



Security in an industrial environment

Andrew Doukhvalov

Andrey.Doukhvalov@kaspersky.com



Industrial Control System (ICS) – – a security point of view

There is a huge number of problems of the critical infrastructures connected with information security

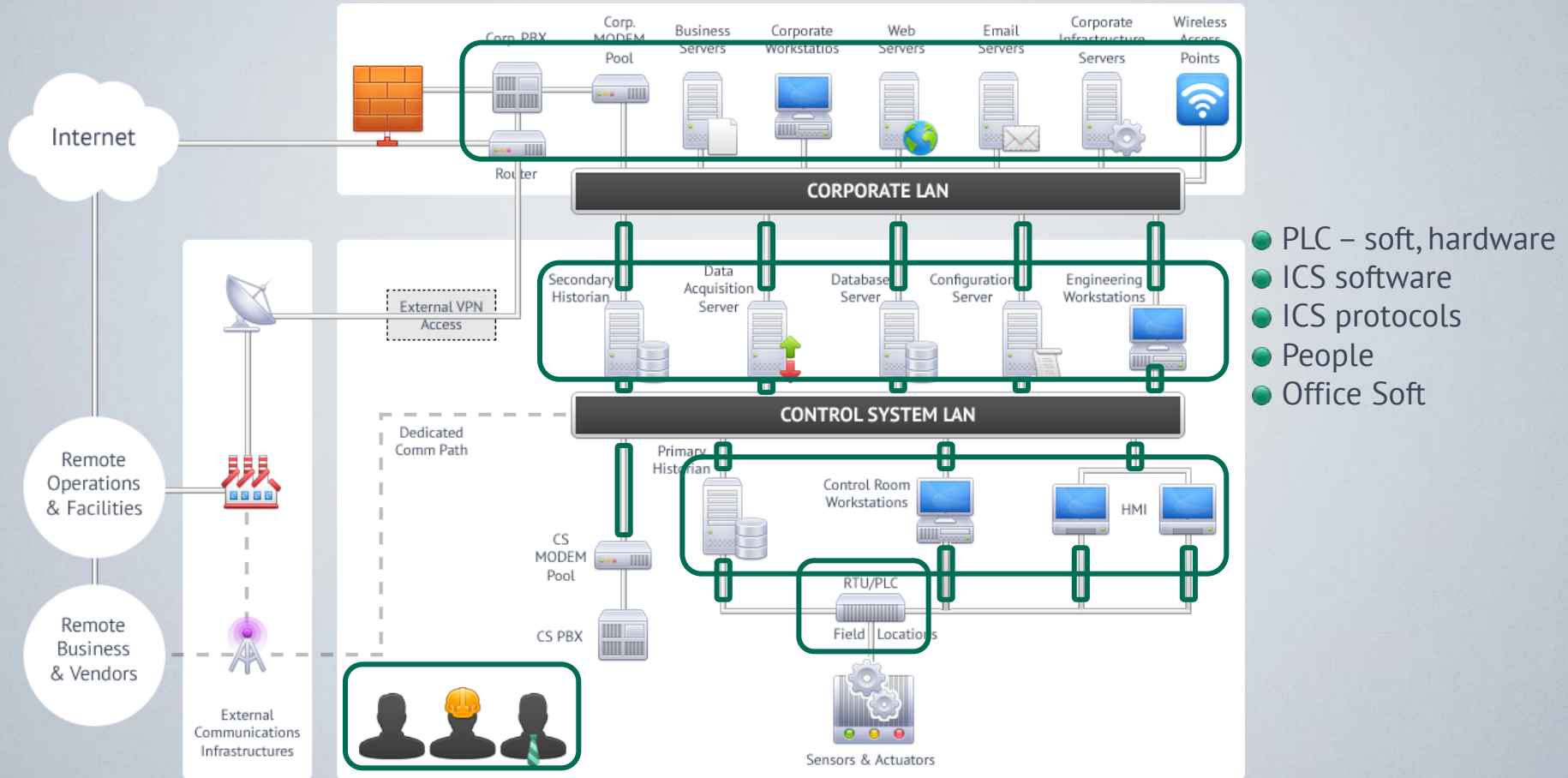
There is a risk of fatal consequences associated with the failure of ICS of critical infrastructures

