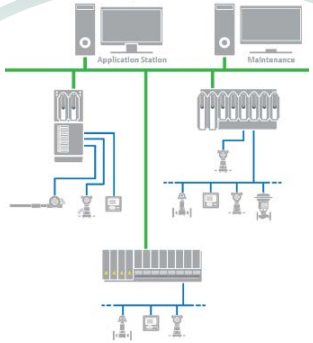
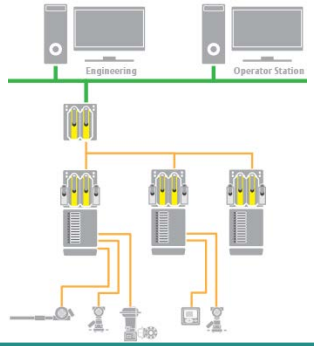

Kaspersky Industrial CyberSecurity
KASPERSKY lab

ТРАДИЦИОННЫЕ ПОДХОДЫ К КИБЕРЗАЩИТЕ СИСТЕМ УПРАВЛЕНИЯ





- **Изоляция сети управления от внешних информационных систем**
- **Сегментация сети**
- **Выделение демилитаризованных зон**

- **Составление правил и инструкций безопасной эксплуатации АСУ ТП**
- **Составление правил и инструкции соблюдения информационной безопасности в ИС АСУ ТП**

- **Использование системы аварийных блокировок**
- **Внедрение система противоаварийной защита**

KASPERSKY lab

GRAHAM CLULEY

award-winning computer security news, advice and opinion

58,7

СИСТЕМЫ БОЛЬШЕ НЕ

News Newsletter Videos Podcasts Speaking Sponsor About

This week's sponsor: Strong Customer Authentication and Risk Analysis under PSD2: how

Microsoft failed to properly patch the Stuxnet USB flaw in 2010... but has now (we hope)

Graham Cluley | March 11, 2015 2:20 am | Filed under: **Malware**, **Microsoft**, **Vulnerability**, **Windows**

2

52 SHARES

I'm sure you remember the notorious Stuxnet worm, used in a joint US/Israeli operation to disrupt activities at the Natanz uranium enrichment facility in Iran.

Besides its tailored attacks against SCADA equipment, meddling with Iranian nuclear centrifuges, Stuxnet was also an eye-opener for its use of zero-day vulnerabilities.

Because Stuxnet was capable of installing itself automatically (with no user interaction required) onto a fully-patched Windows computer from a USB memory stick, even if the user has disabled the Windows AutoRun and AutoPlay feature.

Xnet

ник в систему, преодолев «air gap»

2010

НТРОЛЯ НАД ИХ

JAPANTODAY

NATIONAL CRIME ENTERTAINMENT POLITICS BUSINESS TECH SPORTS WORLI

National

Monju power plant facility PC infected with virus

Jan. 7, 2014 | 03:35 pm JST | 25 Comments

TOKYO — A computer being used at the Monju prototype fast-breeder reactor facility in Tsuruga, Fukui Prefecture, was recently discovered to have contracted a virus, and officials believe that some data from the computer may have been leaked as a result.

According to the Japan Atomic Energy Agency, which operates the facility, the computer in question was being used by on-duty facility employees to file company paperwork when the virus was first detected on Jan 2, TBS reported Tuesday.

Officials said that around 3 p.m., the computer began corresponding with a suspicious outside site. Although the computer contained many company-sensitive emails, employee data sheets and training logs, officials said they do not believe any safety-compromising data was leaked, TBS reported.

It is believed that the computer was infected with the virus when a video playback program was attempting to perform a regular software update. Personnel are investigating the cause of the incident and are creating plans to avoid any such potential safety mishaps in the future, the Japan Atomic Energy Agency said.

odate

заразил узел ПТК
тности персонала

2014


ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
HOME
ABOUT
ICSJWG
INFORMATION PRODUCTS
TRAINING
FAQ
Control Systems
Home
Calendar
ICSJWG
Information Products
Training
Recommended Practices
Assessments
Standards & References
Related Sites
FAQ
Alert (IR-ALERT-H-16-056-01)
More Alerts
Cyber-Attack Against Ukrainian Critical Infrastructure
Original release date: February 25, 2016
Print
Tweet
Send
Share
Legal Notice
All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.
SUMMARY
On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malware was discovered on the companies' computer networks, however it is important to note that the role of BE in this event remains unknown pending further technical analysis.

