Protecting a Nationwide Power Generation Industrial Control Network

Richard Zoni - *www.nozominetworks.com*

Energy and Industrial Cybersecurity

Energy and Industrial companies are prone to sophisticated attacks performed by criminals, terrorists, competitors and states

- Energy
- Telecom
- Transport
- Chemical

Like other IT system they are prone to attacks

The "Stuxnet Effect" on Cybersecurity

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life

TECH

Computer Worm Hits Iran Power Plant

Computer systems at Iran's first nuclear-power plant have been infected with a potent worm capable of taking over their control systems. WSJ's Siobhan Gorman discusses with Simon Constable and Julia Angwin on Digits. Plus: China suffers an iPhone 4 shortage, just a few days after sales started.

By SIOBHAN GORMAN

Updated Sept. 26, 2010 12:01 a.m. ET

The Economist

World politics | Business & finance | Economics | Science & technology | Culture

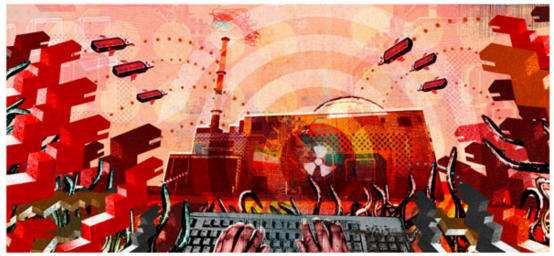
The Stuxnet outbreak

A worm in the centrifuge

An unusually sophisticated cyber-weapon is mysterious but important

Sep 30th 2010 | From the print edition

Timekeeper | Like 197 | Tweet



Tim Marrs

IT SOUNDS like the plot of an airport thriller or a James Bond film. A crack team of experts, assembled by a shadowy government agency, develops a cyber-weapon designed to shut down a rogue country's nuclear programme. The software uses previously unknown tricks to worm its way into industrial control systems undetected, searching for a particular configuration that matches its target—at which point it wreaks havoc by reprogramming the system, closing valves and shutting down pipelines.

ALJAZEERA

News Programmes Opinion Investigations video

Topics: Business & Economy Taliban Azerbaijan Israel Ukraine

Read to me | Share | Tweet | Comment | Print

SCIENCE & TECHNOLOGY 25 SEPTEMBER 2010

Cyber attack 'targeted Iran'

Malicious software discovered on systems around world could have been designed to target Bushehr reactor, experts say.

Experts have suggested that the Bushehr nuclear reactor could have been a target of the virus [File: EPA]

The discovery of so-called malicious software - malware - on systems in Iran and elsewhere across the world has prompted speculation of an attempted cyber attack on Iranian industry, possibly including the Bushehr nuclear reactor.

BBC Sign in | News | Sport | Weather | Shop | Earth | Travel

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment &

Technology

Stuxnet 'hit' Iran nuclear plans

22 November 2010 | Technology

The Stuxnet worm might be partly responsible for delays in Iran's nuclear programme, says a former UN nuclear inspections official.

Iran has always denied that Stuxnet has caused delays to its nuclear power plans

Olli Heinonen, deputy director at the UN's nuclear watchdog until August, said the virus might be behind Iran's problems with uranium enrichment.

Discovered in June, Stuxnet is the first worm to target control systems found in industrial plants.

Iran has denied that delays to its nuclear plans were caused by Stuxnet.

SPIEGEL ONLINE INTERNATIONAL

Sign in | Register

Front Page | World | Europe | Germany | Business | Zeitgeist | BeyondTomorrow | Newsletter

English Site > World > Cyber Threats > Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War

Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War

By Holger Stark

The Mossad, Israel's foreign intelligence agency, attacked the Iranian nuclear program with a highly sophisticated computer virus called Stuxnet. The first digital weapon of geopolitical importance, it could change the way wars are fought -- and it will not be the last attack of its kind.

August 08, 2011 – 03:04 PM

Print | Feedback | Comment

Share | Twitter | @ Email | +

The complex on a hill near an interchange on the highway from Tel Aviv to Haifa is known in Israel simply as "The Hill." The site, as big as several soccer fields, is sealed off from the outside world with high walls and barbed wire -- a modern fortress that symbolizes Israel's fight for survival in the Middle East. As the headquarters of Israel's foreign intelligence agency, the Mossad, this fortress is strictly off-limits to politicians and journalists alike. Ordinarily, it is the Mossad that makes house calls, and not the other way around.

From the Magazine

The New York Times

Malware Hits Computerized Industrial Equipment

By RIVA RICHMOND SEPTEMBER 24, 2010 8:41 PM 89

The technology industry is being rattled by a quiet and sophisticated malicious software program that has infiltrated factory computers.

The malware, known as Stuxnet, was discovered by VirusBlokAda, a Belarussian computer security company in July, at least several months after its creation.

Security experts say Stuxnet attacked the software in specialized industrial control equipment made by Siemens by exploiting a previously unknown hole in the Windows operating system. The malware is the first such attack on critical industrial infrastructure that sits at the foundation of modern economies.

It also displays an array of novel tactics — like an ability to steal design documents or even sabotage equipment in a factory — that suggest its creators are much more sophisticated than hackers whose work has been seen before. The malware casts a spotlight on several security weaknesses.

Industrial Cybersecurity is on the News

The Register **August 27th, 2014**

Major cyber attack hits Norwegian oil industry

More than 50 Norwegian oil and energy companies have been hacked by unknown attackers, according to government security authorities. State-owned Statoil, Norway's largest petro company, appears to be the main target of what's described as the country's biggest ever hack attack.
http://www.theregister.co.uk/2014/08/27/nowegian_oil_hack_campaign/

WIRED **January 1st, 2015**

A Cyberattack Has Caused Confirmed Physical Damage

Hackers had struck an unnamed steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—though unspecified—damage.
http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

NBC NEWS **December 23rd, 2015**

Iranian Hackers Claim Cyber Attack on New York Dam

An Iranian hacktivist group has claimed responsibility for a cyber attack that gave it access to the control system for a dam in the suburbs of New York — an intrusion that one official said may be "just the tip of the iceberg".
http://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611

FINANCIAL TIMES **January 5th, 2016**

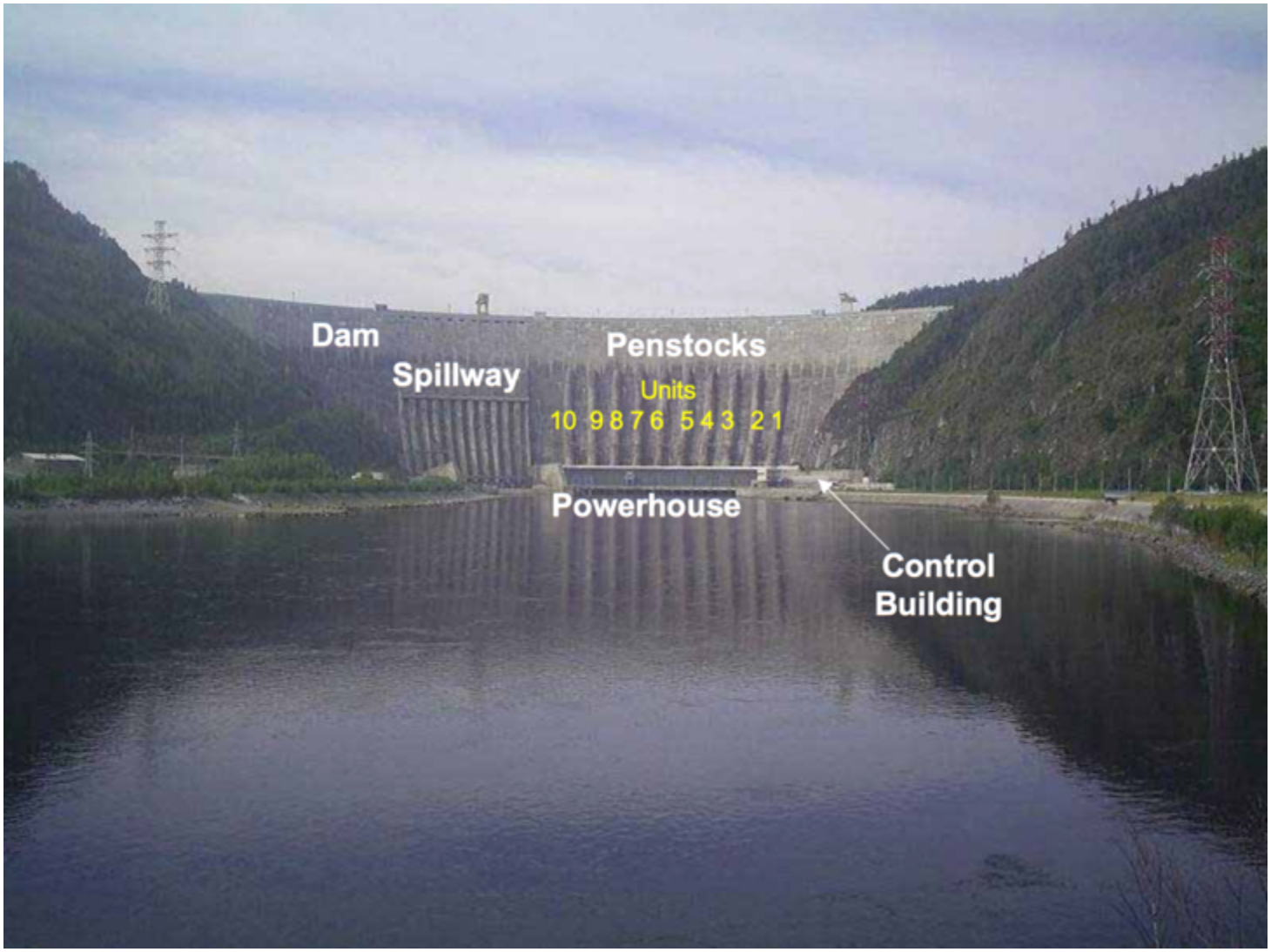
Hackers shut down Ukraine power grid

Hackers brought down the power supply to hundreds of thousands of homes in Ukraine last week, in a cyber attack believed to be the first ever to result in a power outage.
http://www.ft.com/intl/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html

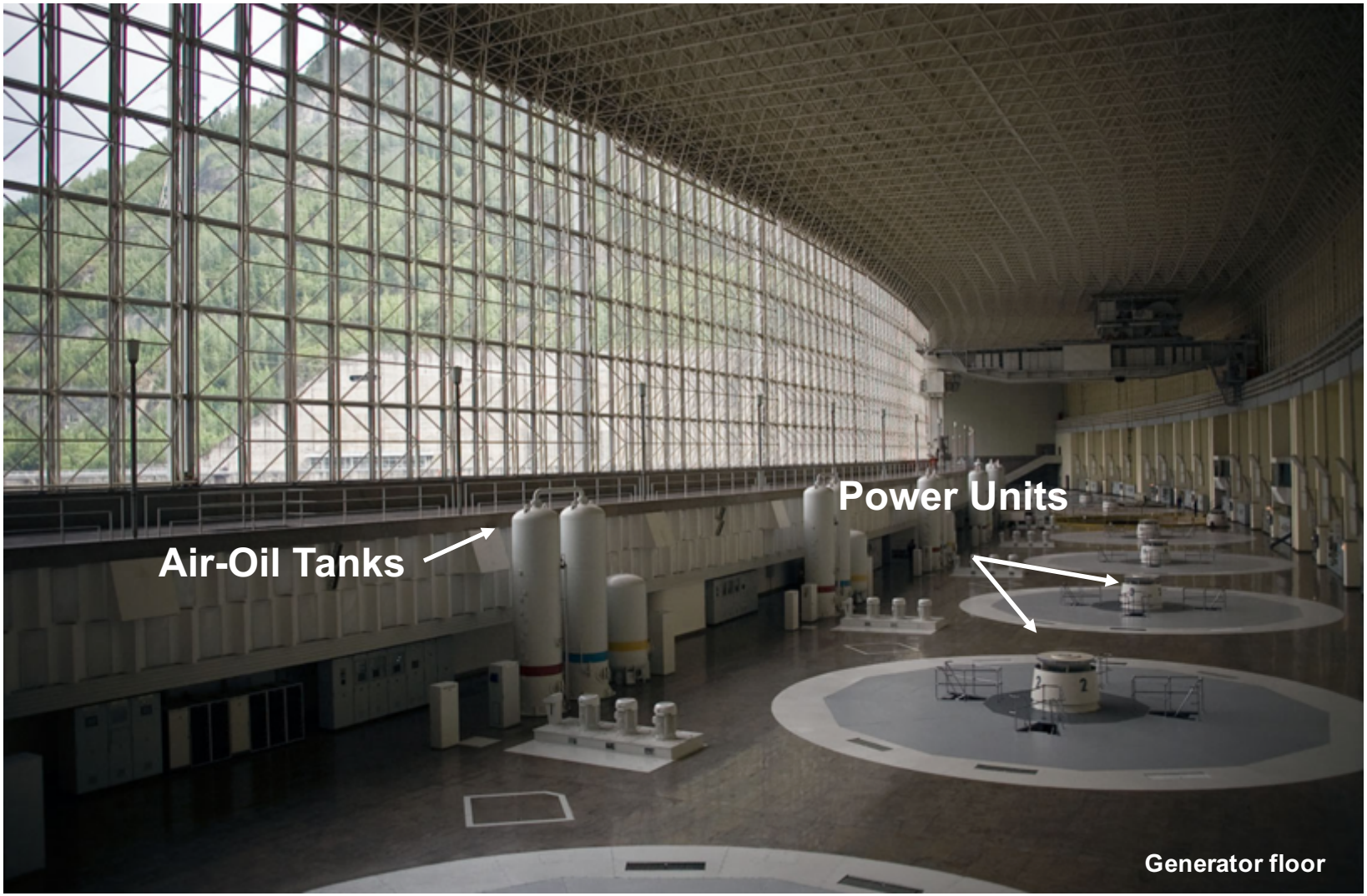
2009 Sayano–Shushenskaya hydroelectric power station accident