KL initiated a project to improve the level of information security in critical infrastructures



ICS components – a security point of view

US ICS-CERT (Defense in Depth): Cumulative scheme



ICS components – a security point of view

PLC vulnerabilities - Digital Bond research

- Allen-Bradley: ControlLogix & MicroLogix
- Schneider Electric: Modicon Quantum
- General Electric: D20ME
- Schweitzer: SEL-2032
- Koyo: Direct LOGIC H4-ES

- ✗ – exist, easily exploited
- ! – exist, difficult to exploit
- ✓ – vulnerability not discovered

					
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

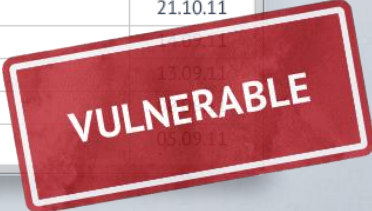
VULNERABLE

ICS components – a security point of view

Software vulnerabilities – Secunia

Found: 44 Secunia Security Advisories, displaying 1-25

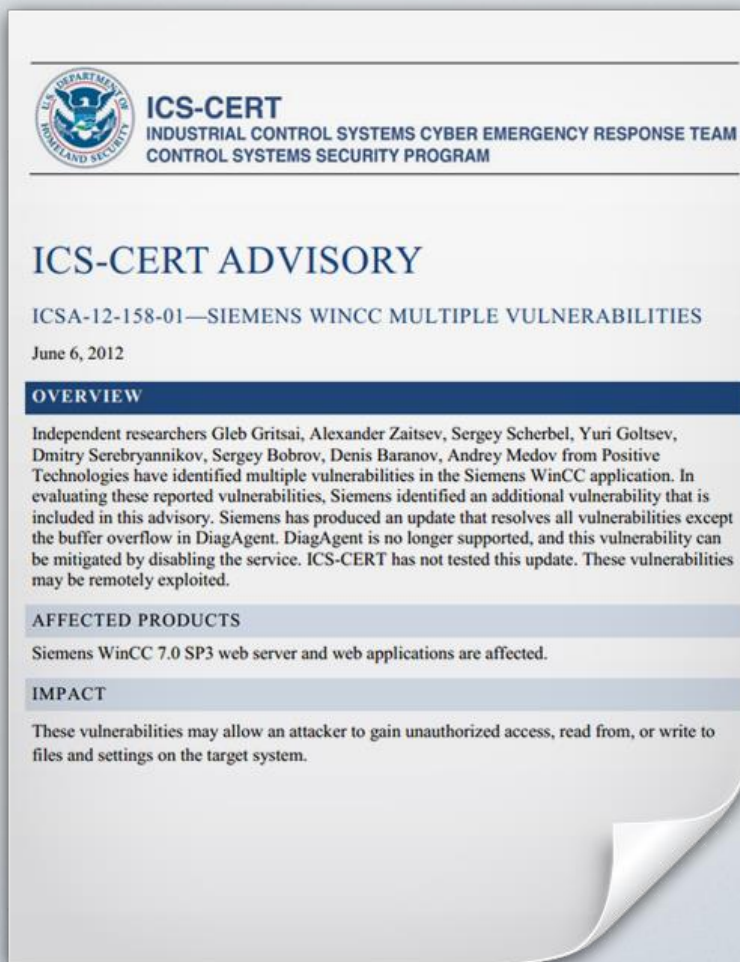
Title	Date
GE Intelligent Platforms Products Two Vulnerabilities	24.01.13
Schneider Electric Interactive Graphical SCADA System Data Collector Buffer Overflow Vulnerability	17.01.13
Proficy HMI/SCADA - CIMPLICITY Web Server Integer Overflow Vulnerability	09.01.13
EOScada Information Disclosure and Denial of Service Vulnerabilities	02.11.12
Invensys Wonderware Products Insecure Library Loading Vulnerability	24.07.12
GE Intelligent Platforms Multiple Products KeyHelp ActiveX Control Two Vulnerabilities	29.06.12
Invensys Products ActiveX Control Buffer Overflow Vulnerabilities	02.04.12
Proficy Historian Data Archiver Service Memory Corruption Vulnerability	14.03.12
xArrow Multiple Denial of Service Vulnerabilities	06.03.12
Schneider Electric Modicon Quantum Cross-Site Scripting and Buffer Overflow Vulnerabilities	23.01.12
Rockwell Automation Products Multiple Vulnerabilities	23.01.12
SEL-2032 Communications Processor Denial of Service Vulnerability	23.01.12
Koyo ECOM100 Ethernet Module Cross-Site Scripting and Denial of Service Vulnerabilities	23.01.12
GE Energy D20/D200 Substation Controller TFTP Service Multiple Vulnerabilities	20.01.12
KingSCADA Credentials Disclosure Security Issue	20.01.12
7-Technologies Interactive Graphical SCADA System Insecure Library Loading Vulnerability	17.01.12
7-Technologies Interactive Graphical SCADA System Two Vulnerabilities	21.12.11
Schneider Electric Products Multiple Vulnerabilities	29.11.11
Schneider Electric CitectSCADA Batch Server Login Buffer Overflow Vulnerability	09.11.11
Mitsubishi MX4 SCADA Batch Server Login Buffer Overflow Vulnerability	09.11.11
Schneider Electric Products UnitelWay Device Driver Privilege Escalation Vulnerability	21.10.11
ScadaPro Multiple Vulnerabilities	15.09.11
ScadaTec ModbusTagServer / ScadaPhone Project Import Buffer Overflow Vulnerability	15.09.11
Procyon SCADA Core Service Buffer Overflow Vulnerability	05.09.11
ClearSCADA 2010 Web Interface Authentication Bypass Vulnerability	05.09.11




