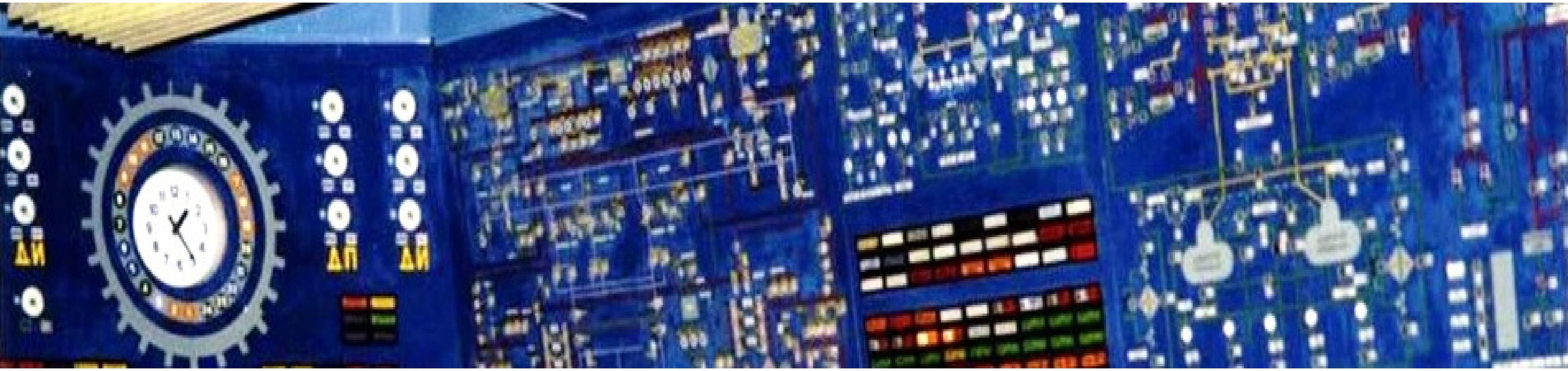


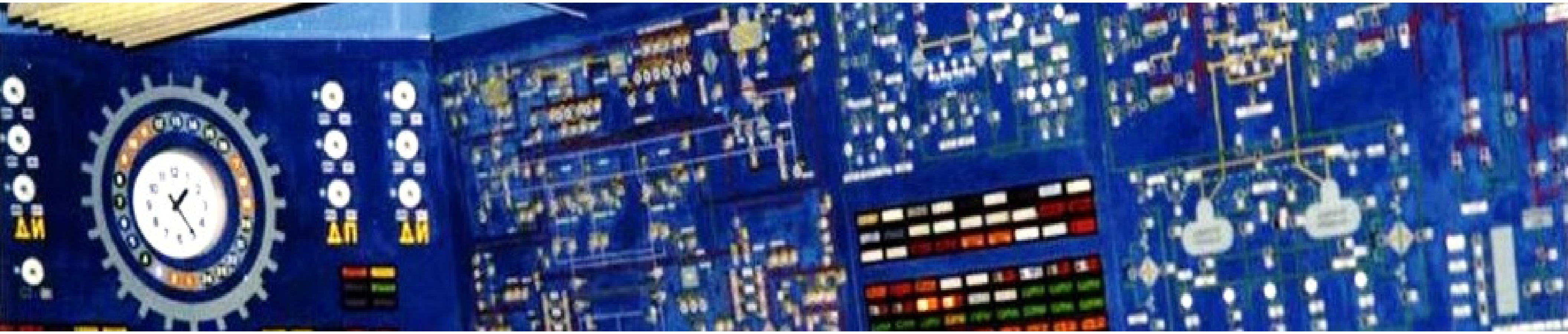
Upgrading Industrial CyberSecurity

Securing Critical National Infrastructure

Dr David E. Probert

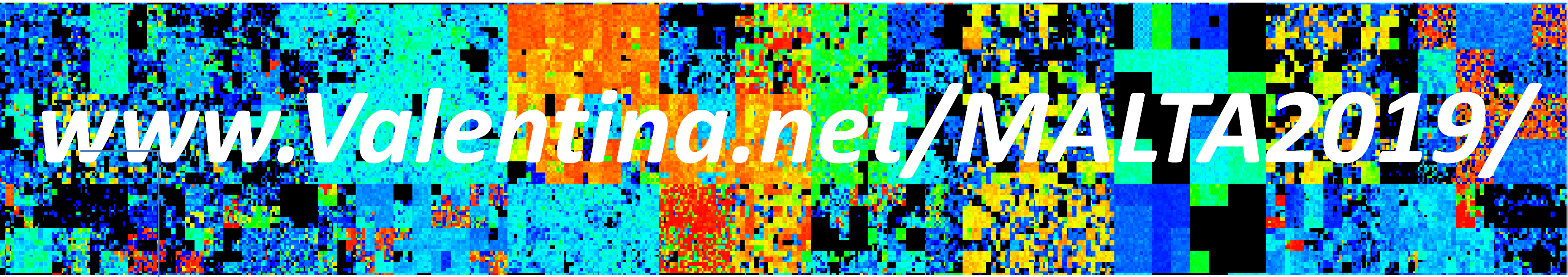
VAZA International

For Ethan, Alice, Hugh, Matthew, Abigail, Micah, Roscoe, Tatiana & Edward!



Модернизация промышленной ***кибербезопасности***

- Защита критической инфраструктуры -



www.Valentina.net/MALTA2019/

Dedicated to Ethan, Alice, Hugh, Matthew, Abigail, Micah, Roscoe & Tatiana!

Our Cyber Trilogy: Finance, Industry & Futures!

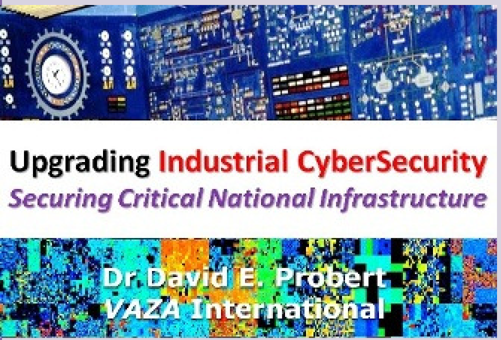
Theme (1) - *21stC Cyber Trends in Finance: AI & Machine Learning in Banking!...*

21stC Cyber Trends in Finance
- AI & Machine Learning in Banking -
Dr David E. Probert
VAZA International

- *Review of Finance Sector – Technology & Market Innovation*
- *Mitigation of Cyber Attacks with AI, Machine & Deep Learning*
- *Using Real-Time Analytics & Big Data to Secure Finance Transactions*

"Cyber Strategies for Finance & Banks!" ***11th Nov: 9:45 – 10:30***

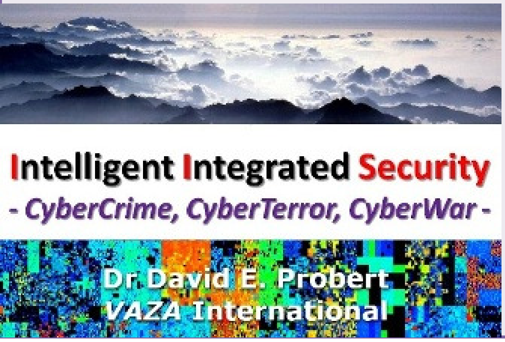
Theme (2) – *Upgrading Industrial CyberSecurity: Securing Critical Infrastructure!...*


Upgrading Industrial CyberSecurity
Securing Critical National Infrastructure
Dr David E. Probert
VAZA International

- *21stC Cyber Landscape for Critical Industrial & Energy Security*
- *Upgrading Legacy Devices & Control Systems to 21stC Standards*
- *Securing Critical Assets with Intelligent Self-Learning Cyber Solutions*

"CyberSecurity for Critical Sectors! " ***11th Nov: 15:15 – 16:00***

Theme (3) – *Intelligent, Integrated Security: CyberCrime, CyberTerror & CyberWar!...*

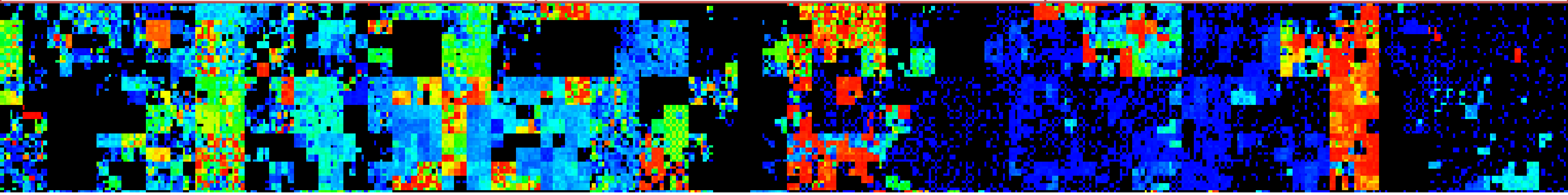

Intelligent Integrated Security
- CyberCrime, CyberTerror, CyberWar -
Dr David E. Probert
VAZA International

- *Understanding and Mapping Worldwide Cyber Threats*
- *Exploring Intelligent Cyber Tools & Real-Time Analytics*
- *Discussion of CyberSecurity Scenarios for **Next 10 Years** & Beyond !...*

"CyberVisions for Intelligent Futures!" ***11th Nov: 12:30 – 13:15***

Upgrading Industrial CyberSecurity!...

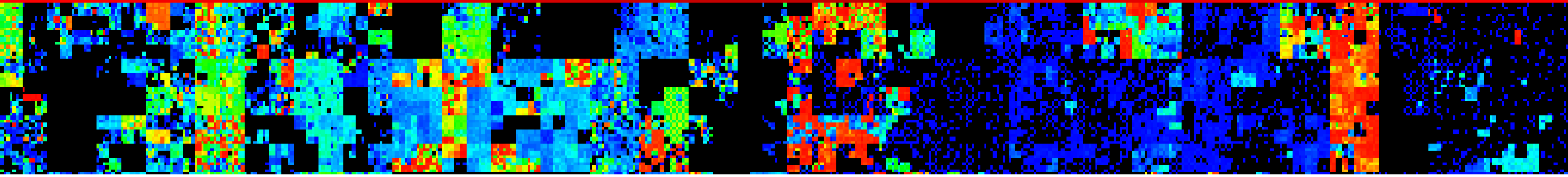
1–Critical Security: Industry & Energy “From Legacy to Smart”	2 – ICS: Industrial Control Systems ”Upgrade ICS/SCADA”	3–Case Studies:Recent Cyber Attacks! “Crime, Spies & Terror”
4 – Security Transition: 2020 – 2025+ “From Physical to Cyber”	5 – Critical Sector Supply Chains “Asset Authentication”	6 – Cyber Surveillance & Espionage “Systems Privacy”
7 –Advanced Cybersecurity Solutions! “Intelligent & Integrated”	8 –10 New Ways to Secure Systems “Real-Time Learning!”	9 – Defend YOUR Industry NOW! “SMART Business Plan”



Upgrading Industrial CyberSecurity!...

1 –Critical Security: Industry & Energy

"Legacy to Smart"

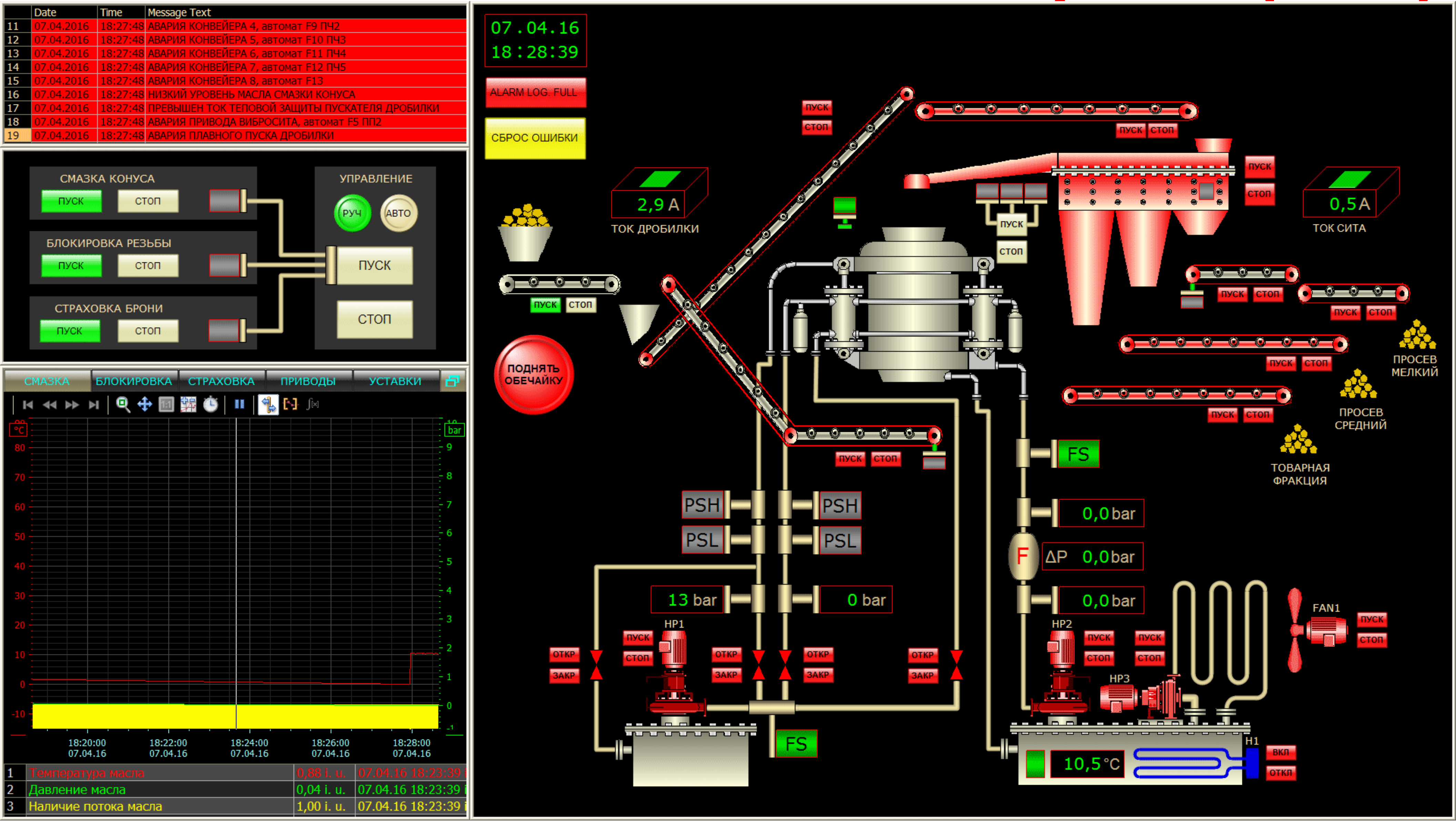


Critical Industrial & Energy Security

- **Legacy:** Many Industrial Control & Monitoring Systems were designed "Pre-CyberSecurity"
- **"ICS" =** Industrial Control Systems & SCADA are frequently the target of criminal cyber attacks!
- **"SCADA"=** Supervisory Control & Data Acquisition
- **Smart:** Industries are now upgrading & replacing legacy ICS/SCADA to mitigate cyber threats!

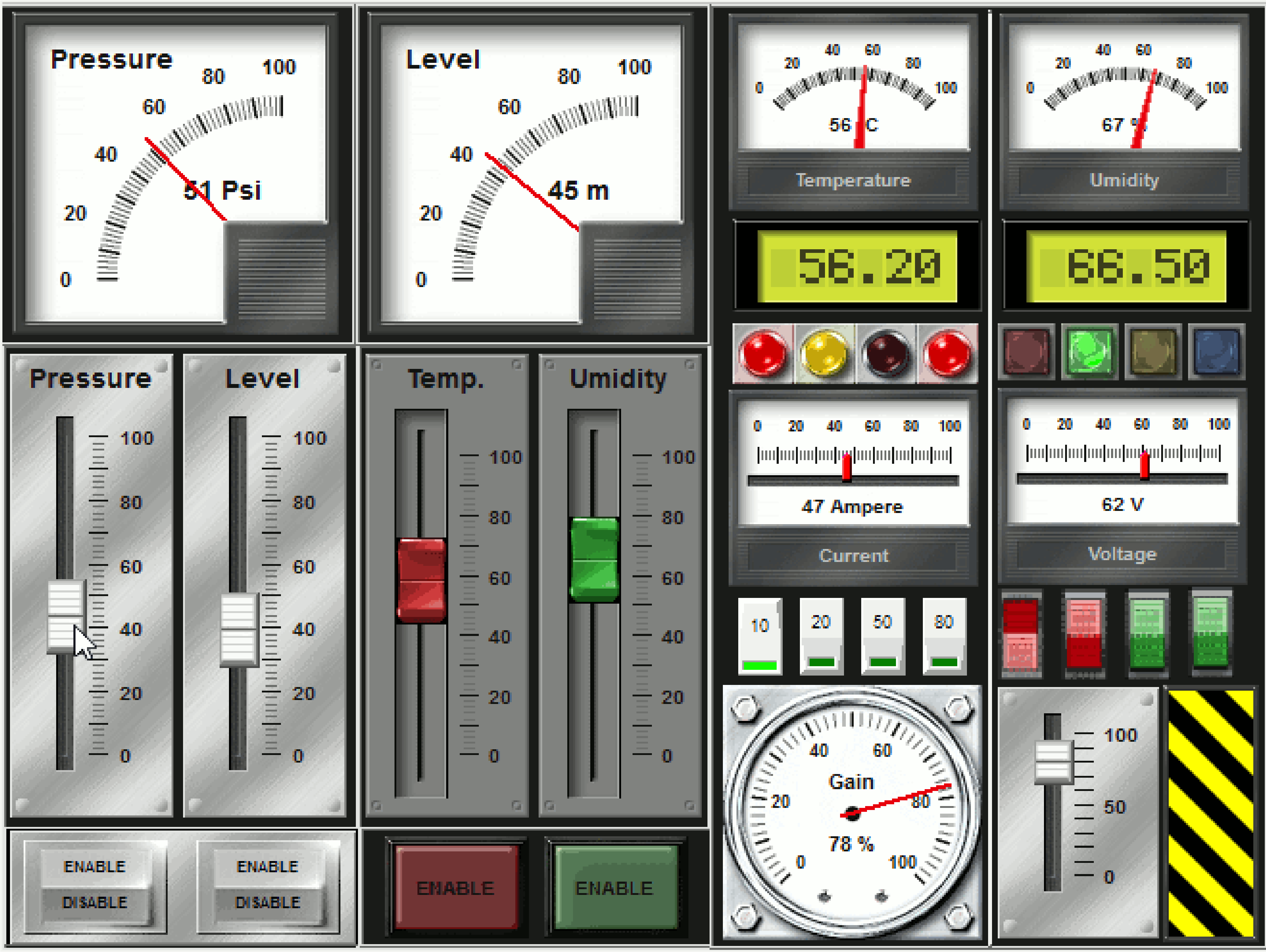
Cyber Upgrades: We discuss the Cyber Threats & Practical Options for Industry to Upgrade Legacy Systems to Smart Cyber Systems!...

ICS/SCADA Systems are embedded in *ALL* Industrial Automation & Control Systems(IACS)



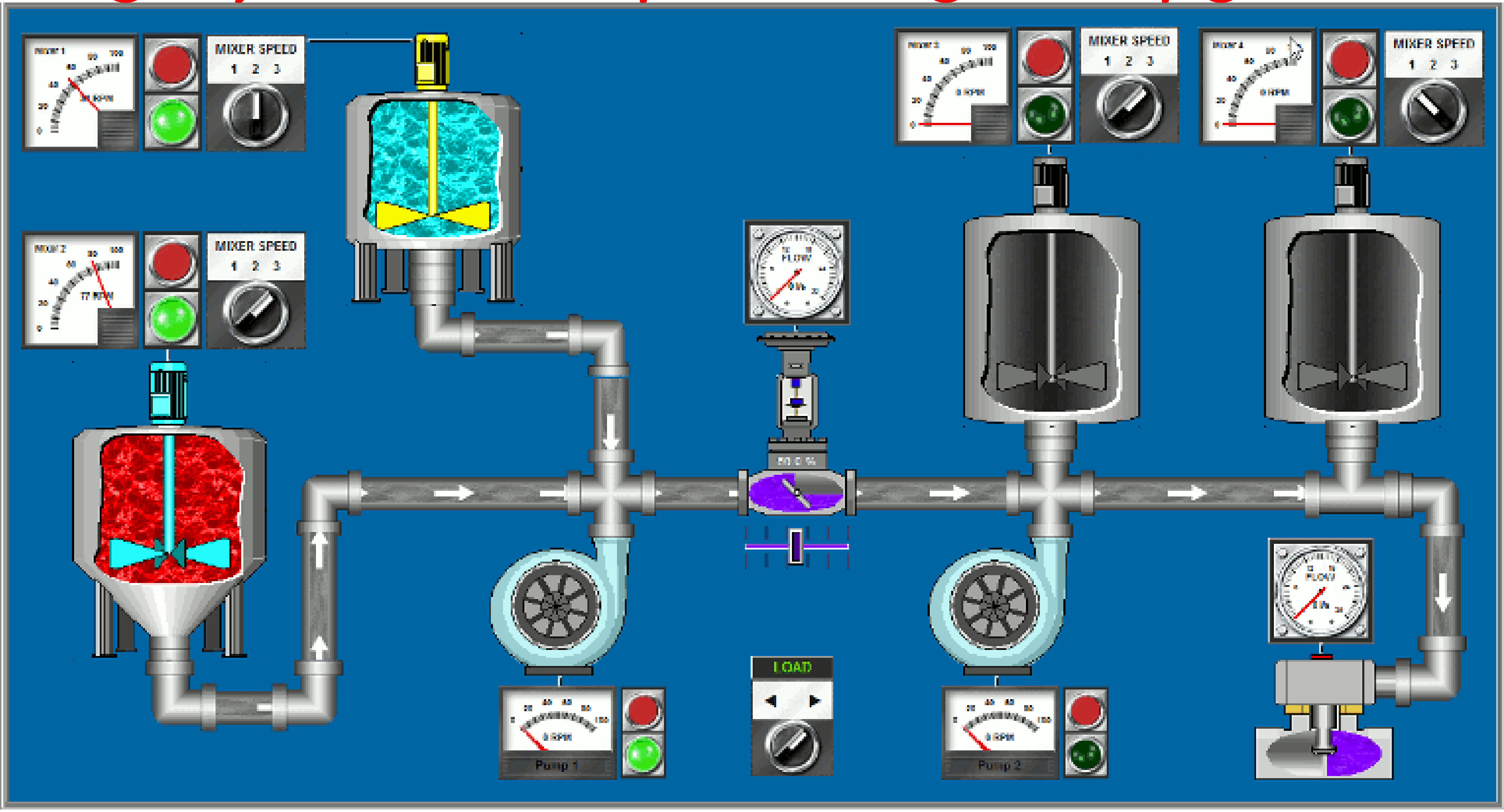
	Date	Time	Message Text
11	07.04.2016	18:27:48	АВАРИЯ КОНВЕЙЕРА 4, автомат F9 ПЧ2
12	07.04.2016	18:27:48	АВАРИЯ КОНВЕЙЕРА 5, автомат F10 ПЧ3
13	07.04.2016	18:27:48	АВАРИЯ КОНВЕЙЕРА 6, автомат F11 ПЧ4
14	07.04.2016	18:27:48	АВАРИЯ КОНВЕЙЕРА 7, автомат F12 ПЧ5
15	07.04.2016	18:27:48	АВАРИЯ КОНВЕЙЕРА 8, автомат F13
16	07.04.2016	18:27:48	НИЗКИЙ УРОВЕНЬ МАСЛА СМАЗКИ КОНУСА
17	07.04.2016	18:27:48	ПРЕВЫШЕН ТОК ТЕПОВОЙ ЗАЩИТЫ ПУСКАТЕЛЯ ДРОБИЛКИ
18	07.04.2016	18:27:48	АВАРИЯ ПРИВОДА ВИБРОСИТА, автомат F5 ПП2
19	07.04.2016	18:27:48	АВАРИЯ ПЛАВНОГО ПУСКА ДРОБИЛКИ

1	Температура масла	0,88 i. u.	07.04.16 18:23:39
2	Давление масла	0,04 i. u.	07.04.16 18:23:39
3	Наличие потока масла	1,00 i. u.	07.04.16 18:23:39


Pressure
0
20
40
60
80
100
51 Psi
Level
0
20
40
60
80
100
45 m
0
20
40
60
80
100
56 °C
Temperature
56.20
0
20
40
60
80
100
67 %
Umidity
66.50
Pressure
100
80
60
40
20
0
Level
100
80
60
40
20
0
Temp.
100
80
60
40
20
0
Umidity
100
80
60
40
20
0
0 20 40 60 80 100
47 Ampere
Current
0 20 40 60 80 100
62 V
Voltage
10
20
50
80
Gain
0
20
40
60
80
100
78 %
100
50
0
ENABLE
DISABLE
ENABLE
DISABLE
ENABLE
ENABLE

Industrial Automation & Control Systems:

Legacy SCADA requires Urgent Upgrades!



IIoT = "Industrial "Internet of Things"

40th International East-West Security Conference

" Upgrading Industrial Cybersecurity "

- Securing Critical National Infrastructure-

St Julians, Malta – 10th / 11th Nov 2019

© *Dr David E. Probert : www.VAZA.com* ©

Critical National Infrastructure such as *Nuclear Power Plants* use ICS/SCADA

Control Room: Kola Nuclear Power Station – Polarnye Zori

KolaNet Project for *Nuclear Safety & Security* :1990s

© Vaza International

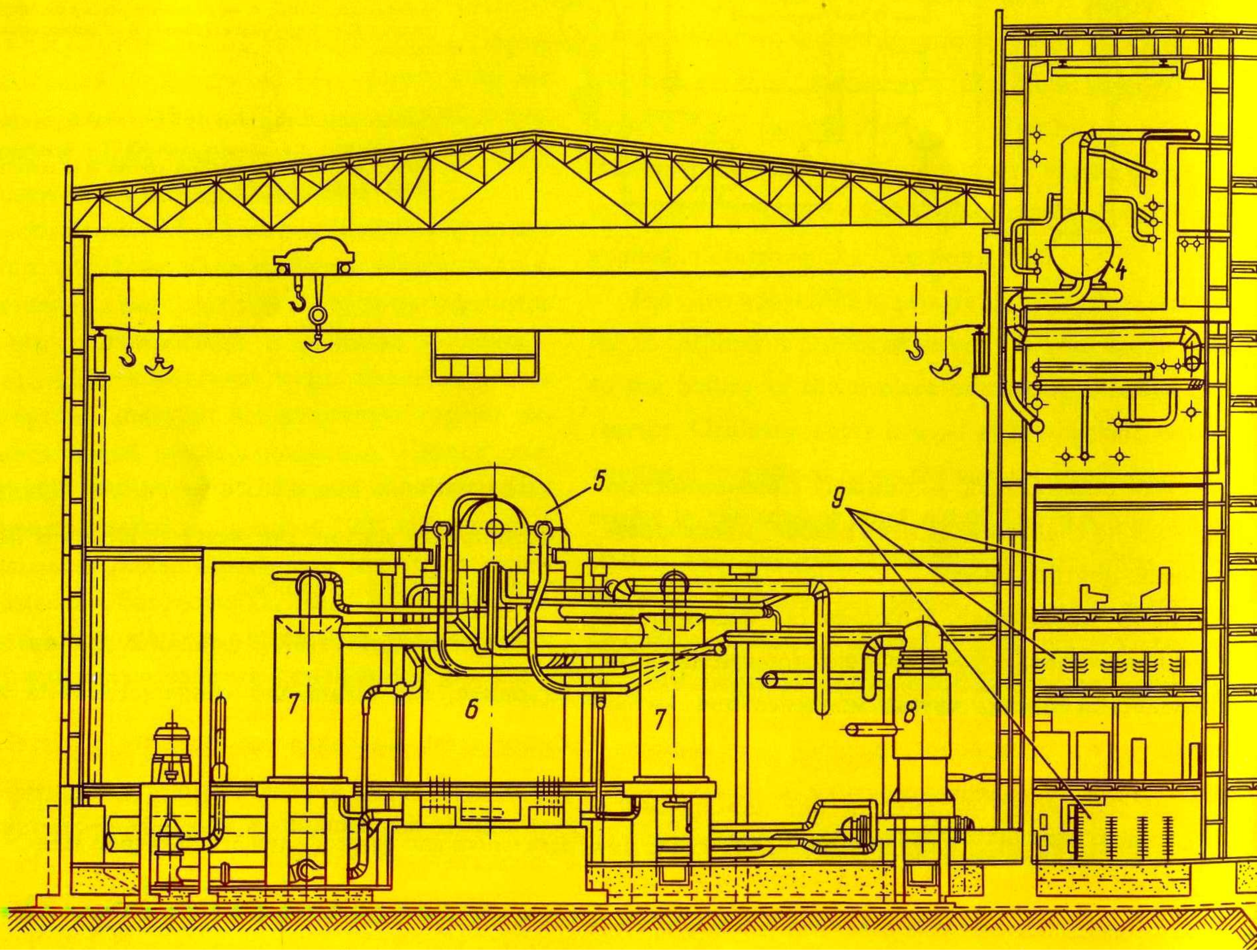
KolaNet Workshop : Sept 1996

ЧЕРНОБЫЛЬСКАЯ АЭС

CHERNOBYL NUCLEAR POWER STATION

ATOMENERGOEXPORT USSR MOSCOW

ATOMENERGOEXPORT


4
5
9
7
6
7
8

РАДИАЦИОННАЯ БЕЗОПАСНОСТЬ АЭС

В схему и конструкцию реактора заложены следующие основные элементы, гарантирующие радиационную безопасность как при нормальной работе АЭС, так и при аварийных ситуациях:

а) высоконадежная СУЗ, включающая около 180 независимых поглотителей, объединенных в группы с автономными датчиками, кабелями, аппаратурой сравнения и усиления сигналов и питанием;

б) средства аварийного теплоотвода (маховики на главных насосах контура, резервы питания для собственных нужд, подача питательной воды в напорный коллектор и др.), исключающие массовые повреждения оболочек ТВЭЛов при всех видах аварий, в том числе общее обесточивание, отключение сразу двух турбин, течи труб диаметром до 300—400 мм и т. д.;

в) средства периодического контроля состояния всех узлов и систем, ответственных за радиационную безопасность, в том числе периодическая инспекция состояния крупных сосудов и коллекторов, практически исключающая их мгновенный полный разрыв по всему сечению;

г) пароприемные устройства, исключающие большие утечки пара в атмосферу.

Именно реактор канального типа, т. е. бескорпусный, открывает в принципе возможность коренного решения вопросов безопасности за счет исключения крупных трубопроводов и дробления контура циркуляции на автономные участки, разрыв каждого из которых является незначительной аварией.