- Number of Units: 10
  Turbine Type: Francis (16 blades)
- Rated Power: 650 MW each
- Rated Discharge per Unit: 358,5 m3/s
- Nominal Speed: 142,86 rpm
  Operation Date: 1978
- Runner Diameter: 6,77 m

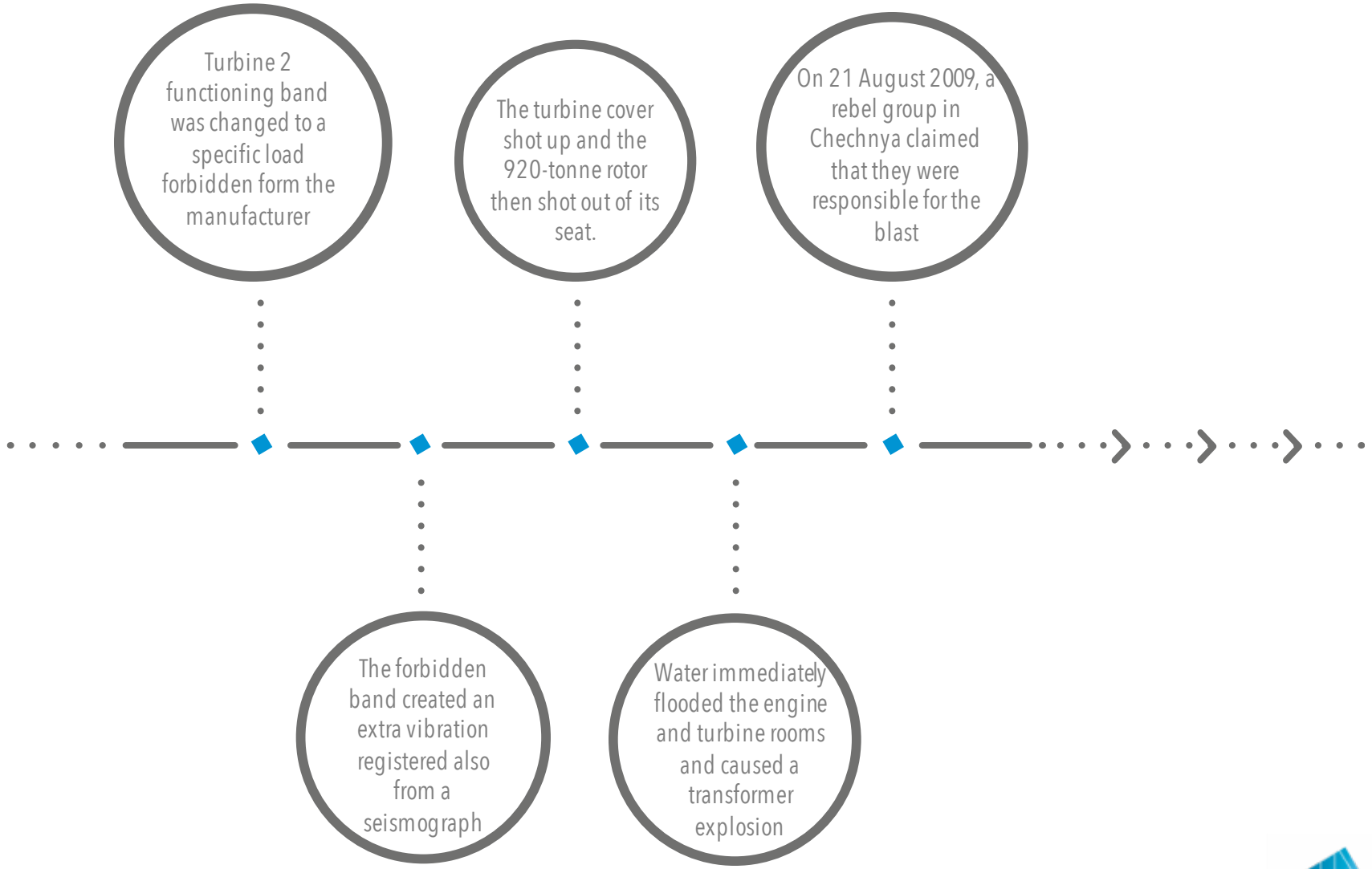
View of the Russian dam



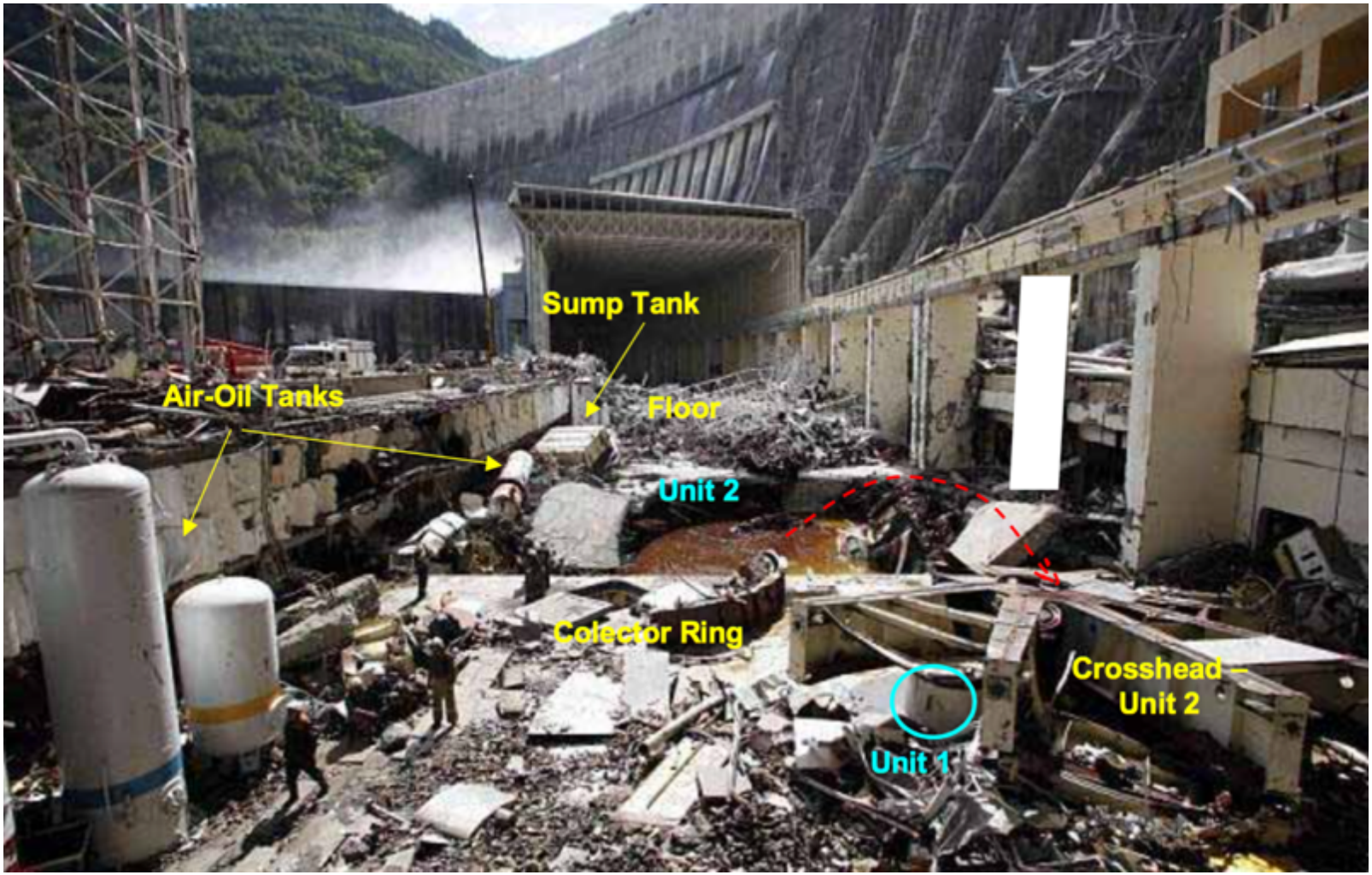
Before the accident…



What's happened..



After the Accident…



Consequences

- 75 people died
- The physical demage was extimted in 310milions
- According to Russian Energy MinisterThey spent almost 2 years and 1.3 bilion Euros to reconstruct the power building
- The production of more than 500,000 tons of aluminum will be lost

Convergence of IT and Operational Technology

What was air gapped and proprietary is now connected and general purpose

In the past, OT was …

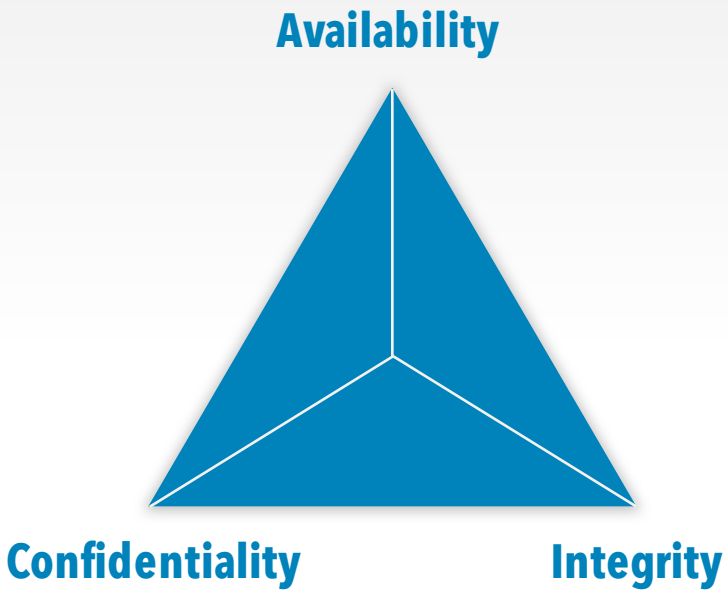
- isolated from IT
- run on proprietary [illegible] protocols
- run on specialized hardware
- run on proprietary embedded operating systems
- connected by copper [illegible] twisted pair

Now OT is …

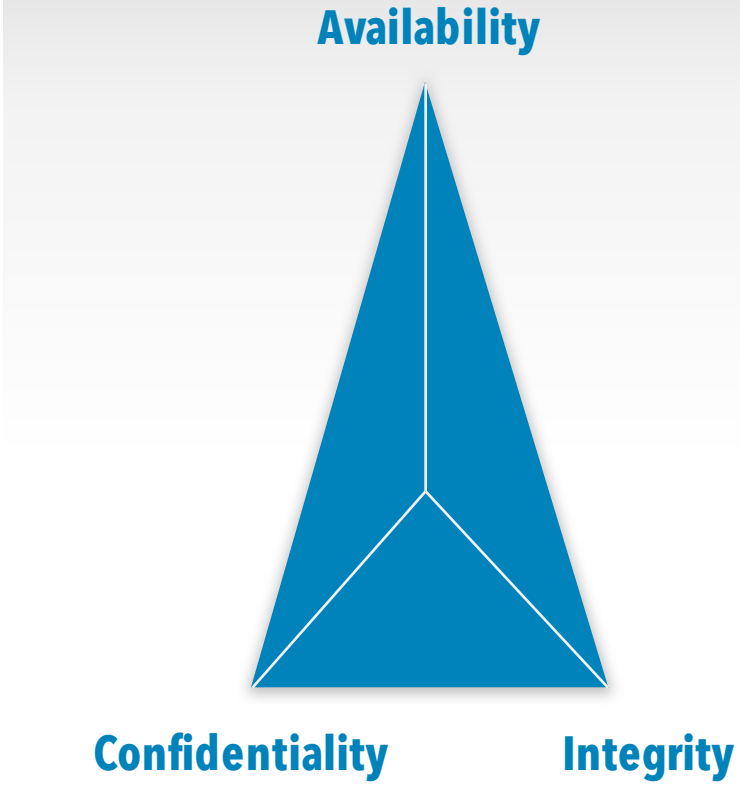
- bridged into corporate networks
- riding common internet protocols
- run on general purpose hardware with IT origins
- running mainstream IT operating systems
- Increasingly connected via standard wireless technologies

Security Requirements: IT vs. OT

Information Technology



Operational Technology



While in the IT the weights of the facets of the CIA triad vary according to the specific scope of application, in the OT the Availability is always the most relevant.