Source: <http://secunia.com/advisories/search/?search=scada>

ICS components – a security point of view

Software vulnerabilities – Positive Technologies

The image shows a document titled 'ICS-CERT ADVISORY' with a header for the 'INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM'. The document is dated June 6, 2012, and discusses multiple vulnerabilities in Siemens WinCC. It includes sections for 'OVERVIEW', 'AFFECTED PRODUCTS', and 'IMPACT'. The bottom right corner of the document is curled up, suggesting it's a scanned page.

 **ICS-CERT**
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-158-01—SIEMENS WINCC MULTIPLE VULNERABILITIES

June 6, 2012

OVERVIEW

Independent researchers Gleb Gritsai, Alexander Zaitsev, Sergey Scherbel, Yuri Goltsev, Dmitry Serebryannikov, Sergey Bobrov, Denis Baranov, Andrey Medov from Positive Technologies have identified multiple vulnerabilities in the Siemens WinCC application. In evaluating these reported vulnerabilities, Siemens identified an additional vulnerability that is included in this advisory. Siemens has produced an update that resolves all vulnerabilities except the buffer overflow in DiagAgent. DiagAgent is no longer supported, and this vulnerability can be mitigated by disabling the service. ICS-CERT has not tested this update. These vulnerabilities may be remotely exploited.

AFFECTED PRODUCTS

Siemens WinCC 7.0 SP3 web server and web applications are affected.

IMPACT

These vulnerabilities may allow an attacker to gain unauthorized access, read from, or write to files and settings on the target system.