Наличие поканальной системы контроля герметичности оболочек и возможность перегрузки без остановки реактора позволяет своевременно обнаруживать негерметичные кассеты и сразу же выгружать их, что обеспечивает минимальное радиоактивное загрязнение теплоносителя.

RADIATION SAFETY

The key elements incorporated in the reactor design to ensure radiation safety both during normal operation and under abnormal conditions may be summarized as follows:

a) a highly reliable control and safety system (CSS), including 180 independent absorbers combined into groups with separate transmitters, cables, comparators and amplifiers, and power supplies;

b) emergency cooling equipment (flywheels on the main pumps of the circuit, a stand-by power supply for auxiliaries, feed water supply to the common header, etc.) to prevent mass rupture of fuel cans under all abnormal conditions, including the failure of the power supply, shut-down of both turbines, leaky of 300—400 mm in pipes diameter, etc.;

c) facilities for regular checks of all the units and systems responsible for radiation safety, including periodic inspection of large vessels and headers, practically excluding the possibility of their instantaneous rupture at a time;

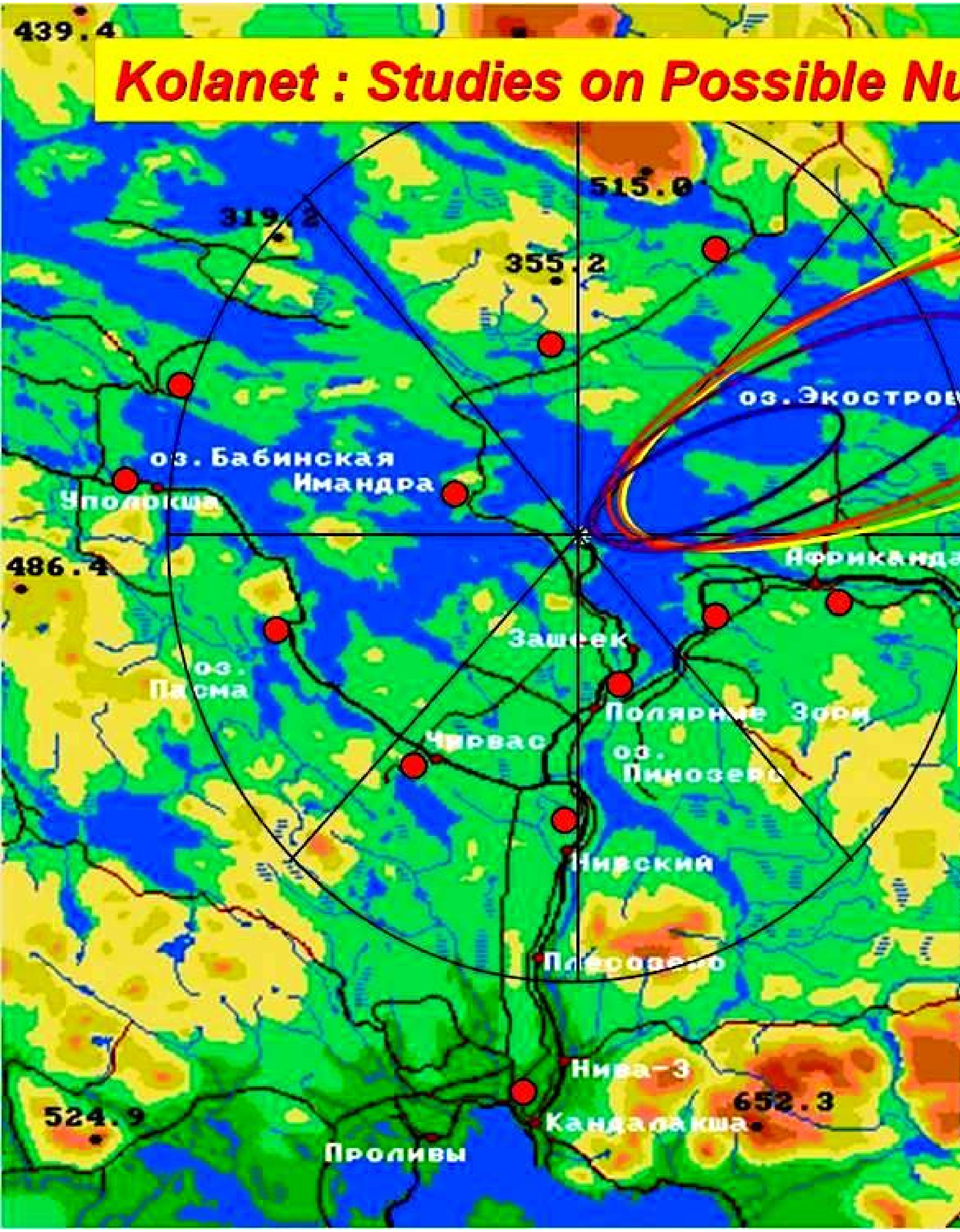
d) steam receivers excluding large releases of steam to the atmosphere.

It is precisely the channel-type reactor, i.e. the reactor having no pressure vessel, which enables the safety problems to be solved in principle, by dispensing with large pipelines and by sectionalizing the circulation circuit, the rupture of each individual section being but a minor accident.

The system of leak detection in every channel and the provisions for on-load refuelling make possible rapid detection of leaking fuel assemblies and their immediate replacement, thus ensuring minimum radioactive contamination of the coolant.

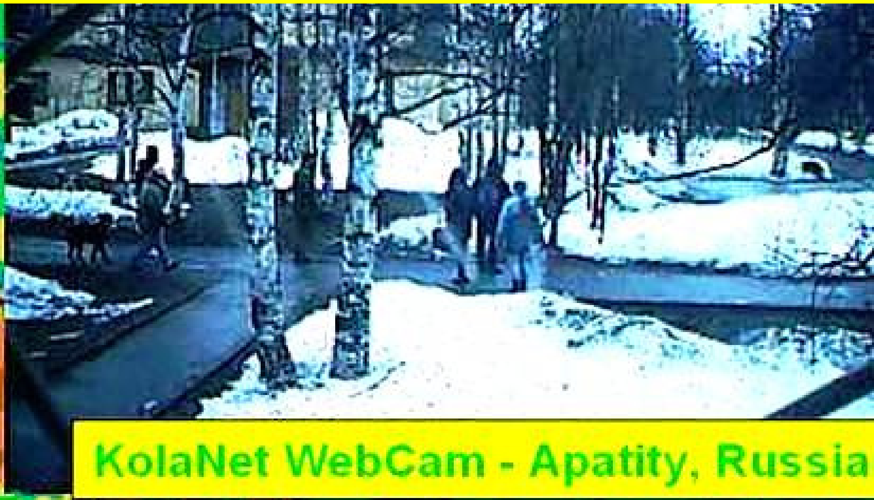
ОРУ 110кВ
ОРУ - 220кВ

Kolanet : Studies on Possible Nuclear Accidents



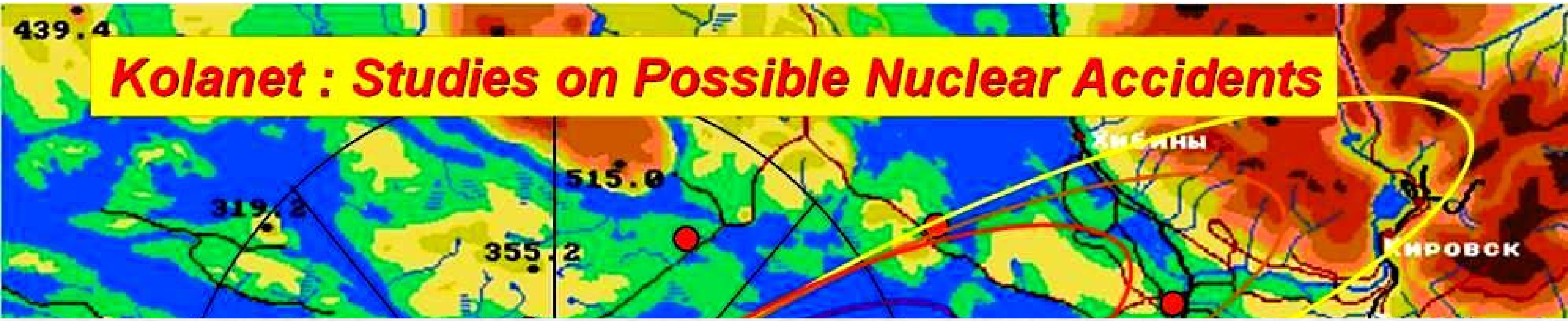
"Radiation Cloud Simulations"

- Dr Alexander Baklanov -

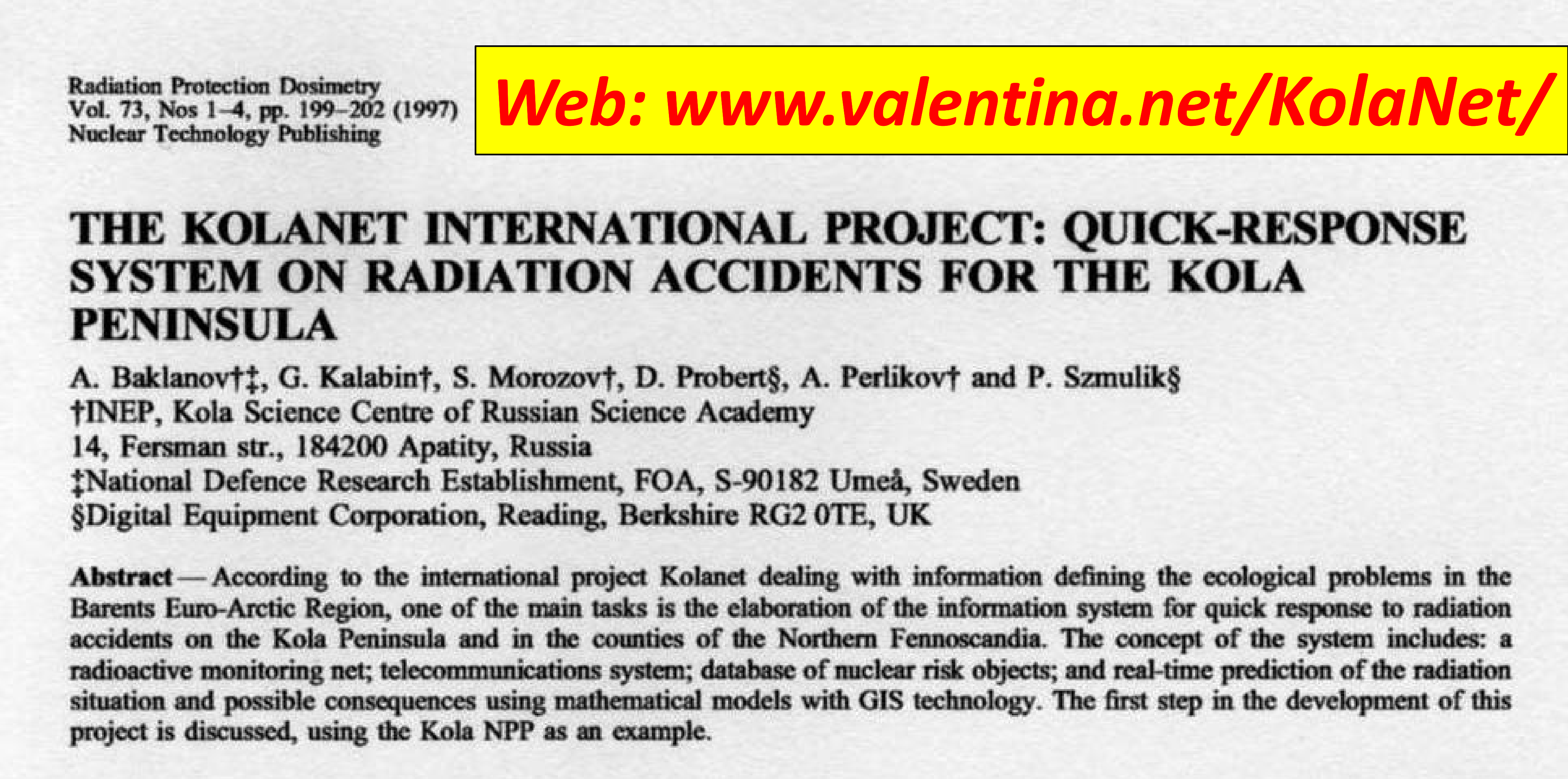


KolaNet WebCam - Apatity, Russia

Kolanet : Studies on Possible Nuclear Accidents



Web: www.valentina.net/KolaNet/

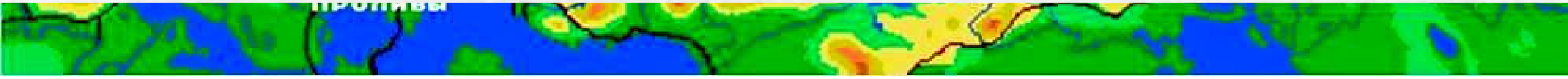


Radiation Protection Dosimetry
Vol. 73, Nos 1–4, pp. 199–202 (1997)
Nuclear Technology Publishing

THE KOLANET INTERNATIONAL PROJECT: QUICK-RESPONSE SYSTEM ON RADIATION ACCIDENTS FOR THE KOLA PENINSULA

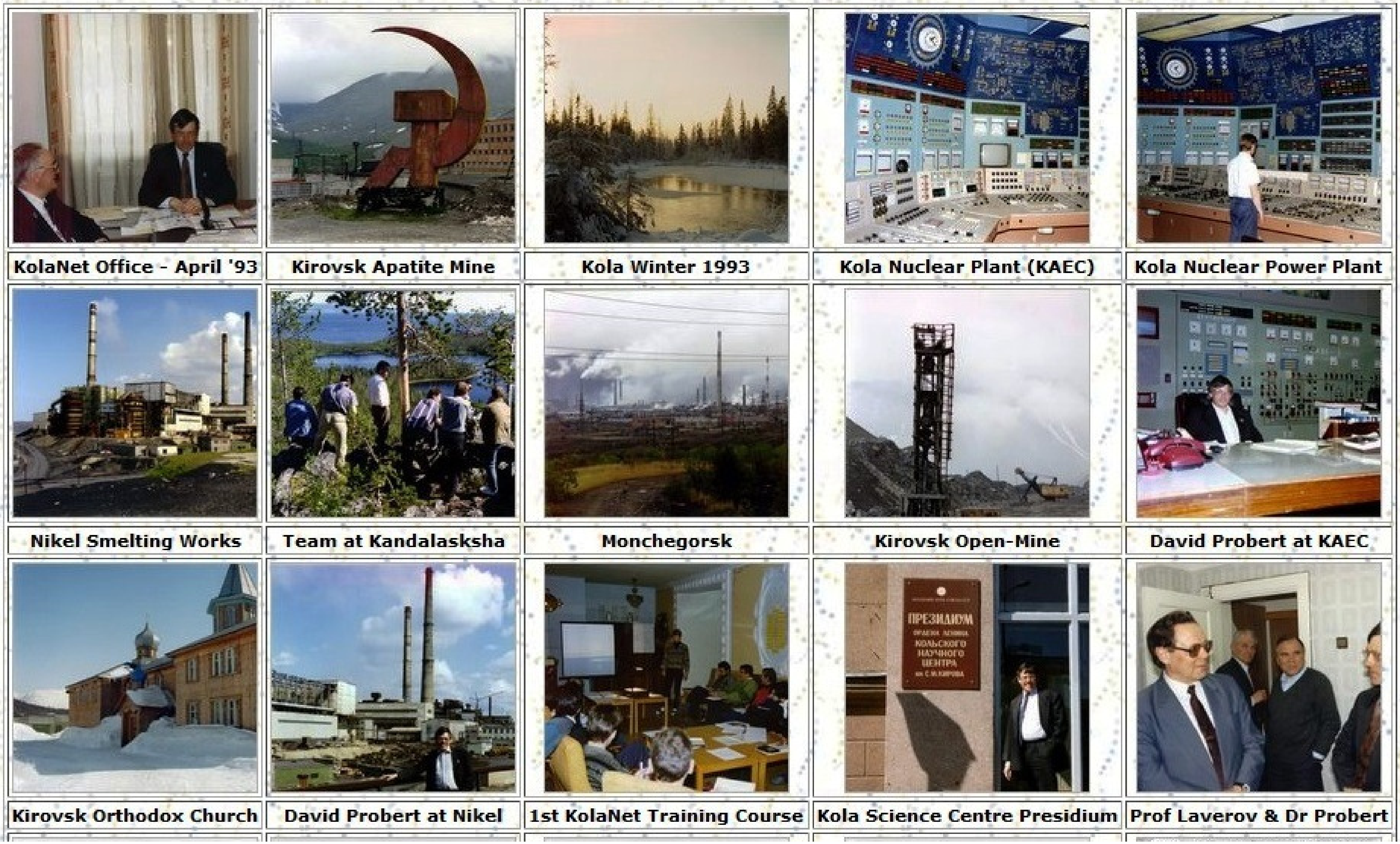
A. Baklanov†‡, G. Kalabin†, S. Morozov†, D. Probert§, A. Perlikov† and P. Szmulik§
†INEP, Kola Science Centre of Russian Science Academy
14, Fersman str., 184200 Apatity, Russia
‡National Defence Research Establishment, FOA, S-90182 Umeå, Sweden
§Digital Equipment Corporation, Reading, Berkshire RG2 0TE, UK

Abstract — According to the international project Kolanet dealing with information defining the ecological problems in the Barents Euro-Arctic Region, one of the main tasks is the elaboration of the information system for quick response to radiation accidents on the Kola Peninsula and in the counties of the Northern Fennoscandia. The concept of the system includes: a radioactive monitoring net; telecommunications system; database of nuclear risk objects; and real-time prediction of the radiation situation and possible consequences using mathematical models with GIS technology. The first step in the development of this project is discussed, using the Kola NPP as an example.



On-Line KolaNet Photo Archives

www.valentina.net/KolaNetProject/kolanetproject.html



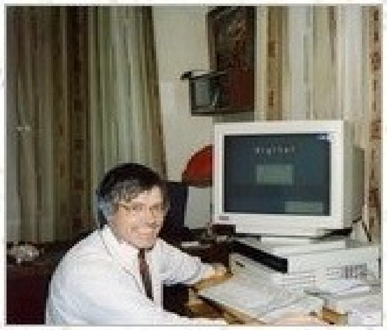
KolaNet Office - April '93	Kirovsk Apatite Mine	Kola Winter 1993	Kola Nuclear Plant (KAEC)	Kola Nuclear Power Plant
Nikel Smelting Works	Team at Kandalasksha	Monchegorsk	Kirovsk Open-Mine	David Probert at KAEC
Kirovsk Orthodox Church	David Probert at Nikel	1st KolaNet Training Course	Kola Science Centre Presidium	Prof Laverov & Dr Probert

KolaNet Team

KolaNet Committee

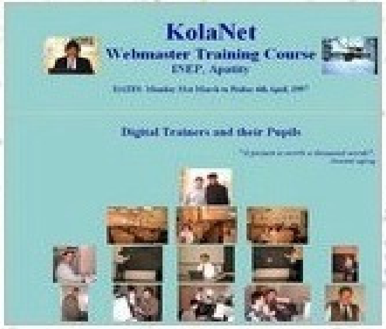
Signing New Protocol

President Kalinikov - KSC


Dr David Probert - Apatity

Apatity Mayor & Team

Visit to Econord


KolaNet

Webmaster Training Course

INEP, Apatity

DATES: Monday 31st March to Friday 4th April 1997

Digital Trainers and their Pupils

"A picture is worth a thousand words"
[illegible]

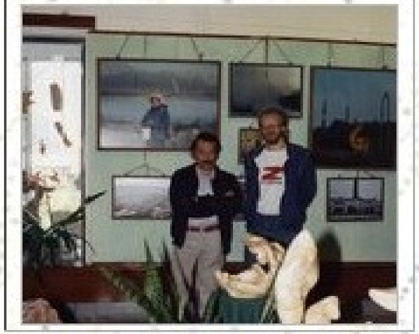
KolaNet Training - 1997

KolaNet Project Office

Outside INEP Lab

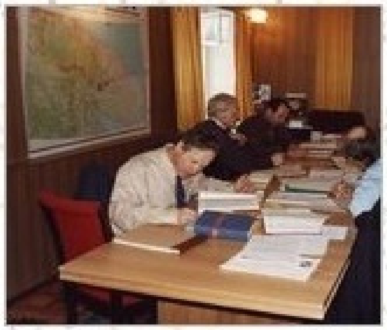
Prof Kalabin's Office

Salma Art Gallery


Salma Art Gallery

Exhibition - "Remont"

Salma Gallery


KolaNet Project Meeting

KolaNet Meeting - April '93

Prof Laverov & Dr Probert

Opening of KolaNet Office

Wolfgang - Dornier

1st Live WebCam in the Kola-Arctic: 1999

1999/06/13 23:20:52 Local time
KolaNet (Apatity, Russia)
1999/06/13 23:19:00 21,78C° 71,21F°
-40 -30 -20 -10 C° 0 10 20 30 4
-40 -20 0 20 F° 40 60 80 10

1st Live WebCam in the Kola-Arctic: 1999

Springtime View from the INEP Computer Laboratory

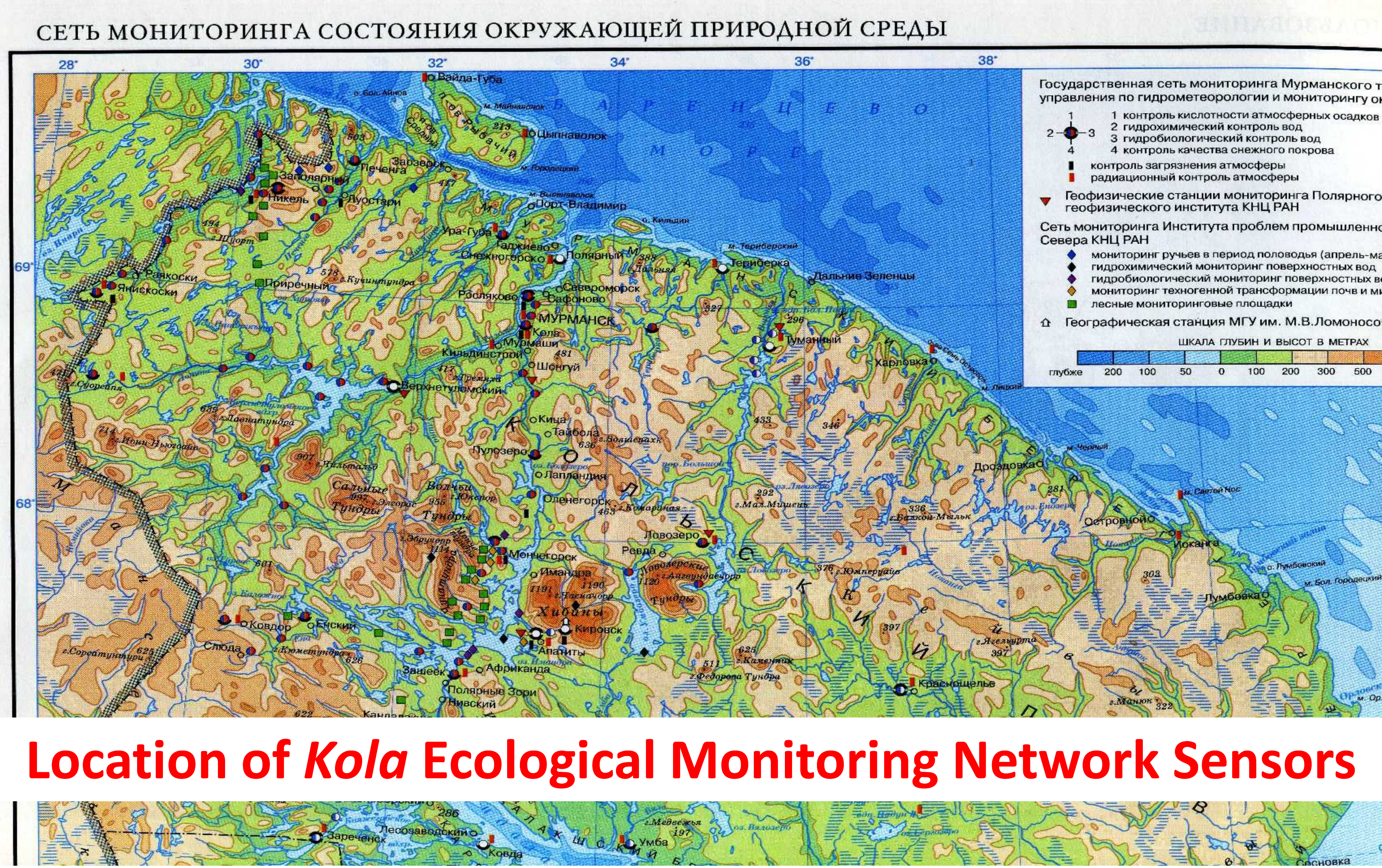
Karnasurt Mine: Revda–Kola Peninsula, Russia: 1999

Mining Data may be as profitable As Mining for Minerals in 20thC!...

“Data is the New Oil”

1st Kola Ecological Atlas: 1999 (Makarova)

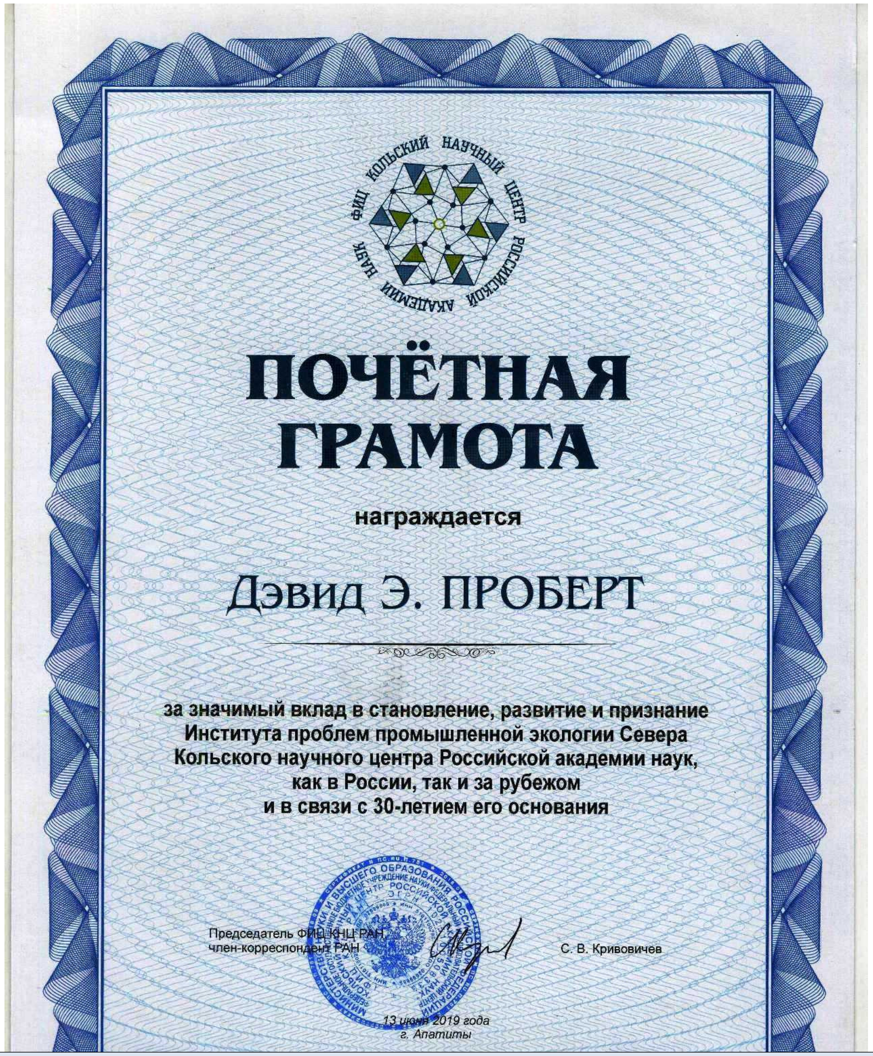
* *KolaNet promoted Applications of GIS* *


СЕТЬ МОНИТОРИНГА СОСТОЯНИЯ ОКРУЖАЮЩЕЙ ПРИРОДНОЙ СРЕДЫ
28°
30°
32°
34°
36°
38°
69°
68°
Государственная сеть мониторинга Мурманского т
управления по гидрометеорологии и мониторингу ок
1 контроль кислотности атмосферных осадков
2 гидрохимический контроль вод
3 гидробиологический контроль вод
4 контроль качества снежного покрова
контроль загрязнения атмосферы
радиационный контроль атмосферы
Геофизические станции мониторинга Полярного геофизического института КНЦ РАН
Сеть мониторинга Института проблем промышленно
Севера КНЦ РАН
мониторинг ручьев в период половодья (апрель-ма
гидрохимический мониторинг поверхностных вод
гидробиологический мониторинг поверхностных в
мониторинг техногенной трансформации почв и ми
лесные мониторинговые площадки
Географическая станция МГУ им. М.В.Ломоносо
ШКАЛА ГЛУБИН И ВЫСОТ В МЕТРАХ
глубже
200
100
50
0
100
200
300
500
БАРЕНЦЕВО МОРЕ
Вайда-Губа
Цыпнаволок
Печенга
Заполярный
Никель
Луостари
Порт-Владимир
Ура-Губа
Гаджиево
Снежногорск
Полярный
Териберка
Дальние Зеленцы
Раякоски
Янискоски
Приречный
Росляково
Североморск
Сафоново
МУРМАНСК
Кола
Мурмаши
Кильдинстрой
Шонгуй
Верхнетуломский
Туманный
Харловка
Кица
Тайбола
Пулозеро
Лапландия
Оленегорск
Дроздовка
Островной
Иоканга
Ловозеро
Ревда
Мончегорск
Имандра
Хибины
Кировск
Апатиты
Ковдор
Енский
Слюда
Зашеек
Африканда
Полярные Зори
Нивский
Лумбовка
Краснощелье
Зареченск
Лесозаводский
Ковда
Умба
Сосновка

Location of *Kola* Ecological Monitoring Network Sensors

Russian Academy of Sciences @ Kola Science Centre

Honorary Diplomas for KolaNet Programme in 1990s!



