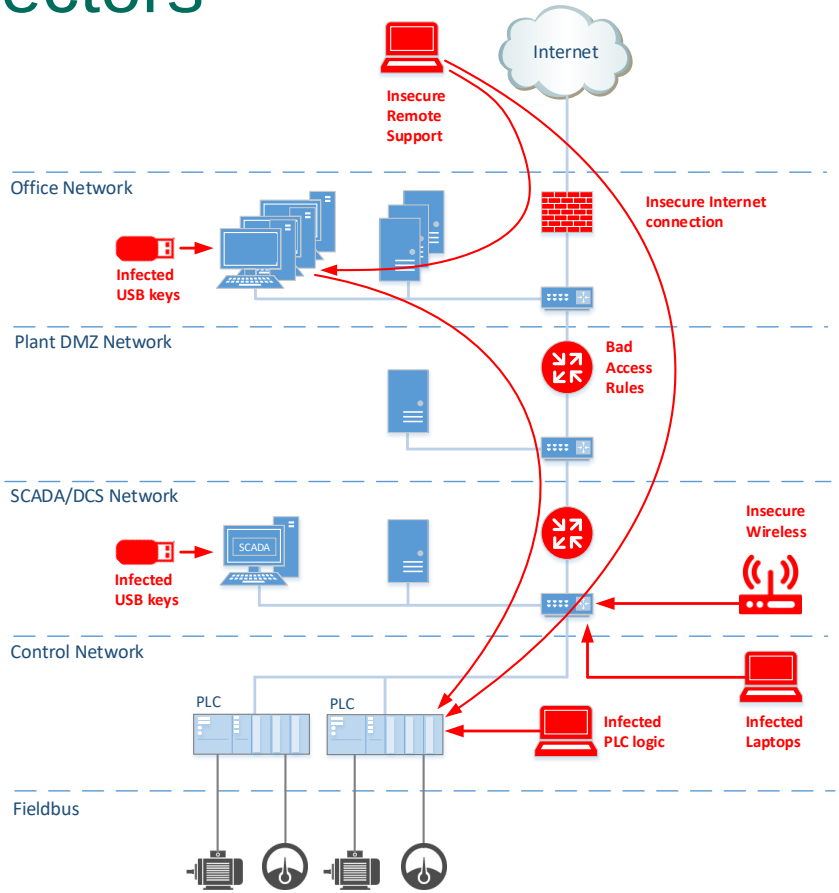
# Kaspersky Industrial CyberSecurity

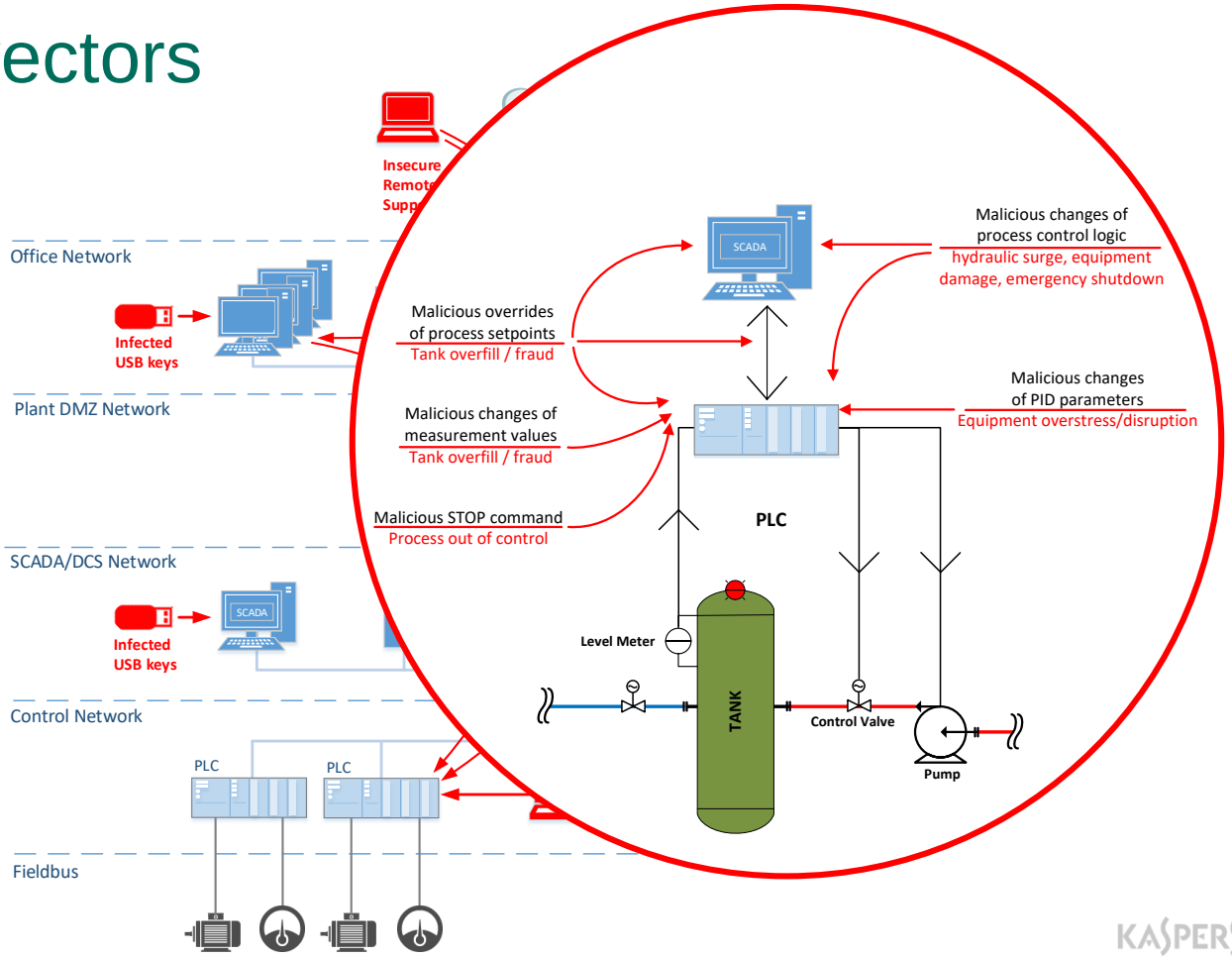
**Антон Шипулин**
*CISSP, CEH, CSSA*
Менеджер по развитию решений
по безопасности критической инфраструктуры
**Лаборатория Касперского**