ICS components – a security point of view

Protocol vulnerabilities

MODBUS	The protocol contains multiple vulnerabilities that could allow an attacker to perform reconnaissance activity	http://tools.cisco.com/security/center/viewAlert.x?alertId=23280
DNP3	The protocol itself lacks any form of authentication or encryption	https://eeweb01.ee.kth.se/upload/publications/reports/2008/XR-EE-ICS_2008_020.pdf
EtherNET/IP	no authentication is required per the standard for many commands	http://www.digitalbond.com/?s=no+authentication+is+required+per+the+standard+for+many+commands&submit.x=0&submit.y=0&submit=Search
PROFIBUS	Profibus lacks authentication inherent to many of its functions, allowing a spoofed node to impersonate a master node	Industrial Network Security http://books.google.ru/books?id=Et9u-mxq0B4C&pg=PA80&lpg=PA80&dq=Profibus+lacks+authentication&source=bl&ots=Rq943klrA8&sig=A9XzX-Z8lxH4EzdYJIMHwCOhNA&hl=ru&sa=X&ei=IXvXT4XrHbH14QJjw0CoAw&ved=0CFMQ6AEwAA#v=onepage&q=Profibus%20lacks%20authentication&f=false
Fieldbus	attacks are possible because the standard is not precise enough at specifying how checks on received data must be implemented	http://alfredo.pironti.eu/research/sites/default/files/tii10_0.pdf
OPC	vulnerability is exploitable through a malformed .NET Remote Procedural Call (RPC) packet	http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-285-01.pdf
IEC 60870-5-104	The protocol itself lacks any form of authentication or encryption.	http://www.ee.kth.se/php/modules/publications/reports/2008/XR-EE-ICS_2008_021.pdf



Most SCADA protocols were designed long before network security perceived to be a problem.

Source: <http://www.ida.liu.se/~rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf>

ICS components – a security point of view

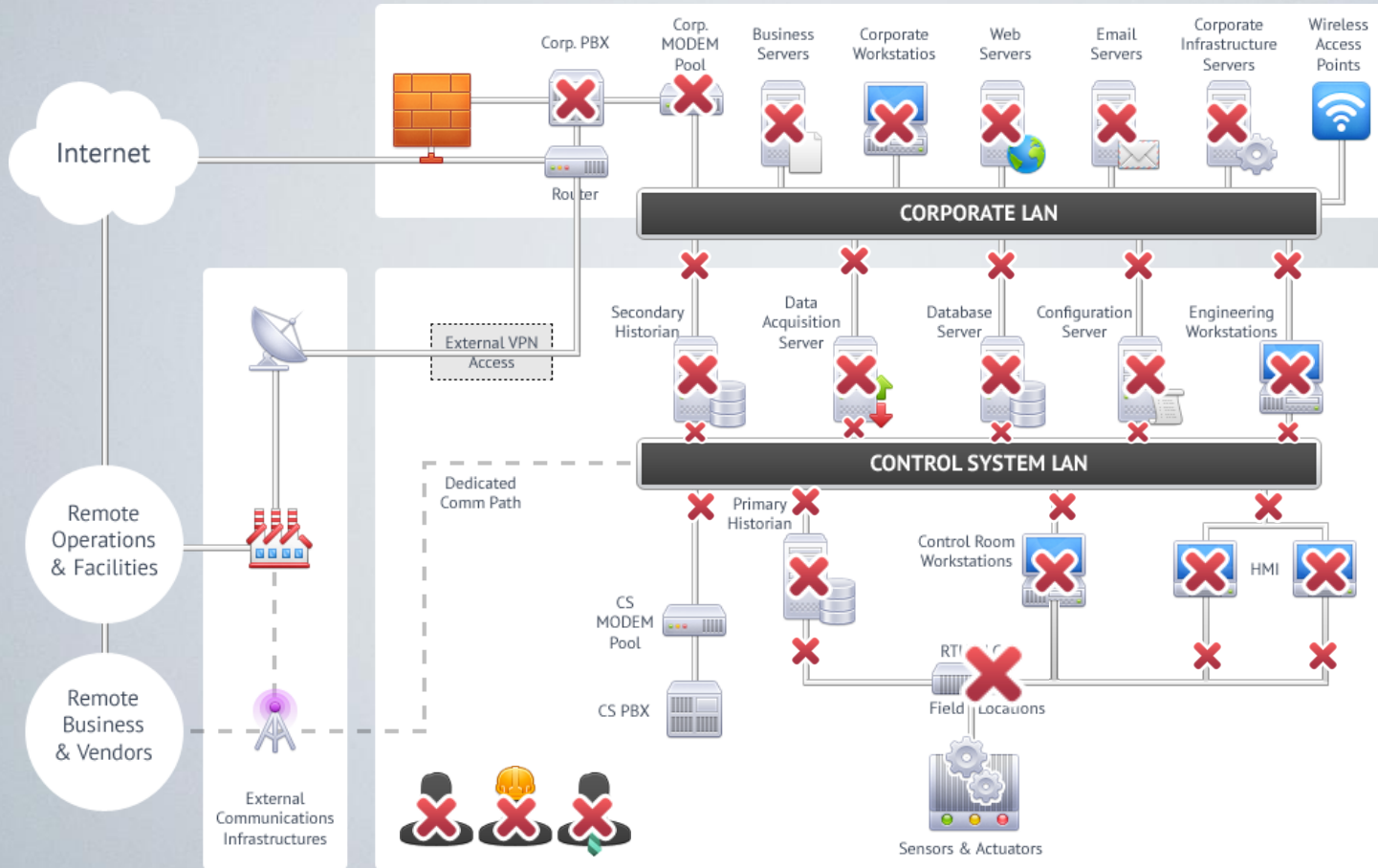
Personnel “vulnerabilities”