ФИЦ КОЛЬСКИЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК

ПОЧЁТНАЯ ГРАМОТА

награждается

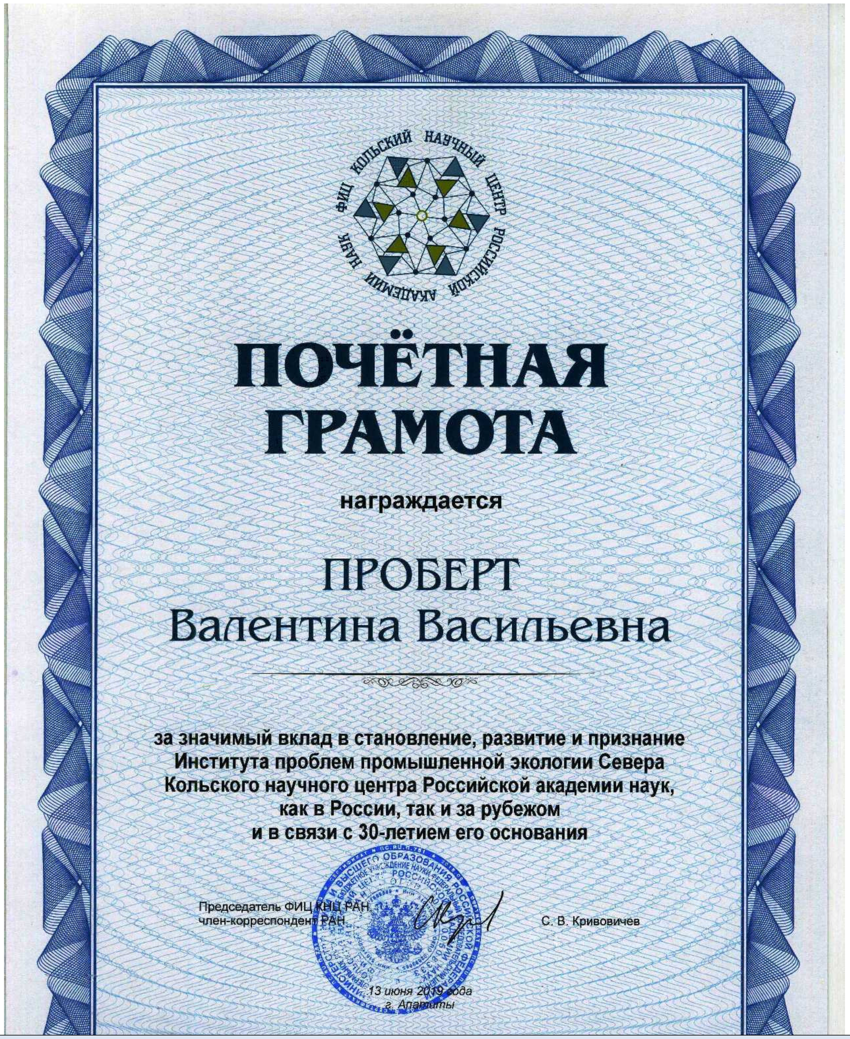
Дэвид Э. ПРОБЕРТ

за значимый вклад в становление, развитие и признание
Института проблем промышленной экологии Севера
Кольского научного центра Российской академии наук,
как в России, так и за рубежом
и в связи с 30-летием его основания

Председатель ФИЦ КНЦ РАН
член-корреспондент РАН С. В. Кривовичев

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР КОЛЬСКИЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК
ФИЦ КНЦ РАН

13 июня 2019 года
г. Апатиты



ФИЦ КОЛЬСКИЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК

ПОЧЁТНАЯ ГРАМОТА

награждается

ПРОБЕРТ
Валентина Васильевна

за значимый вклад в становление, развитие и признание
Института проблем промышленной экологии Севера
Кольского научного центра Российской академии наук,
как в России, так и за рубежом
и в связи с 30-летием его основания

Председатель ФИЦ КНЦ РАН
член-корреспондент РАН С. В. Кривовичев

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

13 июня 2019 года
г. Апатиты

Awarded to David & Valentina Probert @ "Institute of Industrial Ecological Problems of the North"
30th Anniversary Conference – Kola Science Centre, Apatity, Murmansk Region. Russia - June 2019

CyberSecurity @ Nuclear Plants

* Chatham House, London – Sept 2015 *

Chatham House Report

Caroline Baylon with Roger Brunt and David Livingstone
September 2015

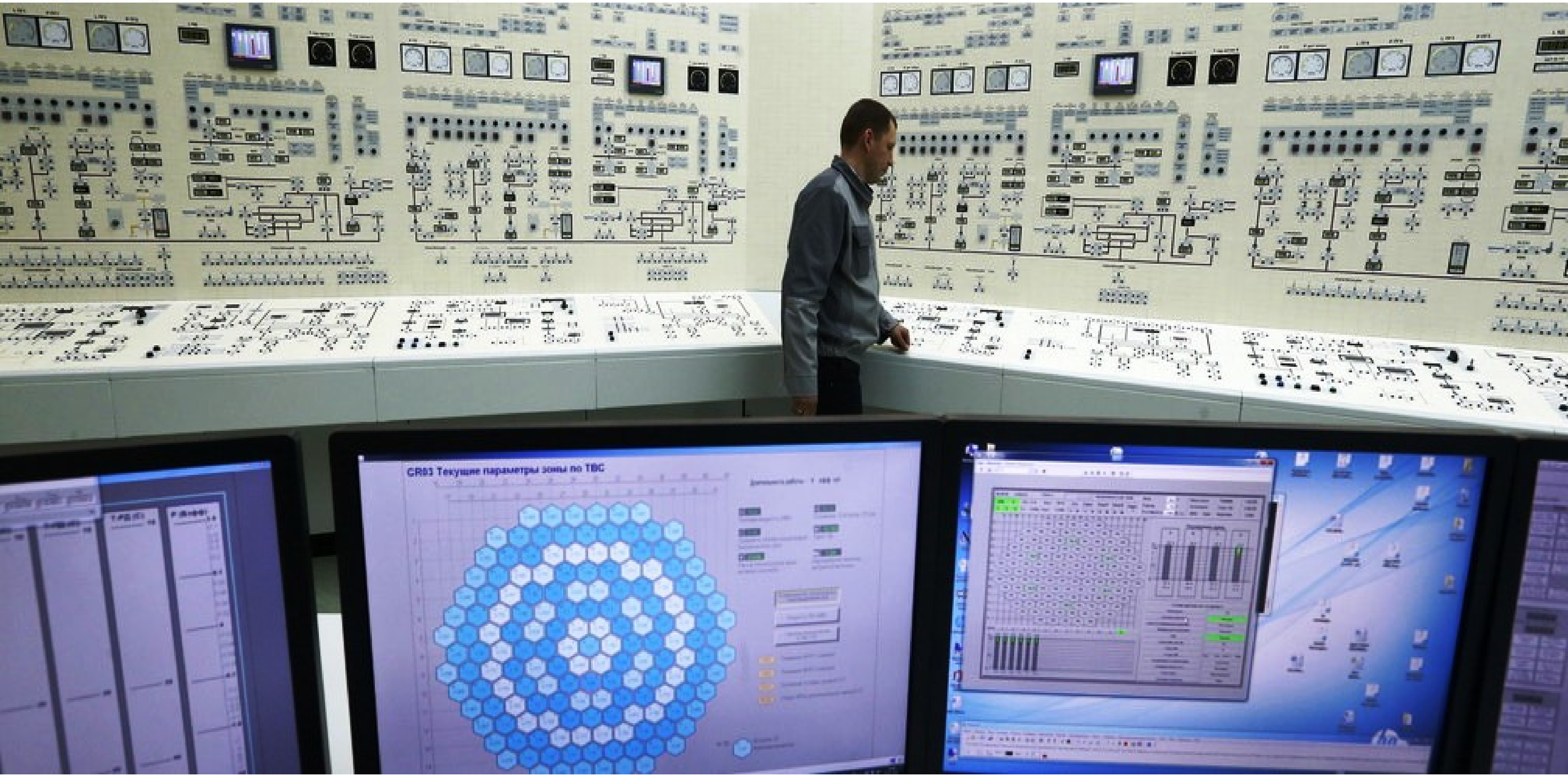
Cyber Security at Civil Nuclear Facilities

Understanding the Risks

Web: www.chathamhouse.org

CyberSecurity @ Nuclear Plants

* Chatham House, London – Sept 2015 *



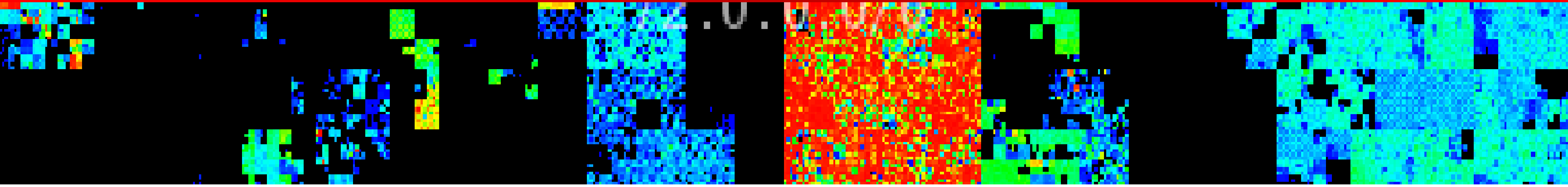
Web: www.chathamhouse.org

40th International East-West Security Conference

Upgrading Industrial CyberSecurity!...

2 – ICS: Industrial Control Systems!

"Upgrade ICS/SCADA"

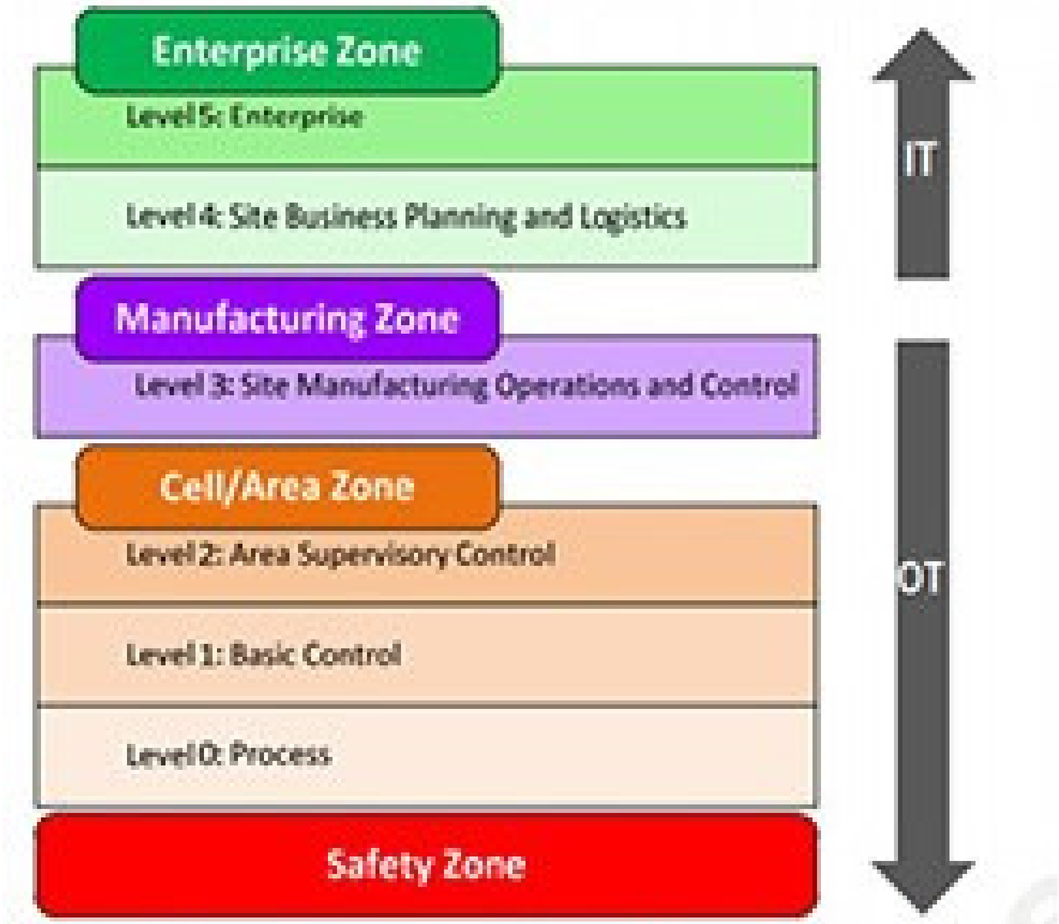


Security Upgrades for ICS/SCADA!

- Device Software/Firmware: Upgrade ICS Device with Secure Access Software & Strong Passwords
- Encrypt Network Traffic: Protect ICS Device from Network using Cryptographic Authentication
- Staff Policy for “Air-Gap”: Ensure that Malware cannot pass from Internet to Critical Systems
- System Replacement: Older Legacy ICS/SCADA may require replacement for High Security Sites!

CyberSecurity Vendors: Most Suppliers have Solutions for ICS/SCADA Security Upgrades but Critical Sites will eventually need replacement

Integration of Operational & Information Control Technologies(OT+IT):“Purdue Model”



Enterprise Zone

Level 5: Enterprise

Level 4: Site Business Planning and Logistics

Manufacturing Zone

Level 3: Site Manufacturing Operations and Control

Cell/Area Zone

Level 2: Area Supervisory Control

Level 1: Basic Control

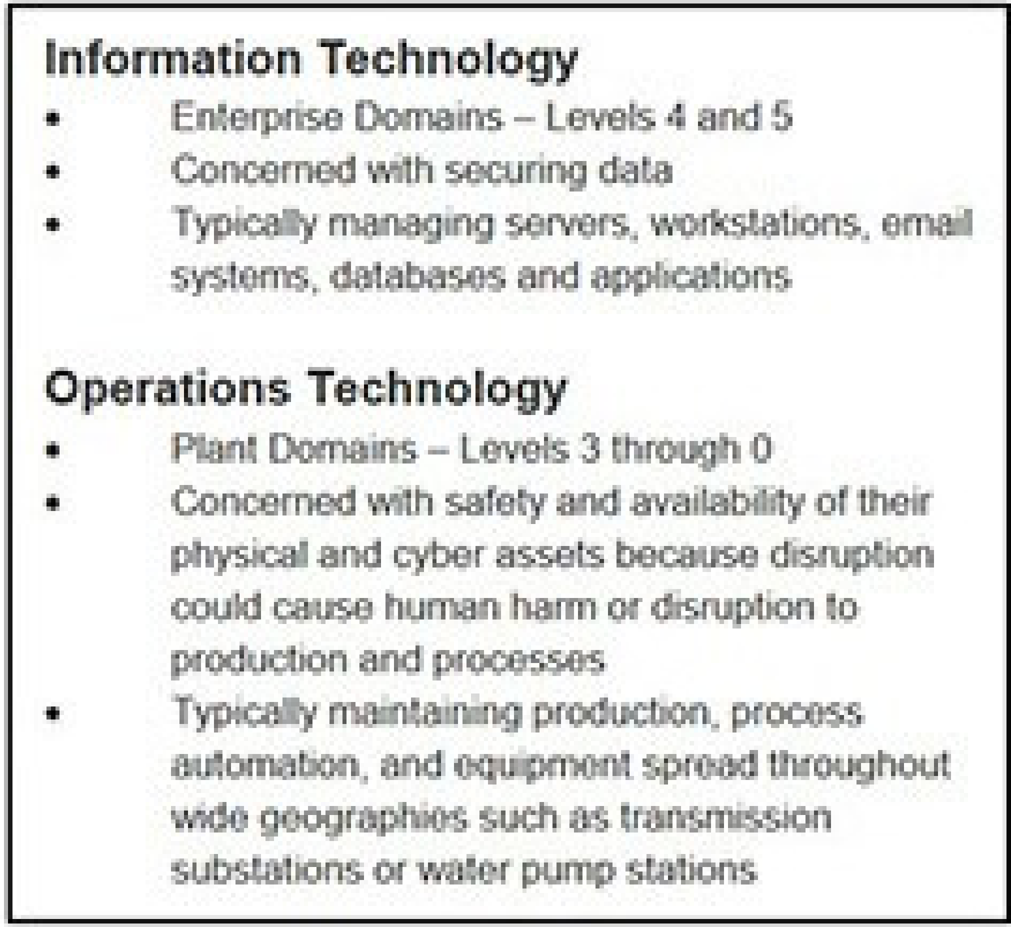
Level 0: Process

Safety Zone

IT

OT

Purdue Model for Control Hierarchy logical framework



Information Technology

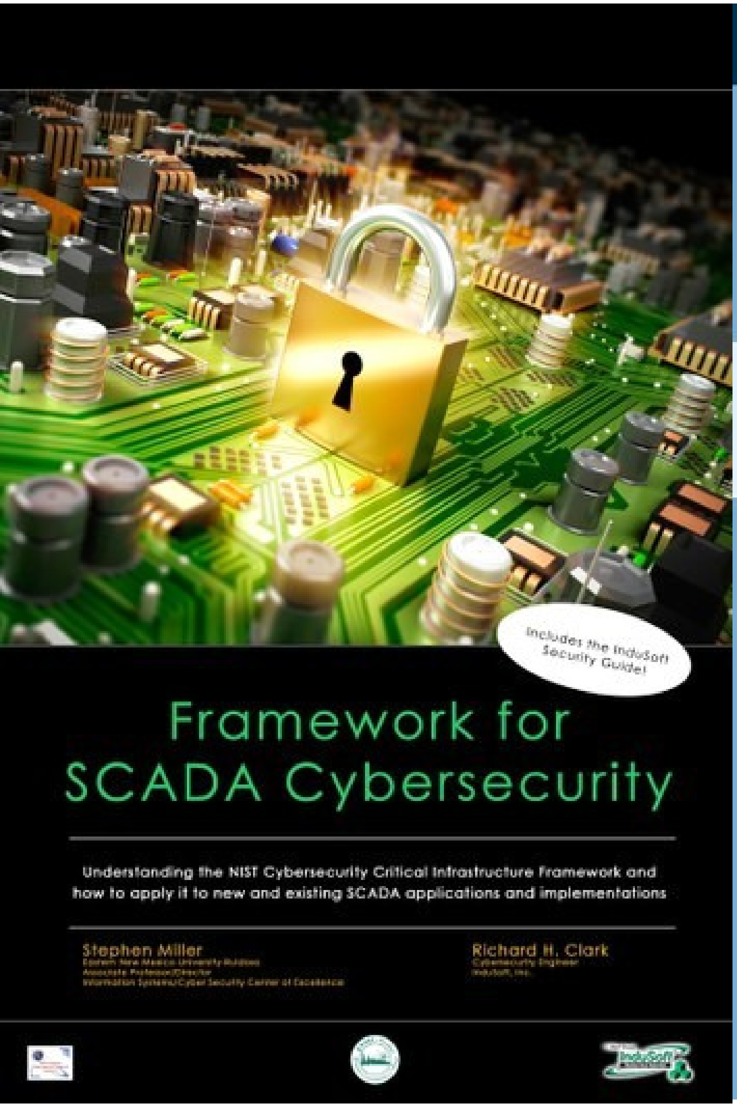
- Enterprise Domains – Levels 4 and 5
- Concerned with securing data
- Typically managing servers, workstations, email systems, databases and applications

Operations Technology

- Plant Domains – Levels 3 through 0
- Concerned with safety and availability of their physical and cyber assets because disruption could cause human harm or disruption to production and processes
- Typically maintaining production, process automation, and equipment spread throughout wide geographies such as transmission substations or water pump stations

ALL Industrial Automation & Control Systems (OT+IT) need Security Upgrades!

Recent Publications on Industrial *CyberSecurity* for *SCADA Systems*



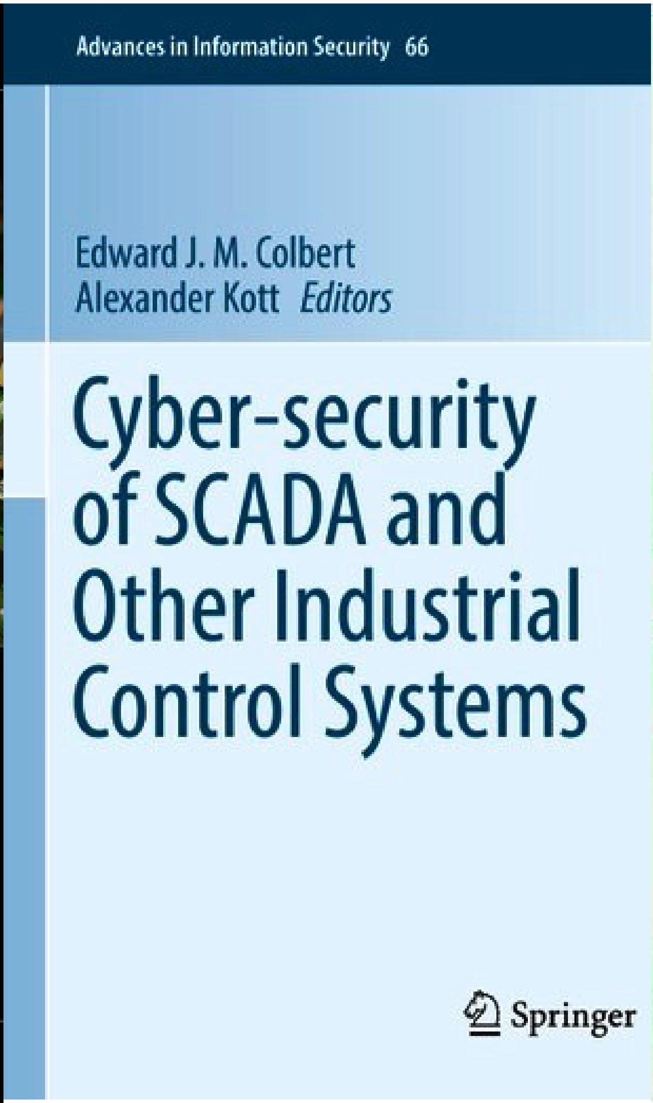
Includes the InduSoft Security Guide!

Framework for SCADA Cybersecurity

Understanding the NIST Cybersecurity Critical Infrastructure Framework and how to apply it to new and existing SCADA applications and implementations

Stephen Miller
Eastern New Mexico University-Ruidoso
Associate Professor/Director
Information Systems/Cyber Security Center of Excellence

Richard H. Clark
Cybersecurity Engineer
InduSoft, Inc.

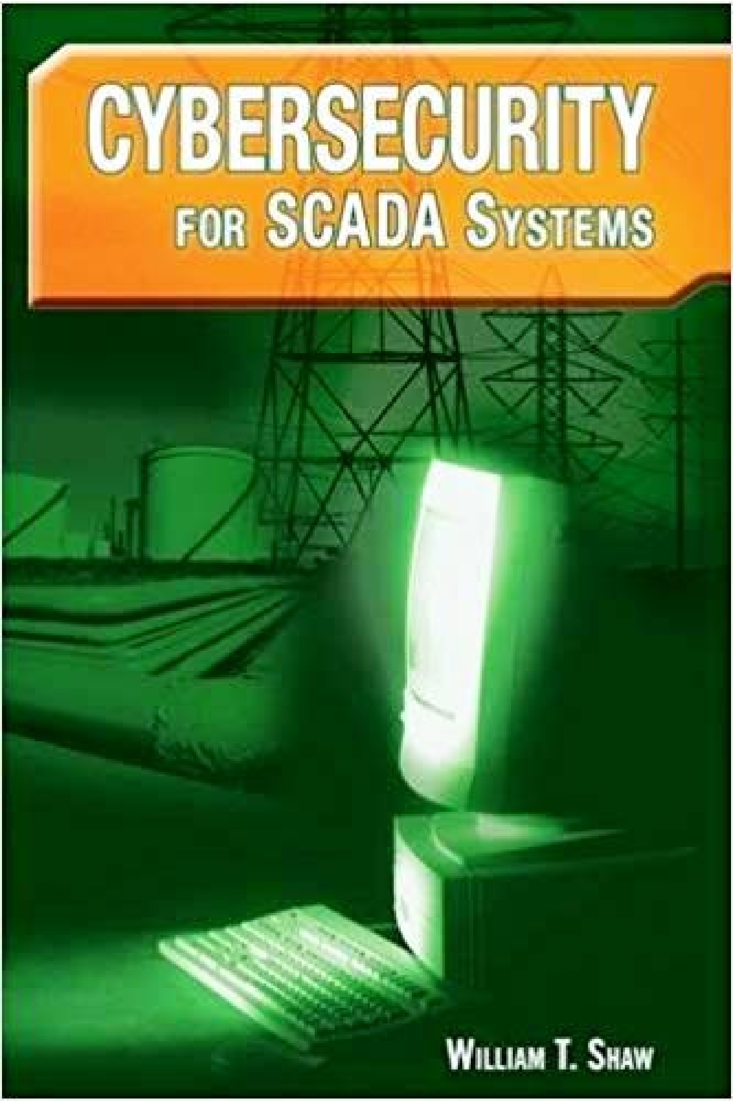


Advances in Information Security 66

Edward J. M. Colbert
Alexander Kott *Editors*

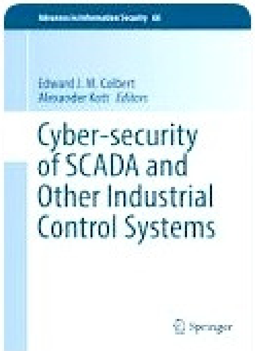
Cyber-security of SCADA and Other Industrial Control Systems

Springer



CYBERSECURITY FOR SCADA SYSTEMS

WILLIAM T. SHAW

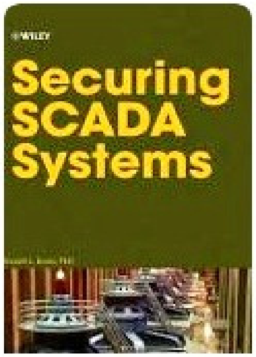


Advances in Information Security 66

Edward J. M. Colbert
Alexander Kott Editors

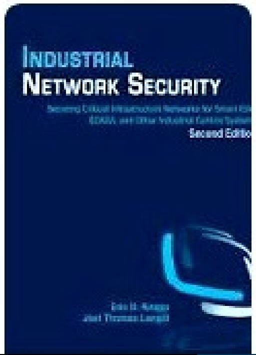
Cyber-security of SCADA and Other Industrial Control Systems

Springer



WILEY

Securing SCADA Systems

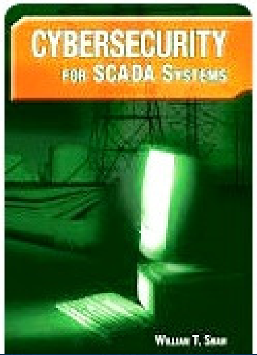


Industrial Network Security

Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems

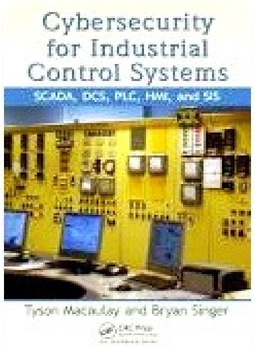
Second Edition

Eric D. Knapp
Joel Thomas Langill



Cybersecurity for SCADA Systems

William T. Shaw

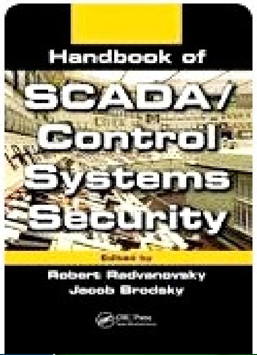


Cybersecurity for Industrial Control Systems

SCADA, DCS, PLC, HMI, and SIS

Tyson Macaulay and Bryan Singer

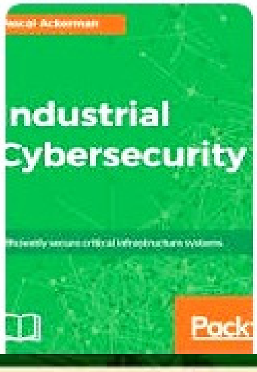
CRC Press



Handbook of SCADA/ Control Systems Security

Edited by
Robert Radvanovsky
Jacob Brodsky

CRC Press

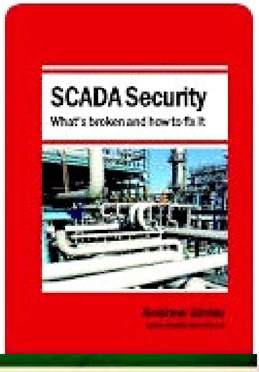


Pascal Ackerman

Industrial Cybersecurity

Efficiently secure critical infrastructure systems

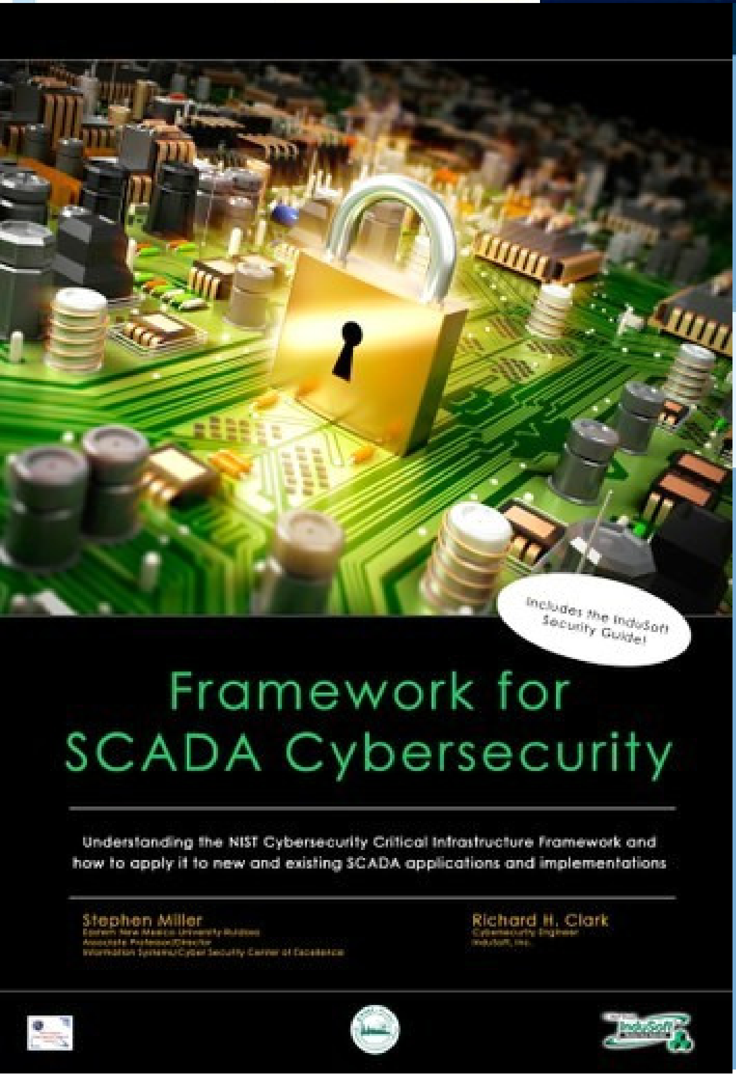
Packt



SCADA Security

What's broken and how to fix it

Andrew Ginter



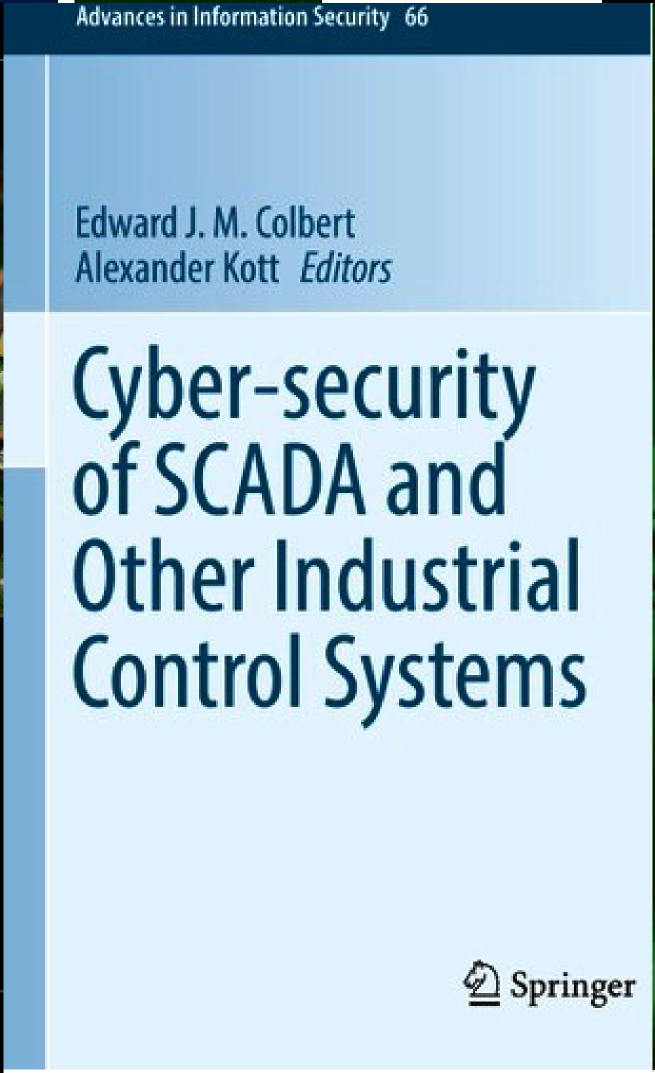
Includes the InduSoft Security Guide!