ДРУГИЕ ПРИОРИТЕТЫ

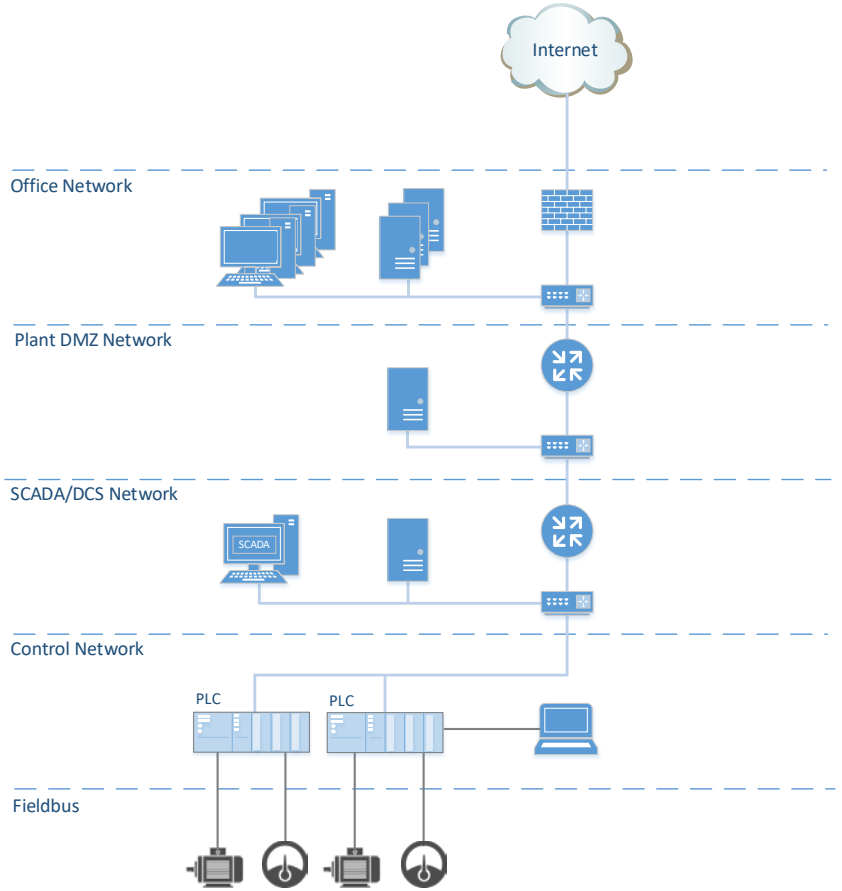
1. ДОСТУПНОСТЬ
2. ЦЕЛОСТНОСТЬ
3. КОНФИДЕНЦИАЛЬНОСТЬ