Typical SCADA components as RTU and PLC are vulnerable

- Programmable Logic Controller (PLC) or Remote Terminal Unit (RTU) are low computational computers built for control physical components as valves, pumps, motors, etc.

- They communicates with dedicated protocols that are prone to specific attacks
  - Lack of authentication
  - Lack of encryption
  - Backdoors
  - Buffer overflow
  - Tailored attacks for control physical components

Nozomi Networks understands Industrial Control Systems peculiarities

ICS/SCADA systems are typically **low computational devices** that control critical installation, characterized by:

- Real time systems
- Protocol designed 30 years ago
- Require to run 24x7
- Older Operating System

Availability and timeliness must be a the base of each security improvement

Standard Approach

Standard Security approach are already obsolete and doesn't work on ICS systems

- Antivirus
- Patching
- Firewall

Nozomi Approach

Nozomi technology protects and monitor your standard Industrial Infrastructure:

- Discover infection
- Visibility (network, protocols and industrial communications)
- Detect suspicious activities
- Detect tailored attacks

Visibility and monitoring are the first steps for increasing ICS security

Visibility

- Recognize the **role of each components** inside the network
- **Build the entire map of the system** useful to validate network diagram or vendor schema

Nozomi developed an **innovative technology** able to passively assess and monitor ICS environments

NOZOMI NETWORKS

Monitoring

- Monitor **high risk communications**
- A learning phase guarantees a **tailored security configuration** based on the monitored ICS
- **Detect vulnerability** or misconfiguration

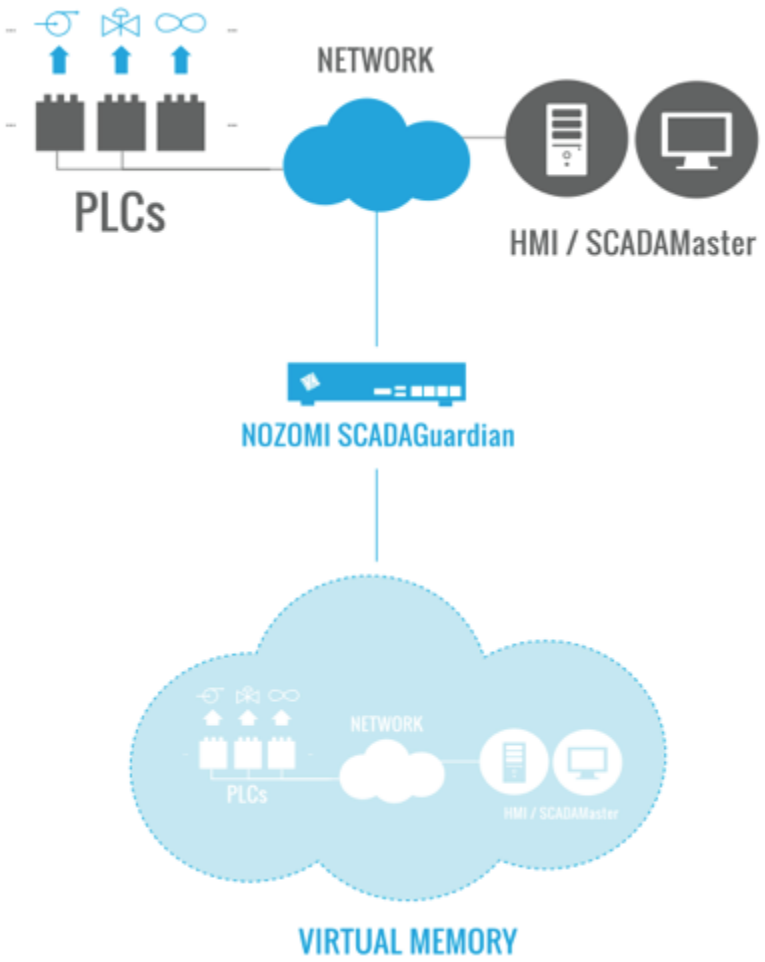
SECURITY

Our Solution

What's SCADAguardian?

SCADAguardian implements an innovative technology for monitoring and assess Industrial Control Systems

- It's the unique technology able to **completely understand the SCADA application level**
- Detects **misconfiguration** on SCADA devices (eg. PLC, DCS, EMS etc..)
- Detects **zero day** vulnerabilities
- Reconstruct entirely the network schema in a passive way (**virtual image)**, recognize the role of each components and assign a **risk level** for each of them
- Detects **standard attacks** (eg. mac spoofing, man in the middle, etc..) and specific SCADA attacks
- **The learning phase** guarantees a specific **configuration tailored** on the SCADA network that we are going to protect or assess
- Detects complex attacks (Critical State) automatically



Nozomi works on different levels with a specific focus on industrial level

Dynamic Global Network Modeling

Physical

- Real time analysis of physical communications in the SCADA networks
- Each physical component connected is analyzed and monitored

Network

- Specific TCP/IP analysis based on network communications
- Internal and external IP analysis

Applications

- Classify and analyze applications
- Discover threat and suspicious behavior related to specific applications
- Deep packet inspection

Industrial

- SCADA communications analysis and classification
- Deep packet inspection of all open and proprietary industrial SCADA protocols
- SCADA behavior detection
- Automatic SCADA signature generation tailored on the industrial process

Global and Correlated Analysis

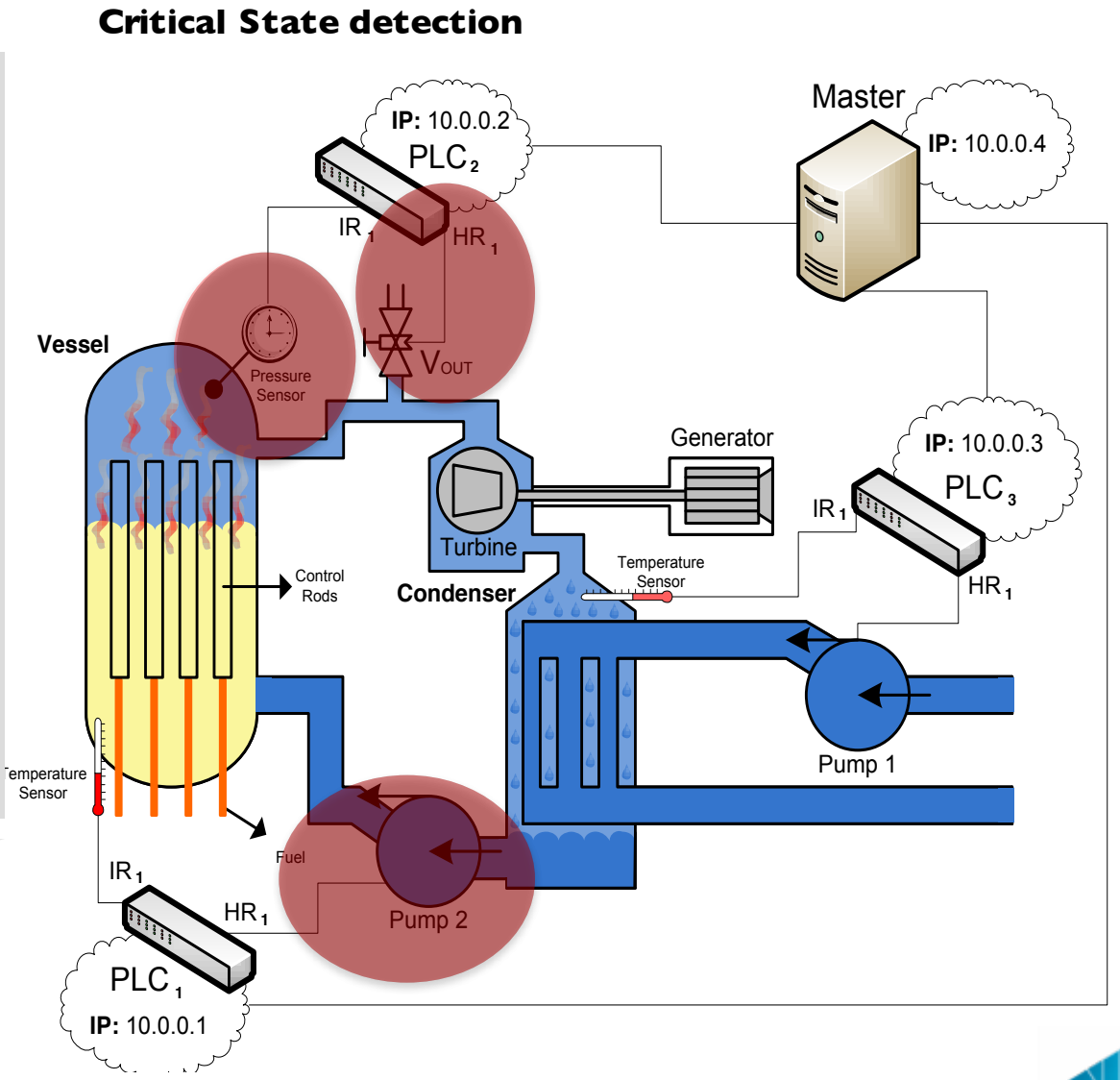
Multidimensional and dynamic analysis of all different levels will create a global view of the industrial network that correlates events, communications and SCADA behaviors in a consolidated view

Example of Industrial critical state detection

A **Critical State (CS)** is a value or a sequence of values that are potentially dangerous for the Industrial Control System:

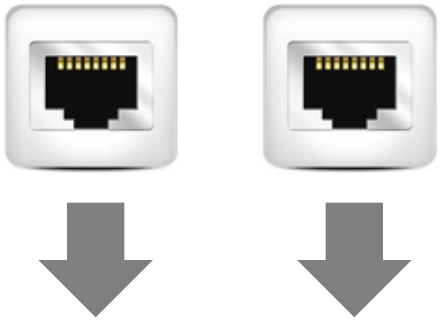
- Injection of malicious packets can put the system in a Critical State
- Single valid packets con bring the system in a Critical State, eg:
  - The figure shows how if the speed pump 2 is set to the maximum speed and in the same time the Valve (HR1) is close, the pressure in the vessel can reach dangerous level
- SCADAguardian is able to detect **correlated Critical State**

Operators that knows the SCADA can **add manually** through a graphic interface a set of CS