KASPERSKY lab

# Cyberattack vectors



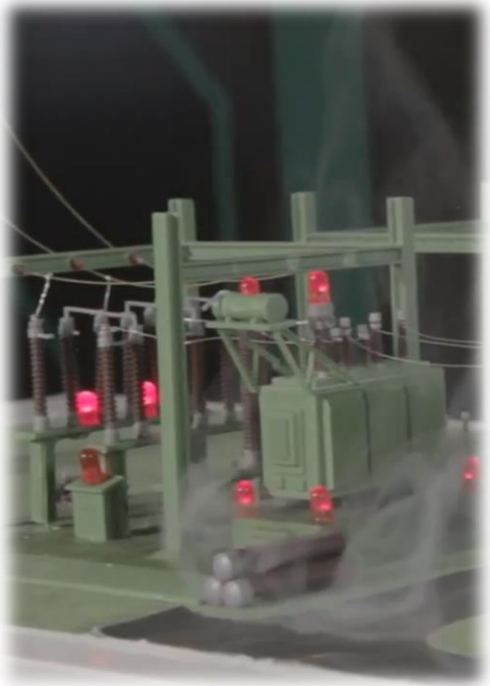
# Cyberattack vectors

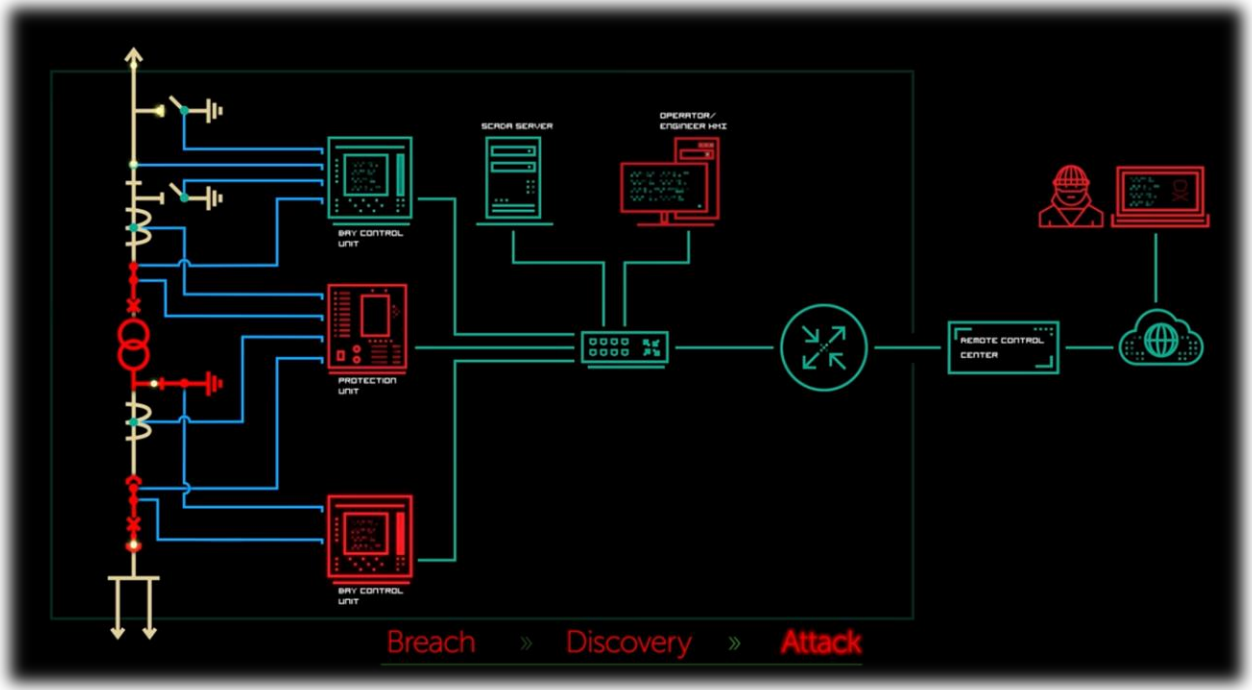




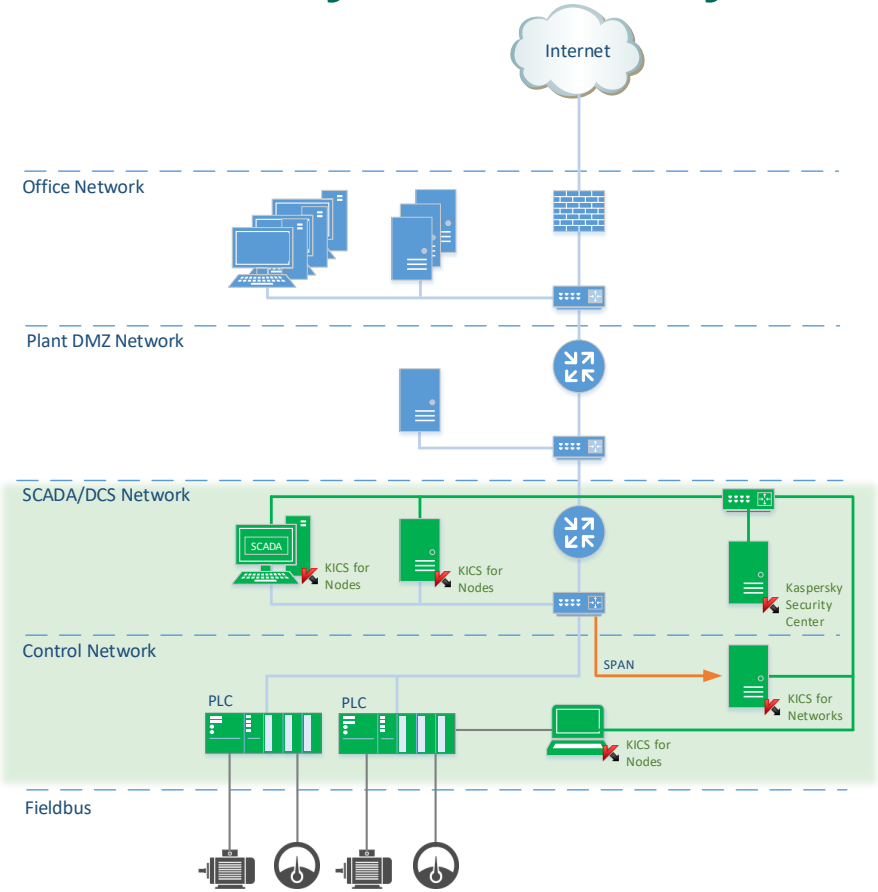

KASPERSKY lab

# Cyberattack vectors

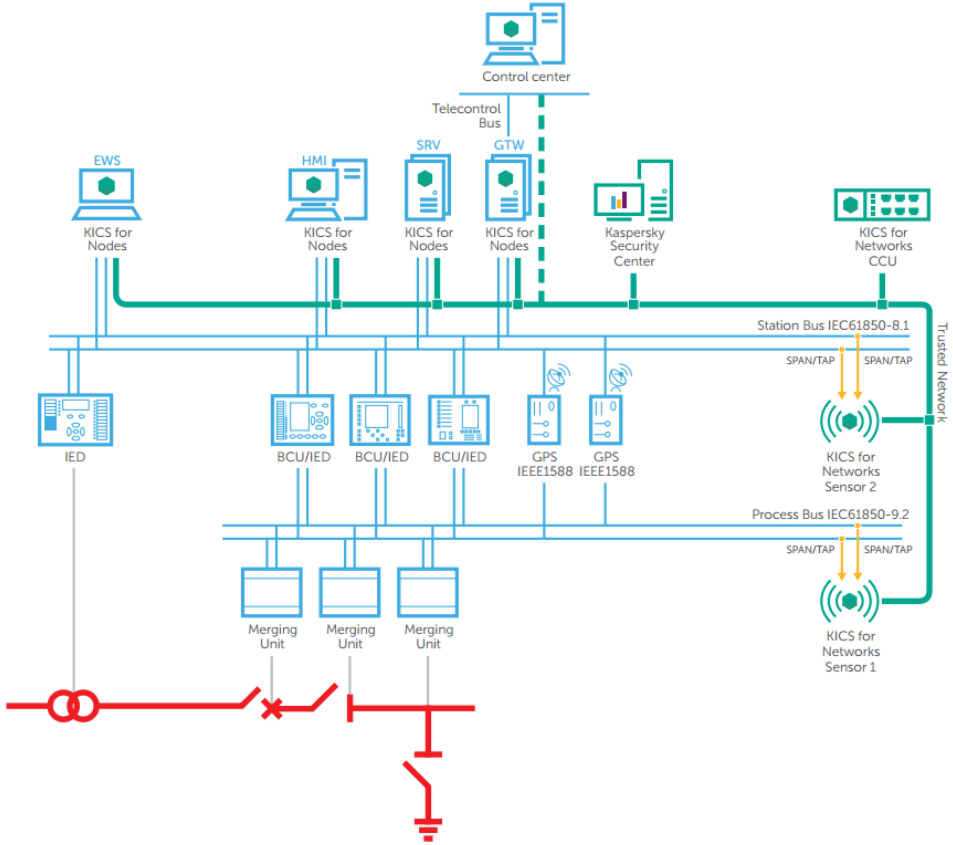




# Kaspersky Industrial CyberSecurity



# Kaspersky Industrial CyberSecurity (for Energy)



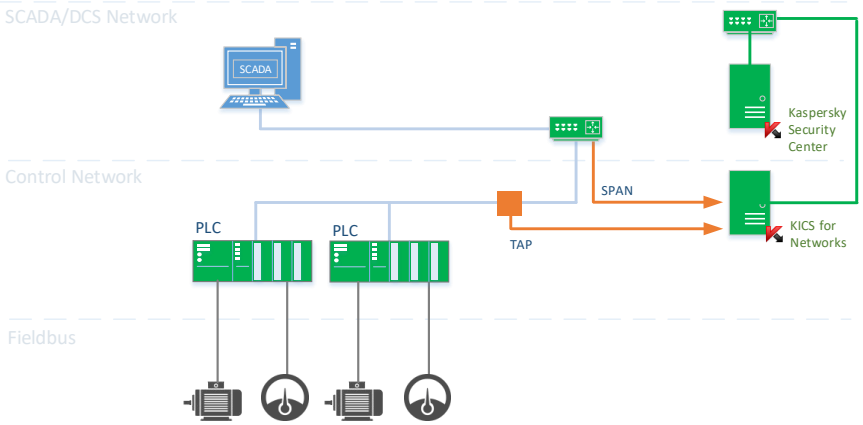
# Жизненный цикл атаки / Kill Chain

**Доступ / Access** ❯ **Разведка / Discovery** ❯ **Cyber-Physical Attack**

| Этап | Сценарий | Реагирование |
|---|---|---|
| Доступ / Access | • Зараженный USB device, модем, Wi-Fi адаптер<br>• Точка доступа в сеть: ноутбук, wireless access point<br>• Установка соединения, получение доступа в сеть | • Device control<br>• Application control<br>• Antimalware<br>• Network Integrity Control (WL)<br>• Intrusion Detection System |
| Разведка / Discovery | • Сканирование сети, поиск устройств и служб<br>• Подбор пароля к оборудованию<br>• Получение конфигурации, параметров и сбор трафика для изучения и планирования атаки | • Network Integrity Control (WL)<br>• Intrusion Detection System<br>• Process Integrity Control (DPI) |
| Cyber-Physical Attack | • Запись вредоносной программы ПЛК через локальное подключение<br>• Запись вредоносной программы ПЛК по сети<br>• Изменение параметра в памяти ПЛК<br>• Подмена параметров, команд в сетевом трафике<br>• Отправка вредоносных команд на ПЛК | • PLC Integrity Checker<br>• Network Integrity Control<br>• Intrusion Detection System (Whitelisting)<br>• Process Integrity Control (DPI) |