1. КОНФИДЕНЦИАЛЬНОСТЬ
2. ЦЕЛОСТНОСТЬ
3. ДОСТУПНОСТЬ

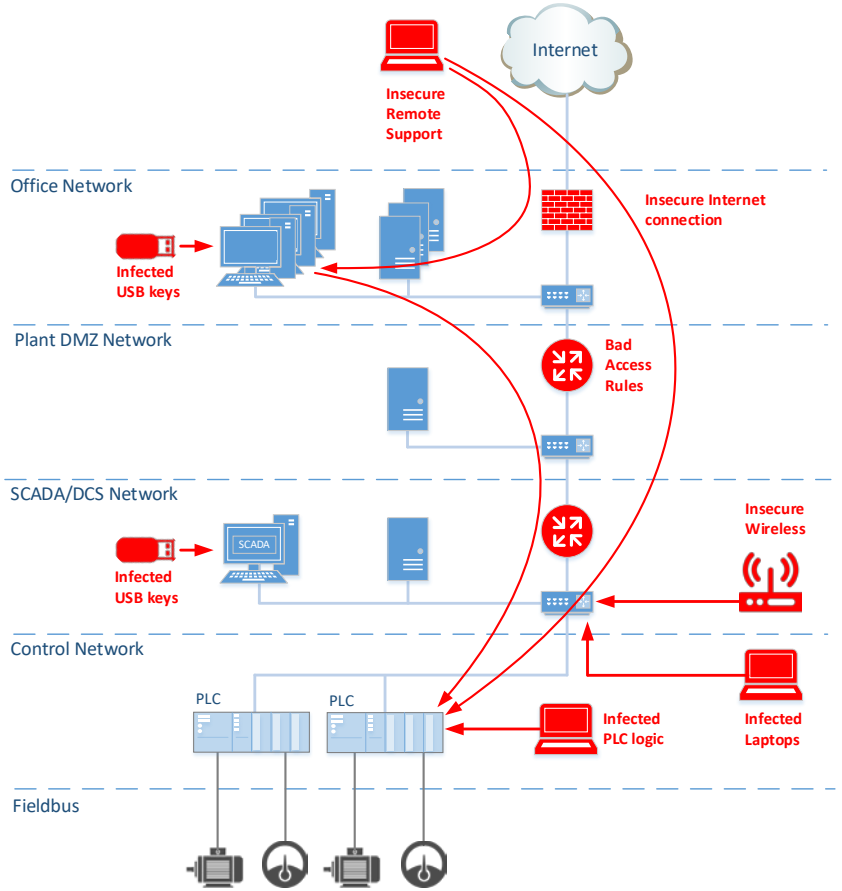
О РЕШЕНИИ

KASPERSKY INDUSTRIAL CYBERSECURITY: СТРУКТУРА РЕШЕНИЯ

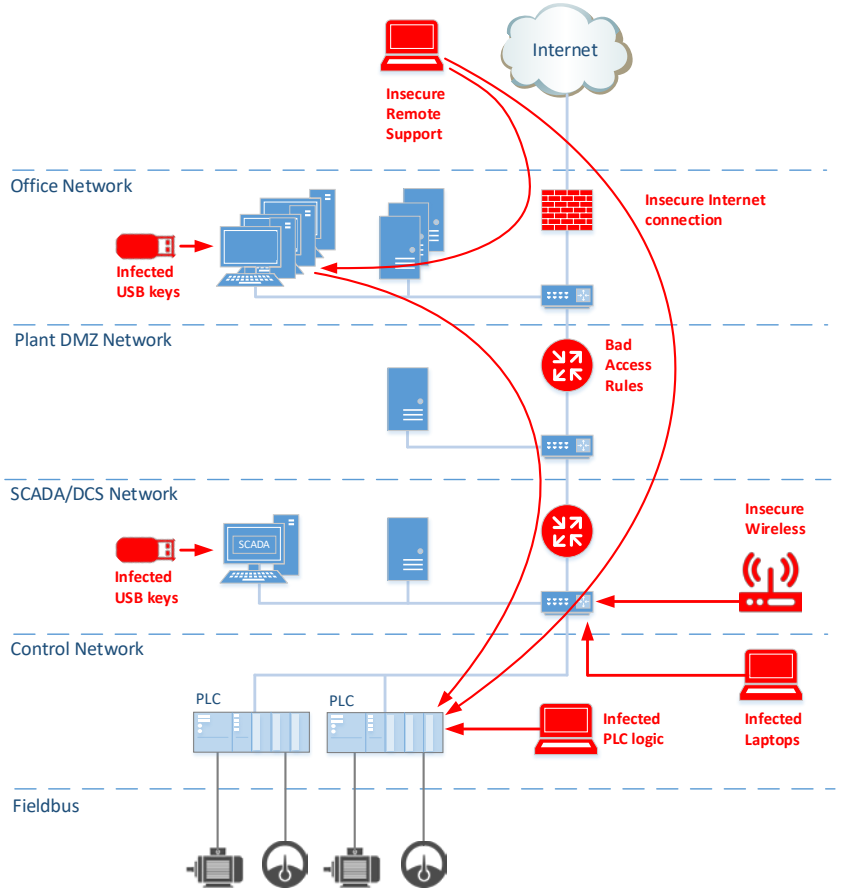
KASPERSKY INDUSTRIAL CYBERSECURITY



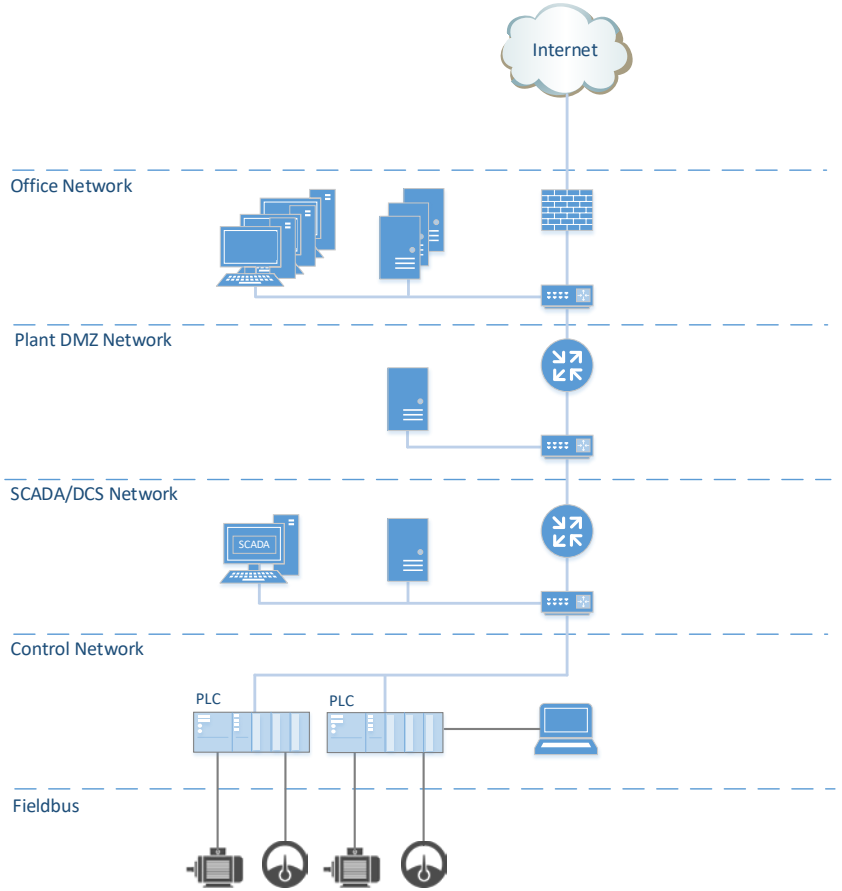