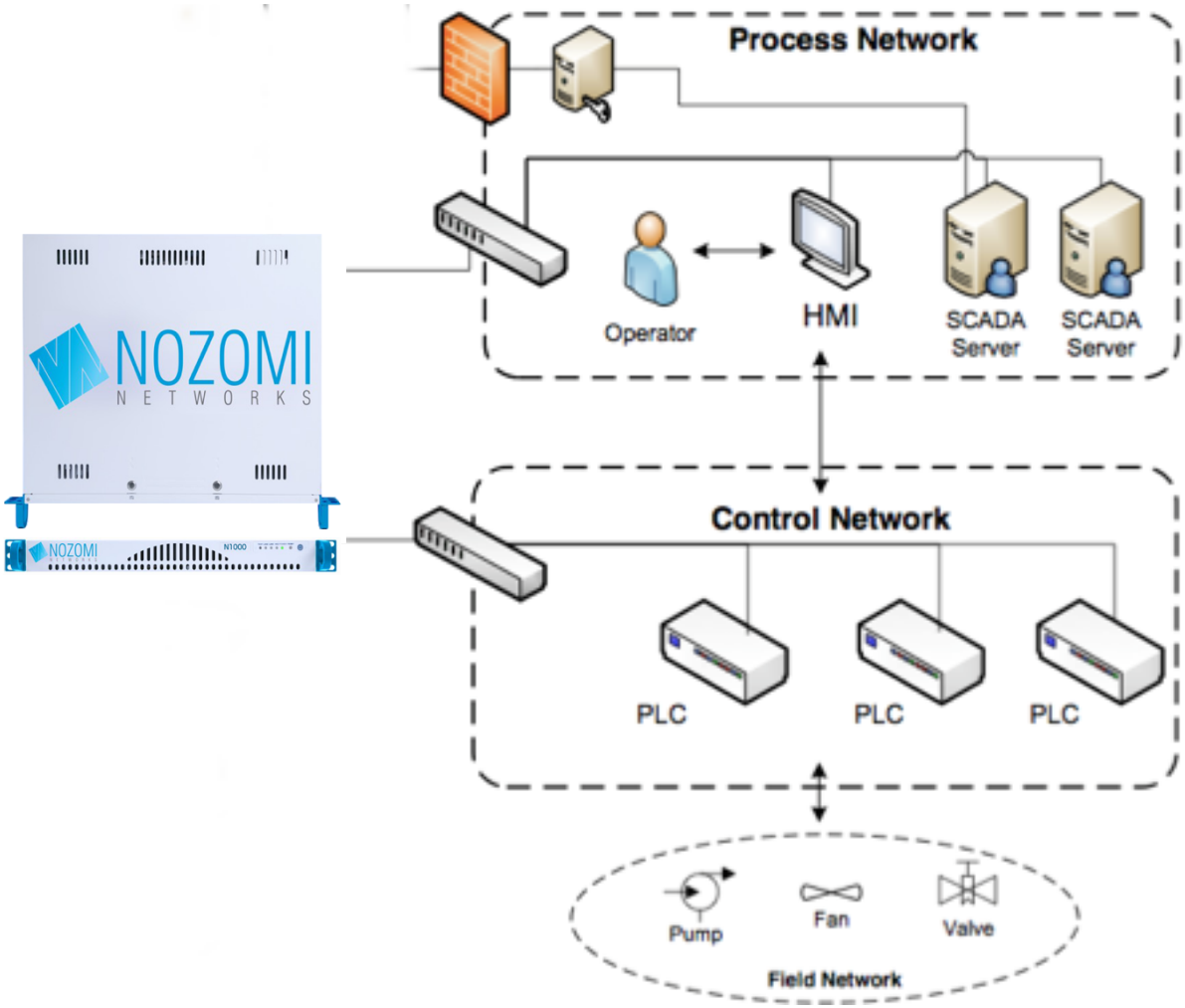
Deployment Scenarios

Nozomi Networks – Standard Deployment Scenario

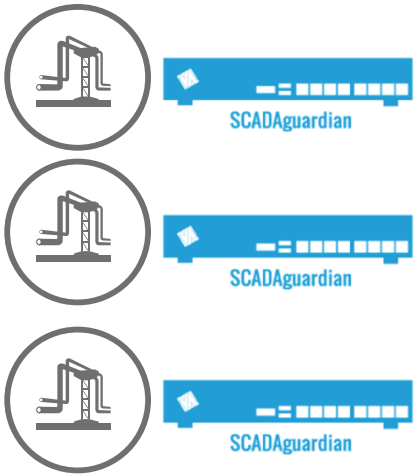


The **Nozomi Networks appliance** must be connected to the SPAN/Mirror port of the network.

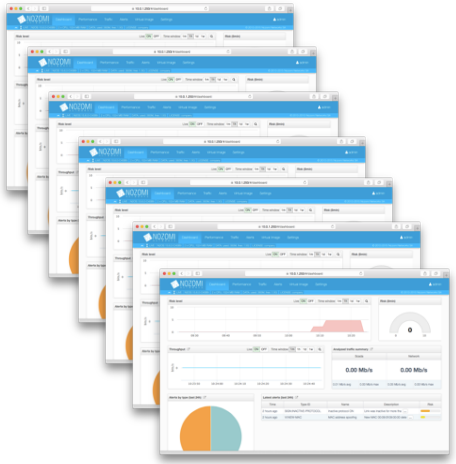
This guarantees a complete isolation of the appliance from the working network, thus enabling a **hot deploy** with **no interferences** on active communications.

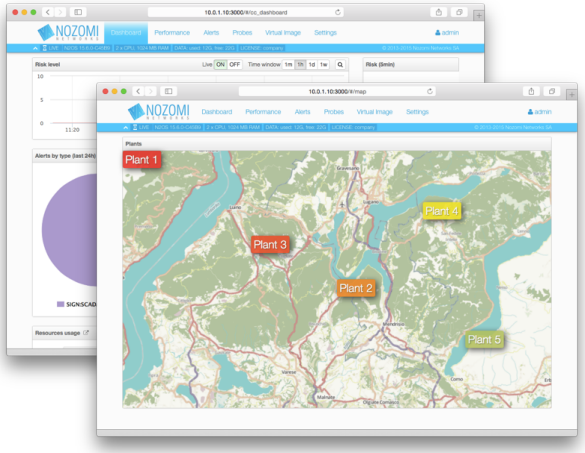


A distributed installation is supported with a Central Console



Nozomi Central Management Console



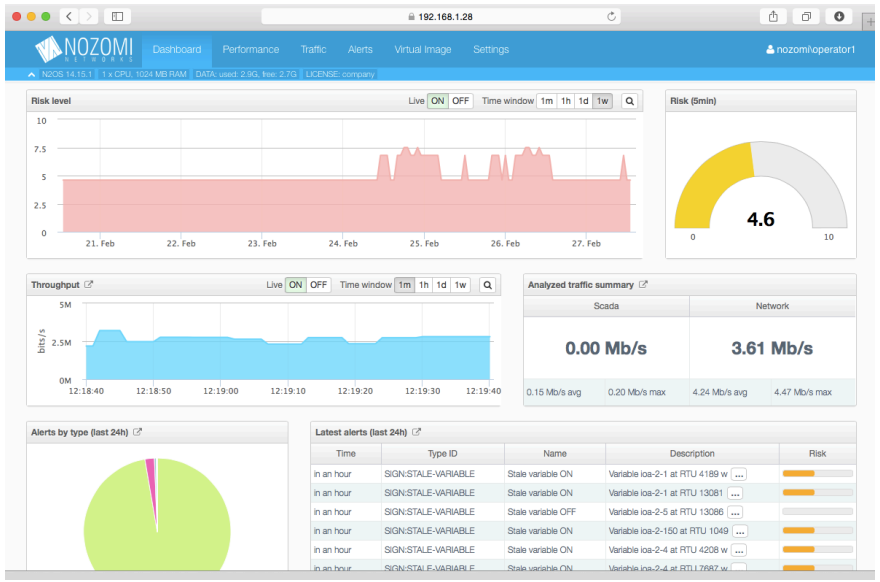


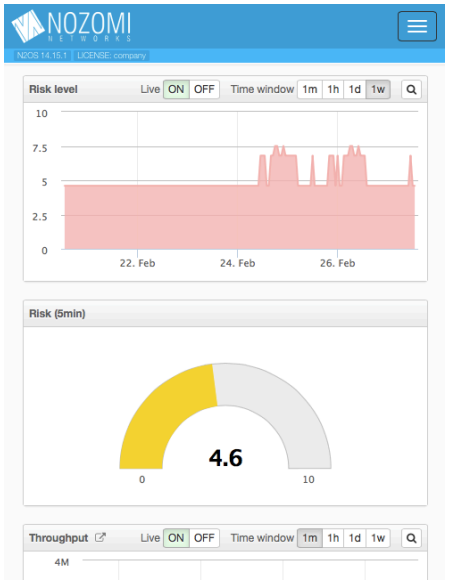
- Supports **hundreds** of probes
- Possibility to create **hierarchical architectures**

- **Total visibility** and control
- **Automated** updates handling

No deployment of client software is required for the console

The console is built with **HTML5** and **Javascript** that enable a fast and responsive interface for all screens.

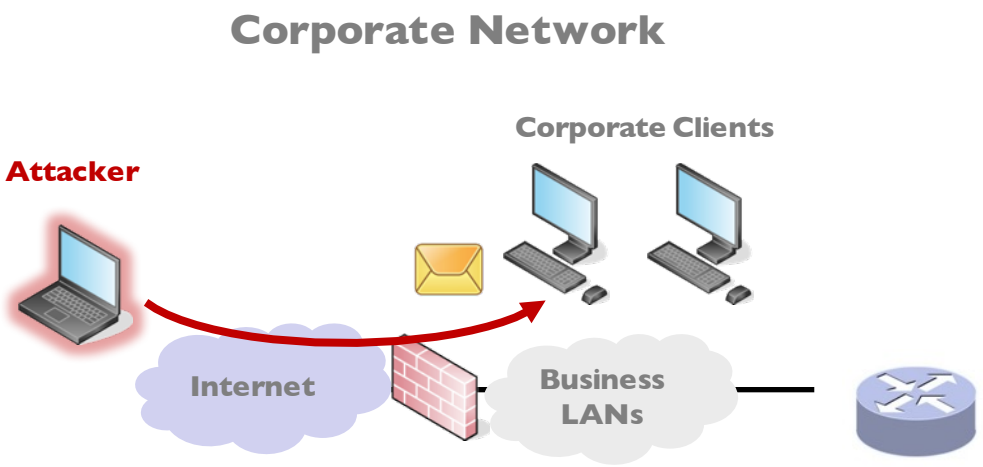




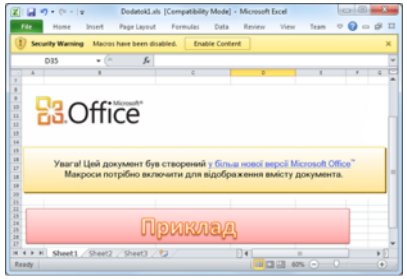
- … no special version of Java required
- … no client to install, update, etc

UKRAINE ATTACK, STEP BY STEP

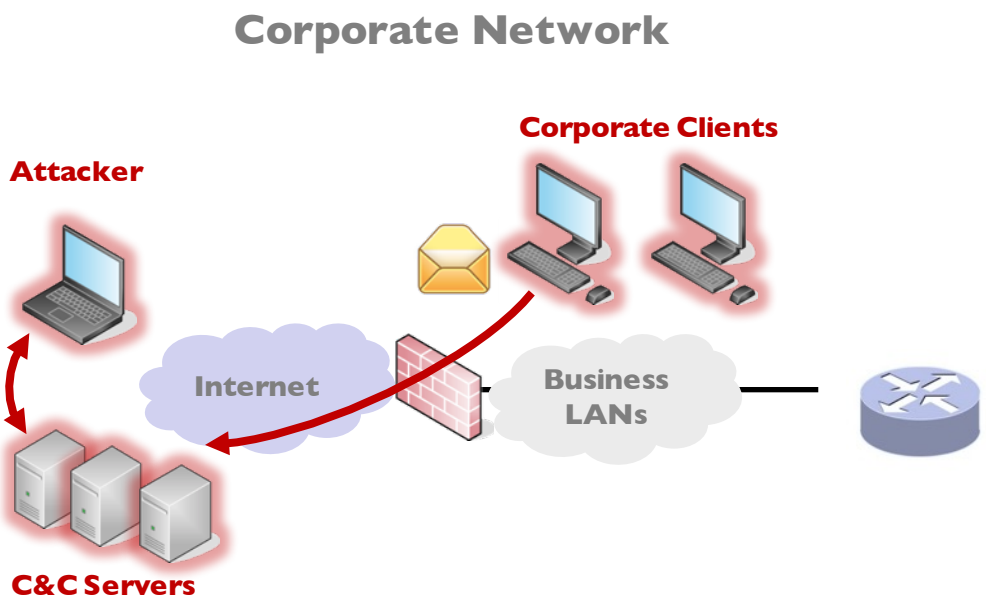
1. Spear Pishing Email



The target gets a spear-phishing email that contains an attachment with a malicious document. The attackers spoofed the sender address to appear to be one belonging to Rada (the Ukrainian parliament) and the document itself contains text trying to convince the victim to run the macro in the document