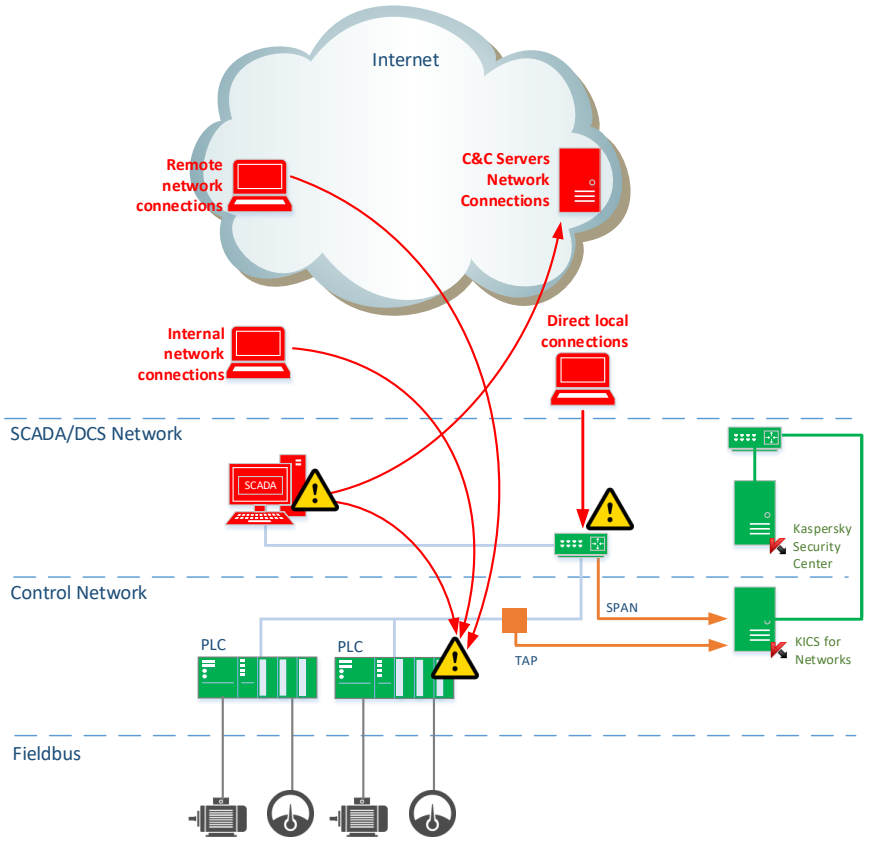
# KICS for Networks

- ► Software, Virtual or Hardware appliance
- ► Only passive / monitoring mode
  - Mirroring port connection (SPAN)
  - In-line connection (TAP)


# KICS for Networks

- Inventory network assets and communications
- Detect unauthorized hosts and communications
- Detect intrusions (IDS)
- Detect critical PLC commands (DPI)
- Control over the technological process parameters (DPI)
- Store and provide incident data for investigation



# KICS for Networks: Supported Industrial hardware

- Ethernet IEEE 802.3 link protocol
- Supported controllers and relays:
  - Siemens Simatic S7-300 series
  - Siemens Simatic S7-400 series
  - Siemens SIPROTEC 4 series
  - Schneider Electric Modicom M340
  - ABB Relion 670
  - Mitsubishi MELSEC-Q
  - Devices with the IEC 60870-5-104 protocols
  - Devices with the IEC 61850 protocols (MMS, GOOSE)
  - Allen-Bradley/ControlLogix 5571

---

  - GE RX3i, C60, B30
  - Emerson Delta – V
  - Schneider Electric Modicon M580
  - IED EKRA BE2704/243
  - Micom P645
  - SEL-421 SU,-401 U
  - … *

* The list can be extended at the customer's request

# PLC Commands Processing

Kaspersky Industrial CyberSecurity for Networks - network control is disabled. [conveyor*]

Manage security policy Settings Help

Process control | Configure events | Network control

Groups: 0, rules: 6, Lua scripts: 0, devices: 1, tags: 44, monitoring points: 1 Monitoring points Exclusions

Process control rules

Show groups Search by rules/scripts

Add group Add rule Add Lua script Remove

| Name | Contains | Description |
|---|---|---|
| Cycle_completed | | Process cycle completed |
| Process_Start | | Process start instruction from HMI |
| Process_Stop | | Process stop instruction from HMI |
| Process_Interlock_Disabled | | Responsible for the bulk transportation |

Device type: Siemens SIMATIC S7-300

Device name: Siemens SIMATIC S7-300

Events: Total: 32 Monitored: 26 Select events

Protocol: Siemens S7comm

Address: IP address: 192.168.0.2 Port: 102 Monitoring point mpoint

Additional address of the device

Traffic: 0 kbps Tags: 0 tag/s Network control is disabled. Network Integrity Control events are not registered.

Select events

- ISO 8073
  - CONNECT REQUEST
  - CONNECT CONFIRM
  - REJECT
  - REQUEST NOT FOUND
  - WRONG PACKET SIZE
  - WRONG PACKET FORMAT
  - UNKNOWN COMMAND
  - PARSING ERROR: UNKNOWN
  - PARSER: BUFFER NOT VALID
  - PARSER: EXCEPTION CAUGHT
- S7comm
  - START PLC
  - STOP PLC
  - TRANSFER PROJECT FROM PLC
  - TRANSFER PROJECT TO PLC
  - MEMORY CLEAR
  - INCORRECT PASSWORD
  - LIST PLC MEMORY BLOCKS
  - DELETE PLC MEMORY BLOCK
  - INSERT NEW PLC MEMORY BLOCK
  - WRONG CONFIGURATION
  - ERROR CODE
  - REQUEST NOT FOUND
  - RESPONSE AND REQUEST MISMATCH
  - INCOMPLETE TAG
  - REGISTER ADDRESS MISMATCH
  - WRONG PACKET SIZE
  - WRONG PACKET FORMAT
  - UNKNOWN COMMAND
  - UNKNOWN SUBCOMMAND
  - PARSING ERROR: UNKNOWN
  - PARSER: EXCEPTION CAUGHT
  - PARSER: BUFFER NOT VALID

OK Cancel

Kaspersky Industrial CyberSecurity for Net

us 05:30 PM

# PLC Command Detection

Kaspersky Industrial CyberSecurity for Networks - network control is disabled. [conveyor*]

Manage security policy Settings Help

KASPERSKY lab

Events: 1000 | Events history | Process parameters | Configure settings

| | | |
|---|---|---|
| 18:20:32.321 02-17-2017 | **Process Integrity Control:** | Protocol: S7comm. TRANSFER PROJECT TO PLC command detected |
| 18:20:32.351 02-17-2017 | **Process Integrity Control:** | Protocol: S7comm. WRONG PACKET FORMAT |
| 18:20:32.406 02-17-2017 | **Process Integrity Control:** | Protocol: S7comm. INSERT NEW PLC MEMORY BLOCK command detected |
| 18:20:30.167 02-17-2017 | **Process Integrity Control:** | Protocol: S7comm. LIST PLC MEMORY BLOCKS command detected |

**Event info**

Importance level: Critical
Category: Process Integrity Control
ID: 66804
Detected: 18:20:32.321 02-17-2017

Description:

TRANSFER PROJECT TO PLC command detected.
Protocol: S7comm
Device: Siemens SIMATIC S7-300
Source: MAC address: 00:0c:29:27:0d:1f; IP address: 192.168.0.30; Port: 49182
Destination: MAC address: 00:1b:1b:45:5c:09; IP address: 192.168.0.2; Port: 102
Monitoring point: mpoint

*PLC program changing attempt detected*

Event **not acknowledged** Acknowledge Close

**Traffic:** 1105 kbps **Tags:** 139 tag/s Network control is disabled. Network Integrity Control events are not registered.