Framework for SCADA Cybersecurity

Understanding the NIST Cybersecurity Critical Infrastructure Framework and how to apply it to new and existing SCADA applications and implementations

Stephen Miller
Eastern New Mexico University-Ruidoso
Associate Professor/Director
Information Systems/Cyber Security Center of Excellence

Richard H. Clark
Cybersecurity Engineer
InduSoft, Inc.

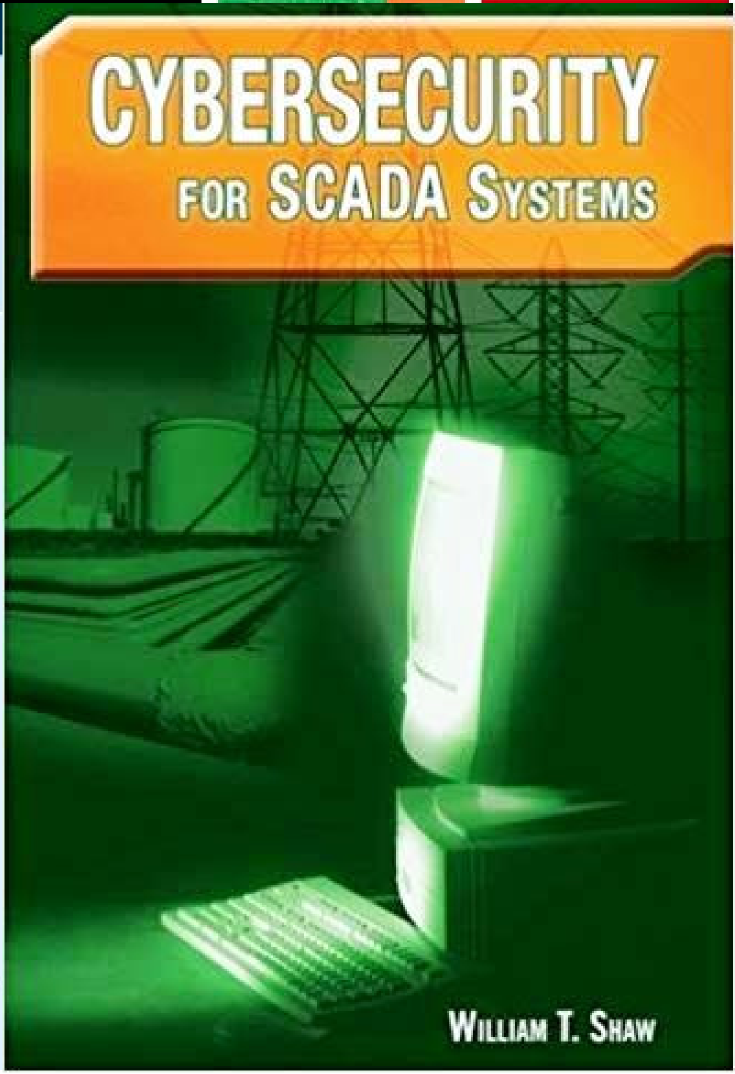


Advances in Information Security 66

Edward J. M. Colbert
Alexander Kott *Editors*

Cyber-security of SCADA and Other Industrial Control Systems

Springer



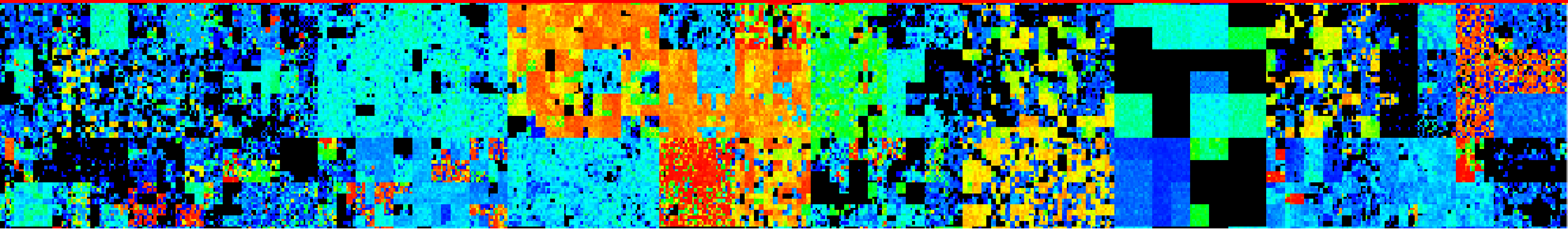
CYBERSECURITY FOR SCADA SYSTEMS

WILLIAM T. SHAW

Upgrading Industrial CyberSecurity!...

3- Case Studies: Recent Cyber Attacks!

"Crime, Spies & Terror"

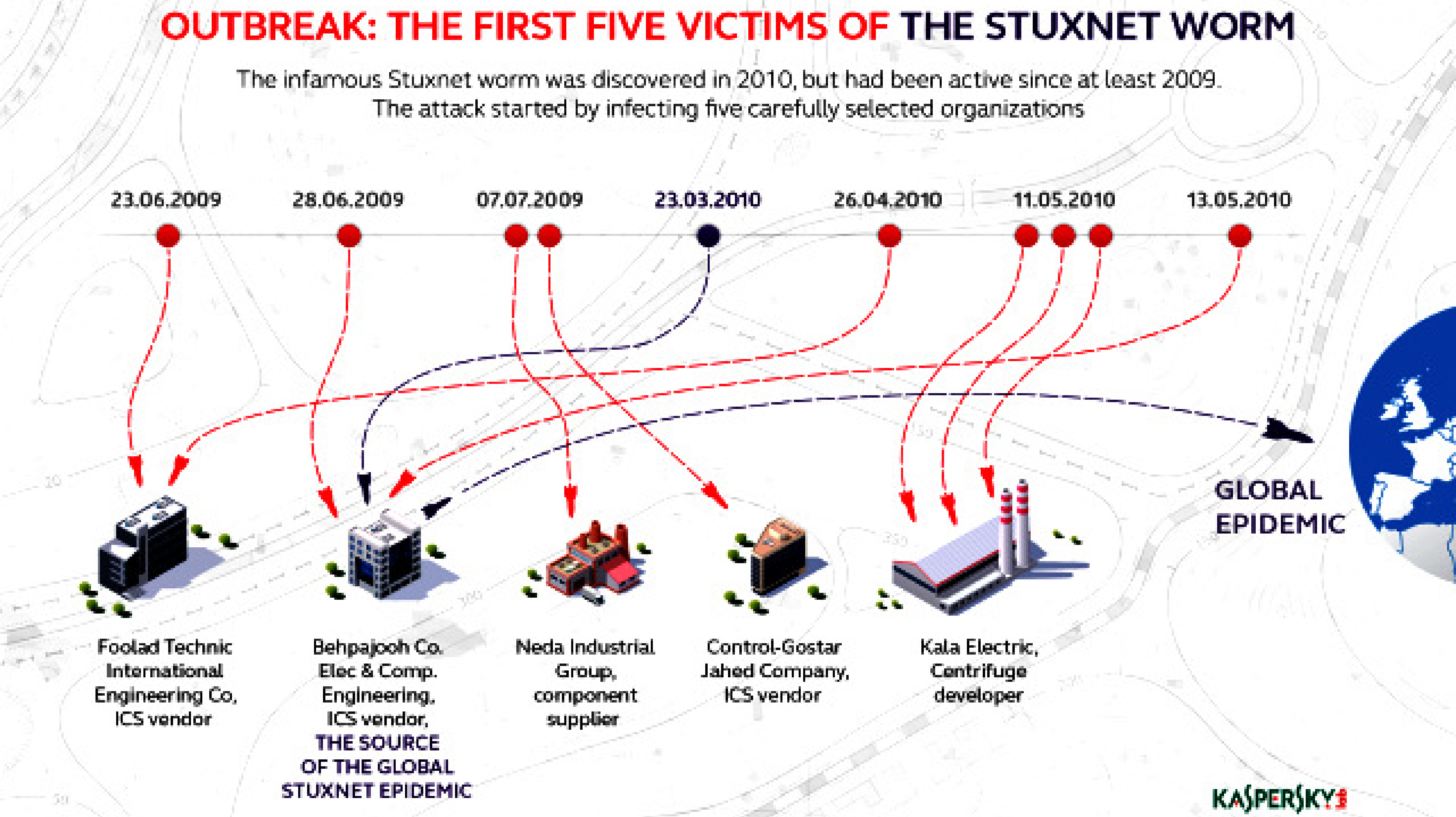


Case Studies: Recent Cyber Attacks!...

- Criminal Attacks: Recent surge of International Ransomware Attacks on Industrial Operations!..
- Industrial Cyber-Espionage: Much easier to “Spy” anonymously on-line for Industrial Secrets!...
- Political & Terror Attacks: Nation States are now using Custom Cyber Weapons to attack & disable Critical Infrastructure such as Stuxnet (2009)!..

High Risk Operations: Major Oil/Gas Refineries, Nuclear Power Stations & Industry are vulnerable to targeted Cyber Attacks on their ICS/SCADA Real-Time Operational Control Systems!........

10 Years since STUXNET Worm - 2009



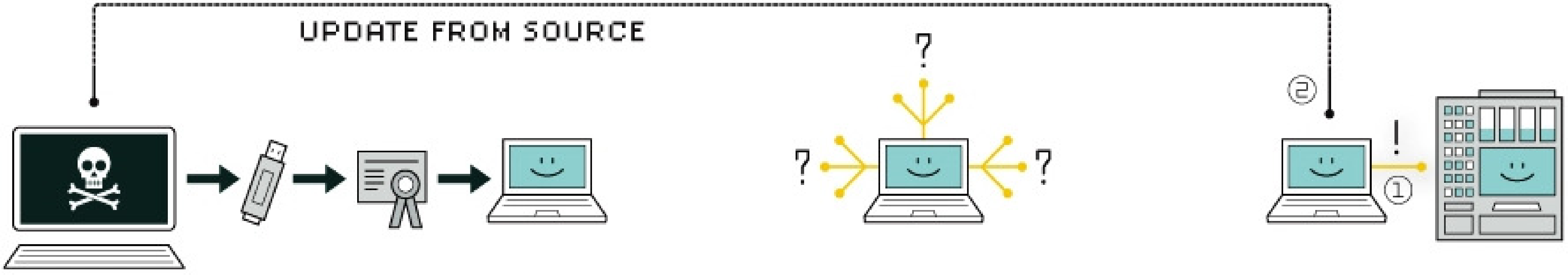
OUTBREAK: THE FIRST FIVE VICTIMS OF THE STUXNET WORM

The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2009.
The attack started by infecting five carefully selected organizations

23.06.2009
28.06.2009
07.07.2009
23.03.2010
26.04.2010
11.05.2010
13.05.2010
GLOBAL EPIDEMIC
Foolad Technic International Engineering Co, ICS vendor
Behpajooh Co. Elec & Comp. Engineering, ICS vendor, THE SOURCE OF THE GLOBAL STUXNET EPIDEMIC
Neda Industrial Group, component supplier
Control-Gostar Jahed Company, ICS vendor
Kala Electric, Centrifuge developer
KASPERSKY

STUXNET = Custom Malware targeted on ICS/SCADA

HOW STUXNET WORKED



1. infection

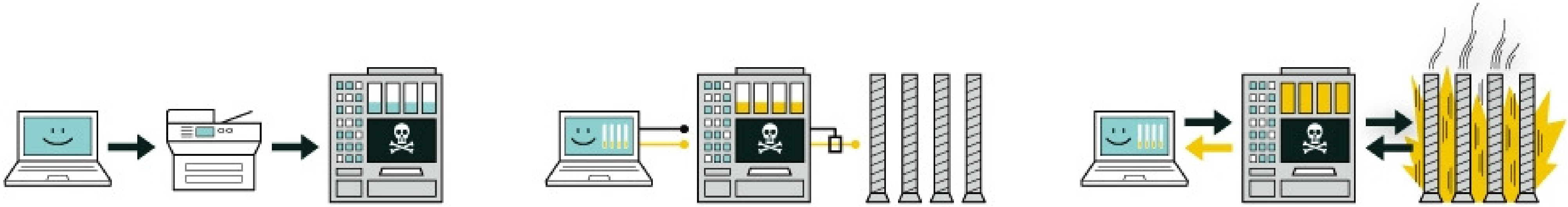
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Maersk: Global Ransomware - June 2017

Cost of Petya CyberAttack = $300Million!...

Norsk Hydro Cyber Attack – March 2019

- Company-Wide "LockerGogo" Ransomware Attack
- Large Impact upon Norsk Hydro Aluminium Production

- Estimated Q1 Cost of Attack = $52 Million!

SANS Security Institute: www.sans.org/ics

Control Systems Are a Target

www.sans.org/ics

www.securingthehuman.org

Network Access

- Internet accessible systems are being mapped by ERIPP or SHODAN, or are easily locatable through search engine queries
- Malware can spread vertically through the network by trusted system to system connections or VPN
- It is very easy to maneuver undetected throughout a control environment
- There is potential to leverage non-routable trusted communication paths

Interconnects

- ICS systems can be attacked by exploiting applications that communicate through network segmentation
- Connections to other organizations, plants or systems
- Many ICS environments are susceptible to network-based Man in the Middle Attacks

Dial-Up

- ICS assets can be remotely accessible through traditional dial-up modems that have little access control protections
- Numerous ICS assets at a location can be accessed through a single dial-up access point with a multiplex device that enables connections to many ICS assets
- Old attack vectors can still be successful in ICS environments

System Management

- Attackers can take advantage of long delays in patching and operating system upgrades
- Attackers can take advantage of systems with no anti-virus, or out-of-date signatures
- Attackers will leverage default usernames and passwords or weak authentication mechanisms
- Attacks will be difficult to detect due to minimal asset security logging capability
- Attackers will leverage file access techniques to move data in and out of the ICS environment through physical removable media or trusted communication paths utilized for system maintenance

Supply Chain

- Third party vendors, contractors or integrators can be attacked in an attempt to ultimately attack an ICS asset owner or multiple asset owners
- ICS hardware and software can be directly breached or impacted prior to arriving in the production ICS environment

You may not realize it, but your organization's Industrial Control System (ICS) environments are a target for cyber attackers. The ICS automation, process control, access control devices, system accounts and asset information all have tremendous value to attackers. This poster demonstrates the many different ways attackers can gain access to an ICS environment and demonstrates the need for active security efforts and ICS engineer training that will enable informed engineering decisions and reenforce secure behaviors when interacting with an Industrial Control System.

In many cases these are not one-off attacks, but are planned for with reconnaissance, multiple attacks and adjustments. These are campaigns that happen over the course of months, and they require system owners and operators to be vigilant and recognize when something is not right.

ICS Security goal: Ensure the safe, reliable and secure operation of ICS environments from procurement to retirement

Abnormal activity or unexplained errors deserve a closer security look

Governance

- Attackers can leverage the lack of corporate security policies, procurement language, asset inventory and standardization that exist in many ICS environments
- Attackers can have greater impacts on ICS environments, as ICS assets are often not considered in the preparation phase of security incident response planning and containment approaches
- ICS risk and hazard assessment are not always evaluated with the loss of cyber integrity which, can lead to a loss of availability, impacts due to interdependencies and misuse of critical components or functions
- In some sectors ICS assets are often architected or assessed from a compliance perspective and not always assessed from a security perspective

Social Engineering

- Request for Proposals often contain a wealth of information regarding an ICS environment
- Vendors frequently post information about a project they are working on for an ICS customer
- Employee social media sites often contain technology architecture information and, possibly, images of ICS work environments
- Engineer professional bios can provide a helpful map of your ICS
- Publically available information regarding an ICS asset owners' vendor relationships, conference attendance, committee participation and domain registrations can all be leveraged against the organization

Physical Security

- Attackers can leverage the physical locations of numerous ICS assets that could be located in remote geographies or are unmonitored, even when little to no physical access controls ICS assets can be physically stolen or obtained
- ICS assets can be physically stolen or obtained secondhand with access to sensitive information that could be used in planning an attack
- Physical changes or alterations to ICS devices are often difficult to detect

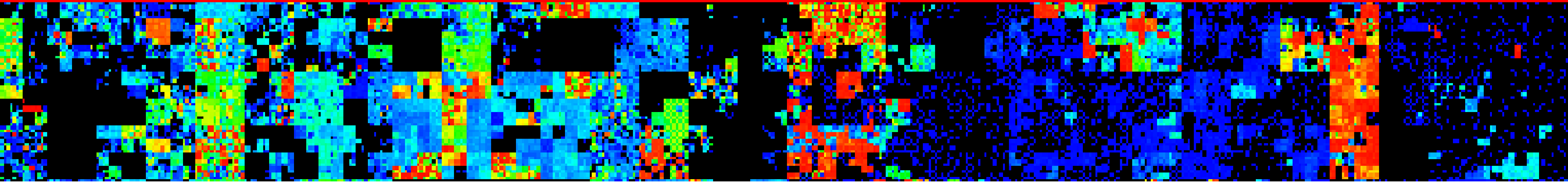
Cyber Actors

- Nation States
- Insiders and other trusted parties (such as contractors / vendors / integrators)
- Criminal Hacker
- Politically motivated attackers (hacktivists)
- Script Kiddies

Upgrading Industrial CyberSecurity!...

4 – Security Transition: 2020 to 2025+

"Physical to Cyber"



Ship: HMT Ascanius – Devonport to Durban - 1917

Security Transition: 2020 to 2025+

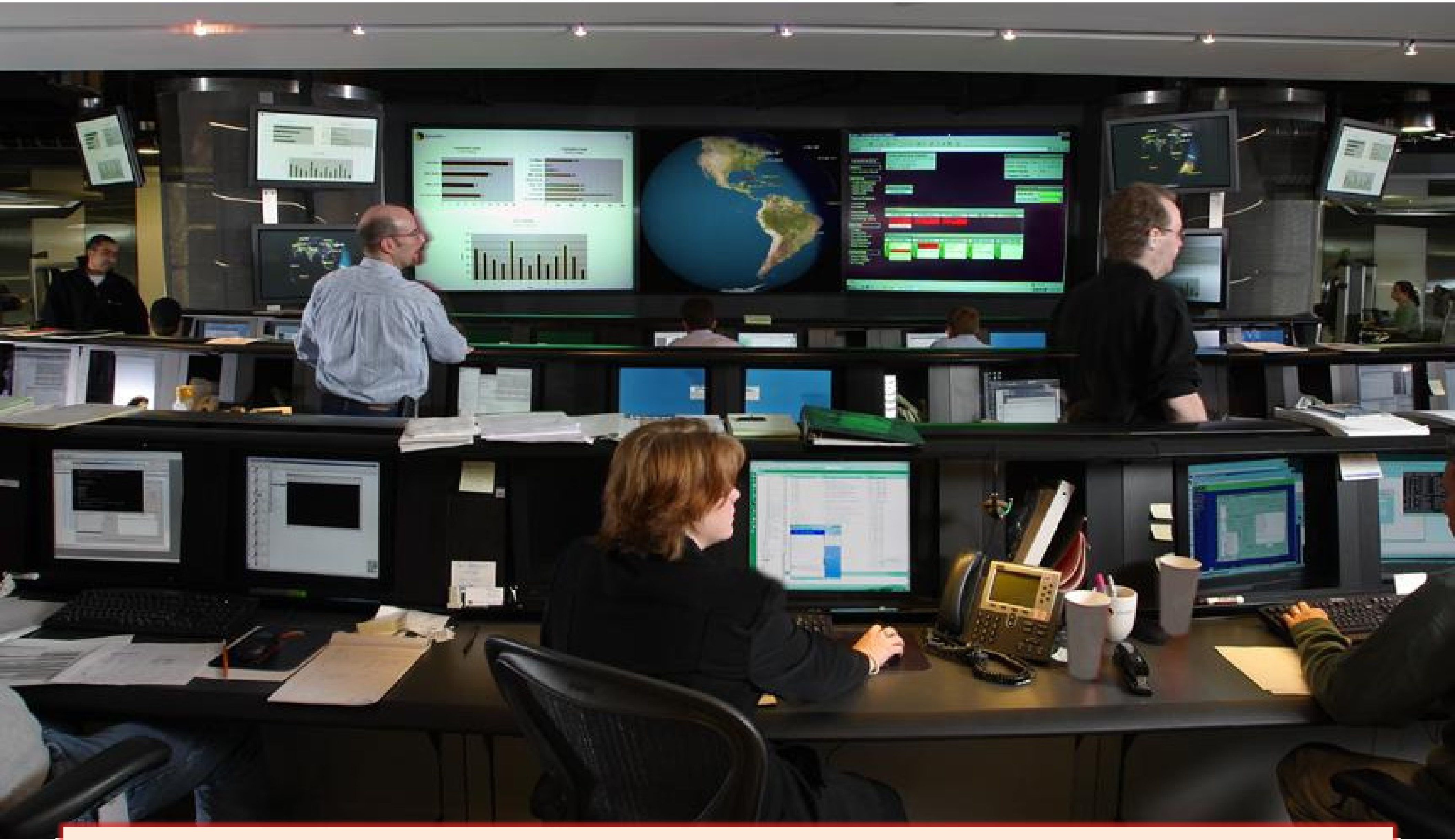
- Physical Security: Critical Industries & Energy Sites traditionally focused on Physical Security such as Perimeters, Access Control & Guards
- CyberSecurity: Industries are now investing in advanced cyber operations due to recent increase in significant cyber threats & attacks

Integrated Cyber-Physical Security: The Industry/Energy Sector will require $ignficant Investment over 5 to10 Years to Transition from 20th Physical Security to Integrated 21stC Cyber-Physical Operations!

Critical Energy Industry Sector: *“Cybersecurity for Industrial Automation & Control Systems (IACS)”*

Cyber Defence against “Stuxnet” Custom Malware that attacks ICS/SCADA (2009)

Cyber Ops: Integrated Command & Control



- *Security Operations Command Centre for Global Security Solutions Enterprise*

Evolution of ”*Cyber-Physical*” Solutions

- **Systems of Systems**
  - Collocation of CPS which intelligently combine their individual abilities in order to provide new abilities
- **Networked intelligent components**
  - Systems composed of several actors and sensors with central intelligence
  - Central interface outwards
    → limited access on subcomponents

Image: GHV

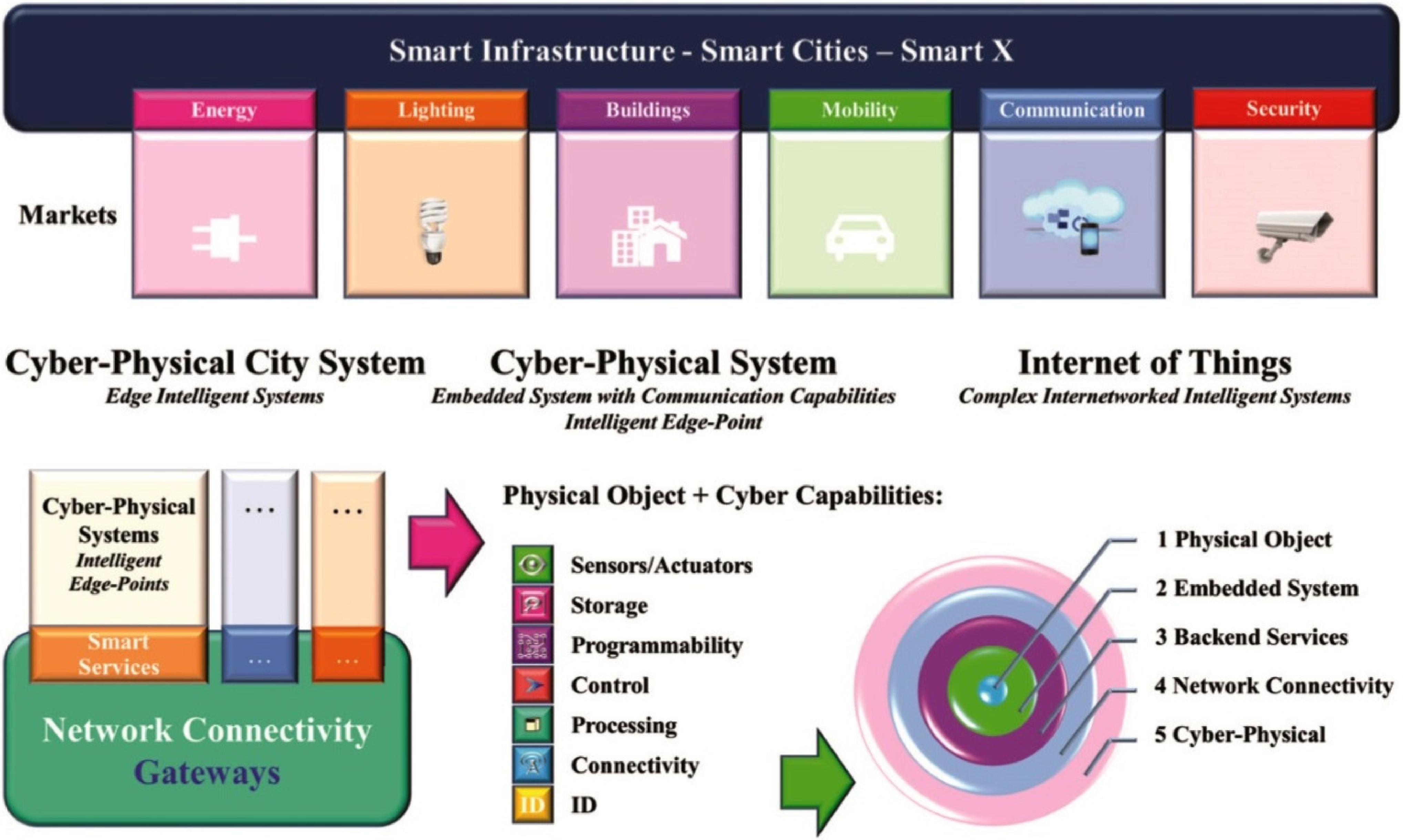
- **Active sensors and actors**
  - Systems with exactly defined, relatively small range of functions

CPS:
cyber-physical
system

- **RFID (Passive)**
  - Distinct (unique) identification
  - Intelligence of the system can be provided only by central services

RFID:
radio
frequency
identification

Cyber-Physical Systems as Basis of *"IoT"*



Smart Infrastructure - Smart Cities – Smart X

Markets

Energy

Lighting

Buildings

Mobility

Communication

Security

Cyber-Physical City System

Edge Intelligent Systems

Cyber-Physical System

Embedded System with Communication Capabilities
Intelligent Edge-Point

Internet of Things

Complex Internetworked Intelligent Systems

Cyber-Physical Systems
Intelligent Edge-Points

…

…

Smart Services

…

…

Network Connectivity
Gateways

Physical Object + Cyber Capabilities:

Sensors/Actuators

Storage

Programmability

Control

Processing

Connectivity

ID

1 Physical Object

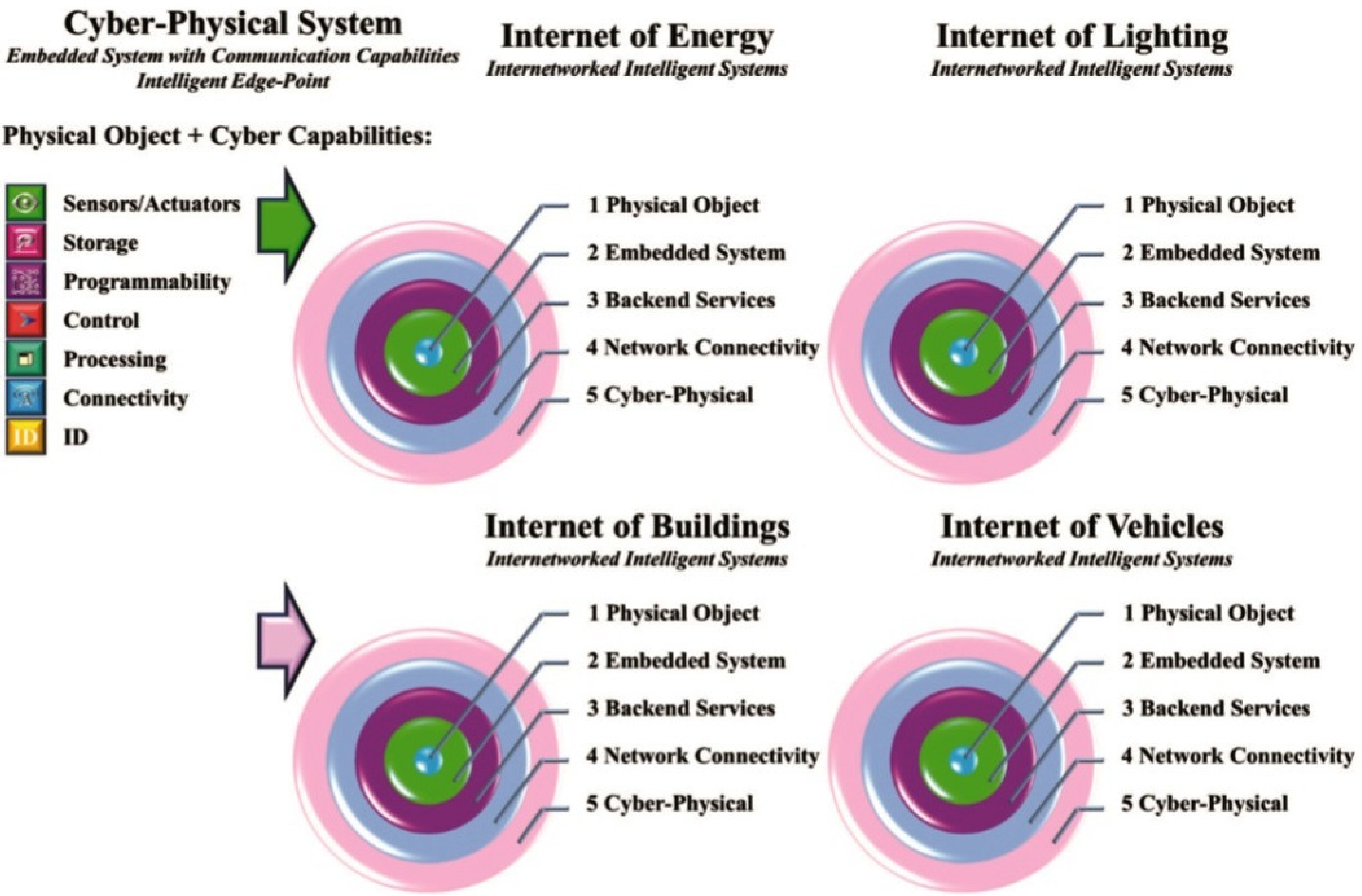
2 Embedded System

3 Backend Services

4 Network Connectivity

5 Cyber-Physical

Cyber-Physical System Modules for "IoT"