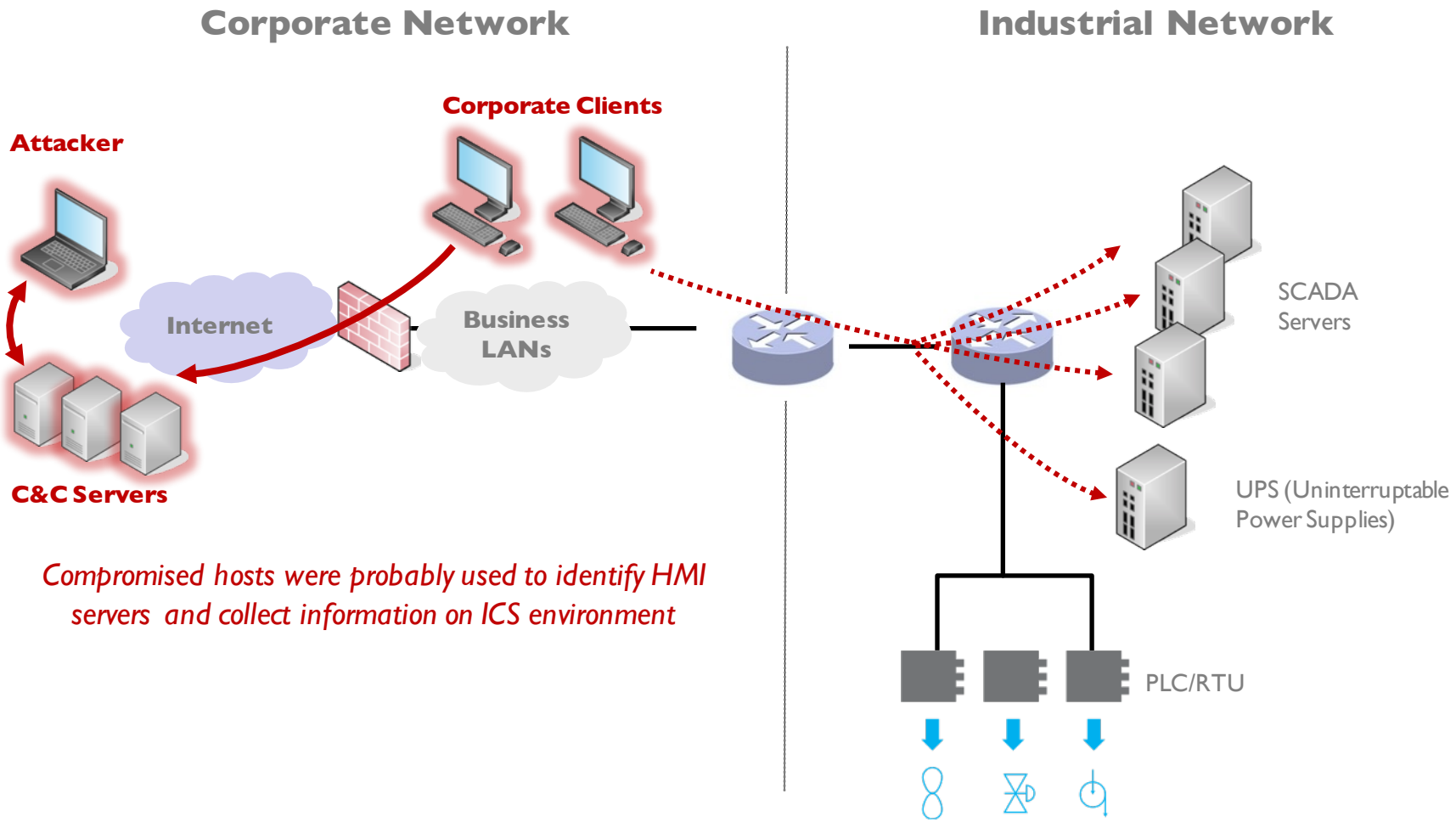


2. Information Gathering



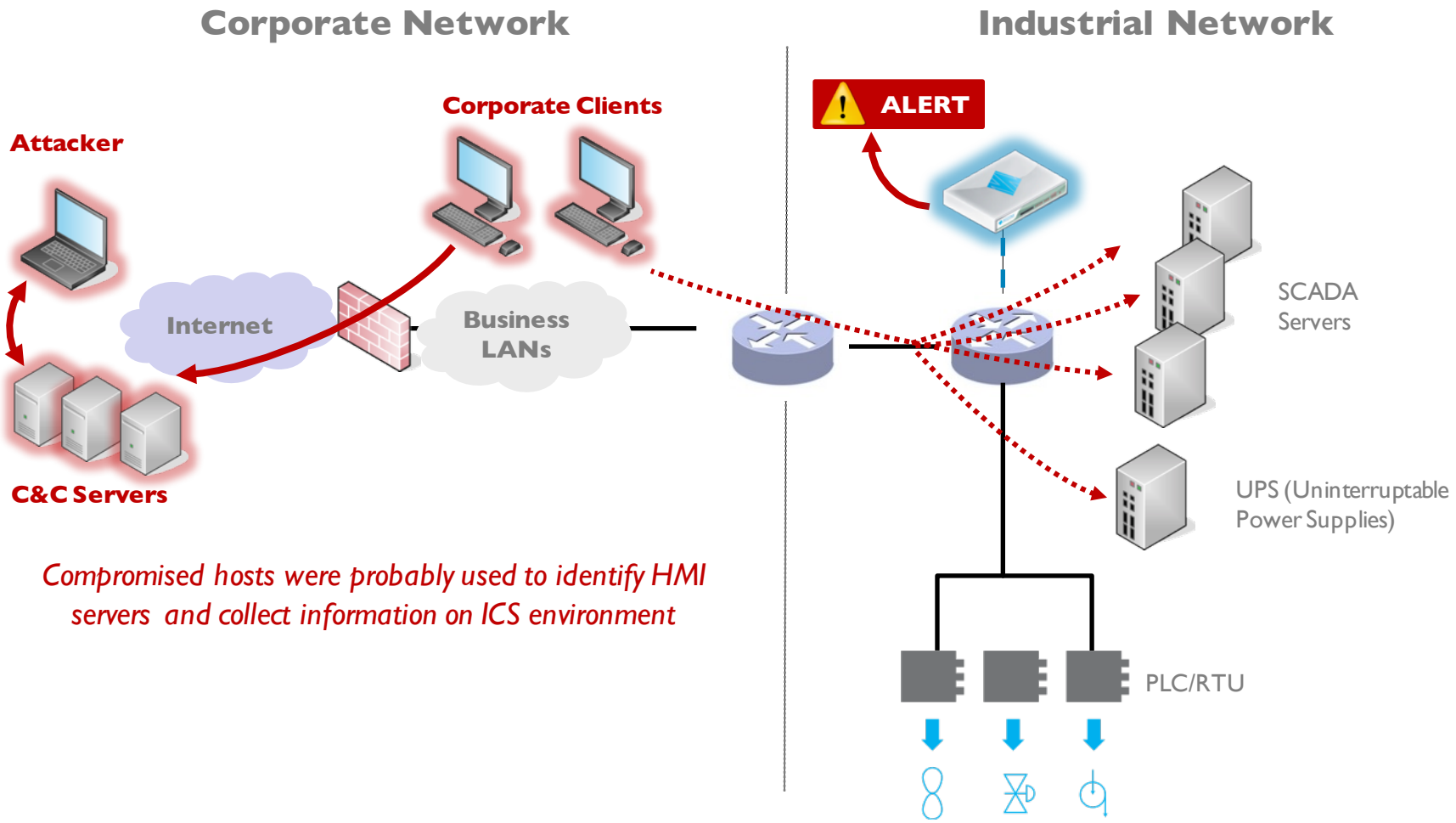
The victims, successfully tricked, executed malicious code to interact with remote Command and Control (C&C) servers. System information was sent to C&C servers, and was used by attackers to gather additional information about targets. Ultimate goal was to execute commands on the victim's hosts or to gain remote access to the target network

3. Lateral Movement



Compromised hosts were probably used to identify HMI servers and collect information on ICS environment

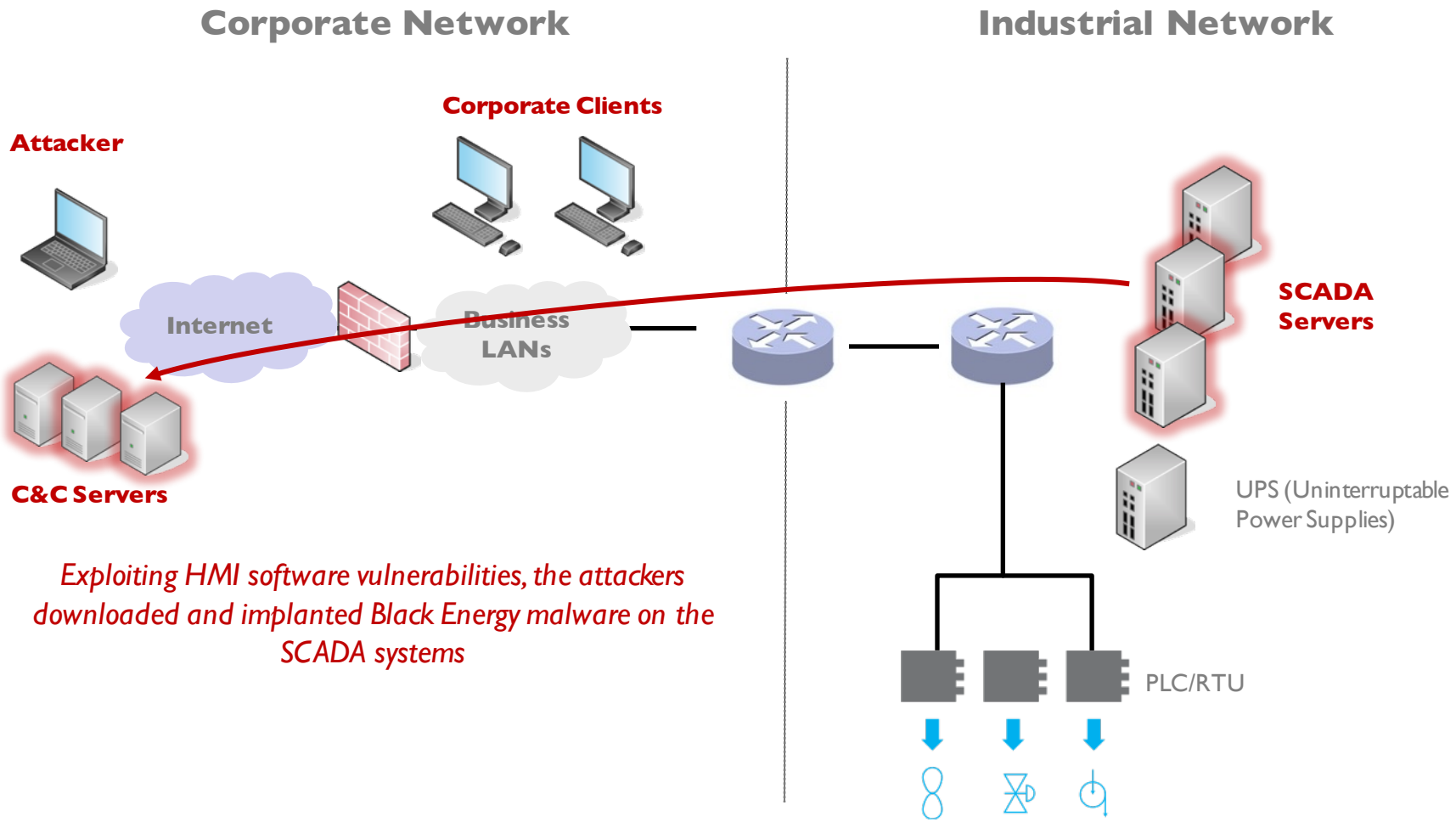
3. Lateral Movement - with NOZOMI SCADAguardian



Compromised hosts were probably used to identify HMI servers and collect information on ICS environment

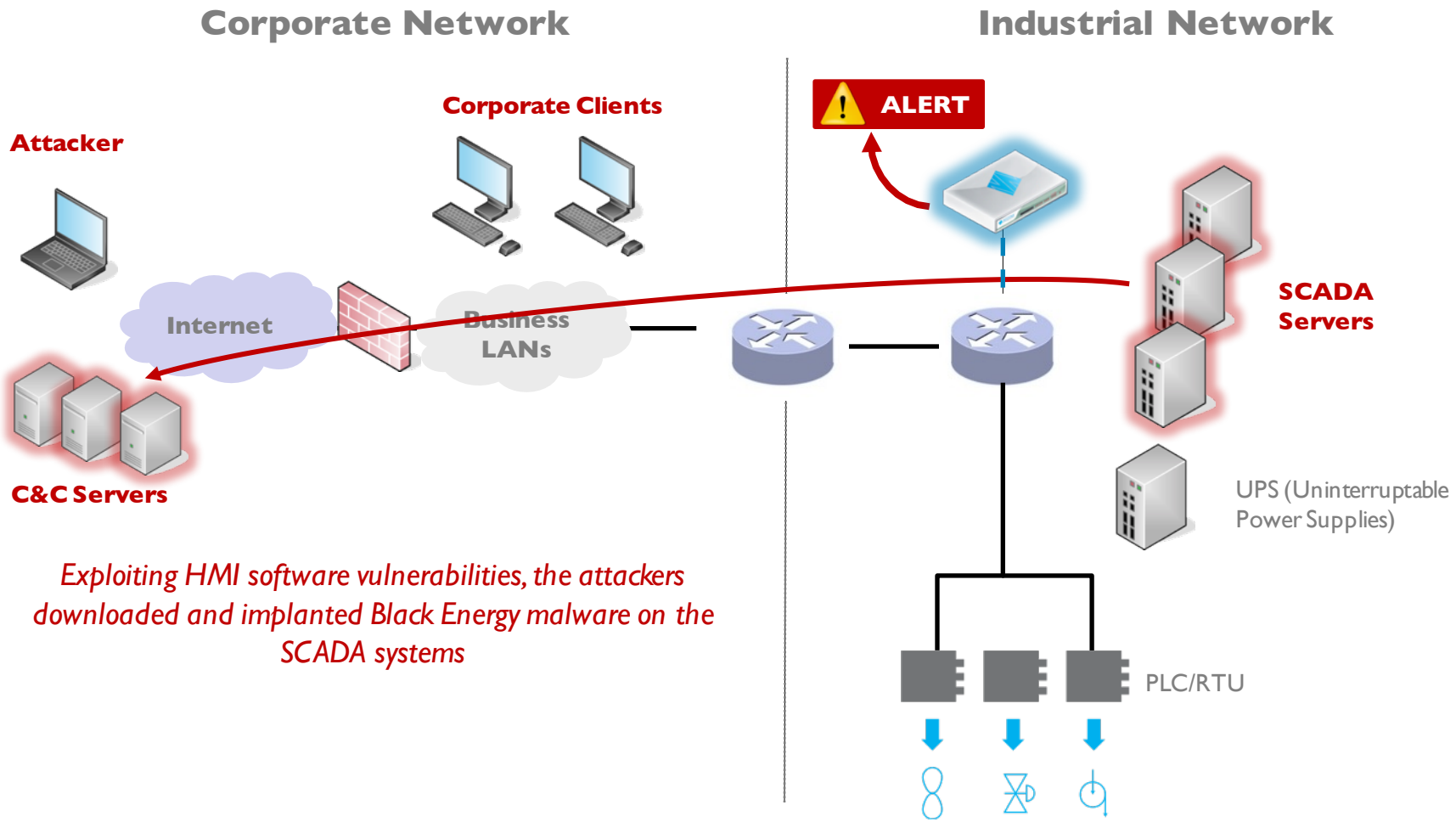
NOZOMI SCADAguardian identifies this type of reconnaissance activity, and raises alerts when they occur