KASPERSKY INDUSTRIAL CYBERSECURITY



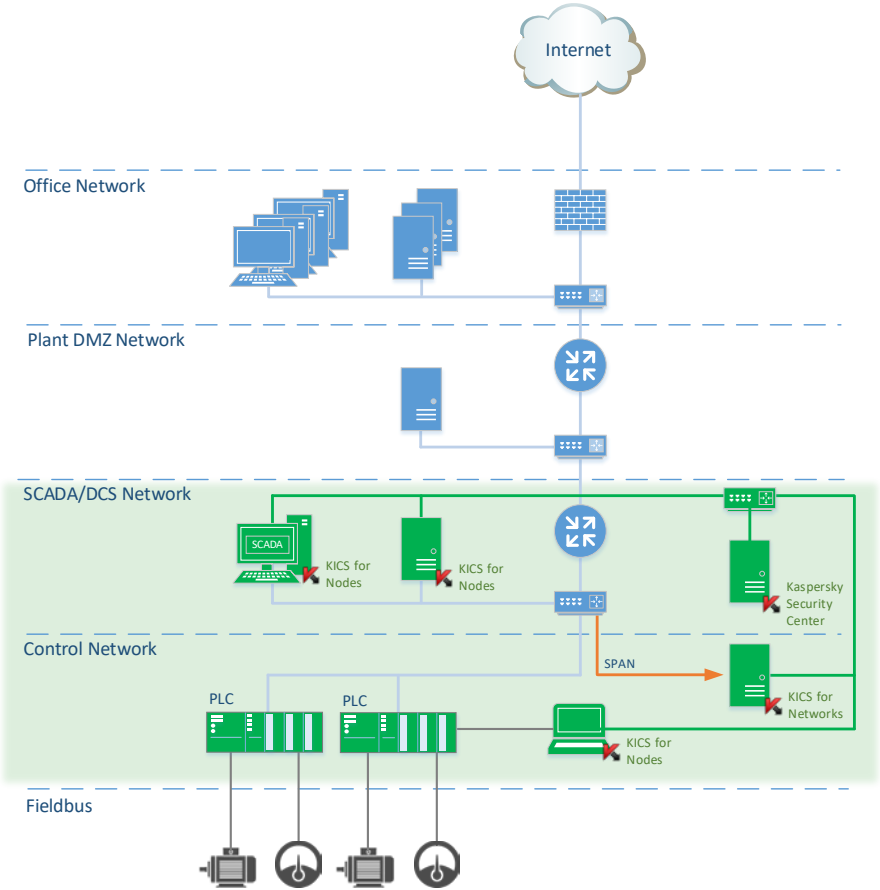
KASPERSKY INDUSTRIAL CYBERSECURITY



KASPERSKY INDUSTRIAL CYBERSECURITY



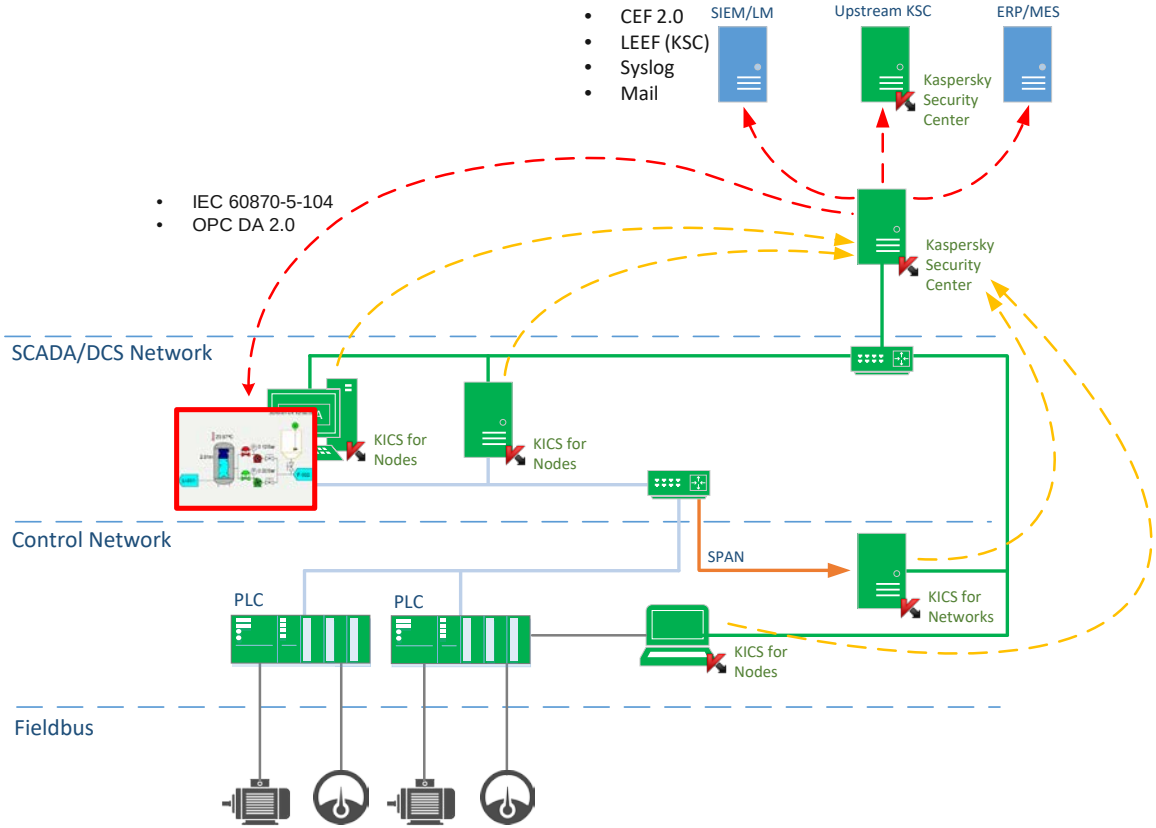
KASPERSKY INDUSTRIAL CYBERSECURITY



KASPERSKY lab

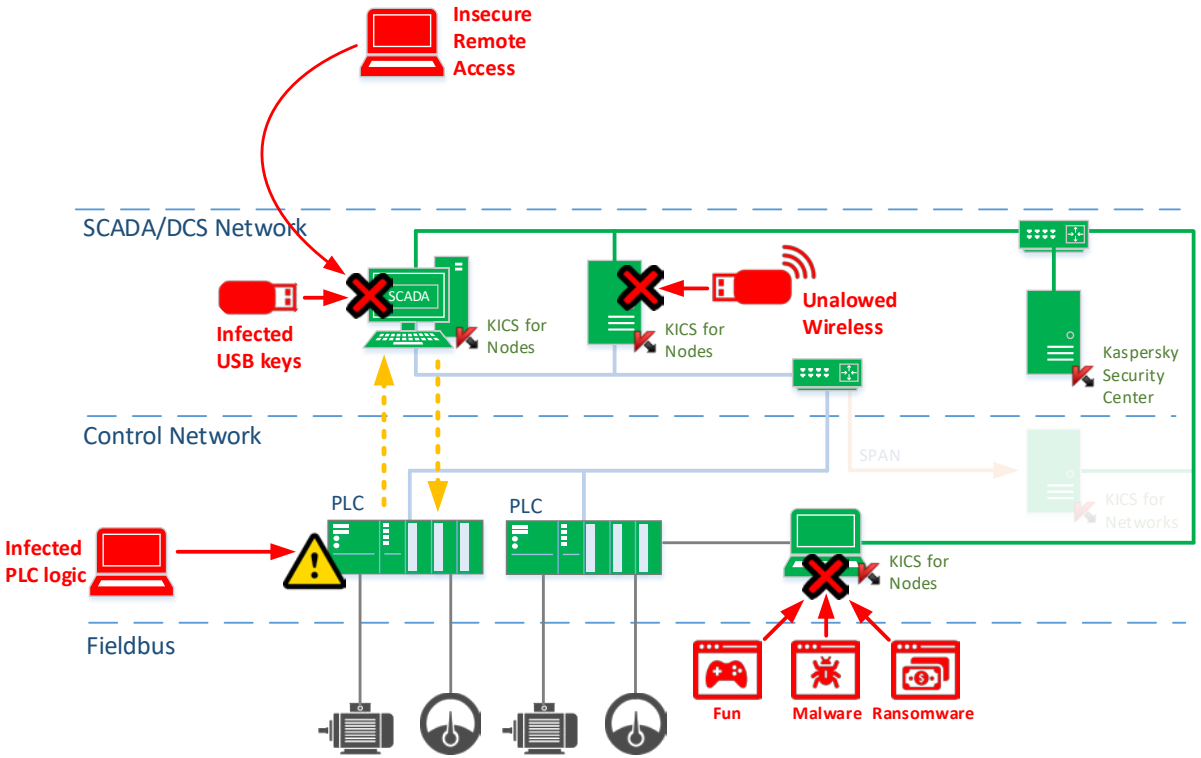