Cyber-Physical System

Embedded System with Communication Capabilities
Intelligent Edge-Point

Physical Object + Cyber Capabilities:

- Sensors/Actuators
- Storage
- Programmability
- Control
- Processing
- Connectivity
- ID

Internet of Energy

Internetworked Intelligent Systems

1 Physical Object
2 Embedded System
3 Backend Services
4 Network Connectivity
5 Cyber-Physical

Internet of Lighting

Internetworked Intelligent Systems

1 Physical Object
2 Embedded System
3 Backend Services
4 Network Connectivity
5 Cyber-Physical

Internet of Buildings

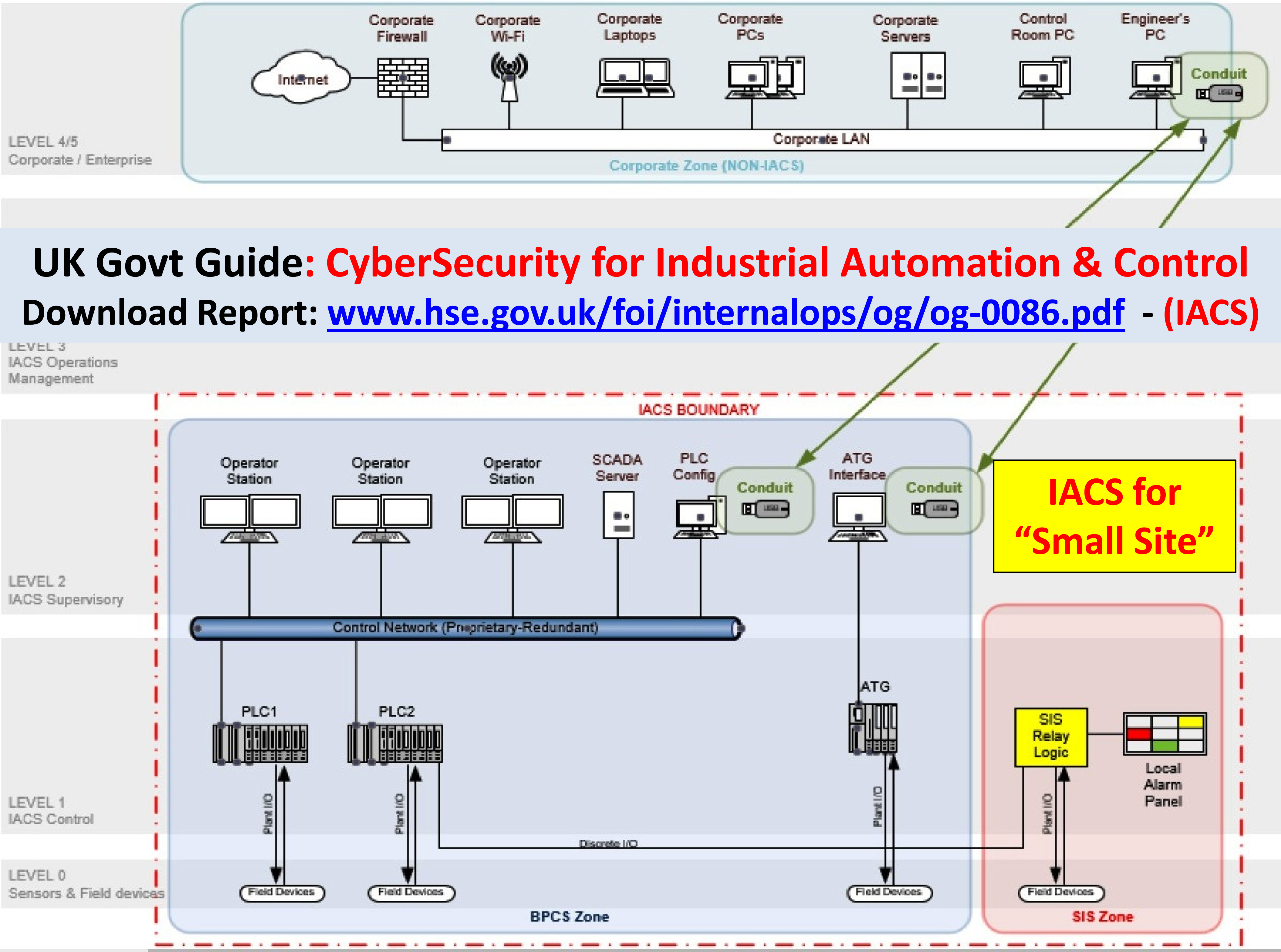
Internetworked Intelligent Systems

1 Physical Object
2 Embedded System
3 Backend Services
4 Network Connectivity
5 Cyber-Physical

Internet of Vehicles

Internetworked Intelligent Systems

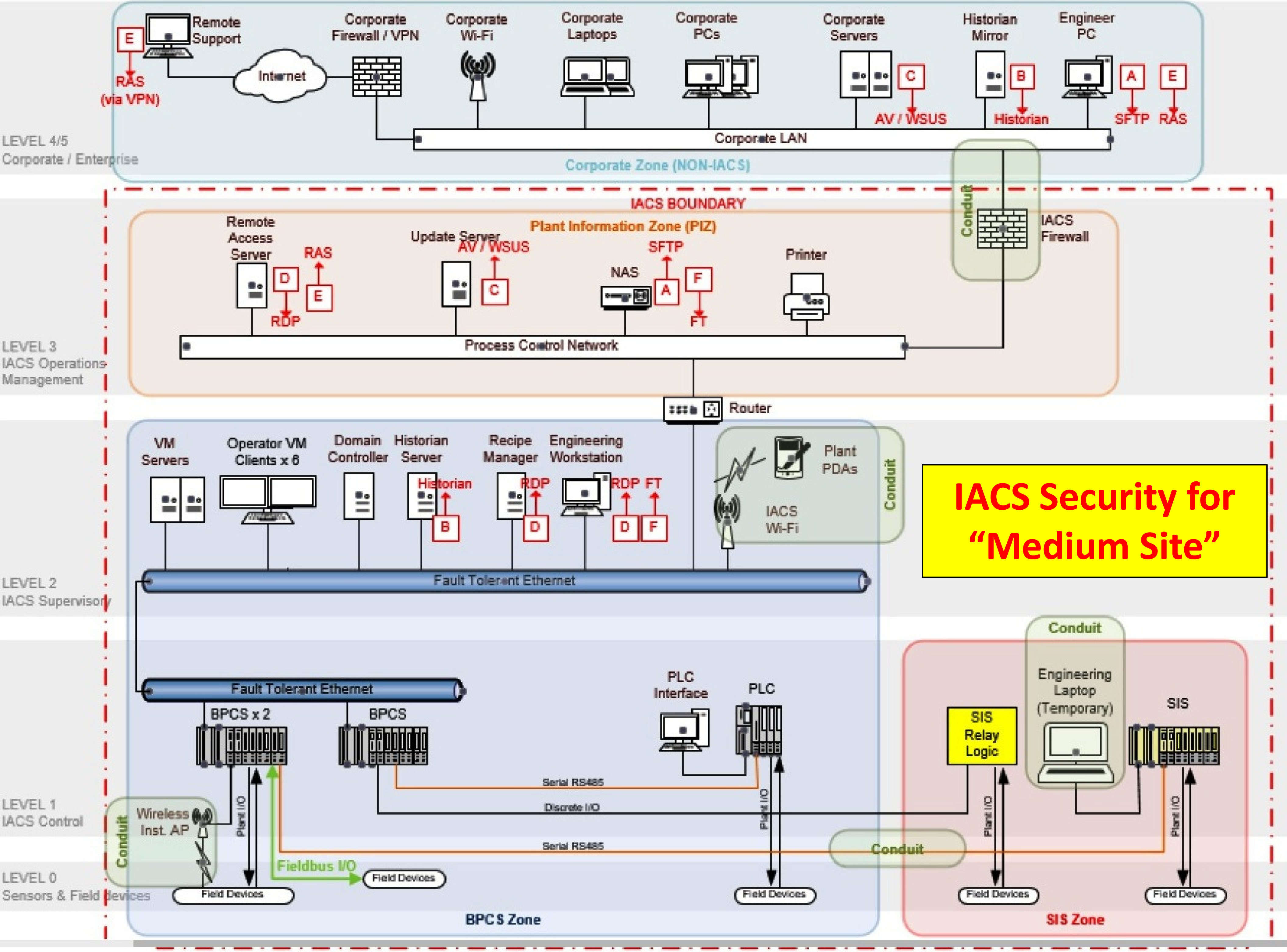
1 Physical Object
2 Embedded System
3 Backend Services
4 Network Connectivity
5 Cyber-Physical



UK Govt Guide: CyberSecurity for Industrial Automation & Control

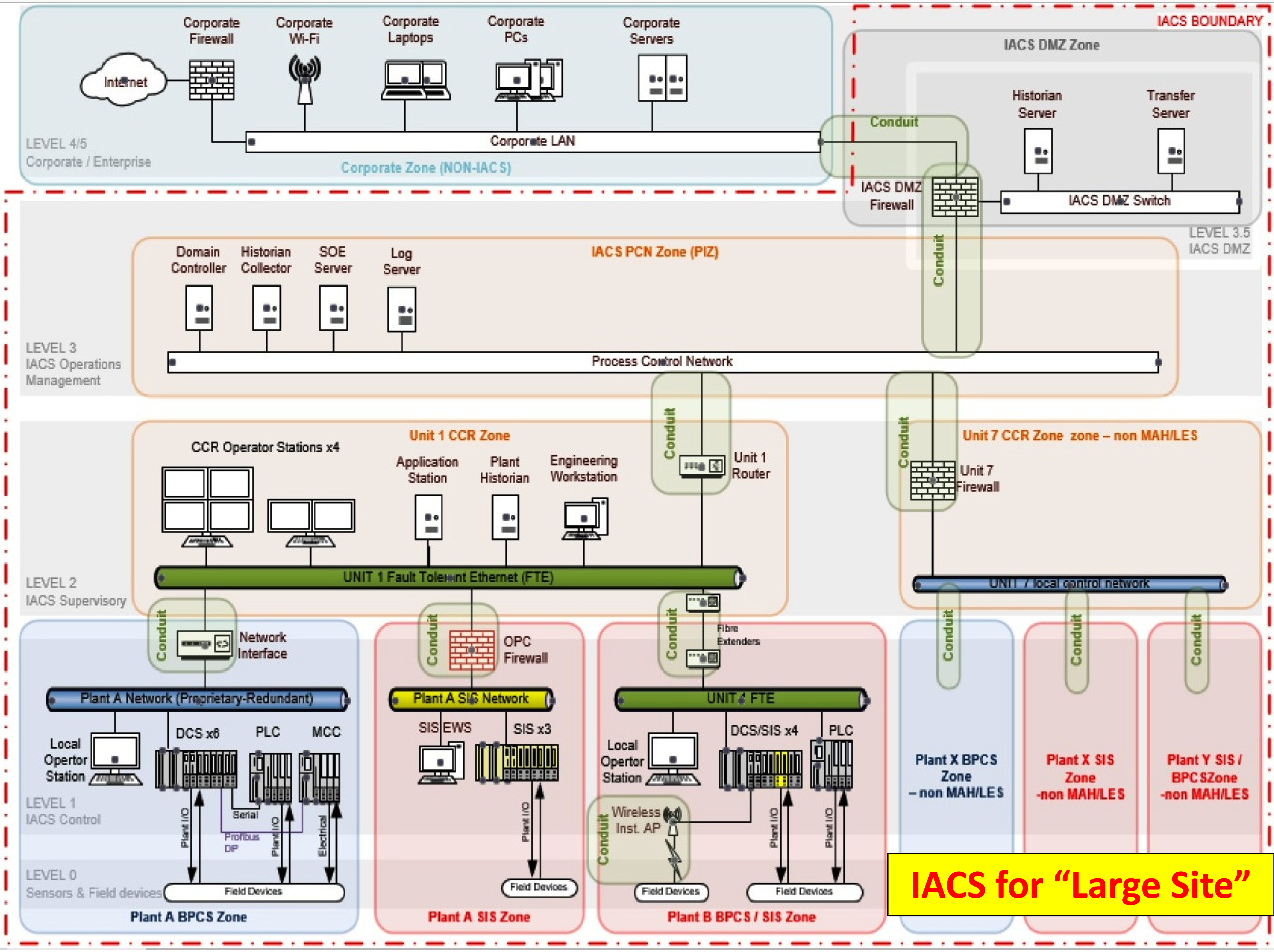
Download Report: www.hse.gov.uk/foi/internalops/og/og-0086.pdf - (IACS)

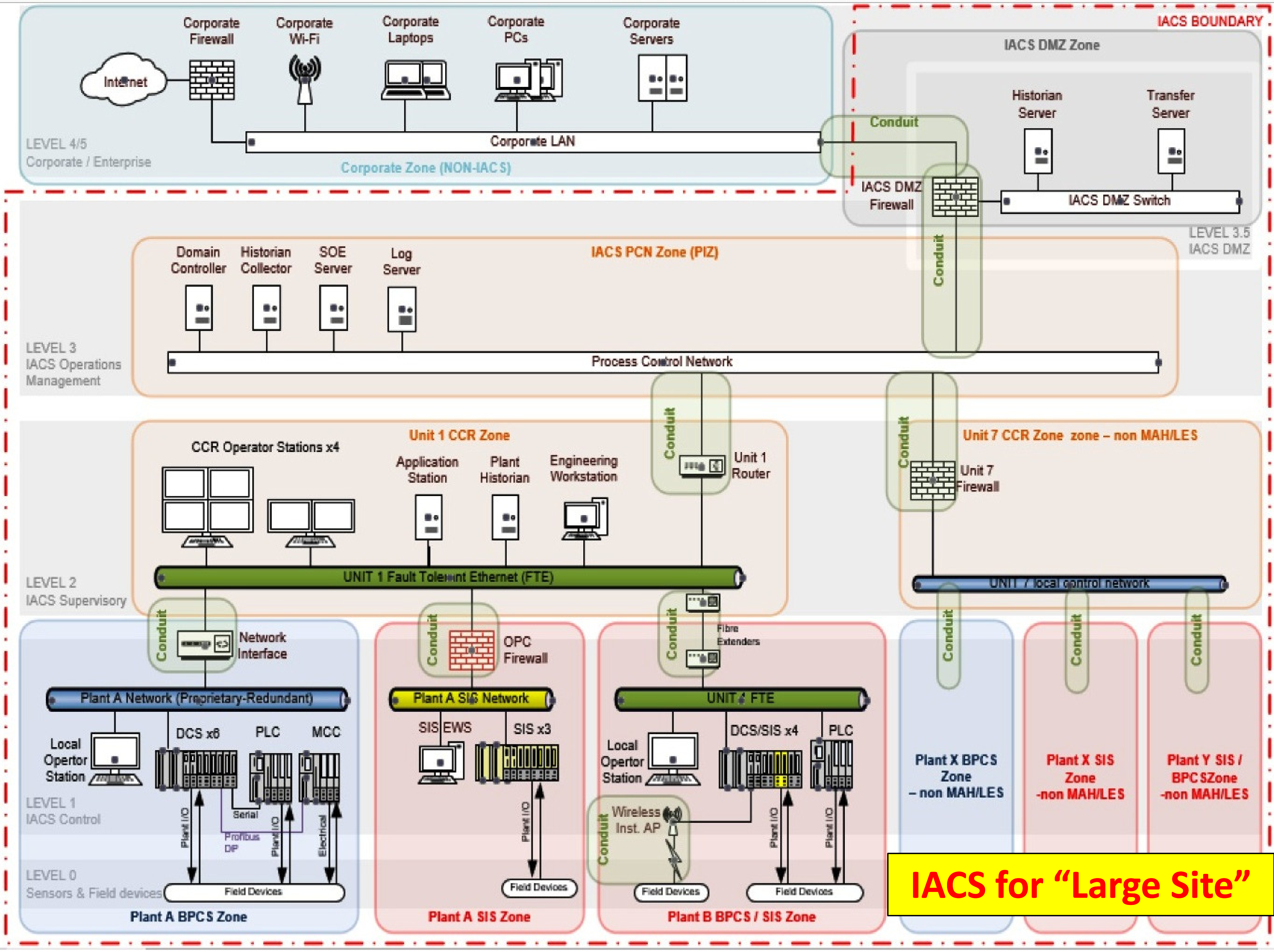
IACS for "Small Site"



IACS Security for "Medium Site"

IACS for “Large Site”



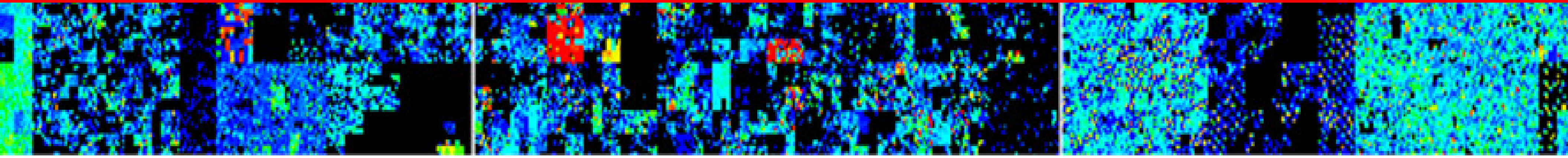


IACS for “Large Site”

Upgrading Industrial CyberSecurity!...

5 – Critical Sector Supply Chains!...

"Asset Authentication"



Critical Sector Supply Chains!...

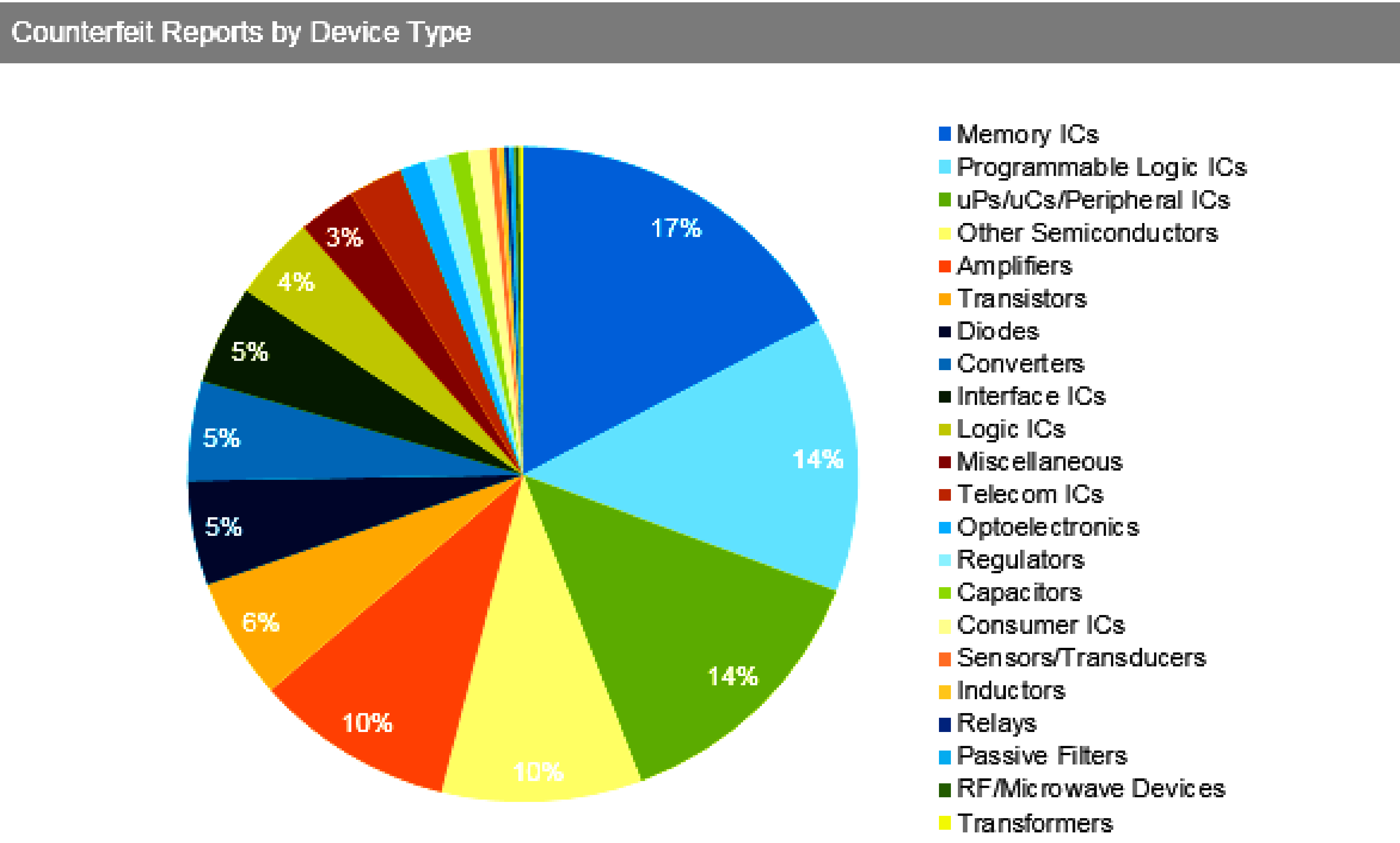
Critical Infrastructure is Highly Vulnerable to Penetration through the Asset Supply Chains!

- Software Apps: Software Patches, Upgrades & Apps should ALL be tested & securely sourced!
- Hardware Supply: Devices, Processors & Chips also need testing from reputable suppliers!
- Network Systems: Regular checks on Internet, Wi-Fi & Mobile Comms + USB & Cloud Storage!

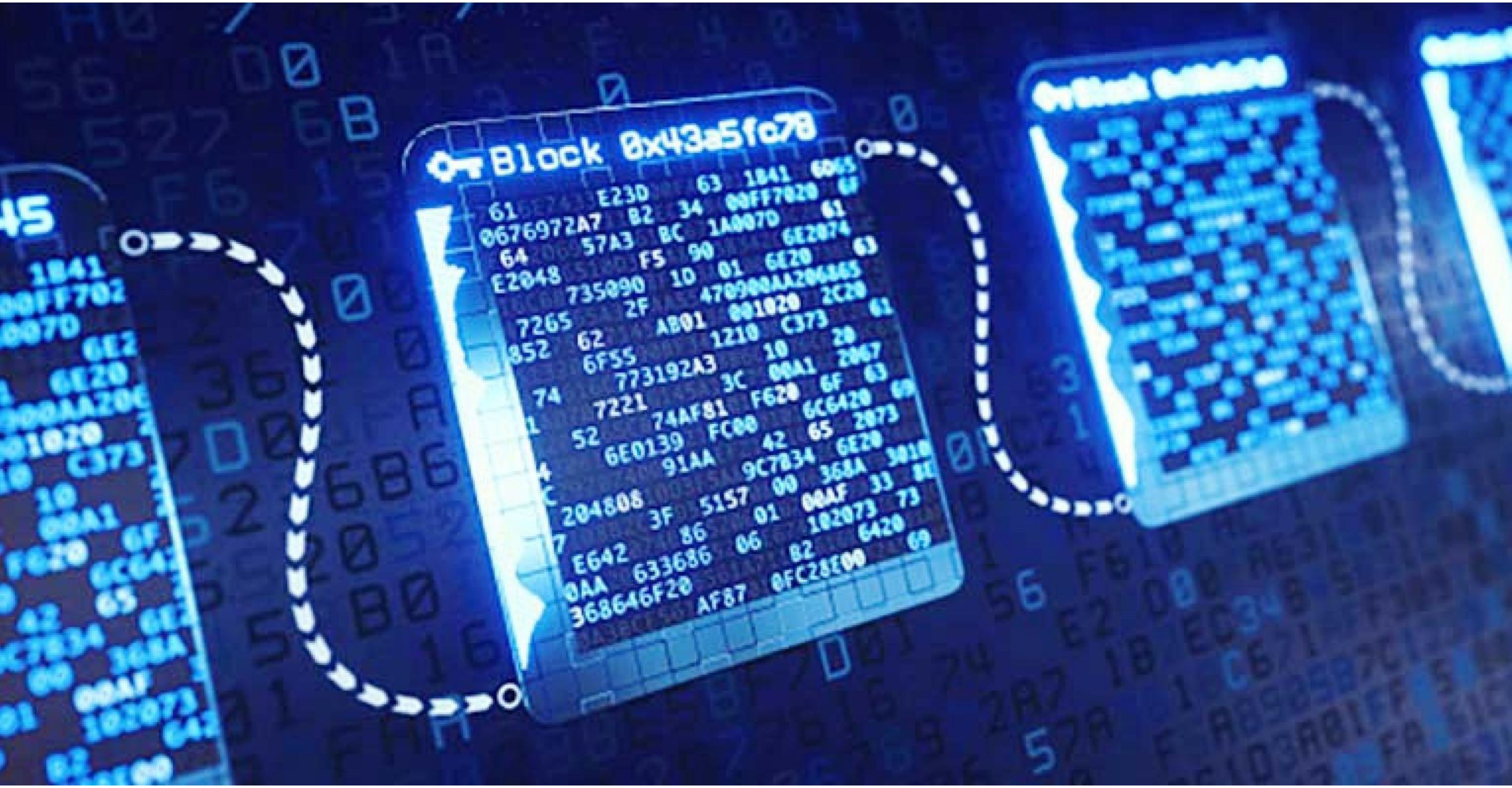
Test & Check ALL Software, Hardware & Network Components from **S**ource to **S**ystem Installation!...

Counterfeit Industrial Components

- Backdoor for Cyber Intrusion & Attacks -



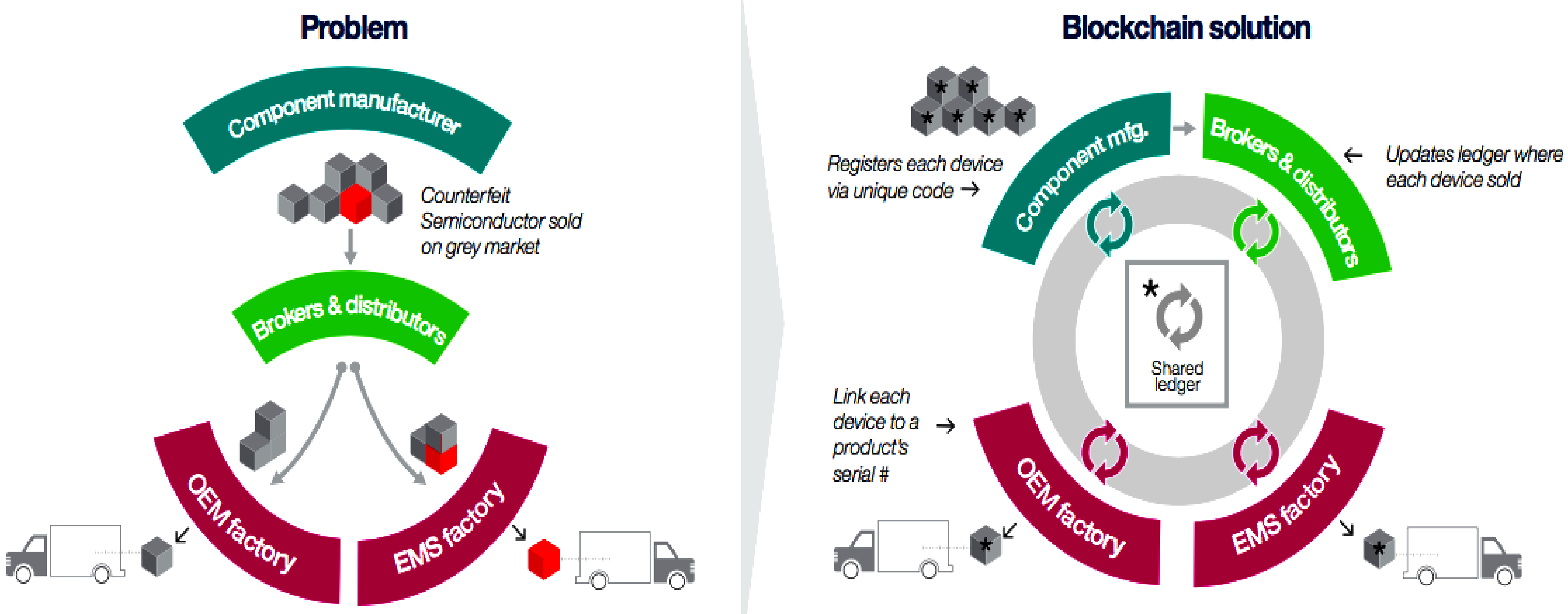
Blockchain Applications to Supply Chains



Industries *upgrade* to Intelligent Supply Chain Tracking in next 5 years!