Former Employees Are Identified as Sources of Recent Cyber-Attacks on Critical Infrastructures	http://voices.yahoo.com/former-employees-identified-as-sources-recent-10665979.html
Downsizing within corporations, has brought on high number of disgruntled employees or ex-employees. An internal attack could result from changes made to the system thru personal computers or PLC interfacing; a disgruntled employee can change settings, turn off motors or pumps, or implant a virus or worm.	http://cmu95752.wordpress.com/2012/04/11/are-scadax-systems-secured/
In 2000, former employee Vitek Boden release a million liters of water into the coastal waters of Queensland, Australia.	http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf
In 1992, former Chevron employee disabled it's emergency alert system in 22 states, which wasn't discovered until an emergency happened that needed alerting	http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf
Computers and manuals seized in Al Qaeda training camps full of SCADA information related to dams and related structures	http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

VULNERABLE

ICS components – a security point of view

US ICS-CERT (Defense in Depth): Cumulative scheme



- PLC – soft, hardware
- ICS software
- ICS protocols
- People
- Office Soft

What is the problem?

Since our goal is to improve a secure level of industrial control system, seems we have a problem
problem is very simple:

ICS does not have single trusted component at all

Possible solution

Step by step improve all and each system component to prepare excellent ICS

- how much resources do we need to employ?
- how much time do we need?

Do customers want to substitute their working but non secure systems with trusted one but not proved it works well?



Possible solution

Constantly research new vulnerabilities and quickly offer adequate countermeasures

- such an approach requires customers to continuously update the IT environment
- with such a reactive approach what is the price of a single unprotected vulnerability?

Are customers willing to jeopardize their systems with a continuously changing control environment?



POSSIBLE

Possible solution

Use simple and trusted unit to monitor all interactions in regular ICS network

- use it as trusted base to build complex trusted systems

Do customers want to improve the security of their functioning systems without making significant changes?



Why KL thinks about secure OS

Simplified scheme of anti-malware battle

- bad guys:
 1. find vulnerability
 2. find a way how to exploit it
- good guys release a method to neutralize it