ФУНКЦИОНАЛЬНЫЕ КОМПОНЕНТЫ

KASPERSKY INDUSTRIAL CYBERSECURITY



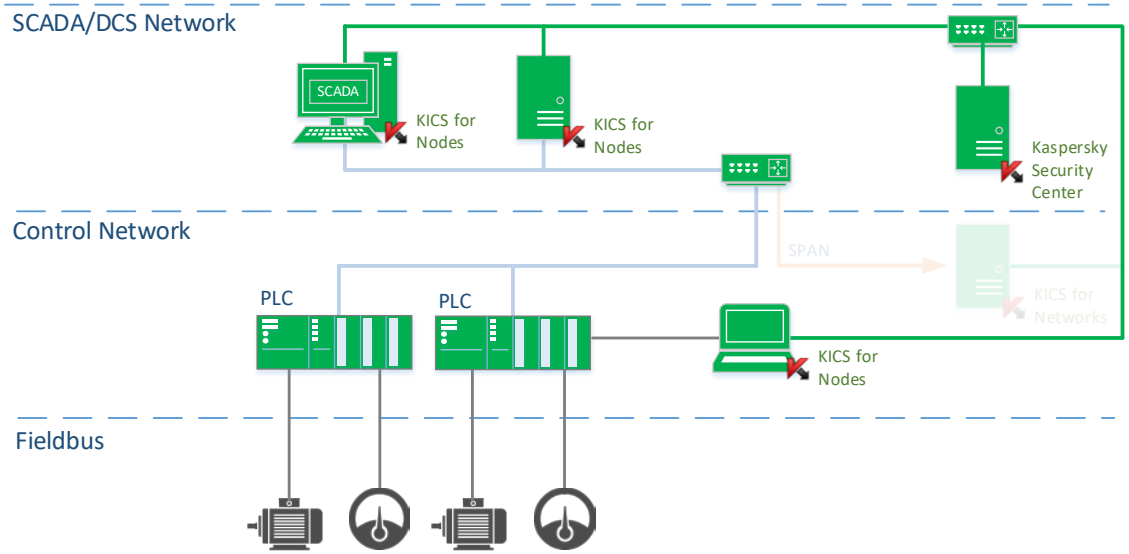
KICS FOR NODES

- Запрет по умолчанию
- Оценка уязвимостей
- Контроль устройств
- Контроль целостности ПЛК
- Режим высокой доступности
- Работает на SCADA-серверах, инженерных рабочих станциях и поддерживает HMI