4. SCADA Infiltration



Exploiting HMI software vulnerabilities, the attackers downloaded and implanted Black Energy malware on the SCADA systems

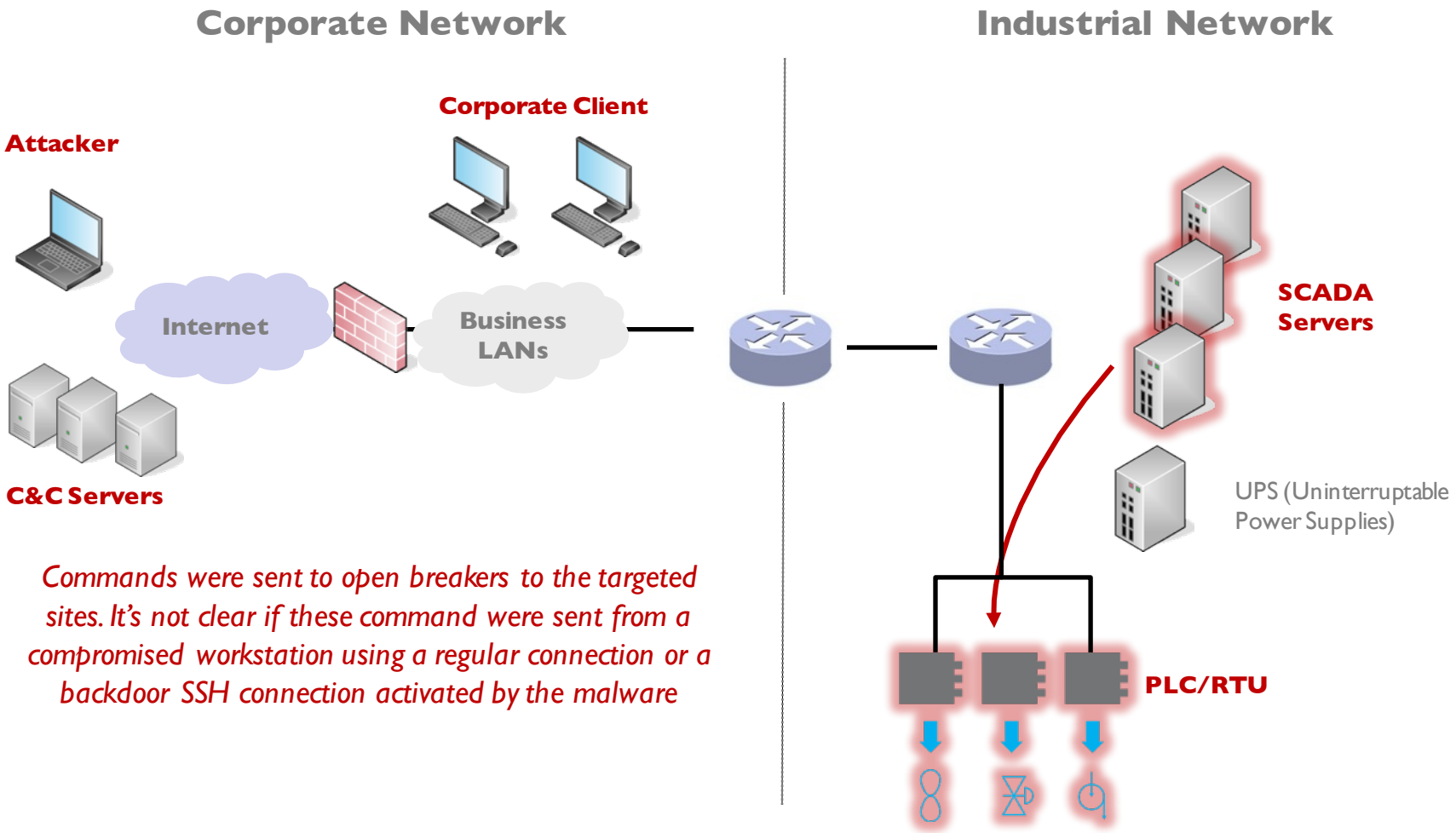
4. SCADA Infiltration - with NOZOMI SCADAguardian



Exploiting HMI software vulnerabilities, the attackers downloaded and implanted Black Energy malware on the SCADA systems

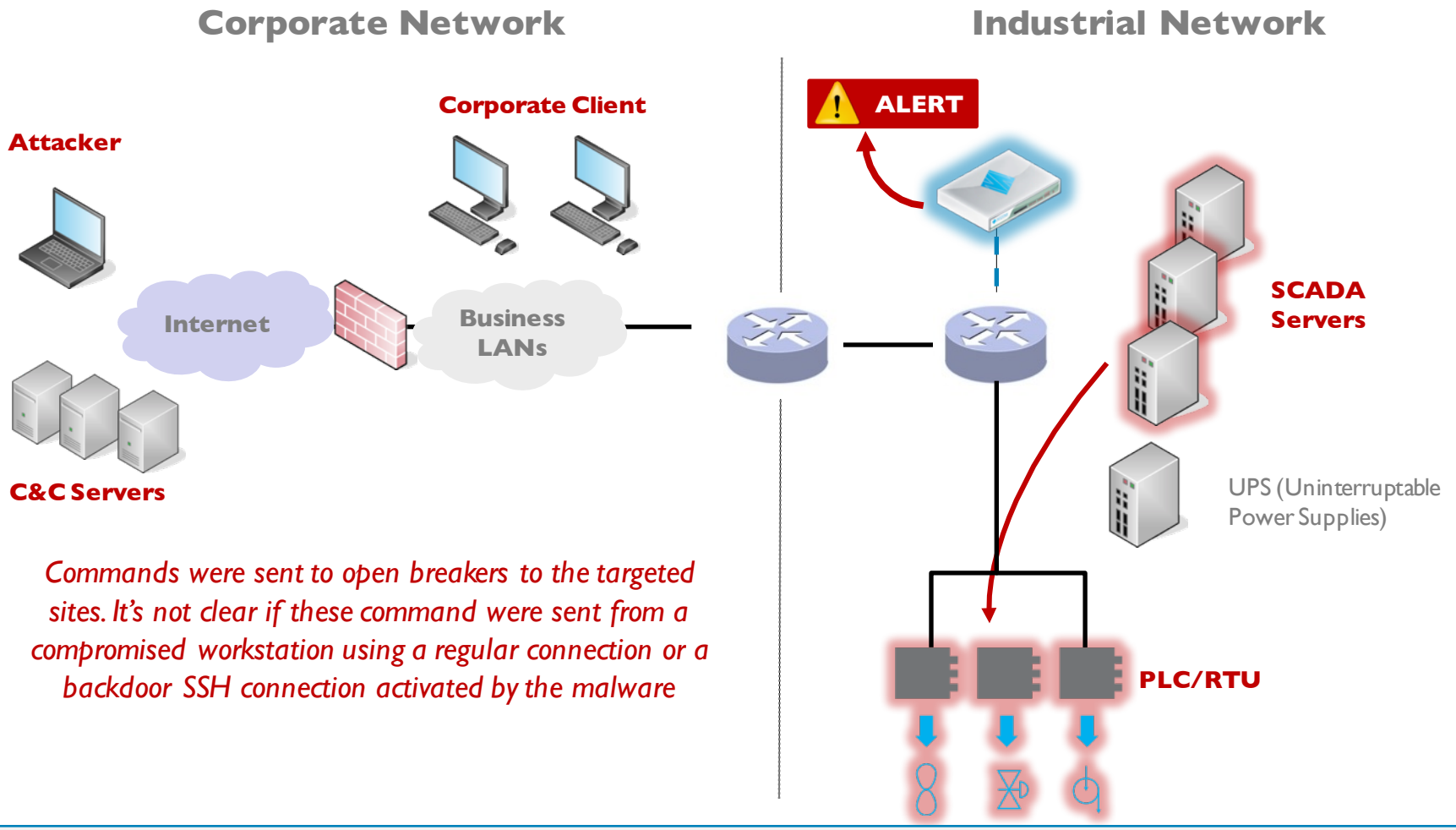
NOZOMI SCADAguardian detects abnormal and suspicious connections, like those from an industrial systems to Internet

5. Electric Outage



Commands were sent to open breakers to the targeted sites. It's not clear if these command were sent from a compromised workstation using a regular connection or a backdoor SSH connection activated by the malware

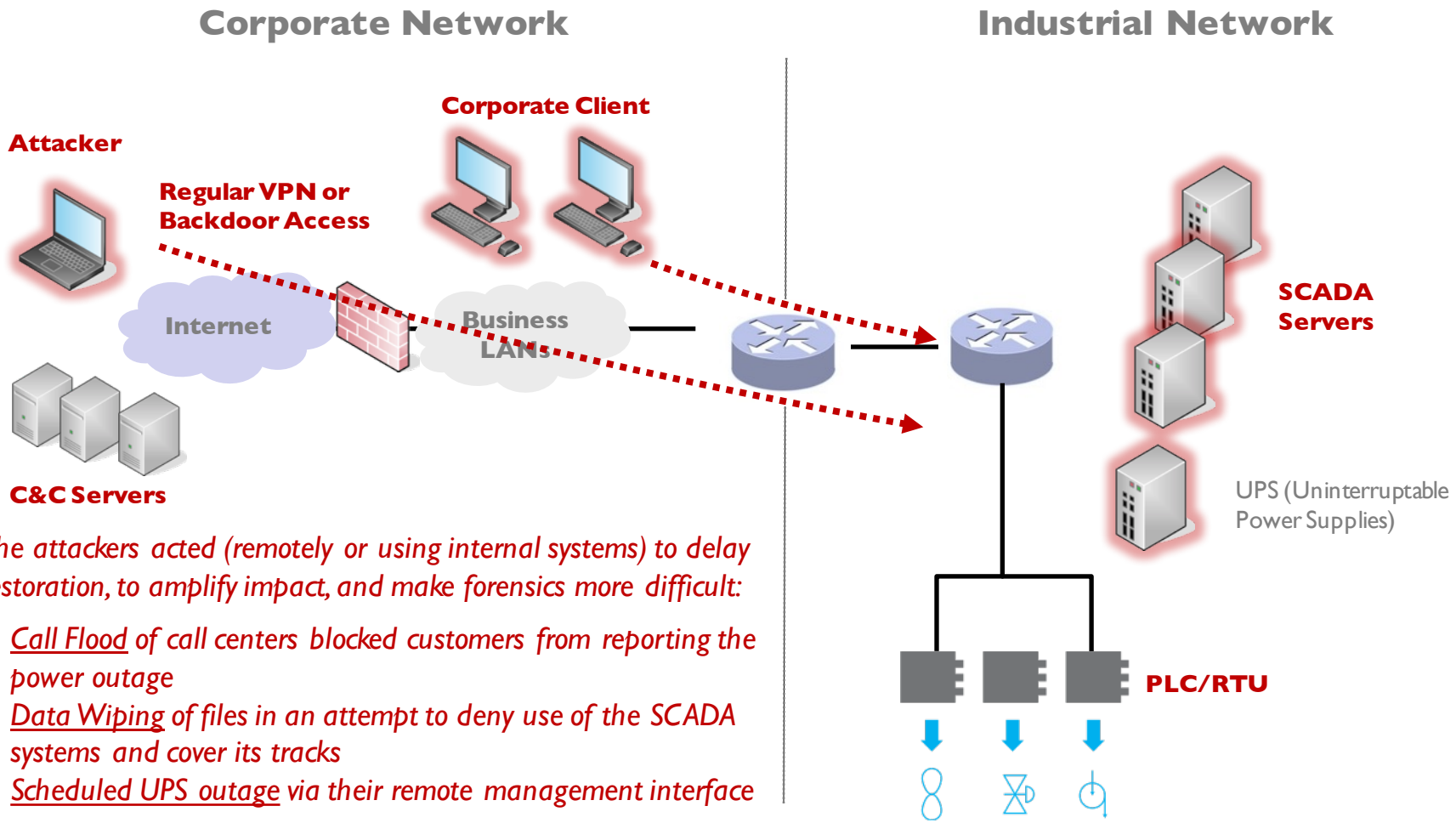
5. Electric Outage - with NOZOMI SCADAguardian