Blockchain Applications to Supply Chains

Counterfeit prevention

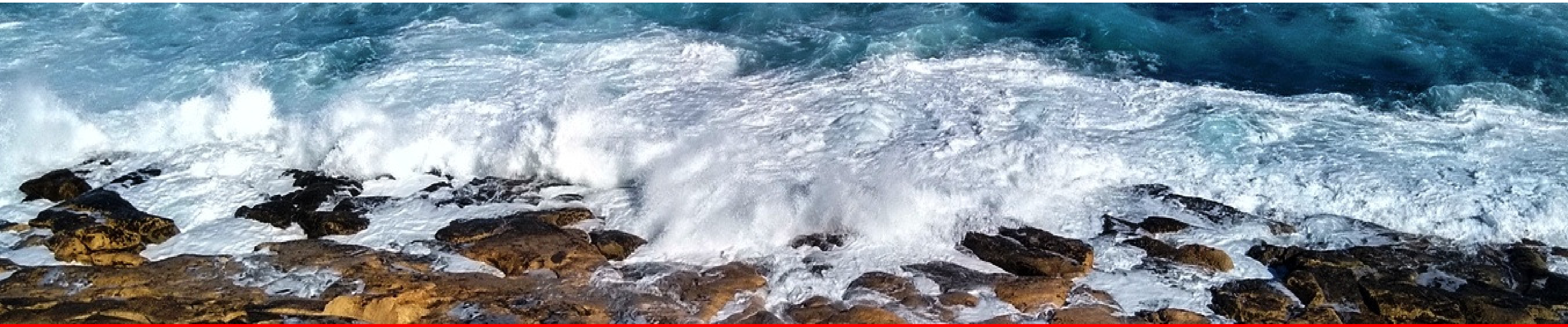

Problem
Component manufacturer
Counterfeit Semiconductor sold on grey market
Brokers & distributors
OEM factory
EMS factory
Blockchain solution
Registers each device via unique code →
Component mfg.
Brokers & distributors
← Updates ledger where each device sold
Shared ledger
Link each device to a product's serial # →
OEM factory
EMS factory

High-end semiconductors are sometimes faked and sold on the grey market.

The semiconductor manufacturer adds a unique code to each device, then registers it in a ledger where it is tracked and traced.

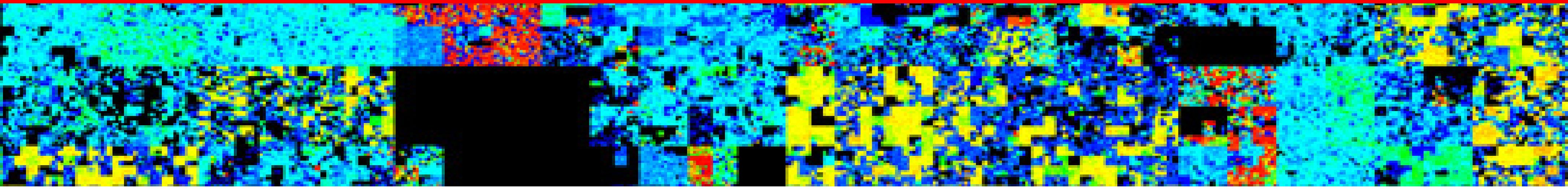
Industries *upgrade* to Intelligent Supply Chain Tracking in next 5 years!

Upgrading Industrial CyberSecurity!...



6 – Cyber Surveillance & Espionage

“Systems Privacy”



Cyber Surveillance & Espionage!...

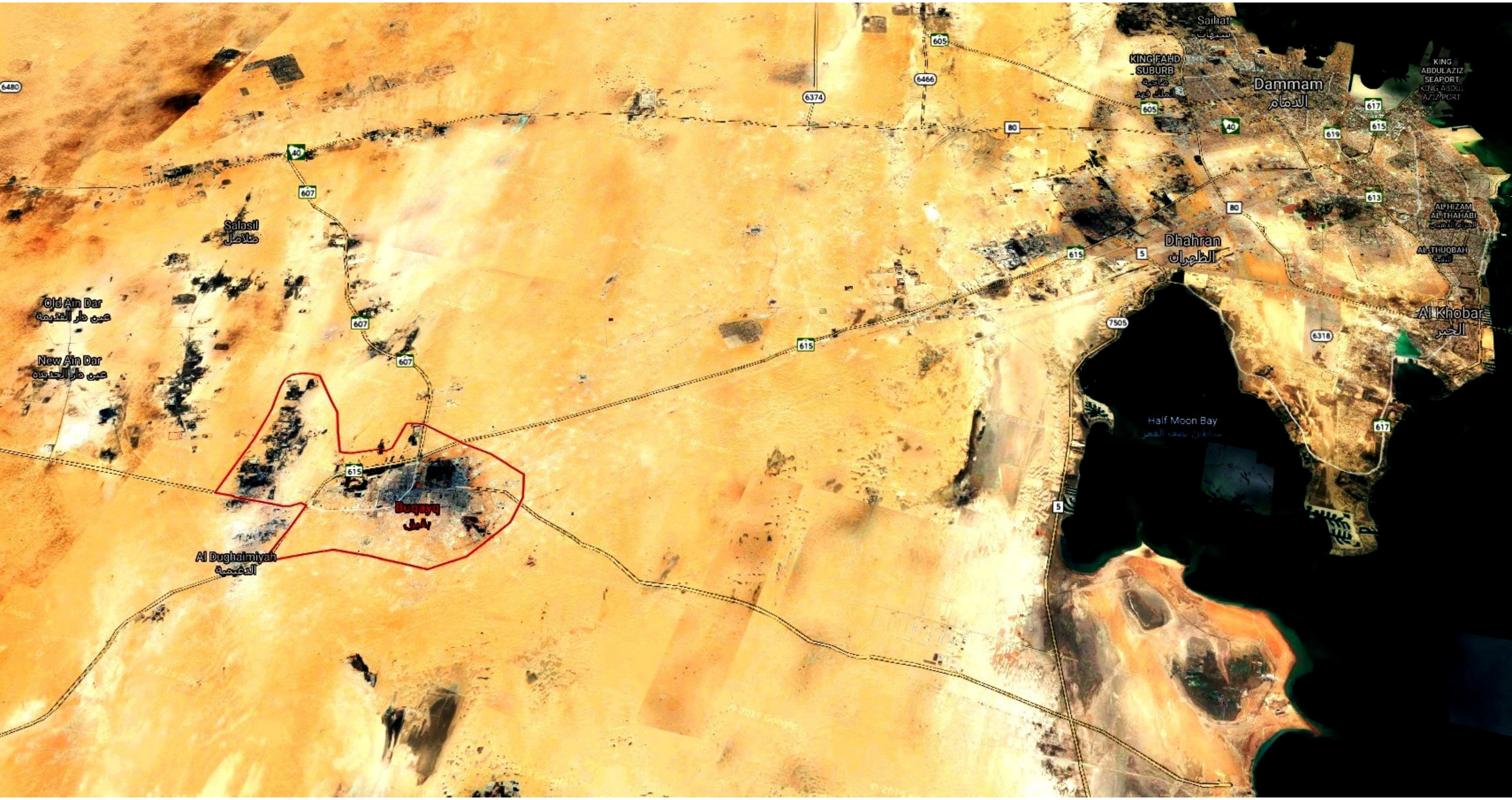
Critical National Sectors such as Energy, Oil/Gas & Defence are open for **Cyber S**urveillance & **E**spionage!

- Industrial Surveillance: Competitors, Governments & Political Agents will use *Cyber Attacks* to steal Product Designs, Patents & Industrial Secrets!...
- Criminal Espionage: Criminals Groups now target Critical Sectors & *Trade* Industrial Knowledge!...

Industrial Data is now more valuable than Oil & Gold!

........*YOUR* Systems Security & Privacy is now *Critical*!

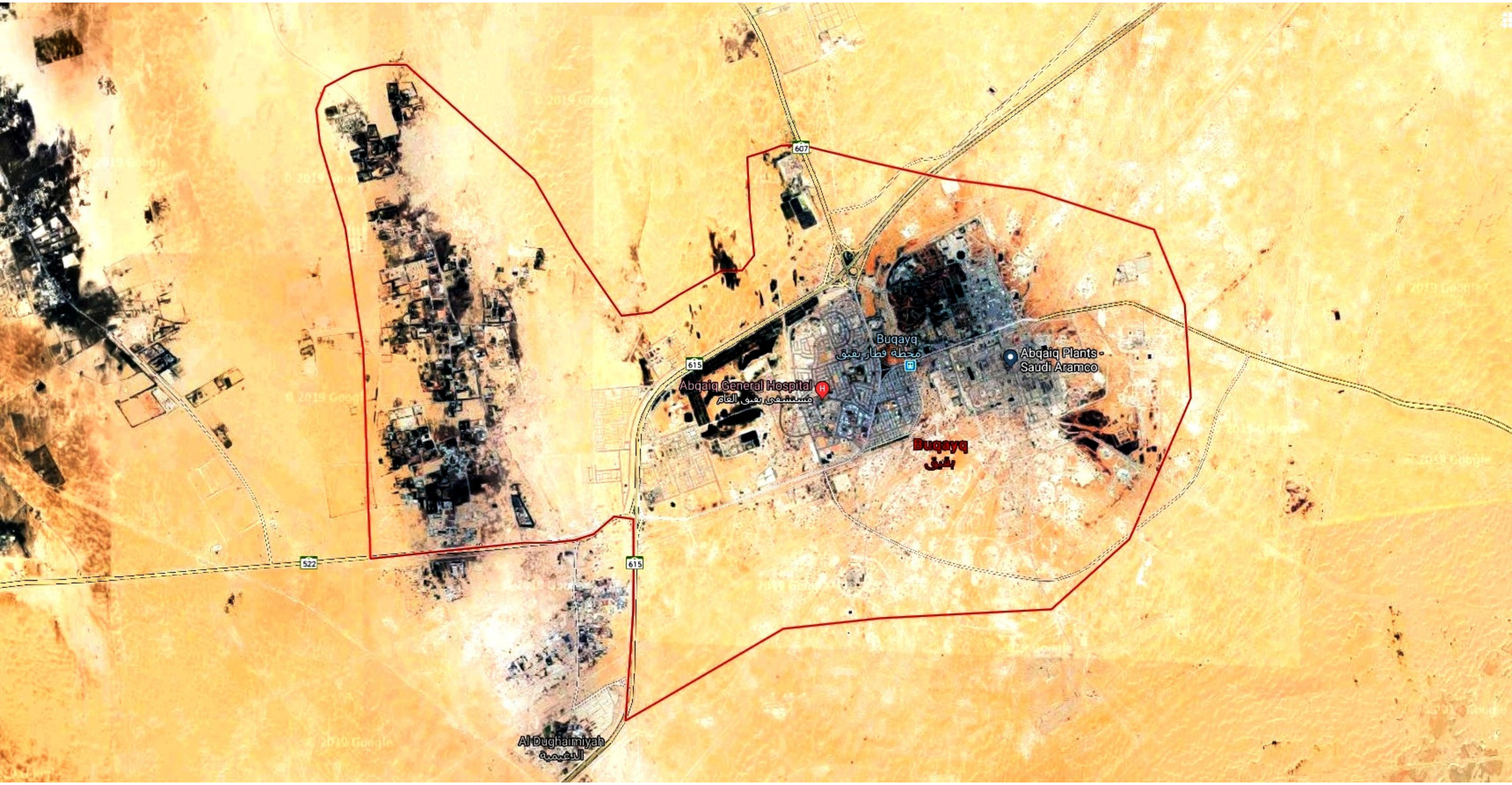
Aerial Surveillance: Oil/Gas Refineries



Abqaiq–Khurais - Aramco Oil Refineries: Drone Attack – 14th Sept 2019

Public Domain Satellite Images: Google Maps

Aerial Surveillance: Oil/Gas Refineries



Abqaiq–Khurais - Aramco Oil Refineries: Drone Attack – 14th Sept 2019

Public Domain Satellite Images: Google Maps

40th International East-West Security Conference

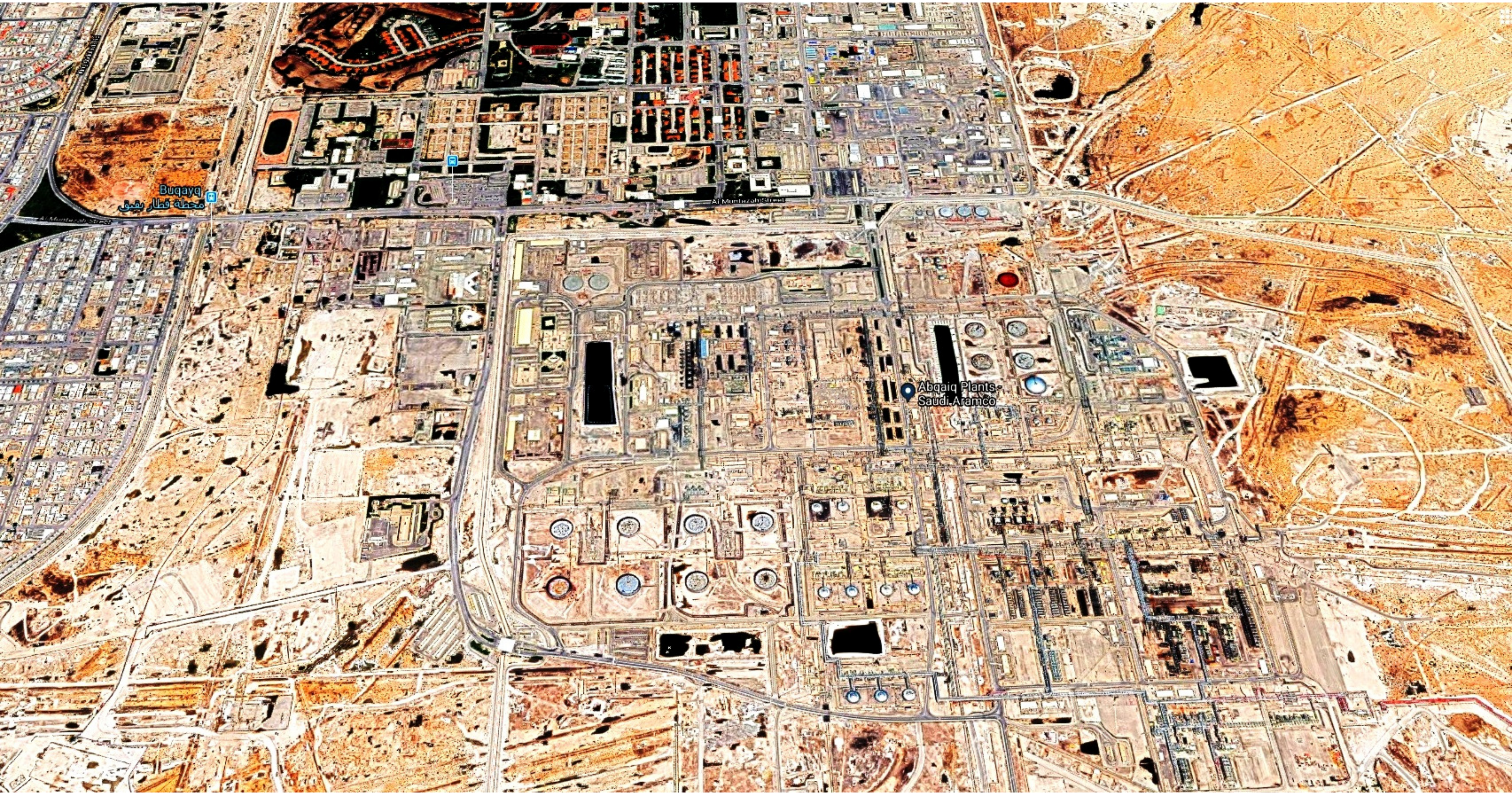
“ Upgrading Industrial Cybersecurity ”

- Securing Critical National Infrastructure-

St Julians, Malta – 10th / 11th Nov 2019

© *Dr David E. Probert : www.VAZA.com* ©

Aerial Surveillance: Oil/Gas Refineries



Abqaiq–Khurais - Aramco Oil Refineries: Drone Attack – 14th Sept 2019

Public Domain Satellite Images: Google Maps

40th International East-West Security Conference

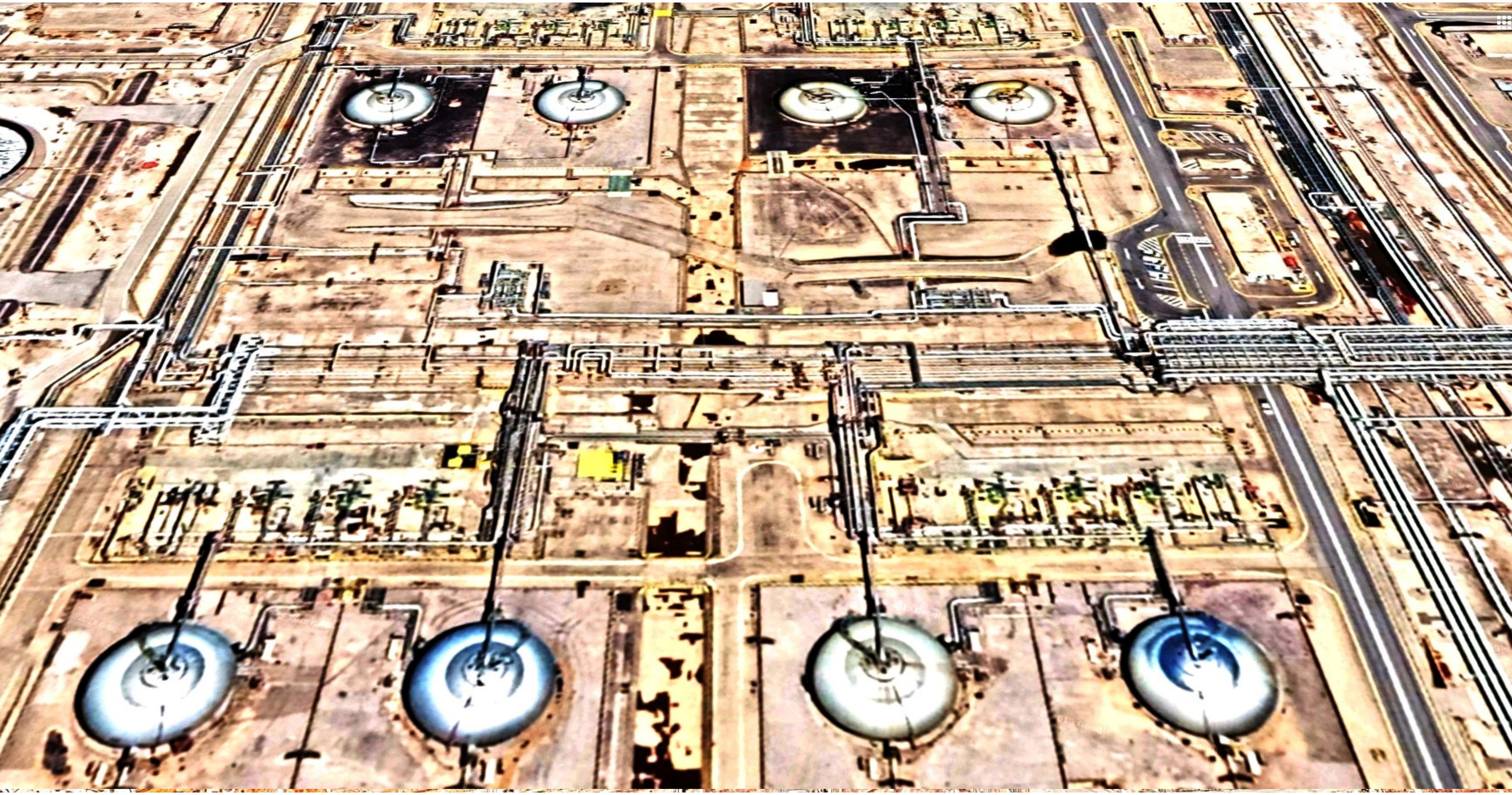
" Upgrading Industrial Cybersecurity "

- Securing Critical National Infrastructure-

St Julians, Malta – 10th / 11th Nov 2019

© Dr David E. Probert : www.VAZA.com ©

Aerial Surveillance: Oil/Gas Refineries

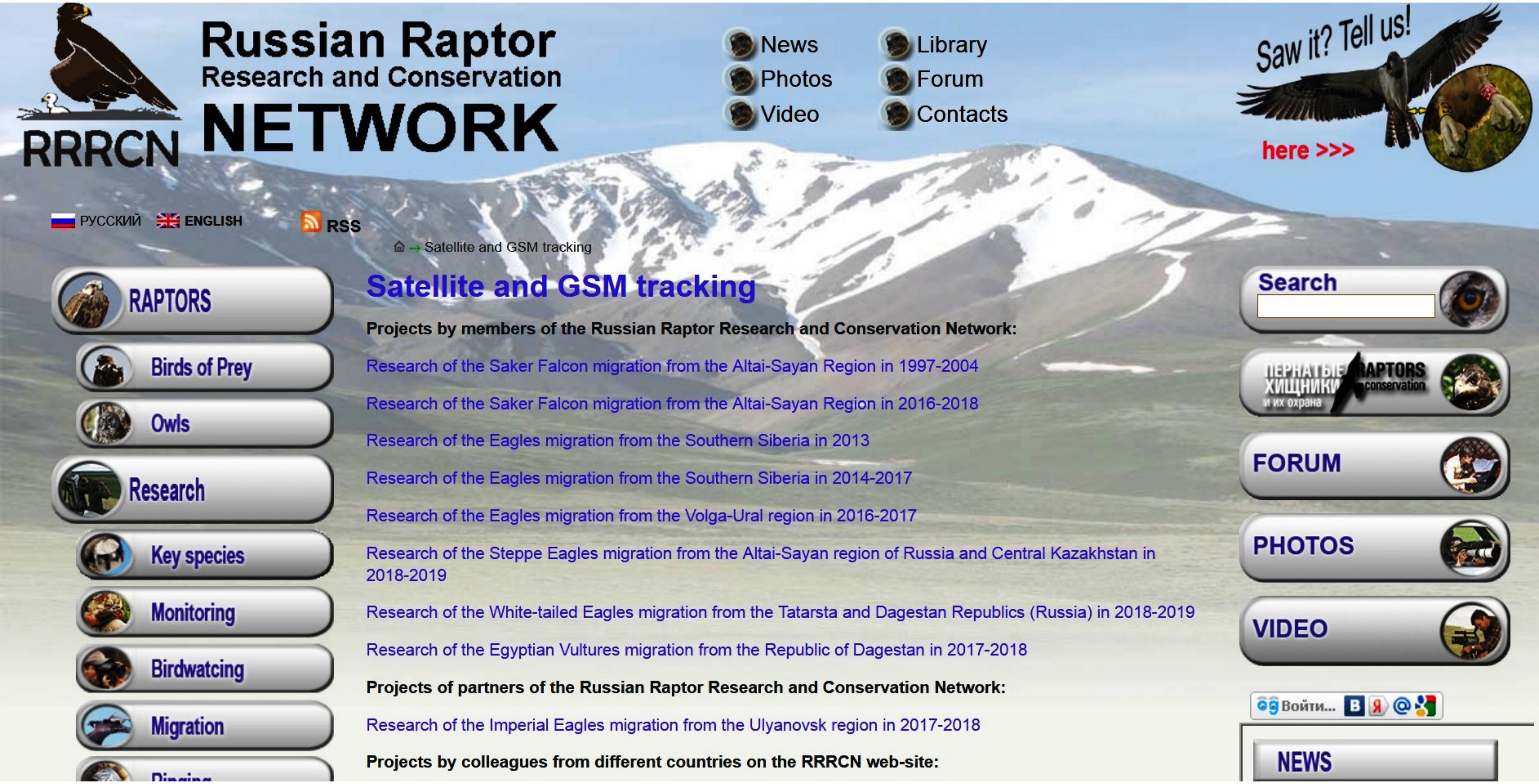


Abqaiq–Khurais - Aramco Oil Refineries: Drone Attack – 14th Sept 2019

Public Domain Satellite Images: Google Maps

Mobile Tracking & Satellite Surveillance

“Russian Steppe & Imperial Eagle Migration”



→ Satellite and GSM tracking

Satellite and GSM tracking

Projects by members of the Russian Raptor Research and Conservation Network:

Research of the Saker Falcon migration from the Altai-Sayan Region in 1997-2004

Research of the Saker Falcon migration from the Altai-Sayan Region in 2016-2018

Research of the Eagles migration from the Southern Siberia in 2013

Research of the Eagles migration from the Southern Siberia in 2014-2017

Research of the Eagles migration from the Volga-Ural region in 2016-2017

Research of the Steppe Eagles migration from the Altai-Sayan region of Russia and Central Kazakhstan in 2018-2019

Research of the White-tailed Eagles migration from the Tatarsta and Dagestan Republics (Russia) in 2018-2019

Research of the Egyptian Vultures migration from the Republic of Dagestan in 2017-2018

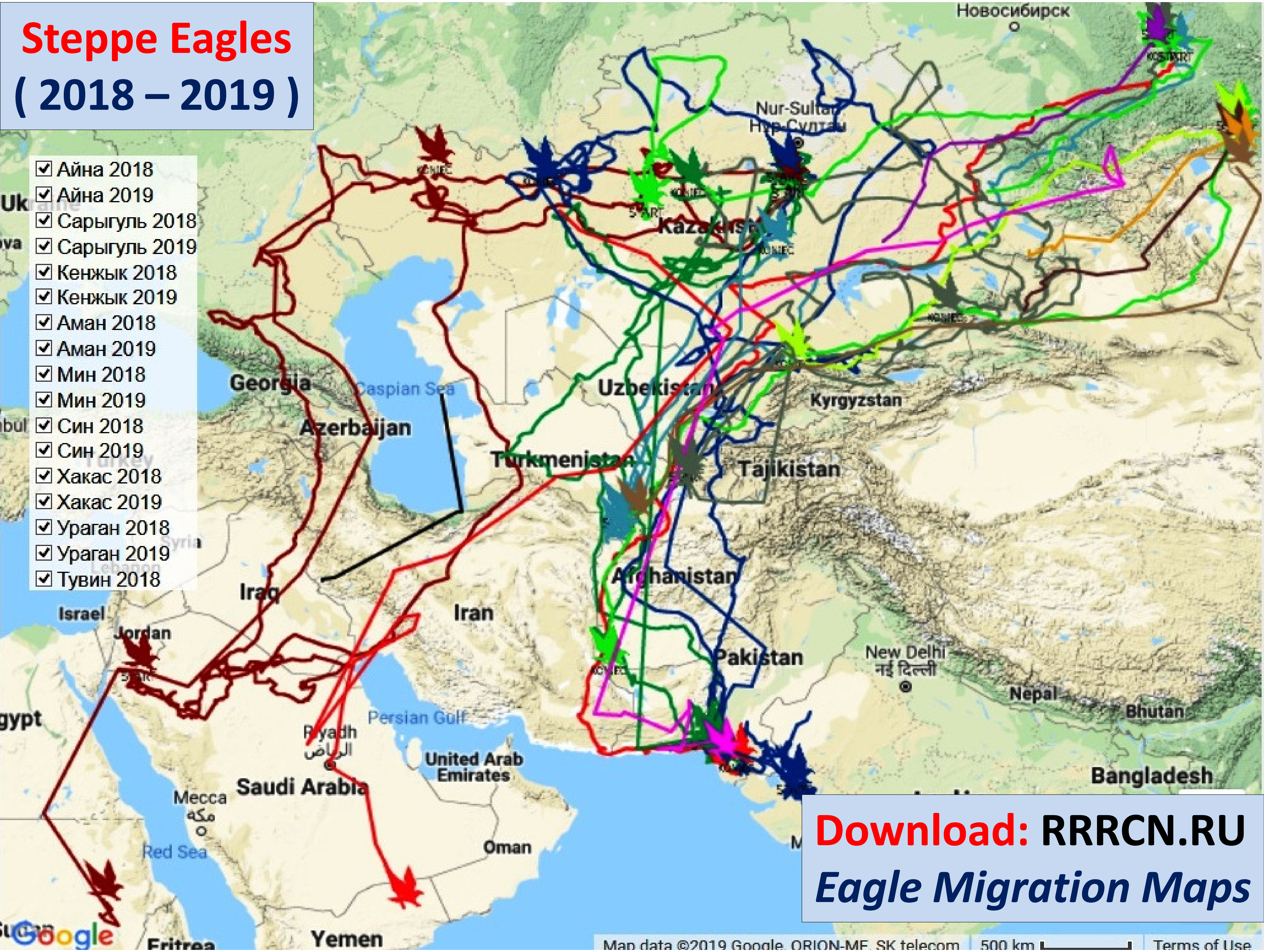
Projects of partners of the Russian Raptor Research and Conservation Network:

Research of the Imperial Eagles migration from the Ulyanovsk region in 2017-2018

Projects by colleagues from different countries on the RRRCN web-site:

Source: RRRCN.RU

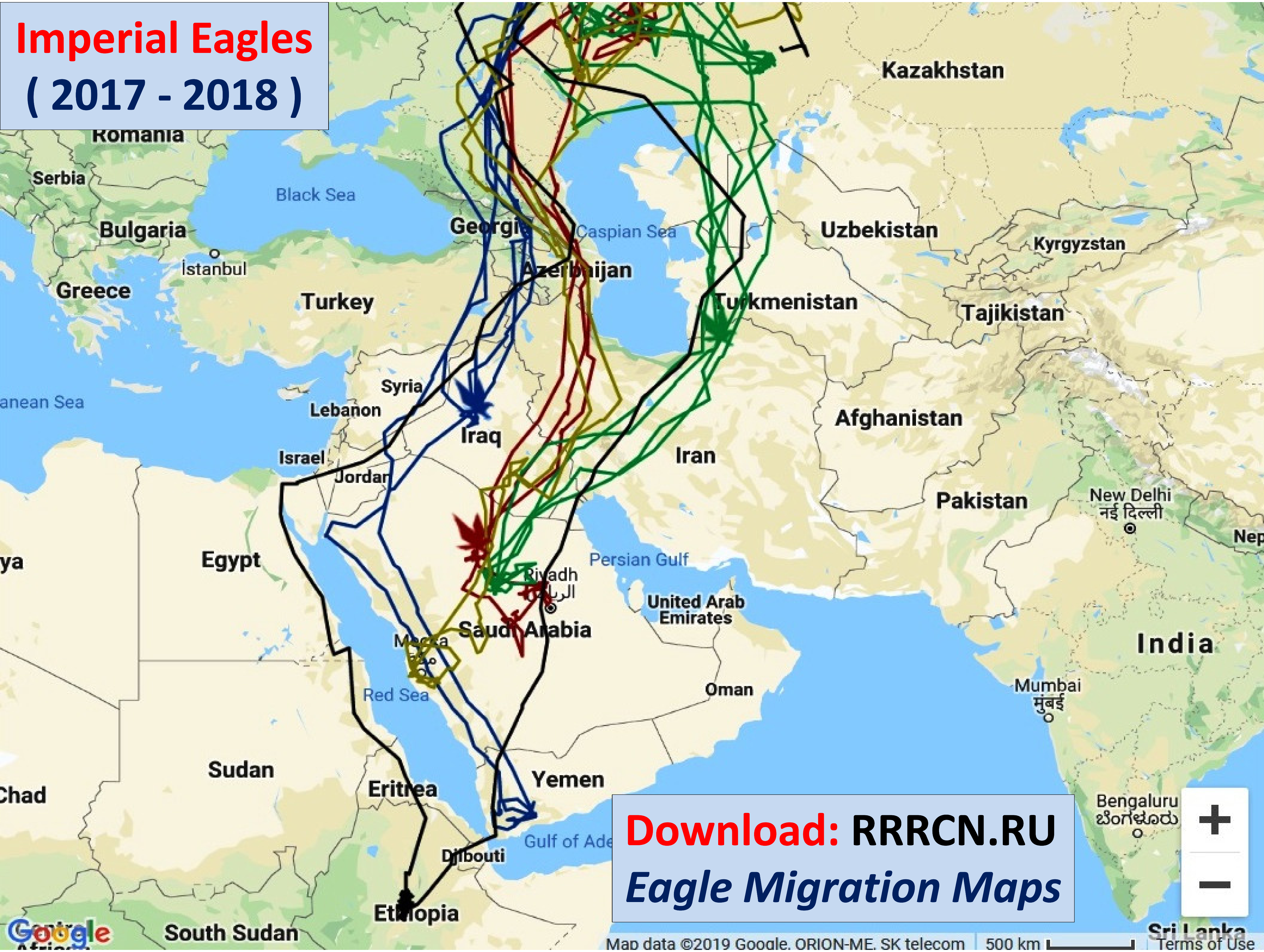
Steppe Eagles
(2018 – 2019)