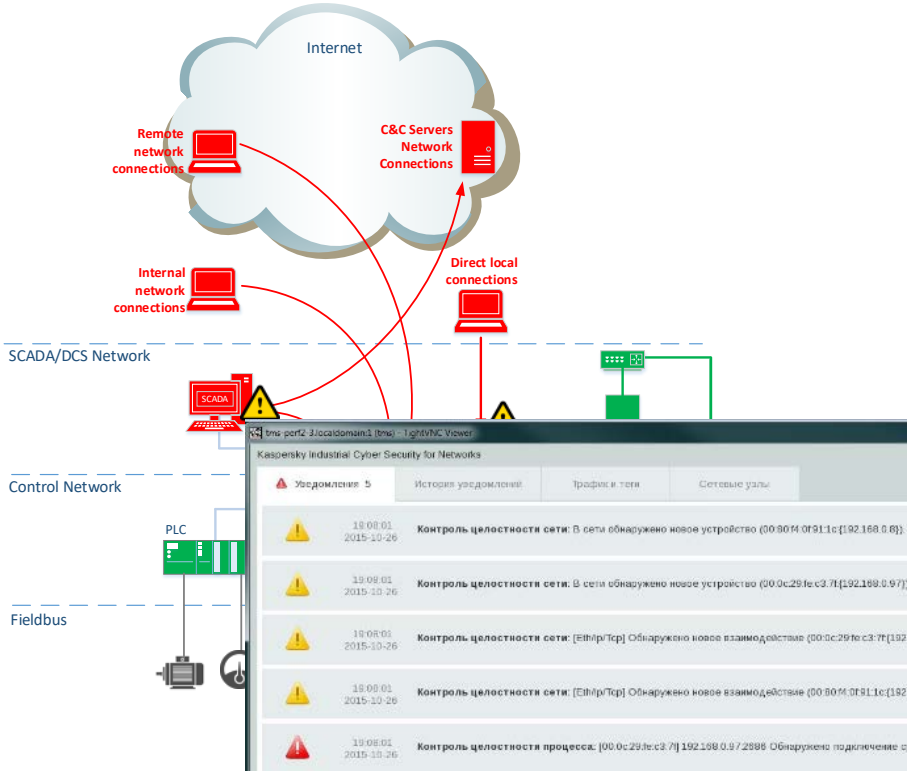
KICS FOR NODES: СПЕЦИФИКА ОТРАСЛИ

- Низкие требования к ПК, 256-512 MB RAM on Windows XP SP2 / XP Embedded
- Режим мониторинга
- Для изолированных сред
- Сертификаты совместимости с ICS вендорами
- Ограниченный набор компонентов