Commands were sent to open breakers to the targeted sites. It's not clear if these command were sent from a compromised workstation using a regular connection or a backdoor SSH connection activated by the malware

NOZOMI SCADAguardian monitors process commands and variables, alerting on critical or undesired conditions

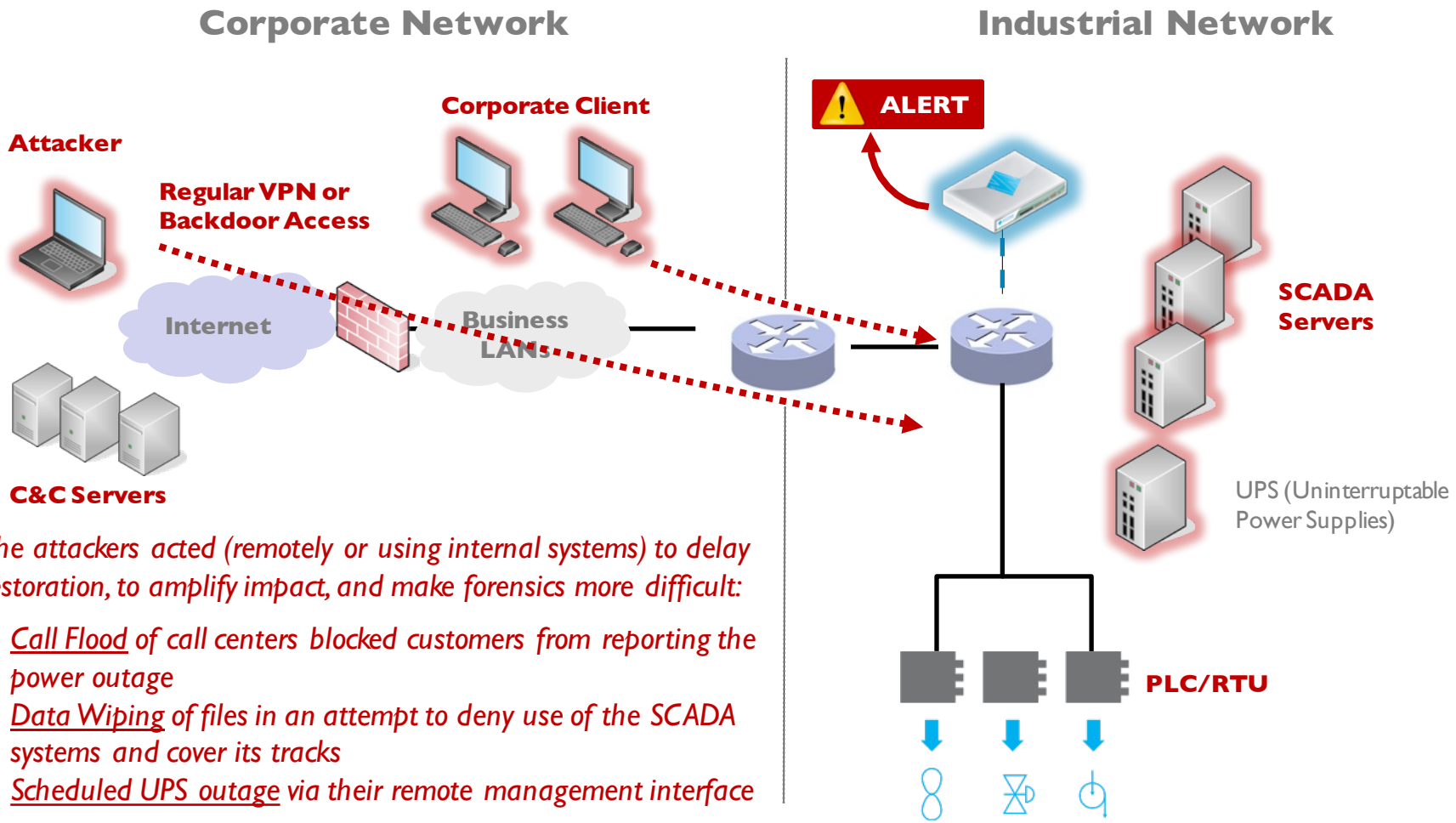
6. Actions to hinder incident response



The attackers acted (remotely or using internal systems) to delay restoration, to amplify impact, and make forensics more difficult:

- *Call Flood of call centers blocked customers from reporting the power outage*
- *Data Wiping of files in an attempt to deny use of the SCADA systems and cover its tracks*
- *Scheduled UPS outage via their remote management interface*

6. Actions to hinder incident response - NOZOMI SCADAguardian

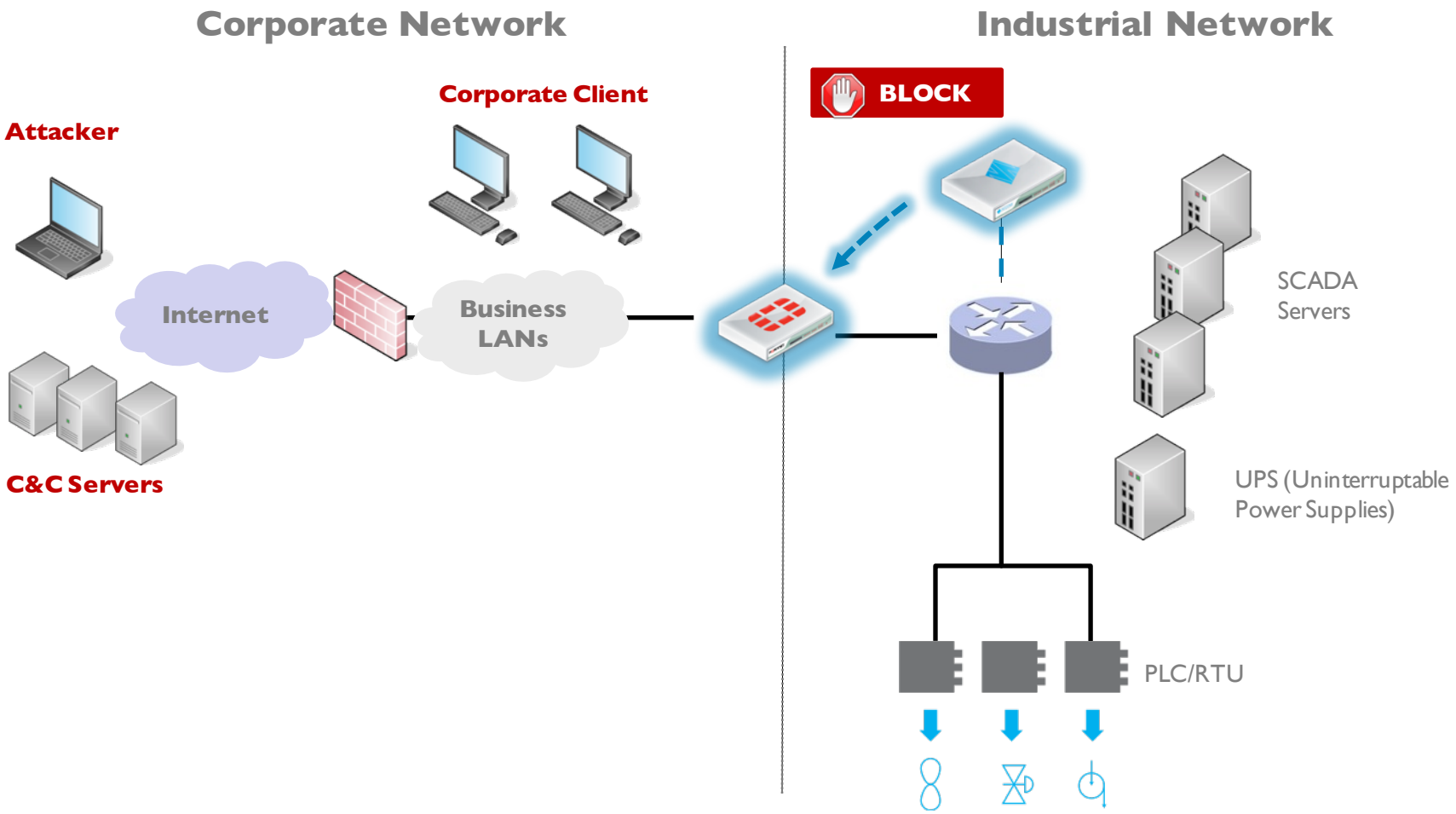


The attackers acted (remotely or using internal systems) to delay restoration, to amplify impact, and make forensics more difficult:

- *Call Flood of call centers blocked customers from reporting the power outage*
- *Data Wiping of files in an attempt to deny use of the SCADA systems and cover its tracks*
- *Scheduled UPS outage via their remote management interface*

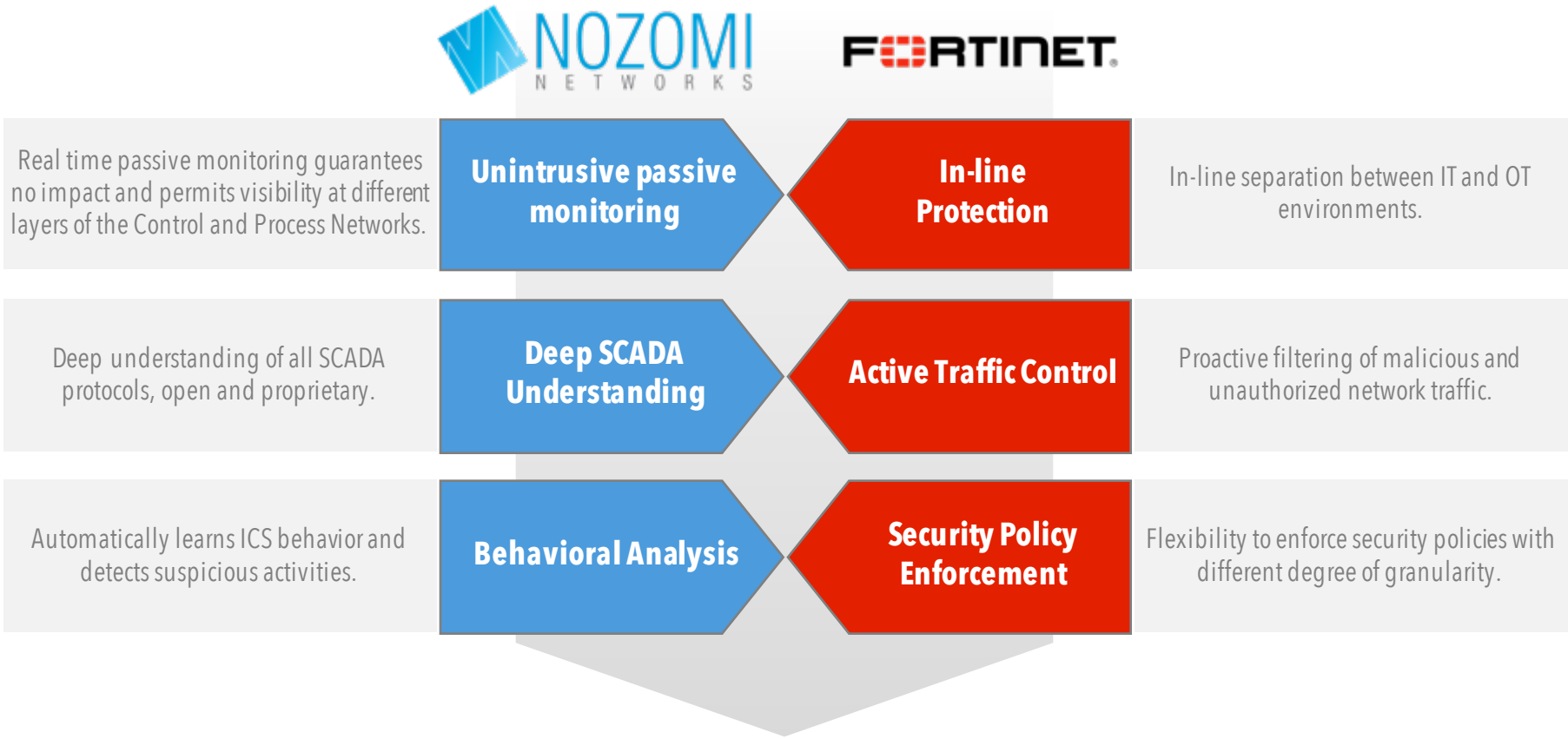
NOZOMI SCADAguardian detects abnormal connections (internal or external), such as those generated during the power outage

Extra Benefit: Proactive response with Firewall Integration



The integration between SCADAguardian and the perimeter firewall provides additional protection against these types of attack