Kaspersky Industrial CyberSecurity for Net us 06:21 PM



KASPERSKY lab

# Process Control Rules

Kaspersky Industrial CyberSecurity for Networks - network control is disabled. [conveyor*]

Manage security policy | Settings | Help

KASPERSKY lab

Process control | Configure events | Network control | Intrusion detection | Monitoring

Groups: 0, rules: 6, Lua scripts: 0, devices: 1, tags: 44, monitoring points: 1 | Monitoring points | Exclusions

**Process control rules**

Show groups | Search by rules/scripts

Add group | Add rule | Add Lua script | Remove

| Name | Contains | Description |
|---|---|---|
| Cycle_completed | | Process cycle completed |
| Process_Start | | Process start instruction from HMI |
| Process_Stop | | Process stop instruction from HMI |
| Process_Interlock_Disabled | | Responsible for the bulk transportation |
| Process_Interlock_Enabled | | Responsible for the bulk transportation |
| DRILLING_TIME_SETPOINT_OUT_OF_RANGE | | Drilling time setpoint out of specified range |

**Devices and tags**

Show tags: All | Search by tags

Import device | Add device | Add tag | Remove

| Name | Unit | Type | Address |
|---|---|---|---|
| 4S7 | | bool | I5.6 |
| 4S8 | | bool | I5.7 |
| Clock | | int8 | M10 |
| expired | | bool | M20.0 |
| SCADA_bit | | bool | M40.3 |
| Drill_time_setp... | | unsigned int16 | M30 |
| start | | bool | M40.0 |
| stop | | bool | M40.1 |
| IsWorking | | bool | M40.2 |
| Interlock | | int8 | M80 |
| Items_Produced | | unsigned int16 | M13 |
| Total_Drilling_T... | | unsigned int32 | M15 |

Edit

Traffic: 0 kbps | Tags: 0 tag/s | Network control is disabled. Network Integrity Control events are not registered.

Kaspersky Industrial CyberSecurity for Net | us | 05:28 PM



KASPERSKY lab

# Process Control Rules

Kaspersky Industrial CyberSecurity for Networks - network control is disabled. [conveyor*]

Manage security policy | Settings | Help

KASPERSKY lab

Process control | Configure events | Network control | Intrusion detection | Monitoring

Groups: 0, rules: 6, Lua scripts: 0, devices: 1, tags: 44, monitoring points: 1 | Monitoring points | Exclusions

**Process control rules**

Show groups | Search by rules/scripts

Add group | Add rule | Add Lua script | Remove

| Name | Contains | Description |
|---|---|---|
| Process_Interlock_Disabled | | Responsible for t... |
| Process_Interlock_Enabled | | Responsible for t... |
| DRILLING_TIME_SETPOINT_OUT_OF_RAN... | | Drilling time setp... |

**Devices and tags**

Show tags: All | Search by tags

Import device | Add device | Add tag | Remove

| Name | Unit of measure | Type | Addre |
|---|---|---|---|
| Interlock | | int8 | M80 |
| Items_Produced | | unsigned int16 | M13 |
| Total_Drilling_Time | | unsigned int32 | M15 |

TPOINT_OUT_OF_RANGE | Drilling time setpoint out of specified range

Condition: Out of range

Tag: Drill_time_setpoint | Read and write

Minimum: Constant | 2

Maximum: Constant | 5

Event: Process control rule violation: $ruleName

Code: 4000002900 Importance level: Critical

Title

Process control rule violation: **$ruleName**

Description

Process control rule violation: **$ruleName**. Values of tags: **$tags**.
Source: **$source**
Destination: **$destination**.
Monitoring point: **$monitoringPoint**.

Alert timeout: 0:00:05 Alert regenerate timeout: 8:00:00

Add condition | Add variable | Save and close | Reset changes

Traffic: 0 kbps Tags: 0 tag/s Network control is disabled. Network Integrity Control events are not registered.

Kaspersky Industrial CyberSecurity for Net | us | 05:26 PM



KASPERSKY lab

# Process Control Change Detection

Kaspersky Industrial CyberSecurity for Networks - network control is disabled. [conveyor]

Manage security policy Settings Help

KASPERSKY lab

Events: 1000 | Events history | Process parameters | Configure settings

| | | |
|---|---|---|
| 15:33:48.325 02-20-2017 | **Process Integrity Control:** | Process control rule violation: DRILLING_TIME_SETPOINT_OUT_OF_RANGE |
| 15:24:14.790 02-20-2017 | **Process Integrity Control:** | Protocol: S7comm. REQUEST NOT FOUND |
| 15:24:12.620 02-20-2017 | **Process Integrity Control:** | PROCESS_START_INSTRUCTION_DETECTED at PLC |
| 18:22:53.500 02-17-2017 | **Process Integrity Control:** | Protocol: S7comm. INCORRECT PASSWORD |

**Event info**

Importance level: Critical
Category: Process Integrity Control
ID: 66812
Detected: 15:33:48.325 02-20-2017

Description:
Process control rule violation: DRILLING_TIME_SETPOINT_OUT_OF_RANGE. Values of tags: tag: Drill_time_setpoint, value: 6.
Source: MAC address: 00:0c:29:79:fd:51; IP address: 192.168.0.4; Port: 49193
Destination: MAC address: 00:1b:1b:45:5c:09; IP address: 192.168.0.2; Port: 102.
Monitoring point: mpoint.

*Parameter value changing attempt detected*
*Mistakenly or intentionally (can cause product damage)*

Event **not acknowledged** Acknowledge Close

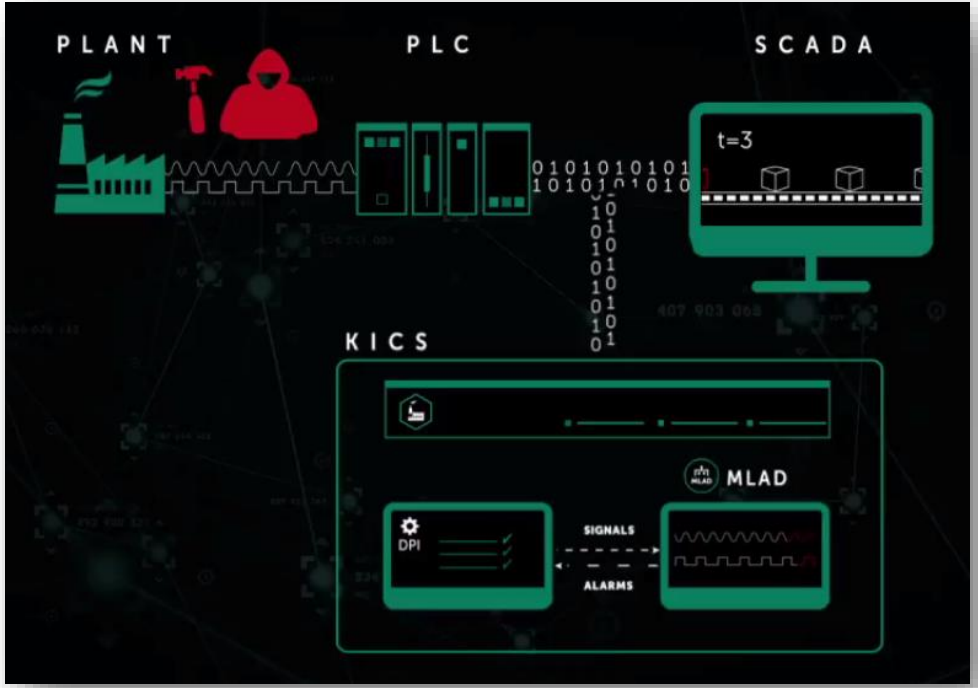
**Traffic:** 38 kbps **Tags:** 81 tag/s Network control is disabled. Network Integrity Control events are not registered.