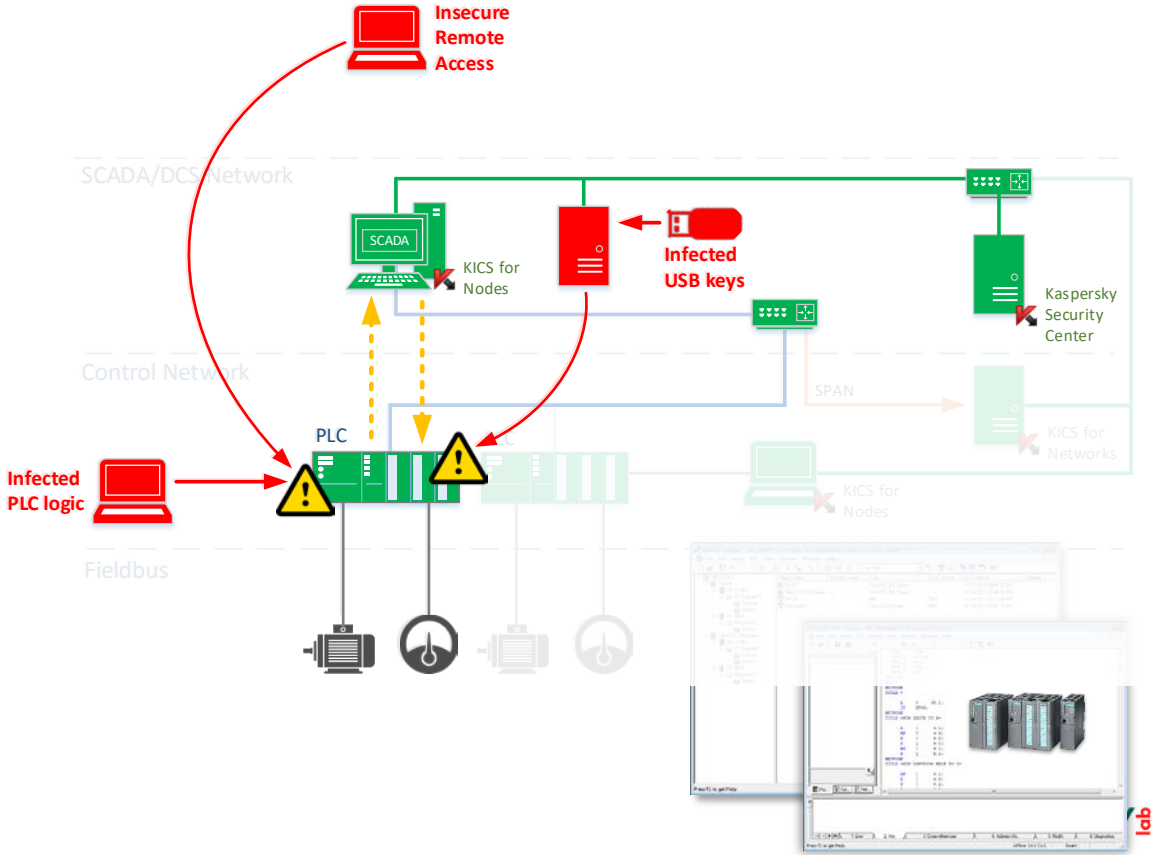
KICS FOR NETWORKS

- Контроль целостности сети (обнаружение новых устройств в промышленной сети)
- Обнаружение аномалий в технологических сетях
- Обнаружение управляющих команд, приводящих к нарушению технологического процесса
- Расследование, мониторинг и средство обнаружения инцидентов

