and non-essential
- Security action plan
  - increase security awareness of all
  - proper training of users, system engineers, ...
  - audit/ monitor status
  - have a well-defined incident management process
- See e.g. to improve Cyber security of SCADA Networks, IEC 61850 Communication networks and systems in substations

C(I)IP and process control 33

### Safeguarding , some difficulties ..

- Management attitude of security goes before cost cut
- No ISO/IEC 17799 appendix for PCSs
- Not many effective application-level firewalls for PCS protocols etc.
- Insecure process control protocols
- Hardly any rigidly tested fail-safe implementations

Do you care and are you prepared?

C(I)IP and process control 34

### Questions ?

luijif@fel.tno.nl

C(I)IP and process control 35

### Publications / background material

- Critical (Information) Infrastructures
  - www.tno.nl either use search engine for 'critical infrastructure'
  - or: www.tno.nl/instit/fel/infoops follow IW-Infra
    - KWINT - Internet as CI and its vulnerabilities
    - Critical Infrastructure protection papers and presentations (some in Dutch)
- Process Control Systems / SCADA
  - www.scadasec.net
  - 21 steps to improve Cyber security of SCADA Networks (OoEA)
  - publications of GAO (GAO-04-140IT)
  - publications by ISS, RipTech, Vigilix, ...
  - publications on PCS for Electrical Power at www.selinc.com
  - IEC 61850 Communication networks and systems in substations (www.iec.ch)
  - EPA report 2005-P-00o2

C(I)IP and process control 36