Active integration between SCADAguardian and Fortigate

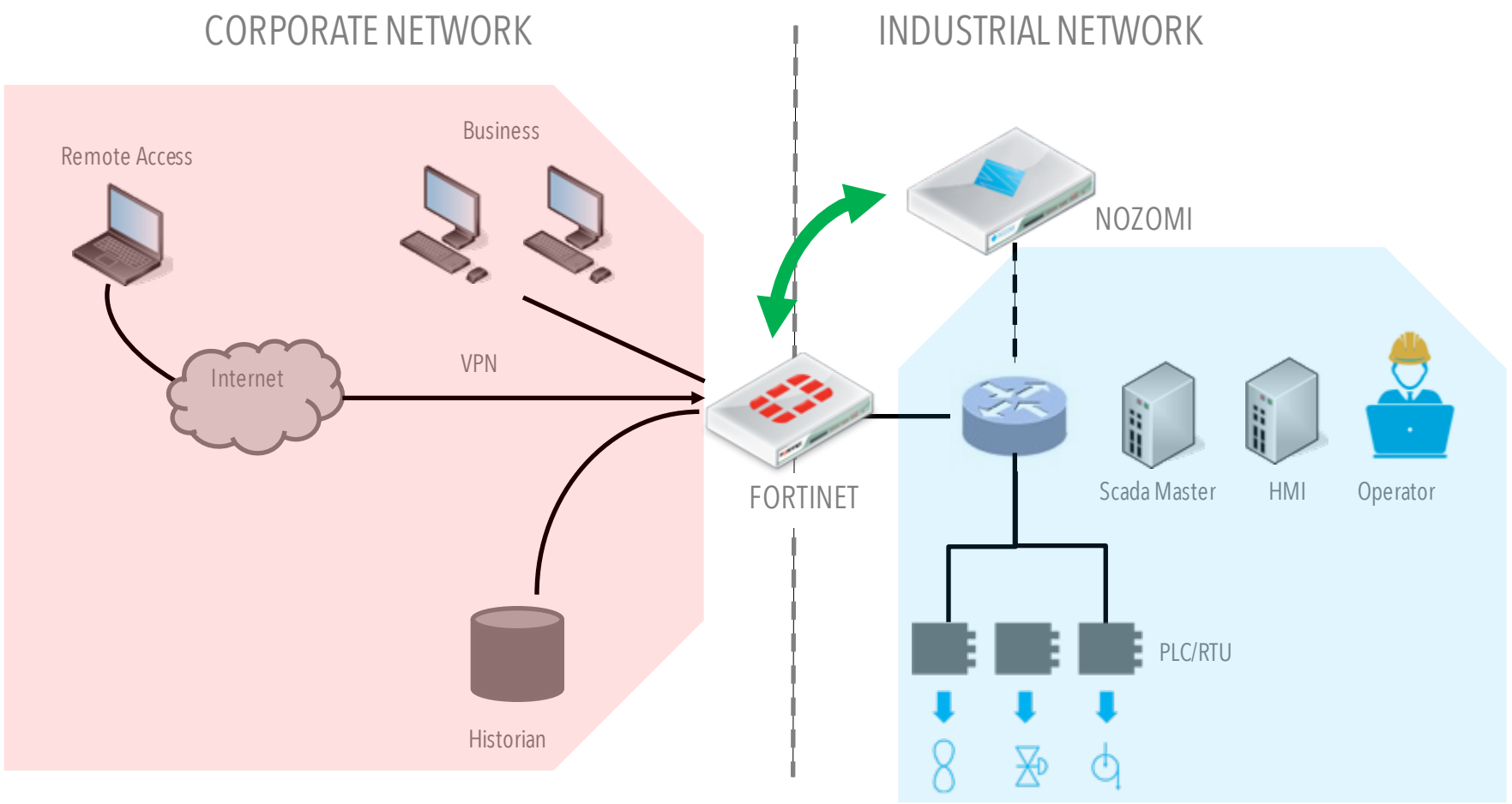


Turn-key Internal and Perimeter Visibility

Fine Tuning, Control and Monitoring of the Firewall Ruleset

Proactive SCADA Security

Typical Customer Scenario



Full Protection, visibility and monitoring thanks to **Nozomi** and **Fortinet**

NOZOMI - FORTINET Benefits Summary

- Early warning of reconnaissance activities
- Real-time alerts for SCADA infiltration
- Real-time alerts for abnormal SCADA commands
- Real-time alert for abnormal network connections
- Blocking ongoing attack via integration with Fortinet firewall

Case Study

The Client - Enel

Enel, a multinational power company operating in more than 30 countries and four continents, selected cybersecurity leader Nozomi Networks to improve the reliability, efficiency, and cybersecurity of its power generation plants and networks.

Enel chose to deploy Nozomi's state-of-the-art SCADAguardian solution in Italy

31+ gigawatts production capacity

31 million customers.

The Challenge - An ideal pilot project

500

POWER GENERATION PLANTS

24/7

ICS AND INDUSTRIAL NETWORK AVAILABILITY

Enel's Remote Control System Team

- Manages and monitors the Regional Control Centers and the Interconnection Centers that connect with Terna, the Italian Transmission System Operator (TSO).
- Controls and remotely regulates the power generation of power plants

The Challenge - An ideal pilot project

BEFORE

- Standard networking tools to manage, monitor, and troubleshoot the Control Network and the Industrial System.
- The operations were manual and time consuming
- Information was difficult to gather and required human knowledge to be understood and correlated.
- A mandatory requirement was the full in-depth support of SCADA protocol IEC 60870-5-104 and support for the security requirements IEC 62351.

AFTER

- Deploy and fine-tune the SCADAguardian system to monitor, troubleshoot, and protect its industrial control network from a central location.
- Gathering information and protecting operations became an automated process
- Correlated and meaningful information.

The Solution

Enel and Nozomi achieved substantial, measurable improvement in control network reliability, efficiency, and cybersecurity. The solution was deployed at one Regional Control Center first, then approved for full-scale rollout following extensive testing and fine-tuning.

FIRST STEP

SCADAguardian probes became operational in all Regional Control Centers

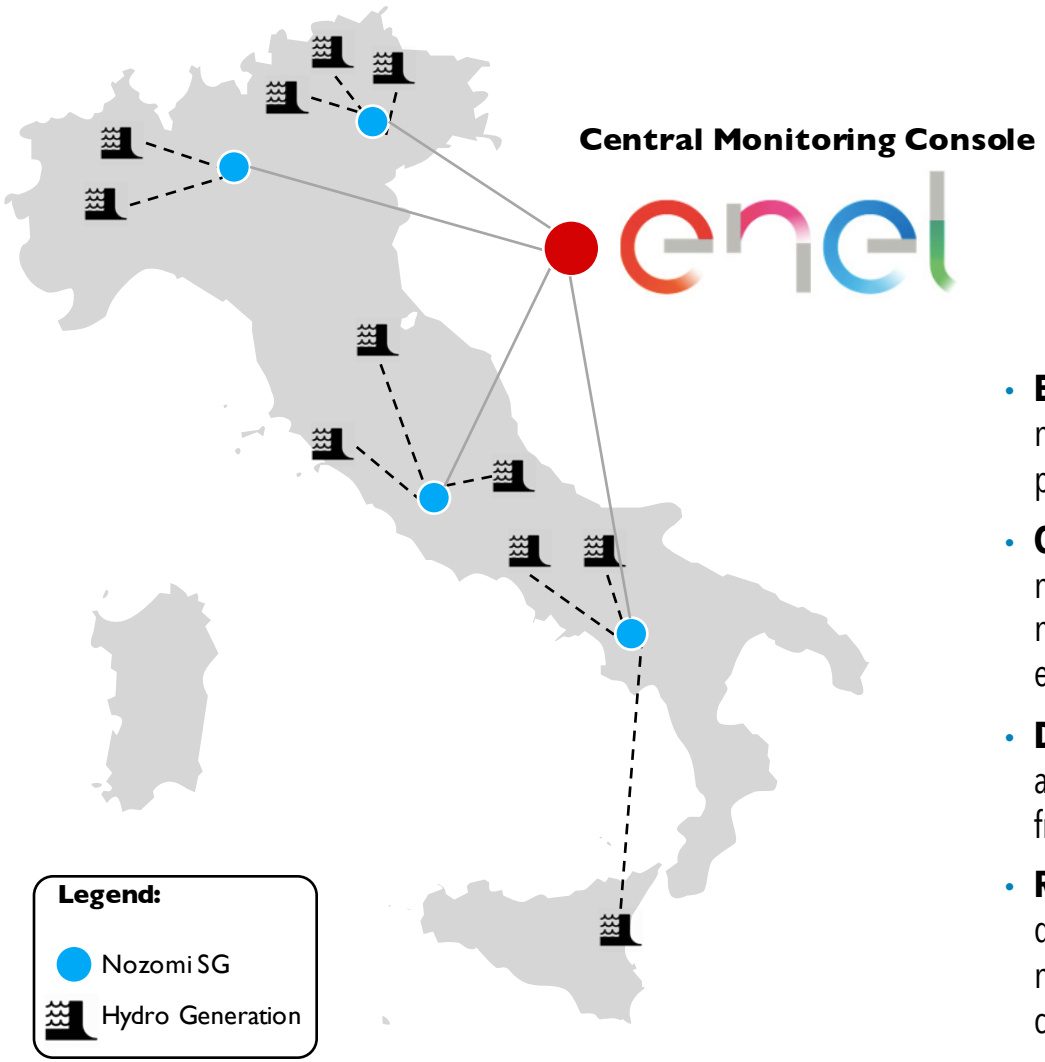
SECONDLY

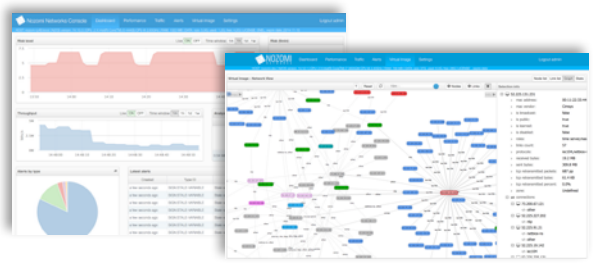
Enel installed Nozomi's central management console to operate, monitor, and update the probes from a central control room.

FINALLY

Enel introduced Nozomi SCADAguardian P500's portable edition to monitor and analyze the segments requiring investigation and troubleshooting in the network.

Nozomi Case Study: ENEL, Hydropower Generation Plants





- **Enel**: a multinational power company with over 61 million customers. It operates over 500 power generation plants in Italy
- **Challenge**: Using standard networking tools to manage, monitor, and troubleshoot the entire industrial control network. Analysis was manual, time-consuming, and error prone
- **Deployment**: Enel deployed 8 Nozomi SCADAguardian appliances in Italy without downtime, and monitors them from 2 centralized control centers
- **Results**: Full visibility and monitoring over entire distributed network. Automated detection of misconfiguration, anomalous activities, critical states, and cyber attacks

The Results

The project yielded numerous tangible results and key learnings, including:

Full visibility and monitoring
over the Enel control network

Extended operational insight
by detecting misconfigurations, anomalous activities, critical states, and standard and advanced security

Automatic real-time notification
of any industrial event of interest

Monitoring of the connections between Enel and the TSO
and traffic analysis for current and future investigations

Conclusion

SCADAguardian's non-intrusive, in-depth network analysis of Industrial Control Systems, powered by state-of-the-art machine learning, big data and deep analytics, is the perfect complement to provide unprecedented protection to the industrial network environments of power generation customers.

"Enel Power Plants are a strategic asset we are committed to protect. Malfunctions or damage to this infrastructure would be a threat to our national security. With Nozomi SCADAguardian we can now detect and collect operational and cybersecurity issues in real time, and take corrective actions before the threat can strike."

GIAN LUIGI PUGNI
ENEL'S HEAD OF CYBERSECURITY DESIGN

"Through this partnership, we have made a substantial improvement in our Remote Control System. Nozomi SCADAguardian is now a fundamental element of our network infrastructure and an essential tool for our daily activities. Nozomi proved to us, through an extensive production pilot in Italy, that their non-intrusive in-depth technology was able to substantially improve the reliability, efficiency, and cybersecurity of our remote control system."

FEDERICO BELLIO
ENEL'S HEAD OF POWER GENERATION REMOTE CONTROL SYSTEM

"The combination of Enel's extensive experience operating power production remote control networks and Nozomi's unique, patented technology for non-intrusive in-depth analysis of Industrial Control Systems, allowed us to improve the reliability, efficiency, and cybersecurity of Enel's power generation in Italy, a national critical infrastructure."

MORENO CARULLO
CHIEF TECHNOLOGY OFFICER OF NOZOMI NETWORKS

Thank You

RICHARD ZONI

HEAD OF SALES AND BUSINESS DEVELOPMENT

richard.zoni@nozominetworks.com

mobile: +41 78 713 4055

office: +41 91 647 0406