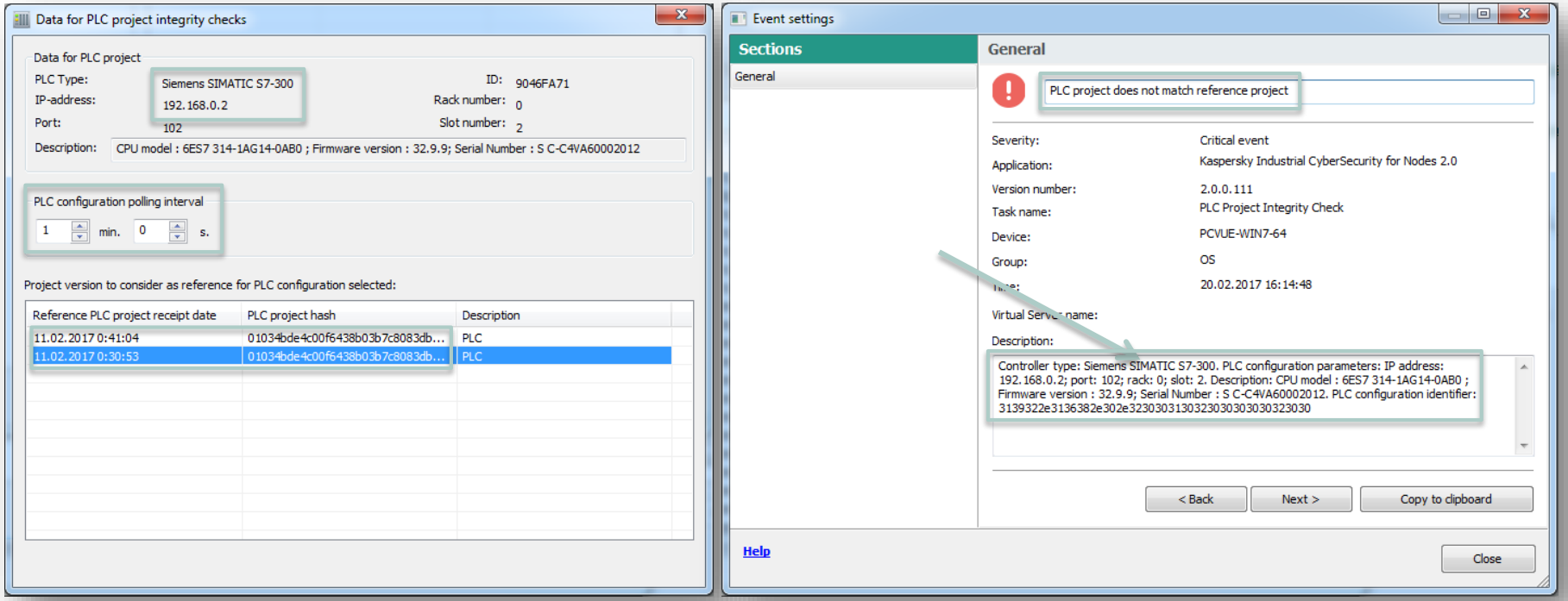


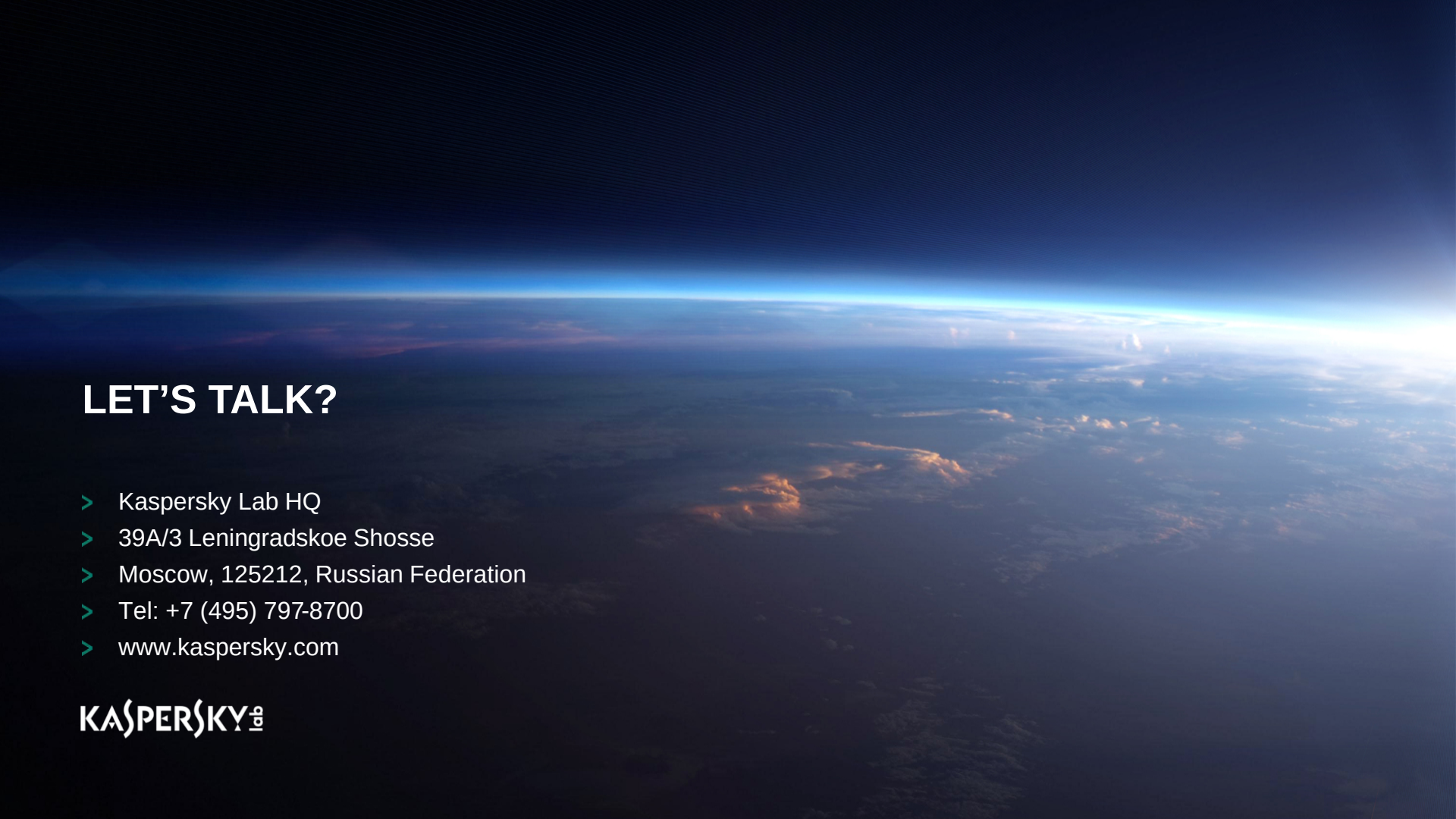
КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОЕКТОВ ПЛК

- ПЛК проект – микропрограмма, написанная для ПЛК
- Проект хранится в памяти ПЛК и поддерживает цикличность индустриального процесса
- Проект может быть загружен на ПЛК локально или по сети
- Неавторизованное модификация ПЛК проекта создает дополнительные риски в области ИБ
- Решения по информационной безопасности не могут быть установлены на ПЛК



КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОЕКТОВ ПЛК





LET’S TALK?

- Kaspersky Lab HQ
- 39A/3 Leningradskoe Shosse
- Moscow, 125212, Russian Federation
- Tel: +7 (495) 797-8700
- www.kaspersky.com

KASPERSKY lab