We always lag behind in this game

To be a leader we have to change game rules

New game rules – **new OS**

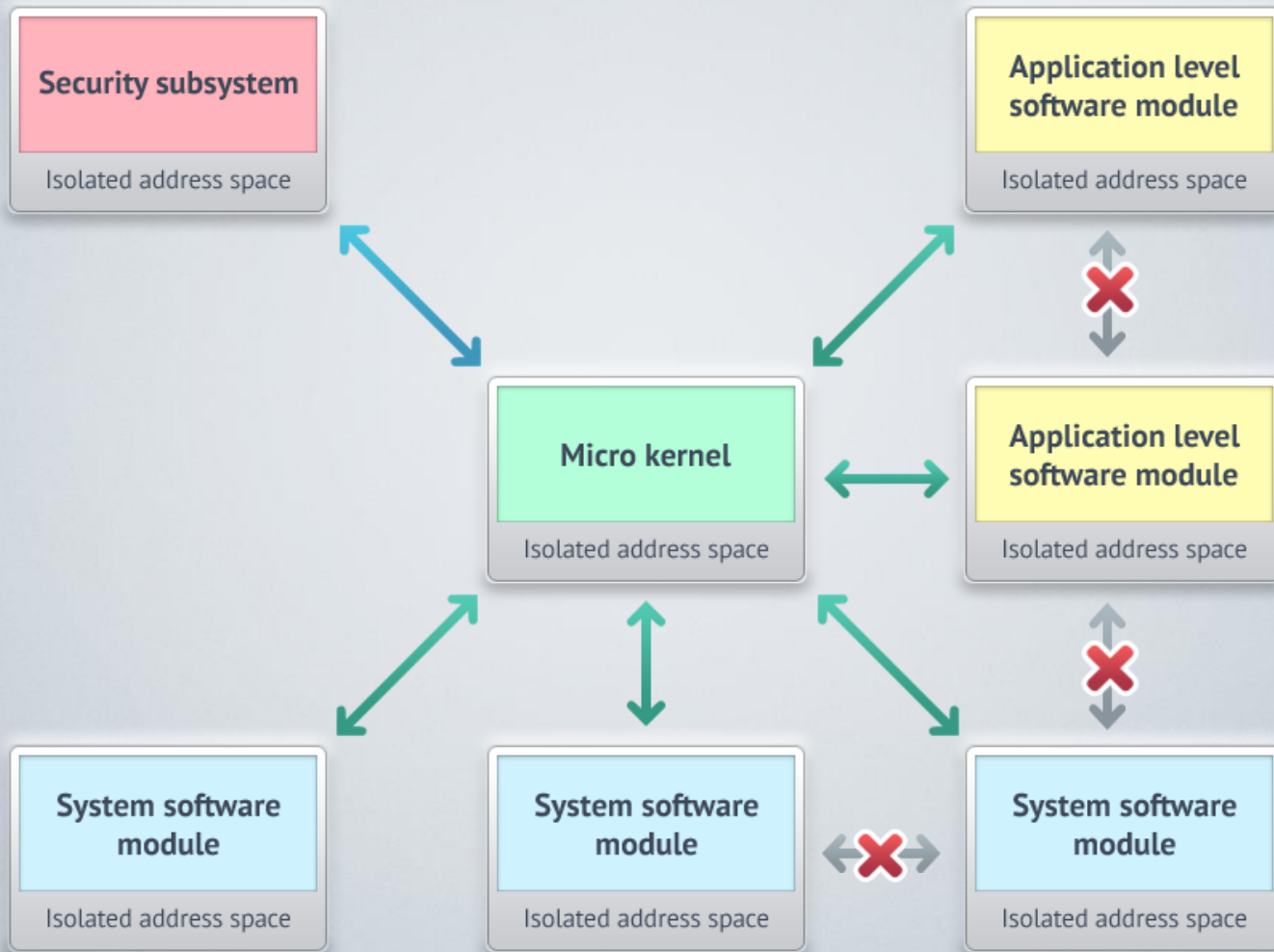
Secure OS

Now we at Kaspersky Lab have proprietary secure OS

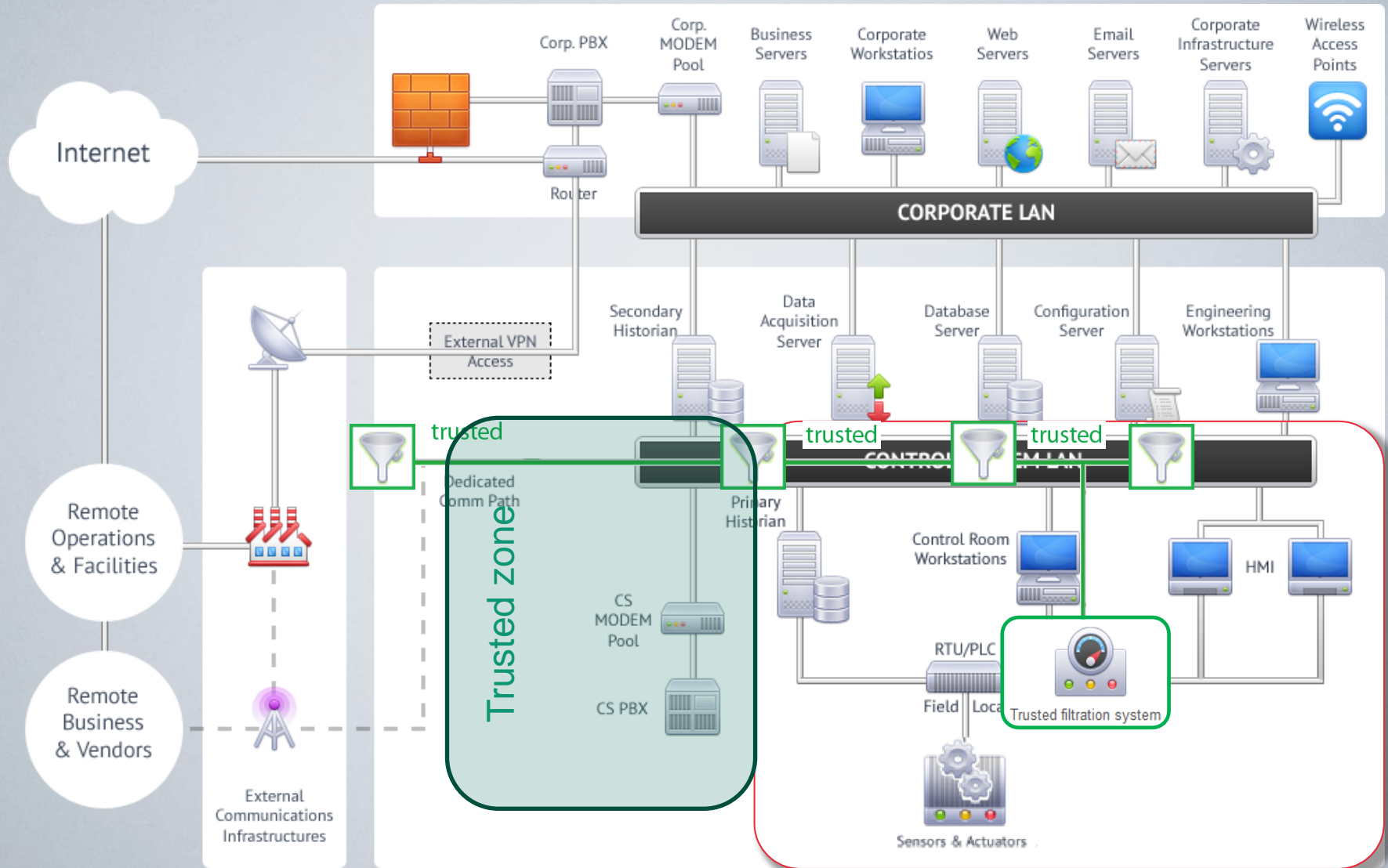
- developed “from scratch”
- developed with “security in mind”
- micro kernel architecture
- highly modular approach
- no direct or uncontrolled communications between any two modules, regardless of system or user level
- run any piece of software, both system and user level, in a secure sandbox with clear security rules
- behavior of any module is compared to the predefined scenario
- **guaranteed impossibility of run undeclared behavior**