Download: **RRRCN.RU**

Eagle Migration Maps

Imperial Eagles (2017 - 2018)



Download: **RRRCN.RU**

Eagle Migration Maps

3D Aerial Images: St Julians, Malta

The George, Urban Boutique Hotel
Golden Tulip Vivaldi Hotel Nov 21 – 22 £50
Qaliet
Luma Residence
The George, Urban Boutique Hotel Nov 21 – 22 £72
Ddream Hotel Malta Nov 21 – 22 £49
Alexandra Hotel Malta Nov 21 – 22 £31
Hotel Valentina Nov 21 – 22 £64
Den
TwentyTwo
Portomaso Car Park
Don Ross
Blue Elephant
Onyx Apartments St Julians
Onyx Apartments St Julians Nov 21 – 22 £50
Portomaso
Portomaso Marina
Zeri's Restaurant
Sale e Pepe

Public Domain Images: Google Maps

3D Aerial Images: St Julians, Malta

3BR LUXURY
PORTOMASO MARINA
Hilton Malta
£100
Ddream Hotel Malta
Nov 21 – 22
£49
Hotel Valentina
Nov 21 – 22
£64
The George, Urban
Boutique Hotel
Nov 21 – 22
£72
Alexandra Hotel Malta
Nov 21 – 22
£31
Luma Residence

Public Domain Images: Google Maps

3D Aerial Images: Valletta Harbour, Malta

Bir Mula
Heritage Museum
Birgu
GRIMALDI
Google

Industrial Oil Rigs – Ship Yard– Valletta Grand Harbour, Malta – Google 3D Maps

3D Aerial Images: Valletta Harbour, Malta

Birgu
Senglea
150'

Industrial Oil Rigs – Ship Yard– Valletta Grand Harbour, Malta – Google 3D Maps

3D Aerial Images: Valletta Harbour, Malta

Industrial Oil Rigs – Ship Yard– Valletta Grand Harbour, Malta – Google 3D Maps

Industrial Economic Cyber Espionage

SECURITY

COUNTERINTELLIGENCE

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE

Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011

October 2011

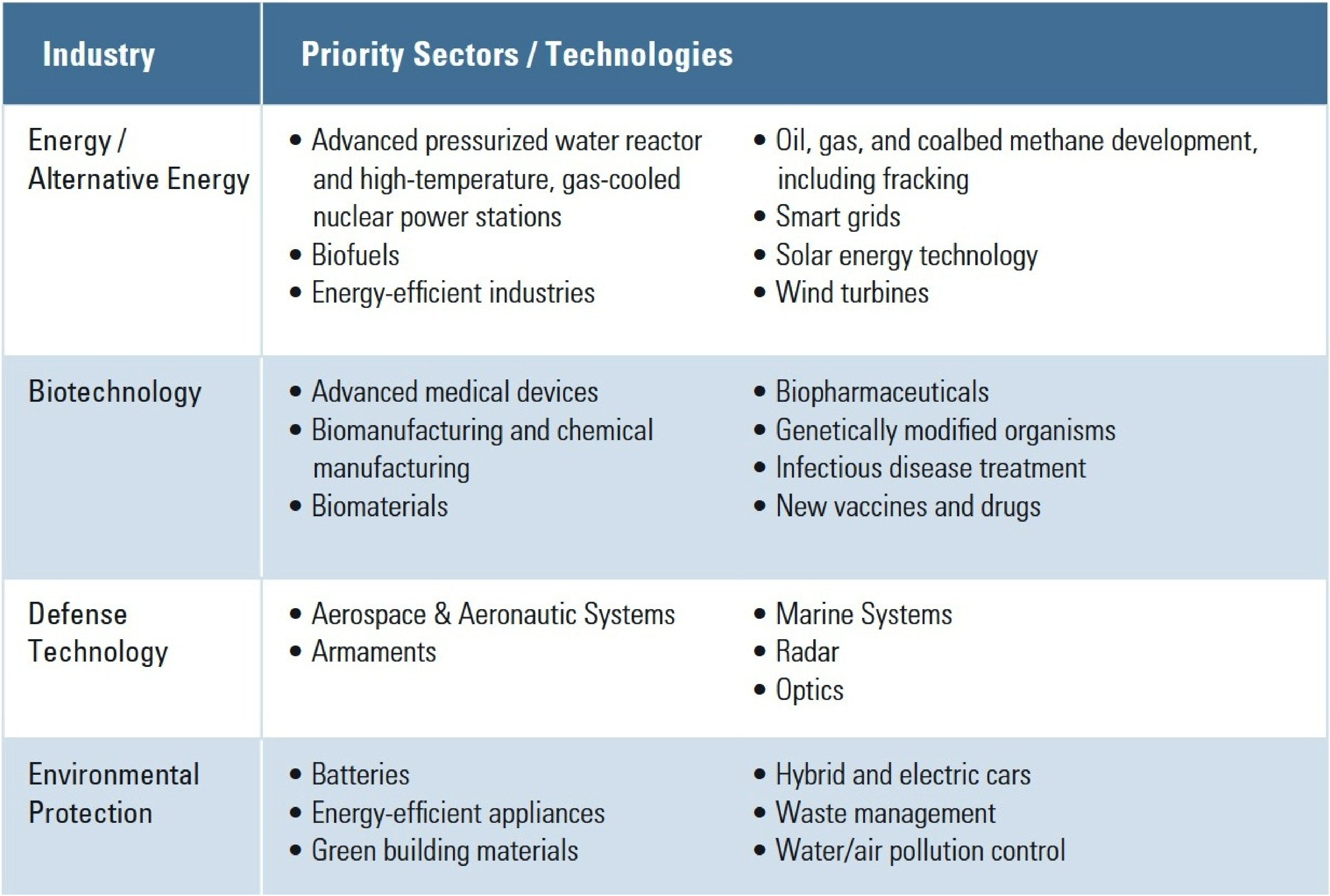
Industrial Economic Cyber Espionage

Foreign Economic Espionage in Cyberspace

2018

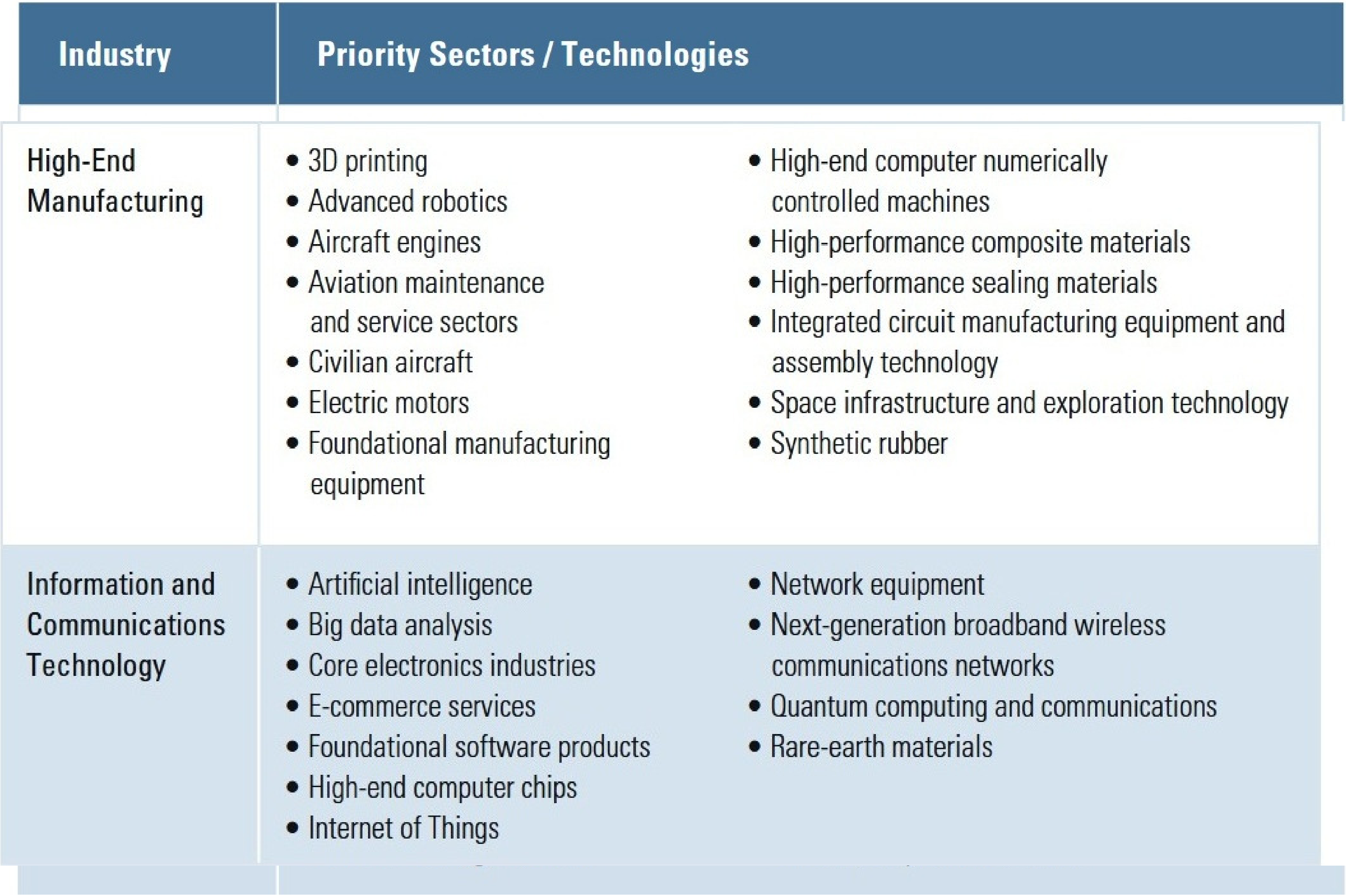
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Critical Sector Targets: Cyber Espionage



Industry	Priority Sectors / Technologies	
Energy / Alternative Energy	• Advanced pressurized water reactor and high-temperature, gas-cooled nuclear power stations • Biofuels • Energy-efficient industries	• Oil, gas, and coalbed methane development, including fracking • Smart grids • Solar energy technology • Wind turbines
Biotechnology	• Advanced medical devices • Biomanufacturing and chemical manufacturing • Biomaterials	• Biopharmaceuticals • Genetically modified organisms • Infectious disease treatment • New vaccines and drugs
Defense Technology	• Aerospace & Aeronautic Systems • Armaments	• Marine Systems • Radar • Optics
Environmental Protection	• Batteries • Energy-efficient appliances • Green building materials	• Hybrid and electric cars • Waste management • Water/air pollution control

Critical Sector Targets: Cyber Espionage

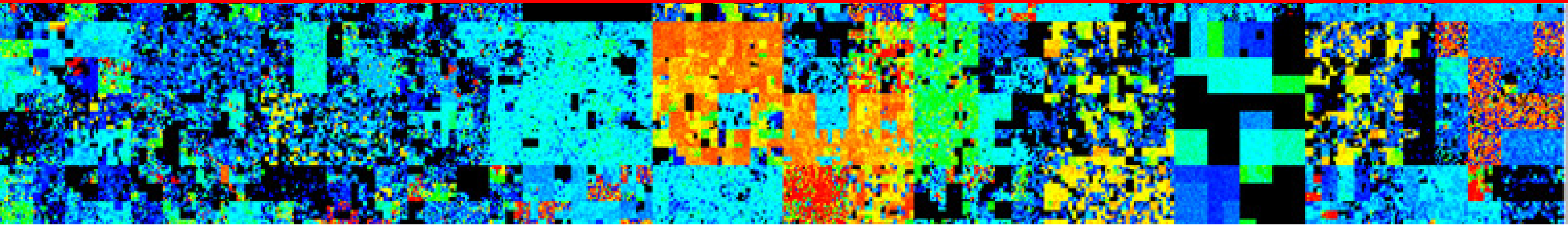


Industry	Priority Sectors / Technologies
High-End Manufacturing	• 3D printing • Advanced robotics • Aircraft engines • Aviation maintenance and service sectors • Civilian aircraft • Electric motors • Foundational manufacturing equipment • High-end computer numerically controlled machines • High-performance composite materials • High-performance sealing materials • Integrated circuit manufacturing equipment and assembly technology • Space infrastructure and exploration technology • Synthetic rubber
Information and Communications Technology	• Artificial intelligence • Big data analysis • Core electronics industries • E-commerce services • Foundational software products • High-end computer chips • Internet of Things • Network equipment • Next-generation broadband wireless communications networks • Quantum computing and communications • Rare-earth materials

Upgrading Industrial CyberSecurity!...

7 –Advanced CyberSecurity Solutions

“Intelligent & Integrated”



Intelligent & Integrated CyberSecurity

Cybersecurity for Critical National Infrastructure requires Advanced Intelligent Cyber Solutions!....

Intelligent & Integrated CyberSecurity

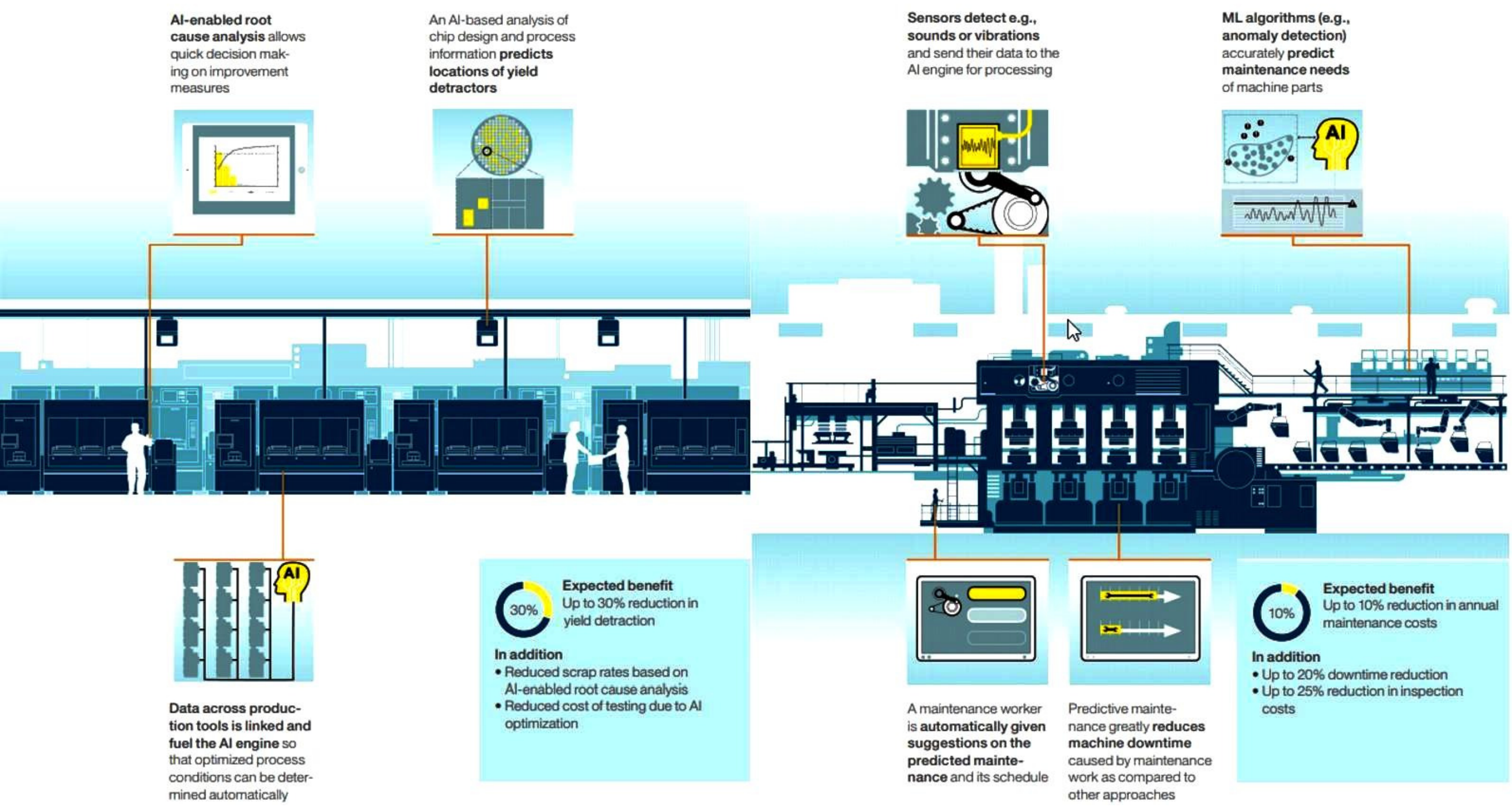
Cybersecurity for Critical National Infrastructure requires Advanced Intelligent Cyber Solutions!....

- Artificial Intelligence: Human Operators are too slow to react to "Cyber Attacks" @ Light Speed, so AI "Bots" will be deployed 24/7 to hunt predators!...
- Machine Learning: Intelligent Self-Learning Models determine "Normal" behaviour of Critical Systems!
- Big Data Analytics: ICS/SCADA Systems & Log-Files are scanned in Real-Time for malware anomalies!

Integrated Cyber-Physical: ONE-Operations Dashboard!

AI & Machine Learning will Optimise & Secure Industrial Automation : IACS.....

AI & Machine Learning will Optimise & Secure Industrial Automation : IACS.....



AI-enabled root cause analysis allows quick decision making on improvement measures

An AI-based analysis of chip design and process information **predicts locations of yield detractors**

Sensors detect e.g., sounds or vibrations and send their data to the AI engine for processing

ML algorithms (e.g., anomaly detection) accurately **predict maintenance needs** of machine parts

Data across production tools is linked and fuel the AI engine so that optimized process conditions can be determined automatically

Expected benefit
Up to 30% reduction in yield detraction

In addition

- Reduced scrap rates based on AI-enabled root cause analysis
- Reduced cost of testing due to AI optimization

A maintenance worker **is automatically given suggestions on the predicted maintenance** and its schedule

Predictive maintenance greatly **reduces machine downtime** caused by maintenance work as compared to other approaches

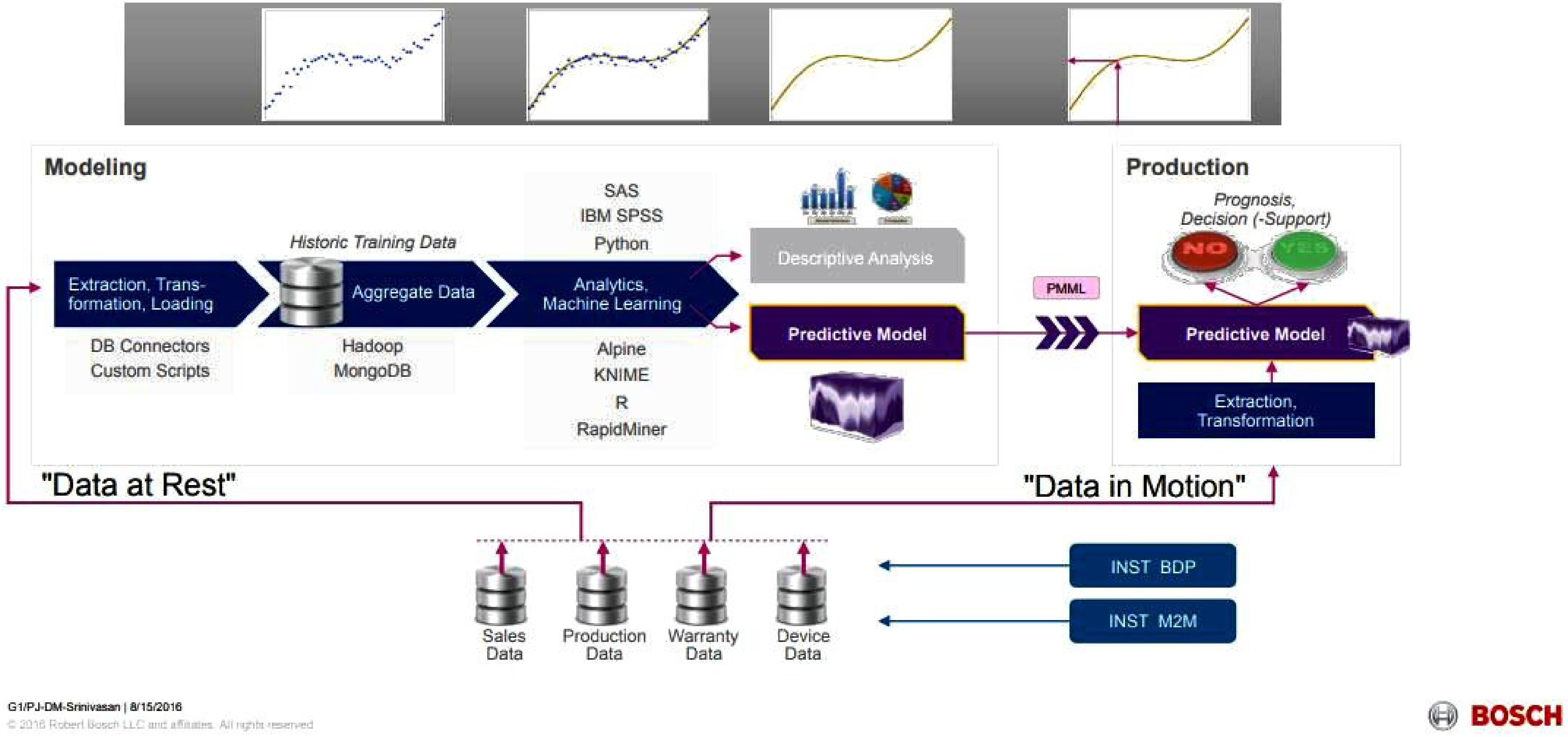
Expected benefit
Up to 10% reduction in annual maintenance costs

In addition

- Up to 20% downtime reduction
- Up to 25% reduction in inspection costs

Machine Learning & Big Data Analytics:

Predictive Modelling for Industrial Controls!



Modeling

Historic Training Data

Extraction, Transformation, Loading

DB Connectors
Custom Scripts

Aggregate Data

Hadoop
MongoDB

SAS
IBM SPSS
Python

Analytics, Machine Learning

Alpine
KNIME
R
RapidMiner

Descriptive Analysis

Predictive Model

PMML

Production

Prognosis, Decision (-Support)

NO YES

Predictive Model

Extraction, Transformation

"Data at Rest"

"Data in Motion"

Sales Data

Production Data

Warranty Data

Device Data

INST BDP

INST M2M

G1/PJ-DM-Srinivasan | 8/15/2016
© 2016 Robert Bosch LLC and affiliates. All rights reserved

BOSCH

Big Data Analytics: Industry Optimisation & Cyber Intrusion Detection

Integration of Physical and Cyber Security

Integrated CSO-led Management Team – *Merged HQ Operations*

Physical Security Operations

Cyber Security Operations

Shared

Alerts

Smart Security = ***Virtual Integration***

Corporate CSO-led Security Team

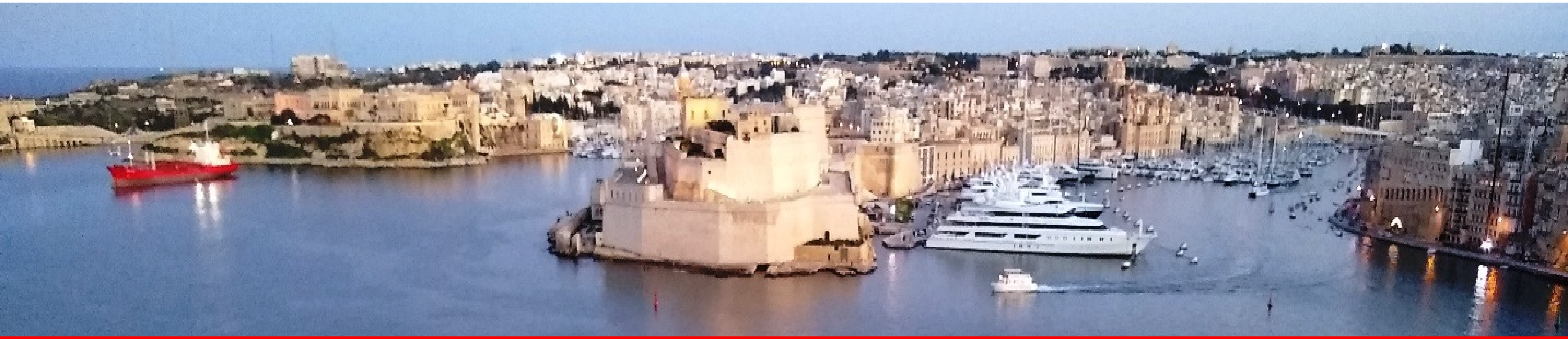
ONE – Shopping List!

Integrated Management,
Training, Standards, Plans

ONE – Architecture!

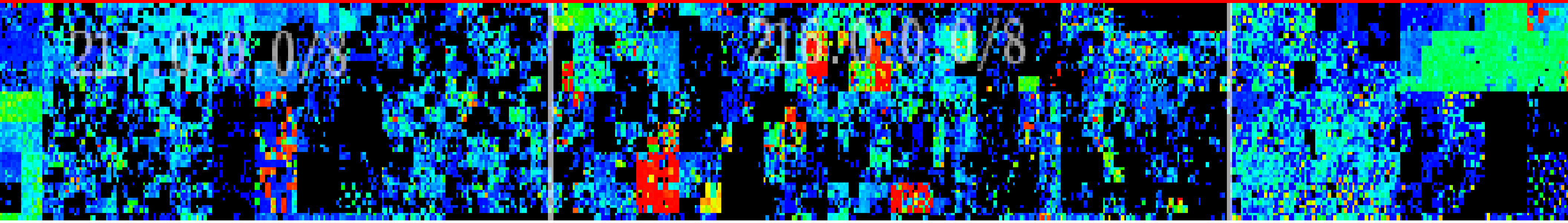
Final** phase of Cyber-Physical Integration - Embedded Intelligence in ALL Devices - **Internet of Things

Upgrading Industrial CyberSecurity!...



8 –10 New Ways to Secure Systems

“Real-Time Learning!”



10 Ways to Secure Industrial Systems!

Industrial Systems are *Highly Vulnerable* to Cyber Attacks!

- Audit ALL ICS/SCADA
- Upgrade ICS Software
- Secure Network Controls
- ISO/NIST Cyber Standards
- Full Compliance Checks
- Check ALL Staff/Contractors
- Monitor Supply Chain
- Maintain SCADA "Air-Gap"
- Trial AI/ML Cyber Solutions!
- Intelligent 24/7 Surveillance!

……YOUR Mission: Transition over 5 to 10 Years from Legacy 20thC ICS/SCADA to Intelligent 21stC Autonomous Self-Learning Systems!