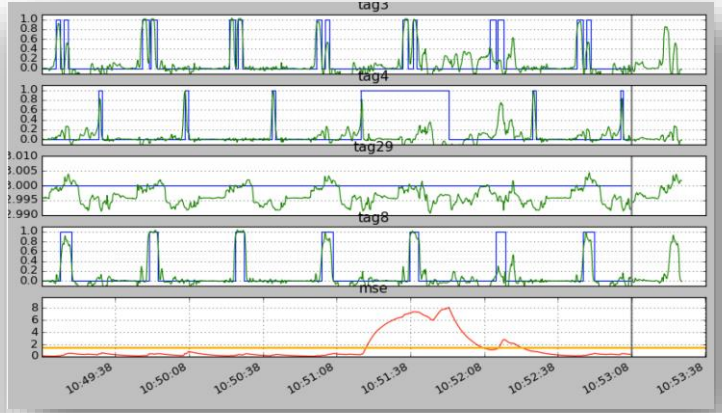
Attempt to start application Console | Kaspersky Industrial CyberSecurity for Net | us | 03:34 PM



KASPERSKY lab

# Machine Learning for a Baseline Profile




# Network Communication Whitelist / Inventory

Kaspersky Industrial CyberSecurity for Networks - network control is disabled. [conveyor*]

Manage security policy Settings Help

KASPERSKY lab

Process control | Configure events | **Network control** | Intrusion detection | Monitoring

**Network control: disabled** Enable Nodes: 10, protocols: 6, rules: 7. Enable learning mode Delete all rules TCP/UDP port numbers

Client nodes — Filter

| IP address | MAC address |
|---|---|
| 192.168.6.2 | 00:0C:29:23:D7:AE |
| 192.168.23.2 | 00:0C:29:3D:3F:D3 |
| 192.168.221.5 | 00:0C:29:64:D6:85 |
| 192.168.23.5 | 00:0C:29:64:D6:8F |
| 192.168.22.2 | 00:0C:29:88:5B:26 |
| 192.168.6.5 | 00:0C:29:C4:03:66 |
| 192.168.220.5 | 00:0C:29:C8:79:1B |
| 192.168.22.5 | 00:0C:29:C8:79:2F |
| 192.168.220.10 | 00:1B:1B:30:A4:AF |
| 192.168.221.10 | 00:1B:1B:62:7A:7A |

Interactions — Filter

| Protocol | Ports |
|---|---|
| TCP | Any ↔ 102 |
| UDP | 138 ↔ 138 |
| TCP | 49424 ↔ 51310 |
| TCP | 58012 ↔ 51310 |
| TCP | 51310 ↔ 51945 |
| TCP | 58074 ↔ 52210 |

Server nodes — Filter

| IP address | MAC address |
|---|---|
| 192.168.6.2 | 00:0C:29:23:D7:AE |
| 192.168.23.2 | 00:0C:29:3D:3F:D3 |
| 192.168.221.5 | 00:0C:29:64:D6:85 |
| 192.168.23.5 | 00:0C:29:64:D6:8F |
| 192.168.22.2 | 00:0C:29:88:5B:26 |
| 192.168.6.5 | 00:0C:29:C4:03:66 |
| 192.168.220.5 | 00:0C:29:C8:79:1B |
| 192.168.22.5 | 00:0C:29:C8:79:2F |
| 192.168.220.10 | 00:1B:1B:30:A4:AF |
| 192.168.221.10 | 00:1B:1B:62:7A:7A |

Add known port | Add rule | Cancel selection

**Traffic:** 0 kbps **Tags:** 0 tag/s Network control is disabled. Network Integrity Control events are not registered.

Kaspersky Industrial CyberSecurity for Net us 05:33 PM



KASPERSKY lab

# Network Communications Detection

Kaspersky Industrial CyberSecurity for Networks [conveyor]

Manage security policy Settings Help

KASPERSKY lab

Events: 1000 | Events history | Process parameters | Configure settings

| | | |
|---|---|---|
| 15:44:22.54 02-20-2017 | **Network Integrity Control:** | Unauthorized network interaction detected via protocol: TCP |
| 15:44:22.55 02-20-2017 | **Network Integrity Control:** | Unauthorized network interaction detected via protocol: ICMP |
| 15:44:13.50 02-20-2017 | **Network Integrity Control:** | Unauthorized network interaction detected via protocol: TCP |
| 15:44:13.51 02-20-2017 | **Network Integrity Control:** | Unauthorized network interaction detected via protocol: ICMP |

**Event info**

Importance level: Important

Category: Network Integrity Control

ID: 66867

Detected: 15:44:22.54 02-20-2017

Description:

Unauthorized network interaction detected. Protocol: TCP.
Source: MAC address: 00:0C:29:79:FD:51; IP address: 192.168.0.4; Port: 51011.
Destination: MAC address: 00:1B:1B:45:5C:09; IP address: 35.38.134.12; Port: 8080.
Monitoring point: mpoint.

*External network connection detected*
*Possible botnet C&C server connection*

Event **not acknowledged**

Create network control rule | Acknowledge | Close

**Traffic:** 41 kbps **Tags:** 314 tag/s

Attempt to start application Console | Kaspersky Industrial CyberSecurity for Net | us | 03:44 PM

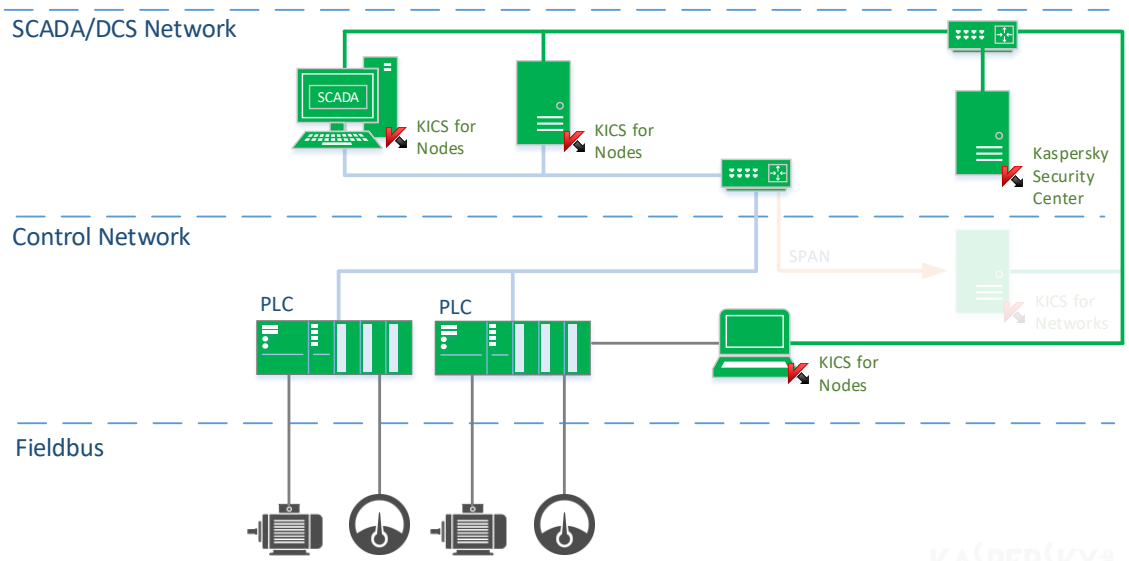


KASPERSKY lab

# KICS for Nodes: Technological Specifics

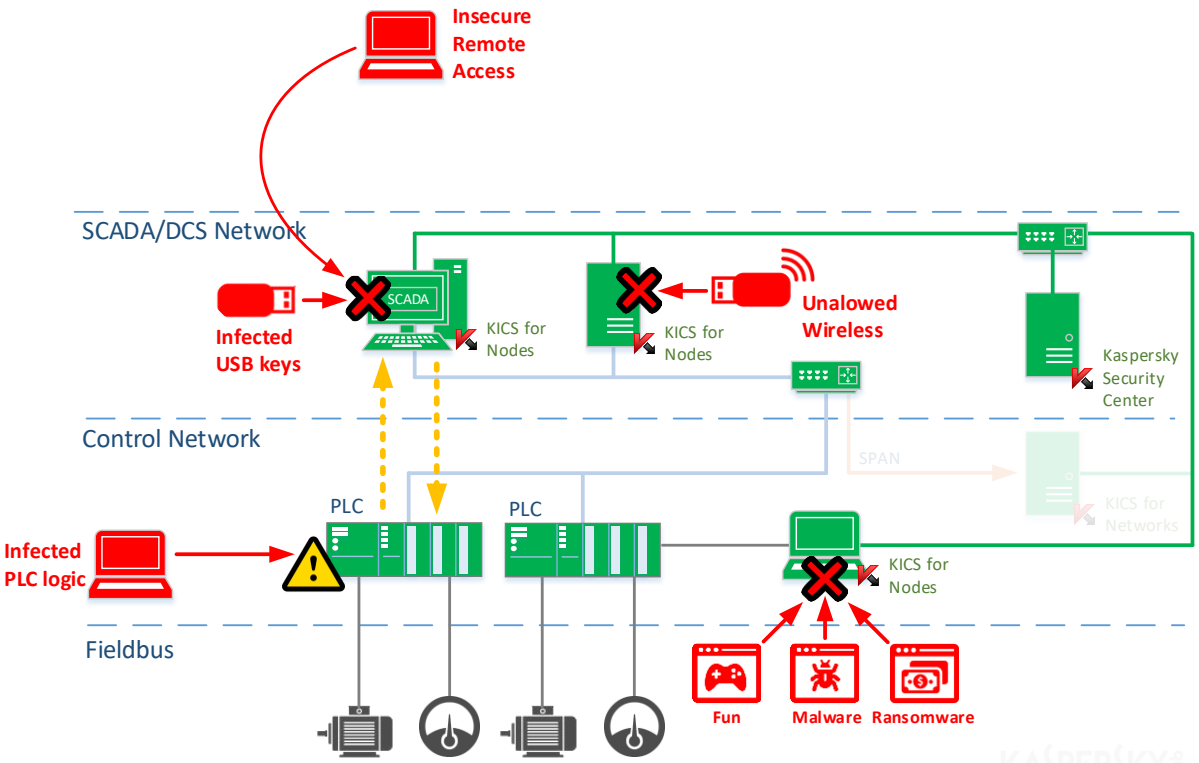
- A dedicated set of components [next slide]
- Computational load is reduced