Secure OS

Principles of OS architecture



Trusted filtration system prototype

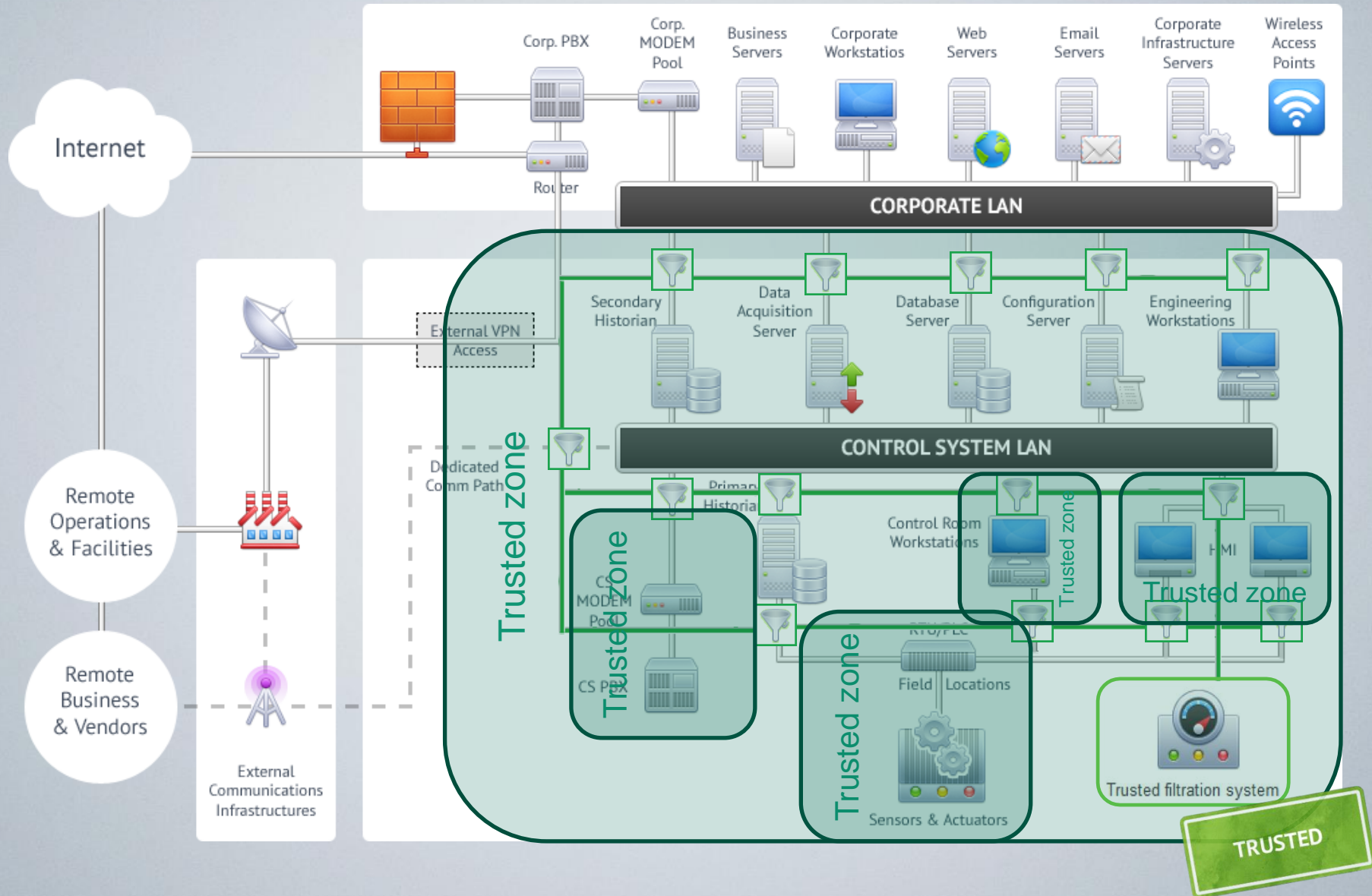


Trusted filtration system prototype features

Main purpose: to check if technological process remains in the boundaries of predefined behavior

- means for describe correct technological process
- logical devices with properties and limitations
- device grouping with limitations on the every level
- mapping the limits of technological process to the control information streams
- track the event chains
- customizable system of alerts and notifications

Trusted filtration system prototype



Thank you!

Questions ?

Andrey.Doukhvalov@kaspersky.com