Guide to **Industrial Security** for **ICS**: **NIST**

Recommended Technical Handbook: **May 2015**

NIST Special Publication 800-82

Revision 2

NIST = National Institute of Standards & Technology

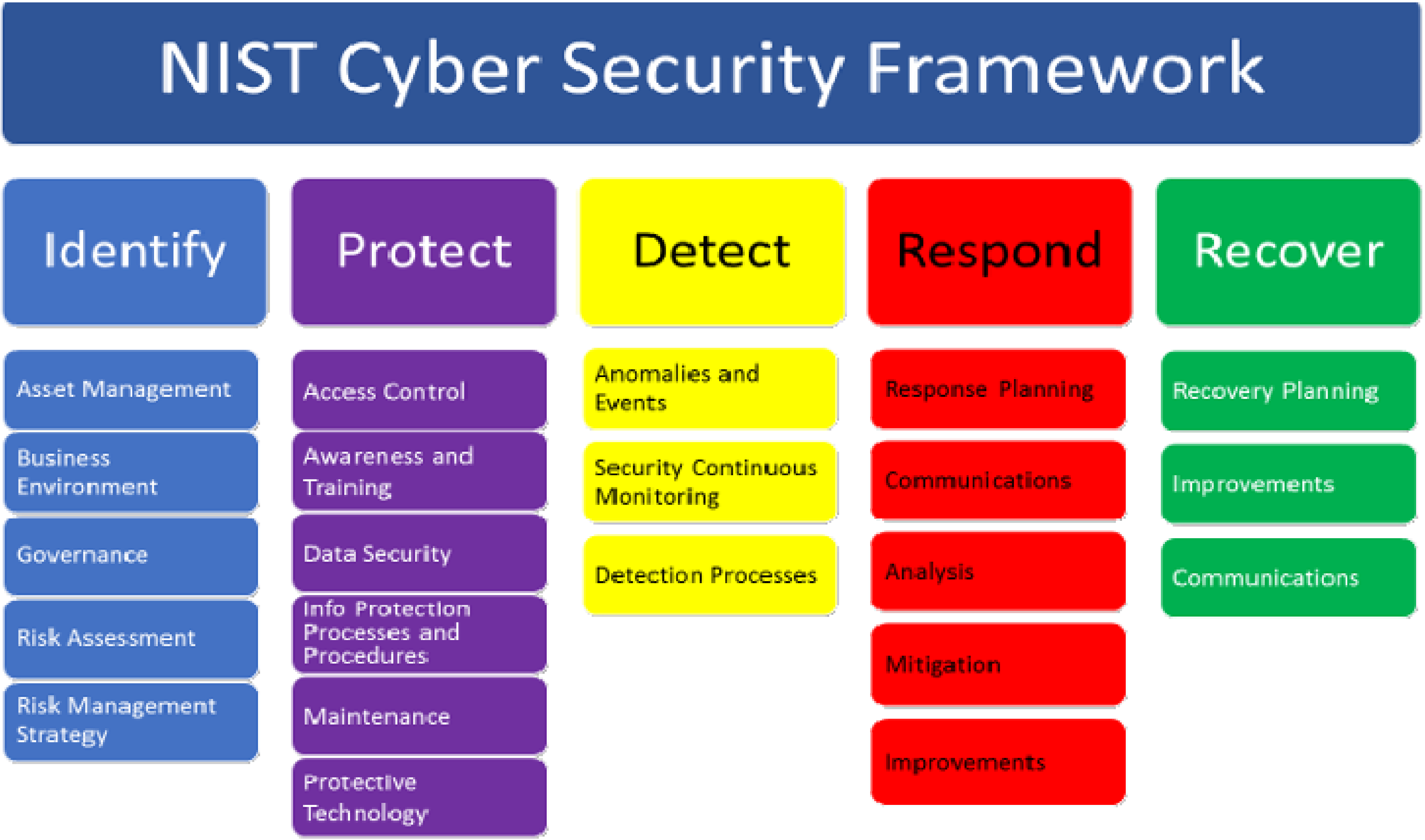
Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

Free Download: **dx.doi.org/10.6028/NIST.SP.800-82r2**

Guide to Industrial Security for ICS: NIST



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Industrial Automation & Control Systems

CISCO Design Guide - (IACS) : August 2019

cisco

Networking and Security in Industrial Automation Environments

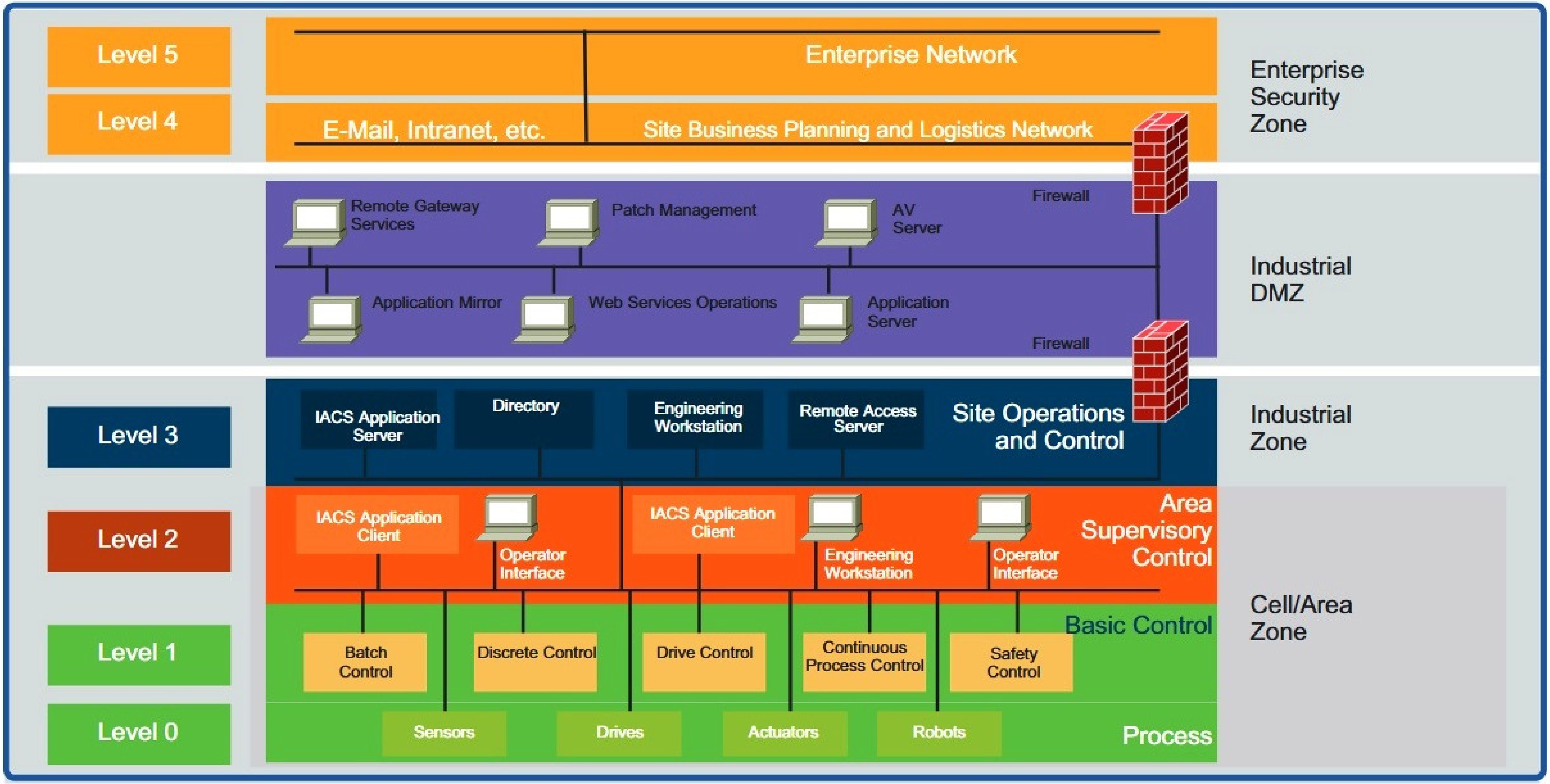
Design and Implementation Guide

Updated: August 2019

Download: www.cisco.com – **Google Search**: ***Industrial SCADA Security***

Industrial Automation & Control Systems

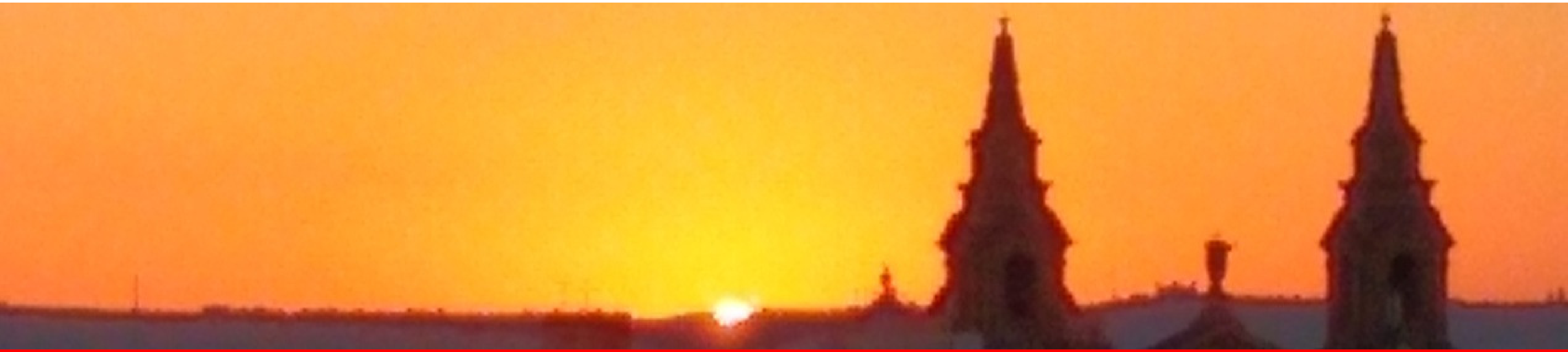
CISCO Design Guide - (IACS) : August 2019



Download: www.cisco.com – Google Search*: Industrial SCADA Security*

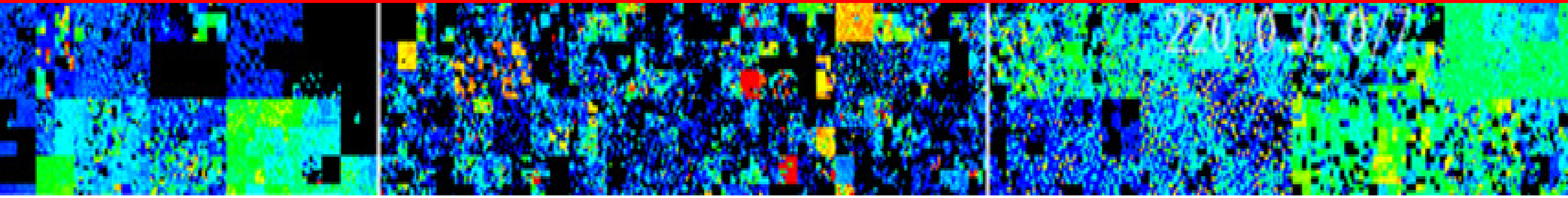
40th International East-West Security Conference

Upgrading Industrial CyberSecurity!...



9 – Defend YOUR Industry NOW!...

“SMART Business Plan”

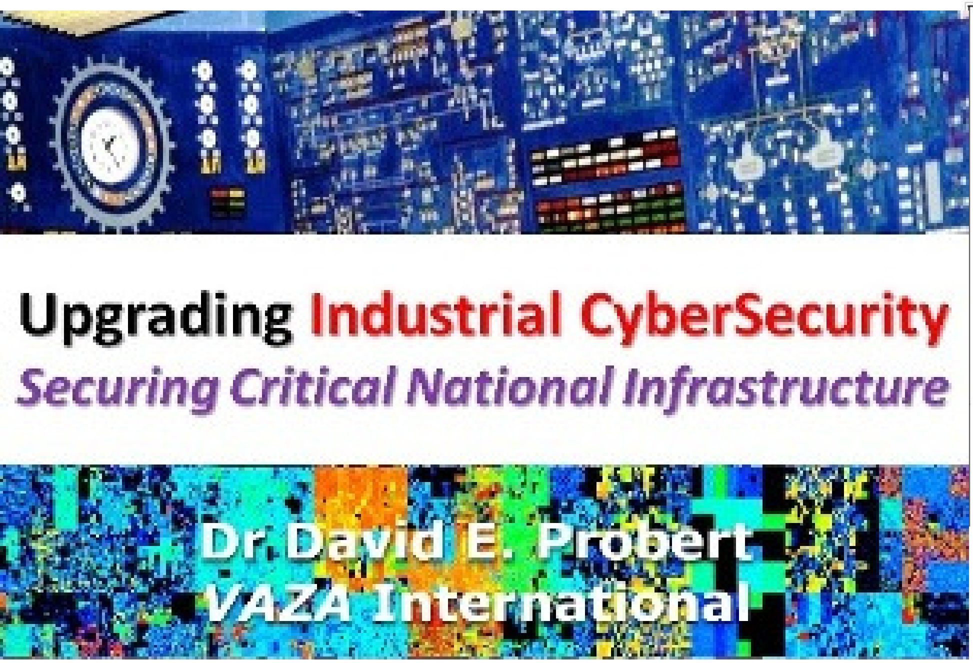


YOUR Smart Security Business Plan!..

- **Action 1:** CSO-Led Board-Level Review & Audit of ALL ***ICS/SCADA*** Net/Systems Assets & Operations – 60 days
- **Action 2:** Investigate ***YOUR*** CyberSecurity Risk Profile & Potential Threat, Attack & Espionage Scenarios – 30 days
- **Action 3:** Develop Multi-Year Security Plan, ***$$$ Budget*** & Roadmap to Mitigate Identified Cyber Risks to include:
  a) Business-Wide "Cyber-Physical" Security Operations
  b) Upgrade *ICS/SCADA* to Global Industry *ISO/NIST* Standards"
  c) Implement New Generation *AI/ML-based* Systems Controls
  d) Professional "*Cyber Security Training*" & Development
  e) Regular Security Staff Scenario Exercises for *"Cyber Alerts"*

Cyber Impact: Board Focus & $$$ Budget for "Cyber" will be $IGNIFICANT!

"Upgrading Industrial CyberSecurity!..."



Upgrading Industrial CyberSecurity

Securing Critical National Infrastructure

Dr. David E. Probert

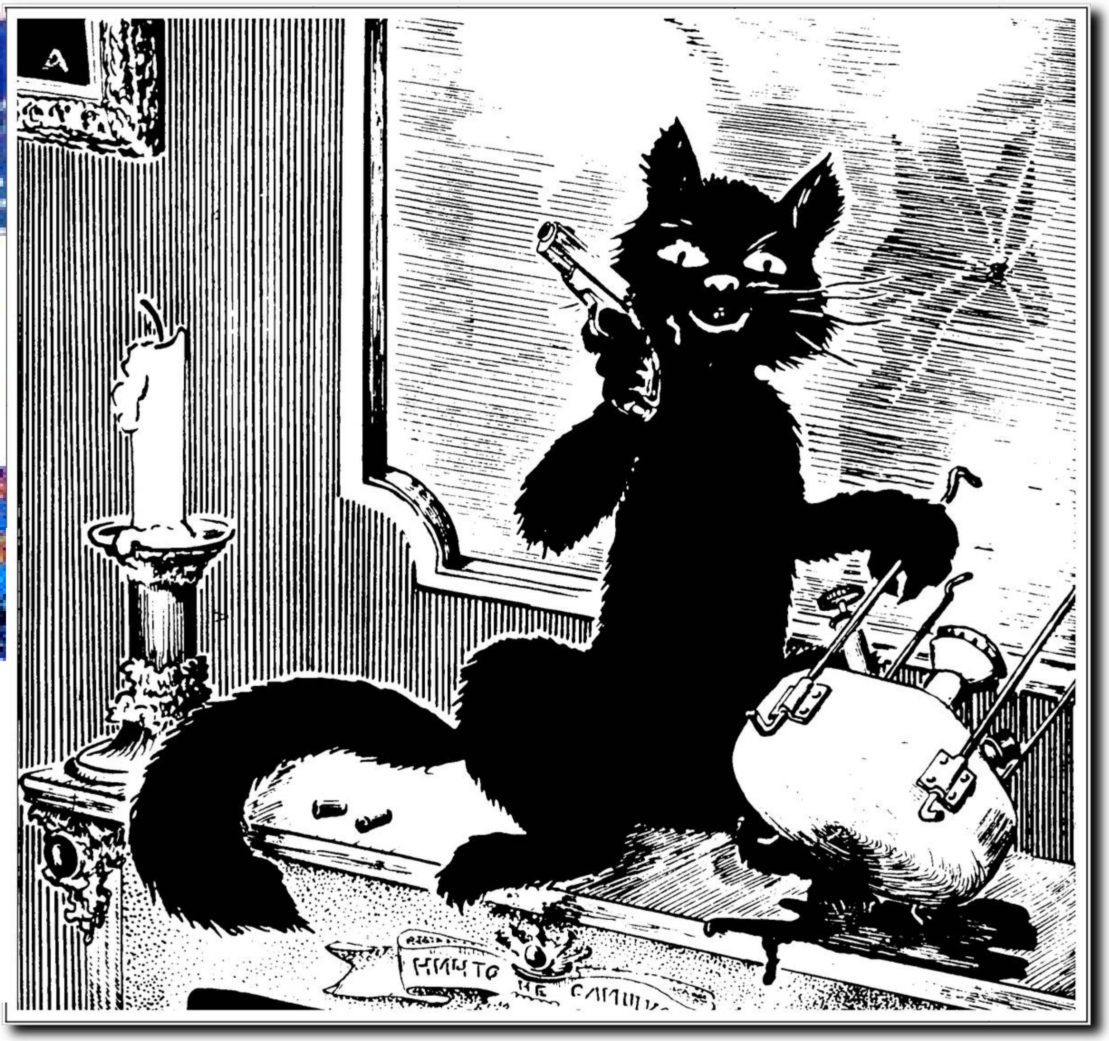
VAZA International

Prepare for Cyber Threats & Attacks!

.........Upgrade YOUR Industry with

Integrated & Intelligent Real-Time

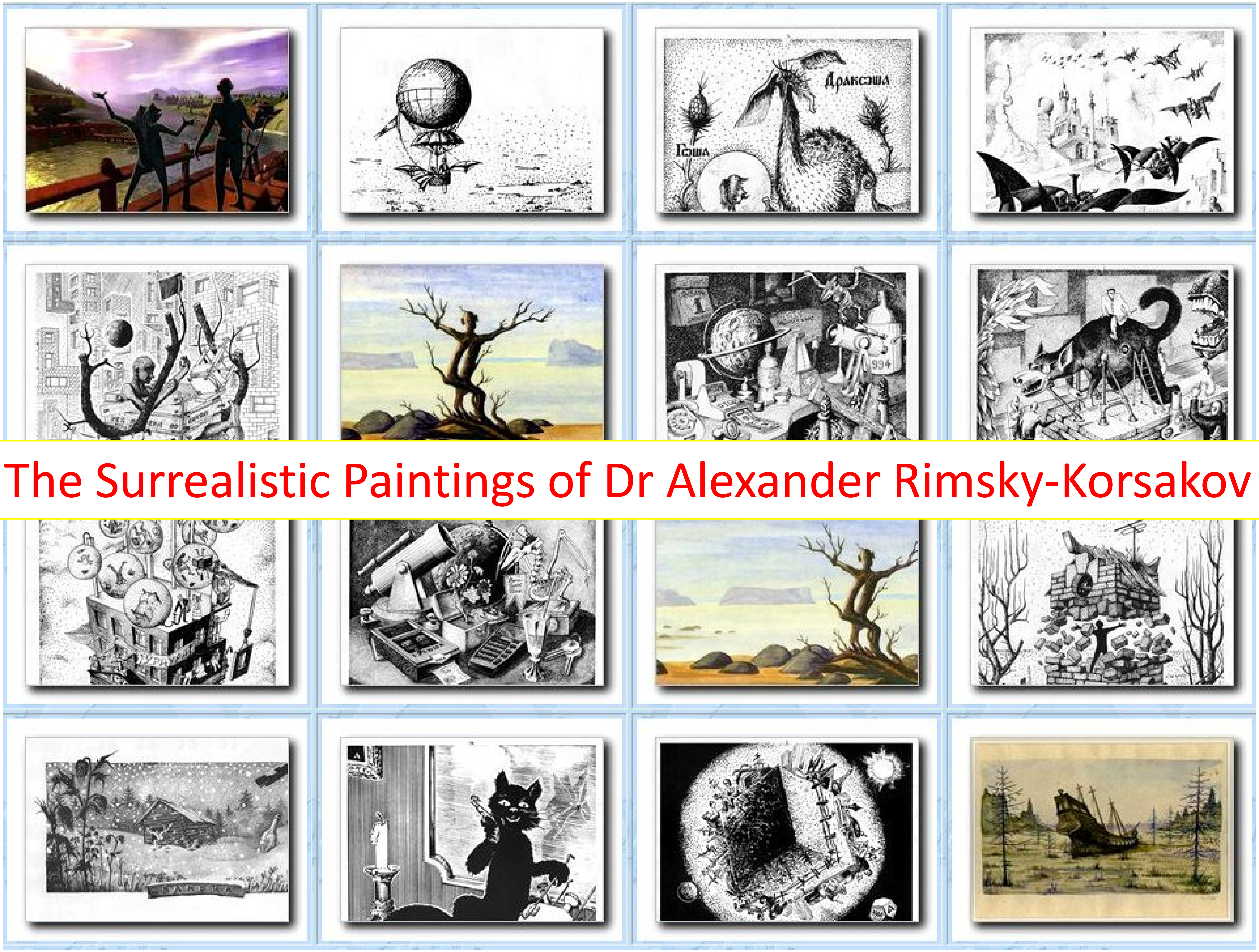
Cyber–Physical Security Operations!



Bulgakov's Satanic Cat – Бегемот - Master & Margarita - 1972

Pen & Ink Drawing by **Dr Alexander Rimski-Korsakov (1936 – 2018)**

The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov



Web Link: www.valentina.net/ARK3/ark2.html

21stC *Cyber* Finance, *Industry* & Futures!

"21stC CyberSecurity": Finance, Industry & Futures!

21stC Cyber Trends in Finance

- AI & Machine Learning in Banking -

Dr David E. Probert

VAZA International

Upgrading Industrial CyberSecurity

Securing Critical National Infrastructure

Dr David E. Probert

VAZA International

Intelligent Integrated Security

- CyberCrime, CyberTerror, CyberWar -

Dr David E. Probert

VAZA International

(1) Financial Security

(2) Industrial Security

(3) Intelligent Security

*** 40th International East-West Security Conference: St Julians, Malta - 2019 ***

Download *Cyber* Slides: www.valentina.net/MALTA2019/

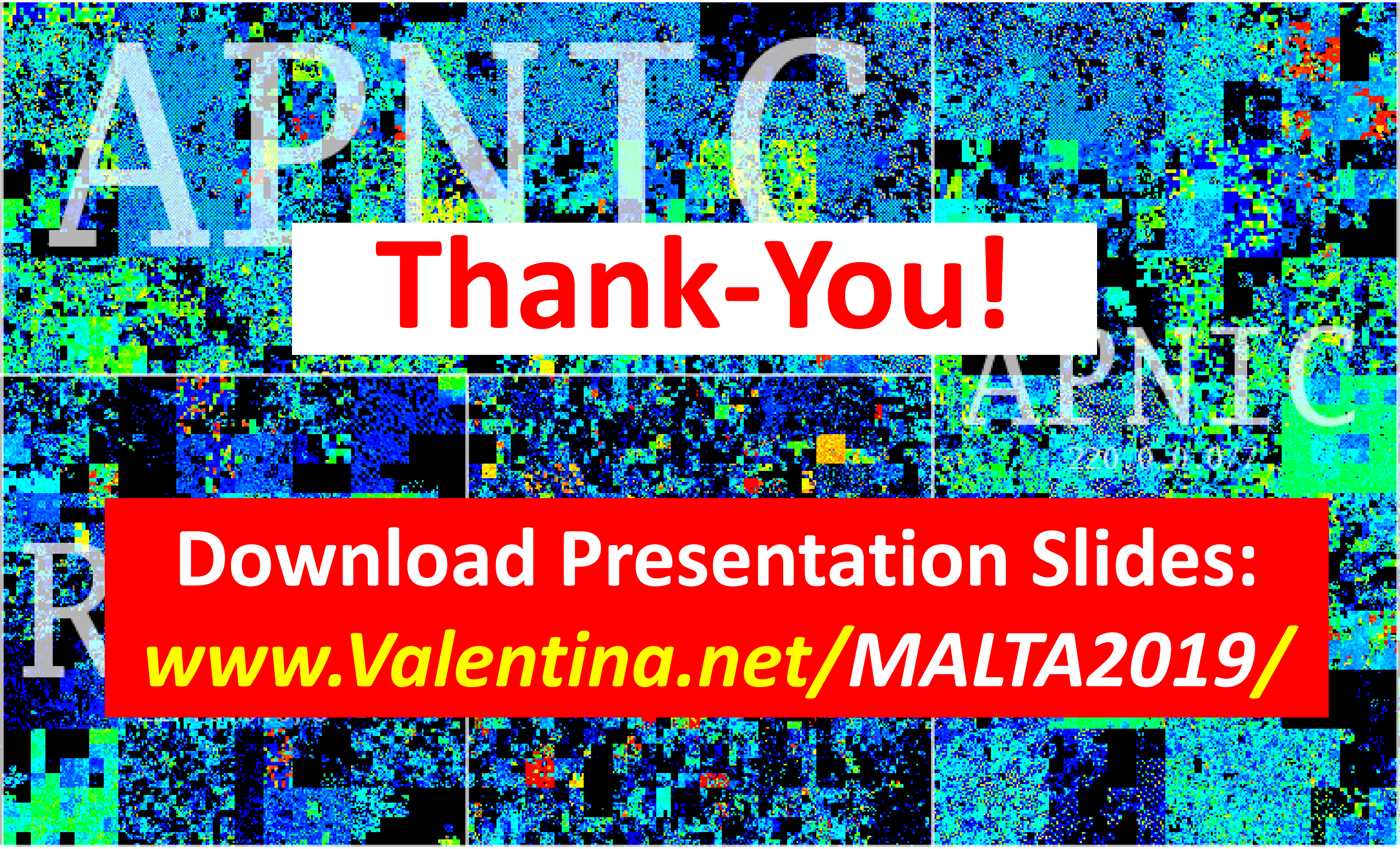
21stC *Cyber* Trends in Finance...

40th East-West Security Conference: Malta

MALTA
-1800 –

21stC *Cyber* Trends in Finance...

40th East-West Security Conference: Malta



Thank-You!

Download Presentation Slides:

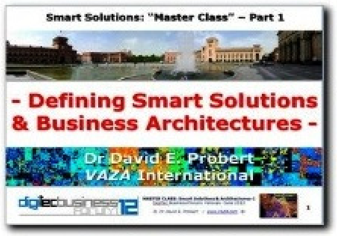
www.Valentina.net/MALTA2019/

Download Presentation Slides:

www.Valentina.net/MALTA2019/

Thank you for your time!

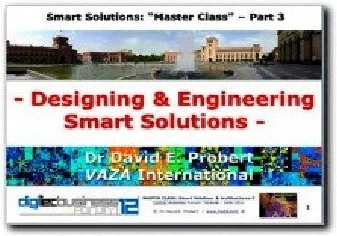
Additional *Cybersecurity* Resources


Smart Solutions: "Master Class" – Part 1

- Defining Smart Solutions & Business Architectures -

Dr David E. Probert
VAZA International

"Master Class - Smart Theory & Practice


Smart Solutions: "Master Class" – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

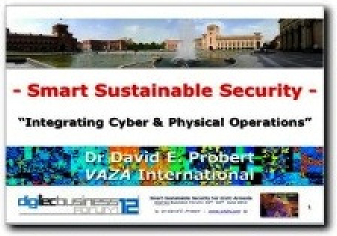
"Master Class 2012 - Smart Design"

- Armenia: Smart Economy -

"Smart Business Architectures for Intelligent Economic Development"

Dr David E. Probert
VAZA International

"21stC Armenia- 2012: Smart Economy"


- Smart Sustainable Security -

"Integrating Cyber & Physical Operations"

Dr David E. Probert
VAZA International

"21stC Armenia - 2012: Smart Security"

- Smart Governance -

"Stimulating Innovation & Economic Growth"

Dr David E. Probert
VAZA International

"21stC Armenia: Smart Governance"

"Real-Time Armenia"

"Securing Government & Financial Enterprise Operations"

"Real-Time Armenia" - White Paper

"Real-Time" ARMENIA!...

...Securing Government & Financial Enterprise Operations

Dr David E Probert
VAZA International

"Real-Time Armenia" - Slides

"Awesome Armenia!"
Photos and Panoramas

Armenia Spring - 2009

Armenia Summer 2009

Armenian Panoramas Summer - 2009

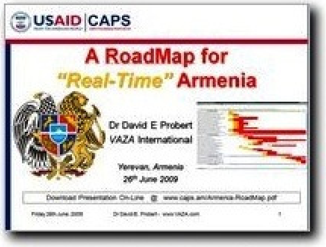
Awesome Armenia: In Photos

"Roadmap for Real-Time Armenia"

"E-Government, E-Commerce and E-Security"

USAID | CAPS

Roadmap for Real-Time Armenia- Report

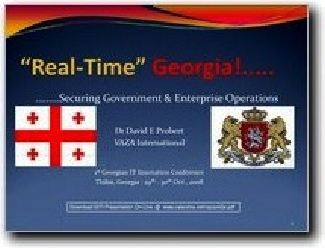

USAID | CAPS

A RoadMap for "Real-Time" Armenia

Dr David E Probert
VAZA International

Yerevan, Armenia
26th June 2009

RoadMap for Real-Time Armenia- Slides


"Real-Time" Georgia!.....

...Securing Government & Enterprise Operations

Dr David E Probert
VAZA International

"Real-Time Georgia" - GITI 2008 Slides

"Real-Time Georgia"

"Securing Government & Enterprise Operations"

"Real-Time Georgia" - GITI 2008 Paper

"Republic of Georgia"
Photos and Panoramas

Georgian Panoramas Autumn 2007

Caucasus Aerial Panoramas

Georgian Panoramas Autumn 2008

Georgia 2008

Gorgeous Georgia: In Photos

..."21stC Georgia"...

..."Cyber-Vardzia"...

21stC Georgia: "CyberVardzia" - Paper

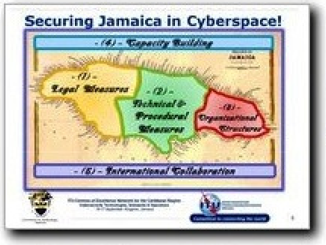
21stC Georgia – "Cyber Vardzia"

"Integrated Cyber & Physical Security"

for e-Government & e-Georgia

Dr David E. Probert
VAZA International

21stC Georgia - "CyberVardzia" - Slides


Securing Jamaica in Cyberspace!

-(4)- Capacity Building

-(1)- Legal Measures

-(2)- Technical & Procedural Measures

-(3)- Organisational Structures

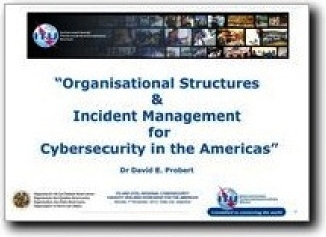
-(5)- International Collaboration

* ITU Cybersecurity Strategy *
"3-Day Workshop Overview"

Workshop Presentations

Group Tasks & Discussions

Dr. David E. PROBERT (Executive Director, VAZA International)


"Organisational Structures & Incident Management for Cybersecurity in the Americas"

Dr David E. Probert

ITU/CITEL: Cybersecurity in the Americas

"Cybersecurity Capacity Building & International Collaboration "

Dr David E. Probert

ITU/CITEL: Cybersecurity Skills Building

Link: www.valentina.net/vaza/CyberDocs

Professional Profile - *Dr David E. Probert*

- ***Computer Integrated Telephony (CIT)*** – Established and led British Telecom's £25M EIGER Project during the mid-1980s' to integrate computers with telephone switches (PABX's). This resulted in the successful development and launch of CIT software applications for telesales & telemarketing
- ***Blueprint for Business Communities*** – Visionary Programme for Digital Equipment Corporation during late-1980's that included the creation of the "knowledge lens" and "community networks". The Blueprint provided the strategic framework for Digital's Value-Added Networks Business
- ***European Internet Business Group (EIBG***) – Established and led Digital Equipment Corporation's European Internet Group for 5 years. Projects included support for the national Internet infrastructure for countries across EMEA as well as major enterprise, government & educational Intranet deployments. Dr David Probert was a sponsoring member of the European Board for Academic & Research Networking (EARN/TERENA) for 7 years (1991 ➔1998)
- ***Supersonic Car (ThrustSSC)*** – Worked with Richard Noble OBE, and the Mach One Club to set up and manage the 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record.
- ***Secure Wireless Networking*** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.
- ***Networked Enterprise Security*** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.
- ***Republic of Georgia*** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament, and then by UN/ITU to review Cybersecurity for the Government Ministries.
- ***UN/ITU*** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

Dr David E. Probert is a Fellow of the Royal Statistical Society, IEEE Life Member and 1st Class Honours Maths Degree (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata) , and his full professional biography is featured in the Marquis Directory of Who's Who in the World: 2007-2020 Editions.

Upgrading Industrial CyberSecurity!...

40th East West Security Conference: Malta

BACK-UP SLIDES