  256-512 MB RAM on Windows XP SP2 / XP Embedded
- Monitoring mode
- For isolated environment (airgap)
- ICS vendors certification



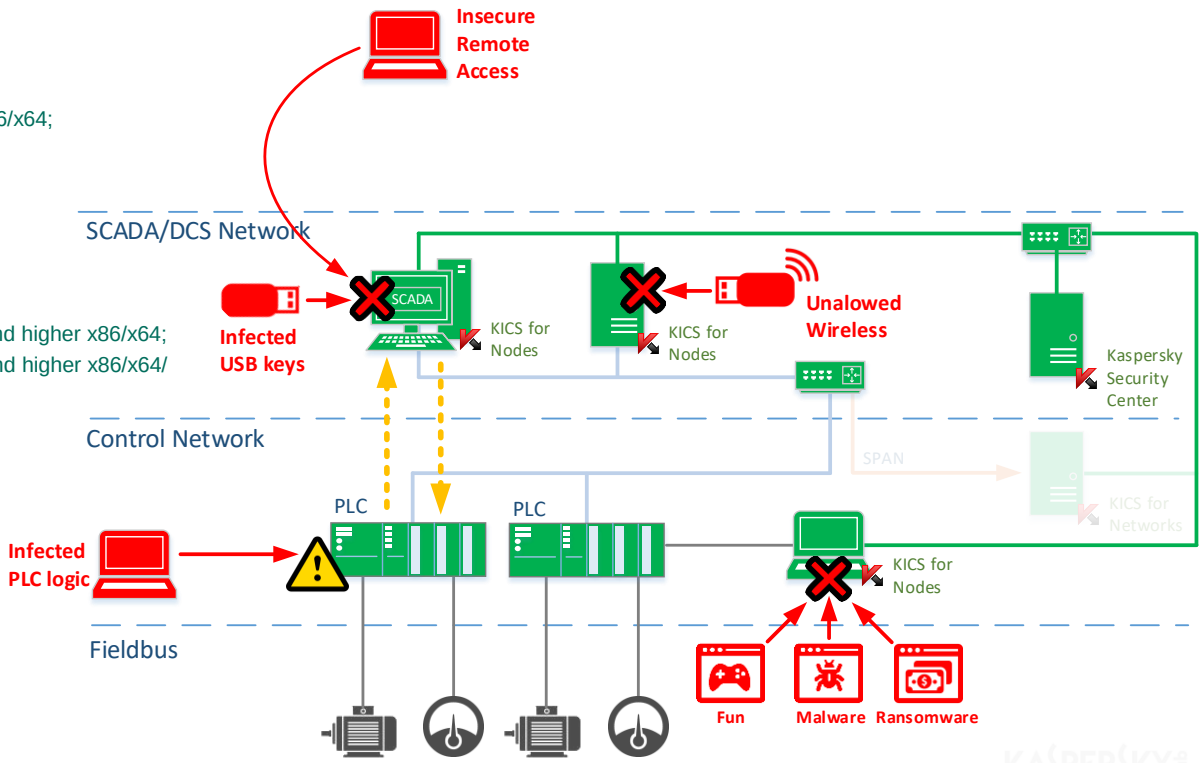
# KICS for Nodes

- Application Startup Control
- Device Control
- Antimalware Engine
- Anti-Cryptor
- Wi-Fi network control

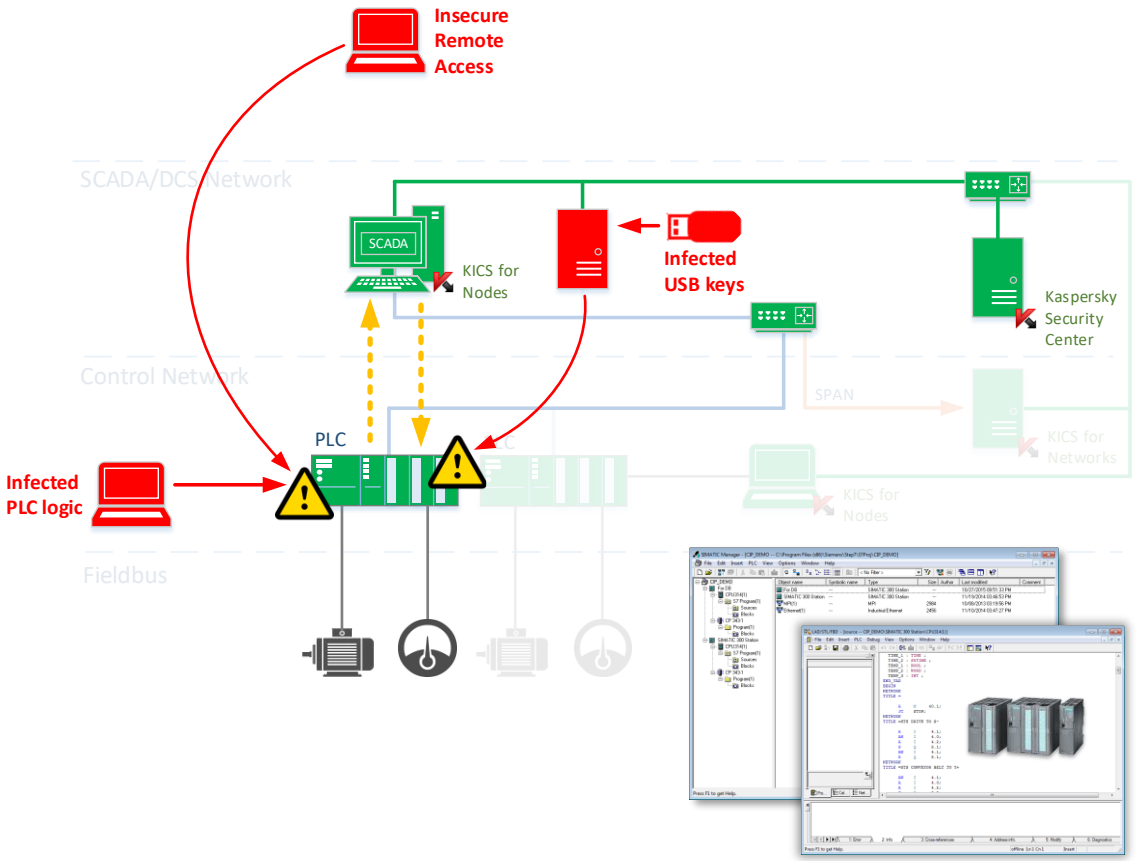


# KICS for Nodes: Supported OS

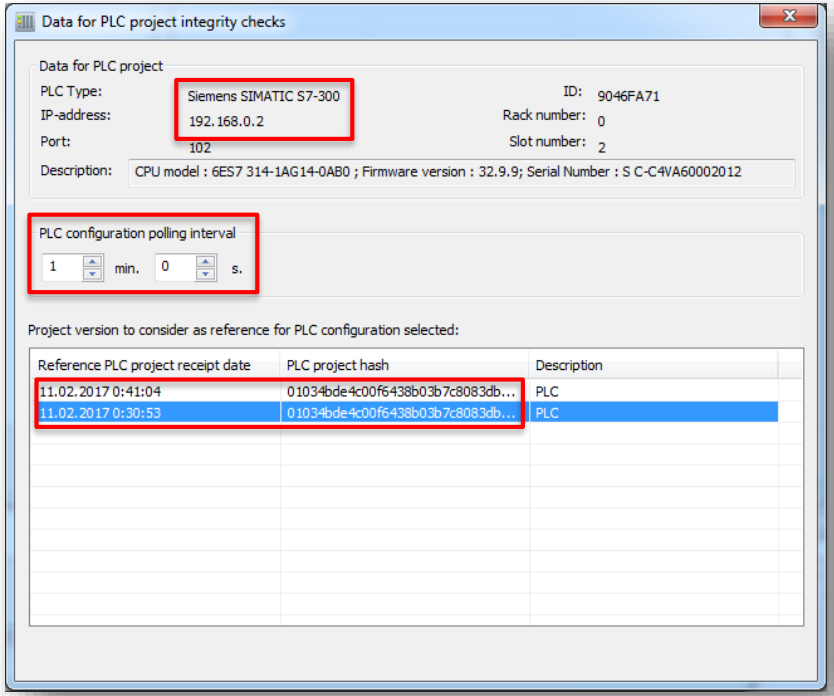
- Windows XP Professional with SP2 and higher x86;
- Windows Vista with SP 2 x86/x64;
- Windows 7 Professional x86/x64;
- Windows 7 Enterprise/Ultimate x86/x64;
- Windows 7 Professional with SP1 and higher x86/x64;
- Windows 7 Enterprise/Ultimate with SP1 and higher x86/x64;
- Windows 8 Pro x86/x64;
- Windows 8 Enterprise x86/x64;
- Windows 8.1 Pro x86/x64;
- Windows 8.1 Enterprise x86/x64.
- Windows 10 Pro x86/x64;
- Windows 10 Enterprise x86/x64.
- Windows Server 2003 Standard/Enterprise with SP1 and higher x86/x64;
- Windows Server 2003 Standard/Enterprise with SP2 and higher x86/x64/
- Windows Server 2008 Standard with SP1 and higher;
- Windows Server 2008 Enterprise with SP1 and higher;
- Windows Server 2008 R2 Standard;
- Windows Server 2008 R2 Enterprise;
- Windows Server 2008 R2 Standard with SP1;
- Windows Server 2008 R2 Enterprise with SP1;
- Windows Server 2012 x64;
- Windows Server 2012 R2 x64;
- Windows Server 2016.
- Windows XP Embedded x86;
- Windows Embedded Standard 7 x86/x64;
- Windows Embedded 8.1 Industry Pro x86/x64;
- Windows Embedded 8.0 Standard x86/x64.

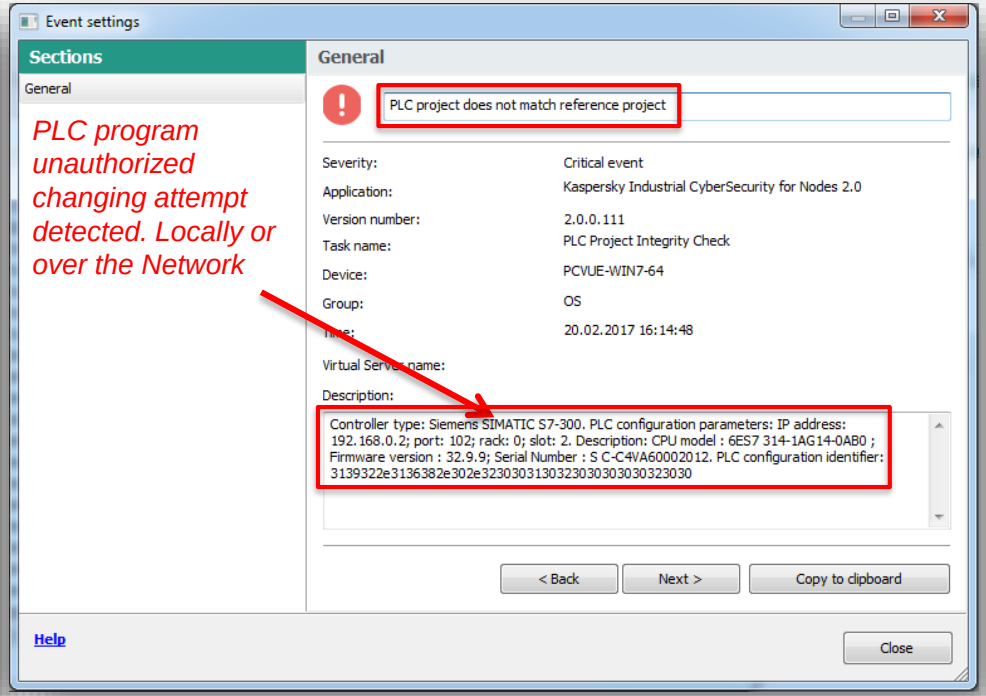


# PLC Integrity Check / Attack Detection



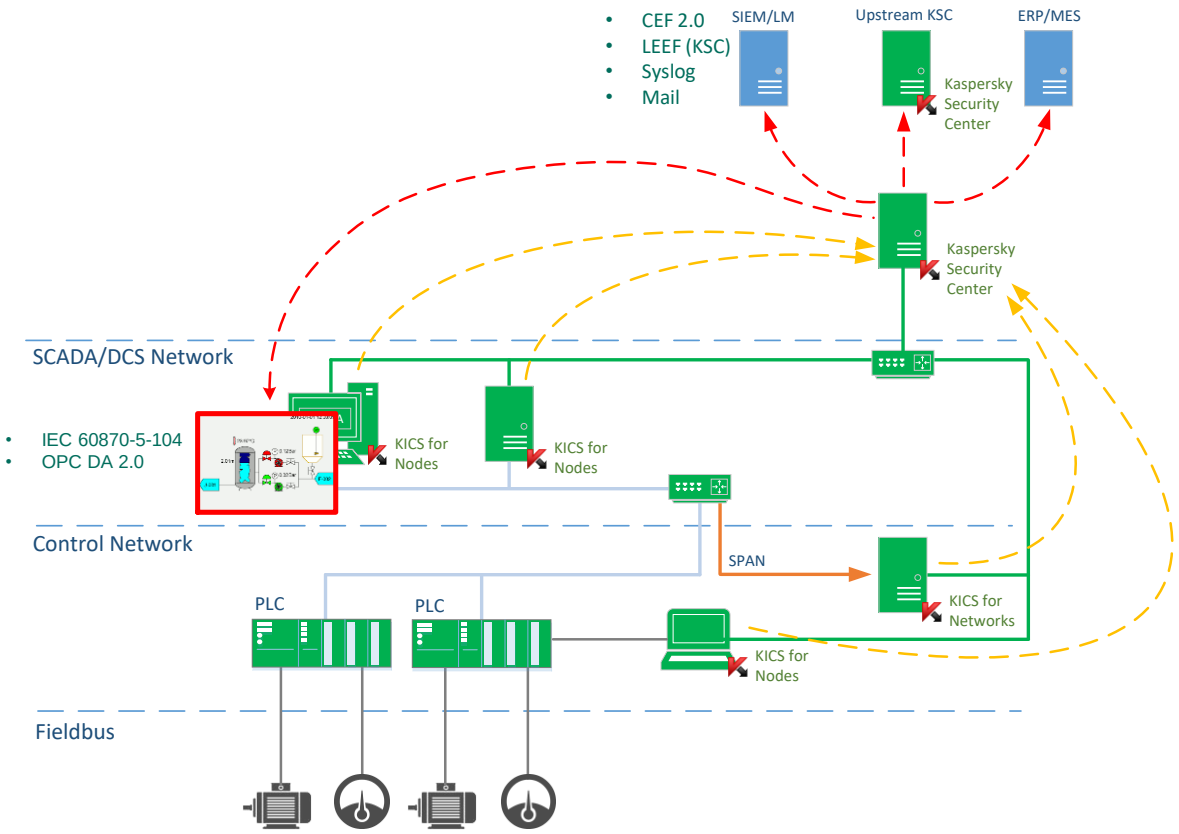
# PLC Project Integrity Checker



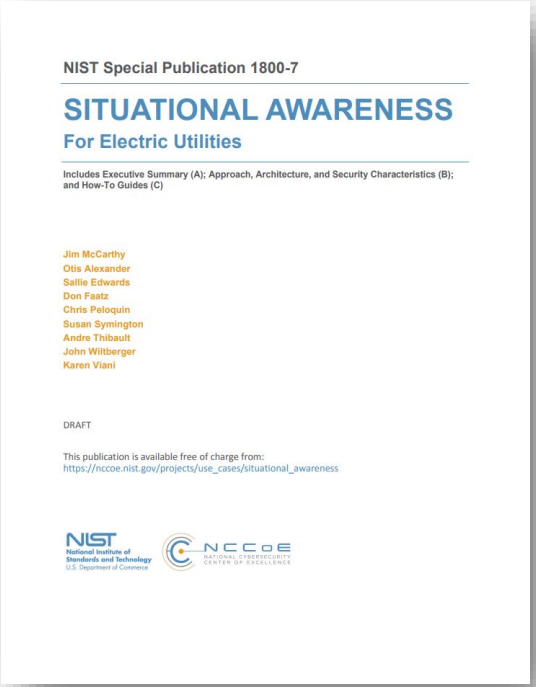




*PLC program unauthorized changing attempt detected. Locally or over the Network*

# KICS Integration



# Situational Awareness



NIST Special Publication 1800-7

SITUATIONAL AWARENESS

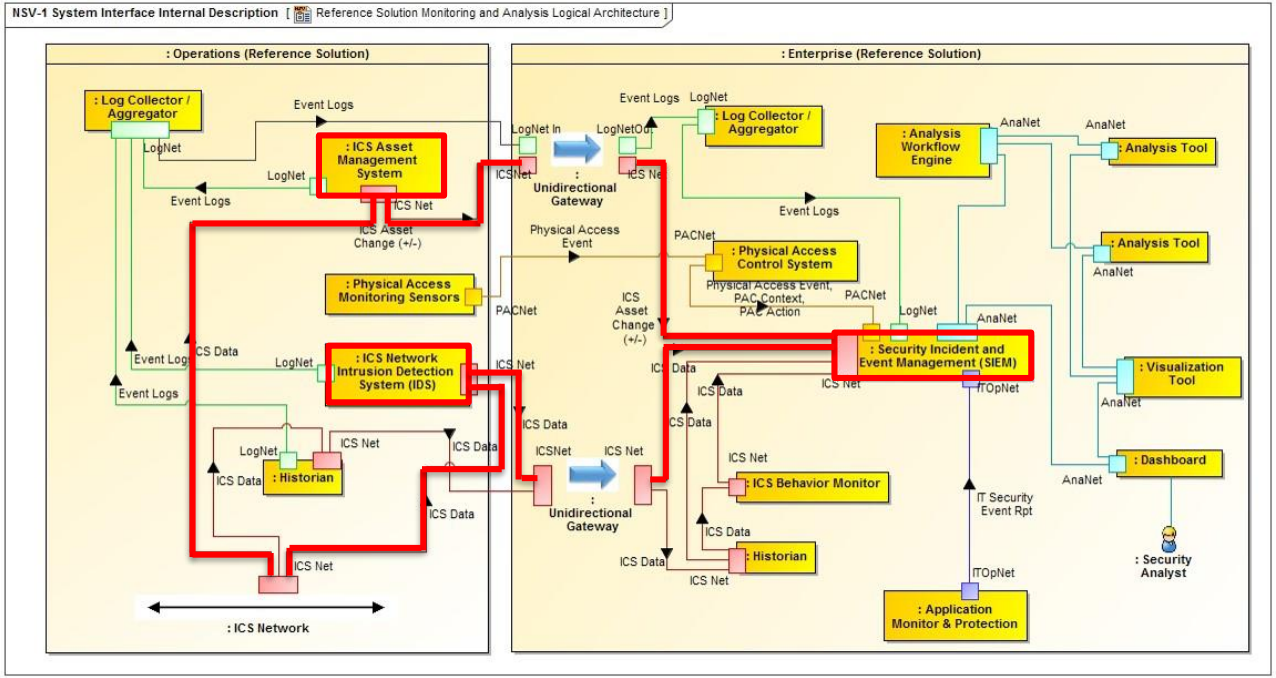
For Electric Utilities

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jim McCarthy
Otis Alexander
Sallie Edwards
Don Faatz
Chris Peloquin
Susan Symington
Andre Thibault
John Wiltberger
Karen Viani

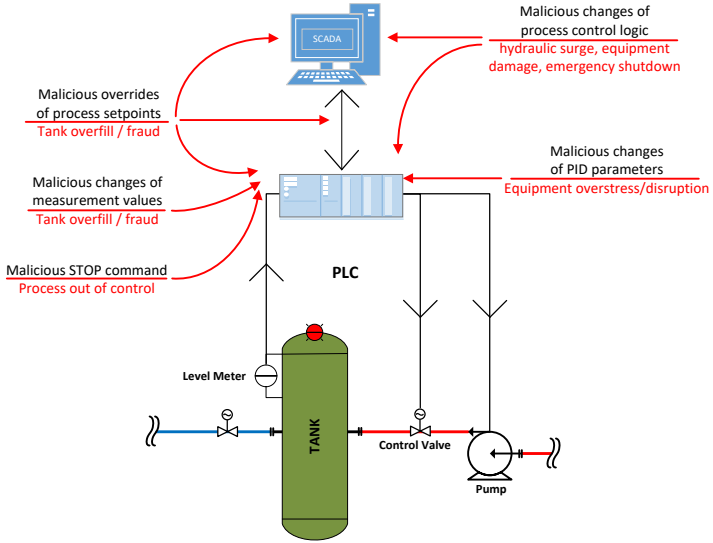
DRAFT

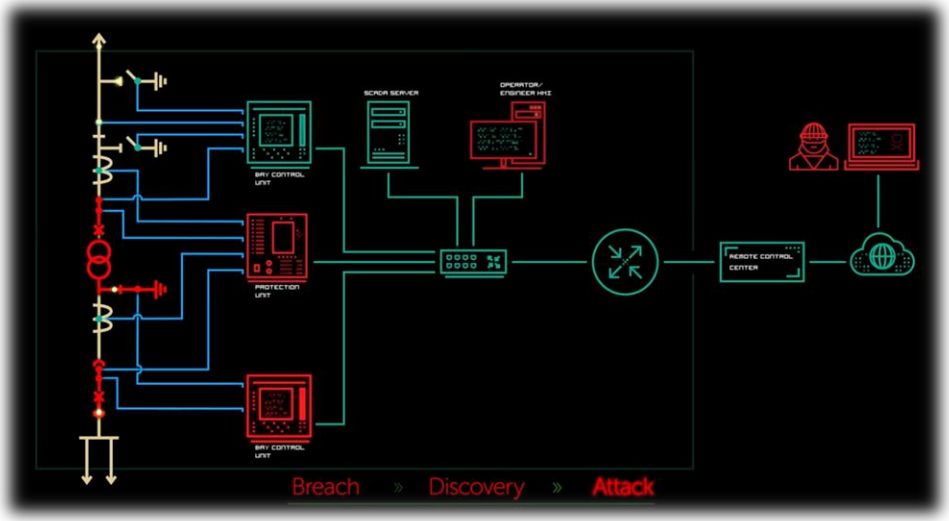
This publication is available free of charge from:
https://nccoe.nist.gov/projects/use_cases/situational_awareness




THE MOST INFAMOUS INDUSTRIAL CYBER ATTACKS
IRAN 2010: ONE STING TO PWN THEM ALL
CLANK!
CLANK!
GERMANY 2014: HACKERS GRIND MILL TO A HALT
DDOS!
UKRAINE 2016: WHO'S GOT THE POWER?
© 2017 AO Kaspersky Lab.
БУДЬ БДИТЕЛЕН!
СЛЕДИ ЗА ТЕМ, ЧТО ПРОИСХОДИТ В ПРОМЫШЛЕННОЙ СЕТИ!
ИСПОЛЬЗУЙ СОВРЕМЕННЫЕ СИСТЕМЫ МОНИТОРИНГА
И ВИЗУАЛИЗАЦИИ КИБЕРБЕЗОПАСНОСТИ
KASPERSKY lab
Kaspersky Industrial CyberSecurity
kaspersky.ru/ics
© АО «Лаборатория Касперского», 2017.
БУДЬ БДИТЕЛЕН И ЗОРОК!
ИСПОЛЬЗУЙ СРЕДСТВА МОНИТОРИНГА БЕЗОПАСНОСТИ
Й ИНФРАСТРУКТУРЫ,
ЗАПРЕЩЕНО:
3
Скачивать файлы из внешних источников в промышленную сеть
6
Загружать постороннее ПО на рабочие станции промышленной сети
9
Заряжать личные устройства через серверы и станции промышленной сети
KASPERSKY lab
© АО «Лаборатория Касперского», 1997 - 2016.

Доступ / Access ❯ Разведка / Discovery ❯ Cyber-Physical Attack






KASPERSKY lab

# Давайте обсудим?


**Антон Шипулин**

*CISSP, CEH, CSSA*

Менеджер по развитию решений по безопасности критической инфраструктуры

**Лаборатория Касперского**

Москва, Ленинградское шоссе, д.39А, стр.3

Т: (495) 797 8700 #1746

Anton.Shipulin@kaspersky.com

www.kaspersky.ru

https://ics.kaspersky.com

https://ics-cert.kaspersky.ru

KASPERSKY lab