SIEMENS
Ingenuity for life

Siemens Australia ISS

Industrial Security Services

Presenter Profile

SIEMENS
Ingenuity for life

Serge Maillet

Organisation	Siemens Australia
Job Function	Business Segment Manager CI & Industrial Cybersecurity
Time in Industry	21 Years
Credentials	MSc. Cybersecurity

my motto: Cybersecurity is only as strong as your weakest link.

Cybersecurity Attacks on Critical Infrastructure 2010 - 2018

SIEMENS
Ingenuity for life

“GreyEnergy”	2017	2010	Stuxnet
“Triton”–	2017	2011	Virus “Duqu”
“WannaCry”, “Petya” and “Not-Petya”	2017	2012	Telvent
Iran petrochemical	2016	2013	Germany steel mill ISC attack
“BlackEnergy”	2015	2014	Black Energy
“Energetic Bear”	2014		

Source: Hackmageddon, Reuters, Sans.org, NY Times, sans.org, Trend Micro, FireEye

Disrupting, delaying, or destroying the power supply is a big incentive

There are a variety of attackers

- Examples: Nation States, Organized Crime, Terrorist, Hacktivists

Attacks have grown in frequency and intensity

- Examples: Ransomware, Insider Threats, Phishing Attacks, Malware, Zero Day

Industrial Cybersecurity
An increasingly factor for the success of the digital economy

SIEMENS
Ingenuity for life

1950s – 1960s
Military, governments and other organizations implement computer systems

1970s
Home computer is introduced

1980s
Computers make their way into schools, homes, business and industry

1990s
Digital enhancement of electrification and automation

1999
The globe is connected by the internet

1991
The World Wide Web becomes publicly accessible

2010s
Cloud computing enters the mainstream

2000s
Mobile flexibility

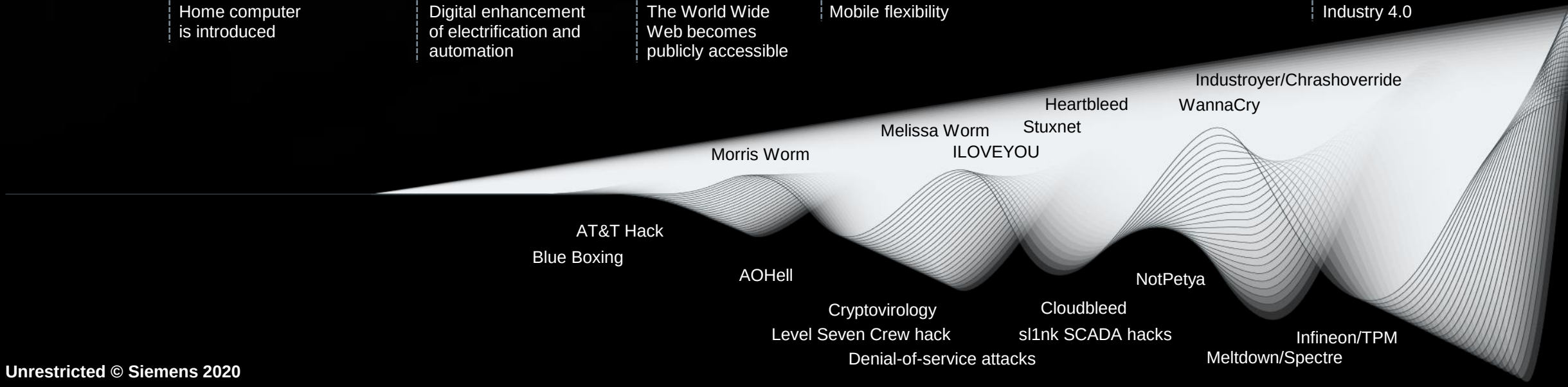
2020s
Internet of Things, Smart and autonomous systems, Artificial Intelligence, Big Data

2020s
Industry 4.0

Digital Information Processing

Digital Connectivity

Digital Automation and Intelligence



Cybersecurity Landscape in Australia

SIEMENS
Ingenuity for life

The current state of Cybersecurity for organisations in Australia:

Australia has recorded its largest increase of Cybersecurity events over the past 12 months compared to all other countries in APAC.

Australia currently has less than 10% of the Cybersecurity expertise that it requires to protect its industries in all industry verticals.

In 2018 – 2019, the spend on external Cybersecurity products and services in Australia reached almost AUD $3.9 billion. The current ratio of cybersecurity services VS. products is currently 70:30.

The current potential economic cost to Cybersecurity incidents in Australia is approximately AUD $29 billion per year (2% of GDP).

Cyber failings are now at a ‘crisis’ levels across most industry verticals in Australia.

Case Study: Toll Group – Ransomware Attack

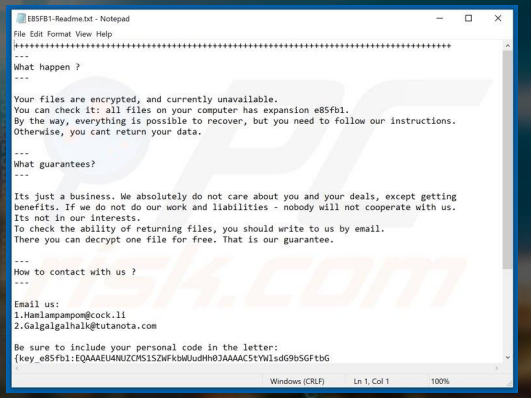
Who:
Toll Group

What:
Ransomware Attack on Toll's IT-OT systems
(~1000 servers infected)

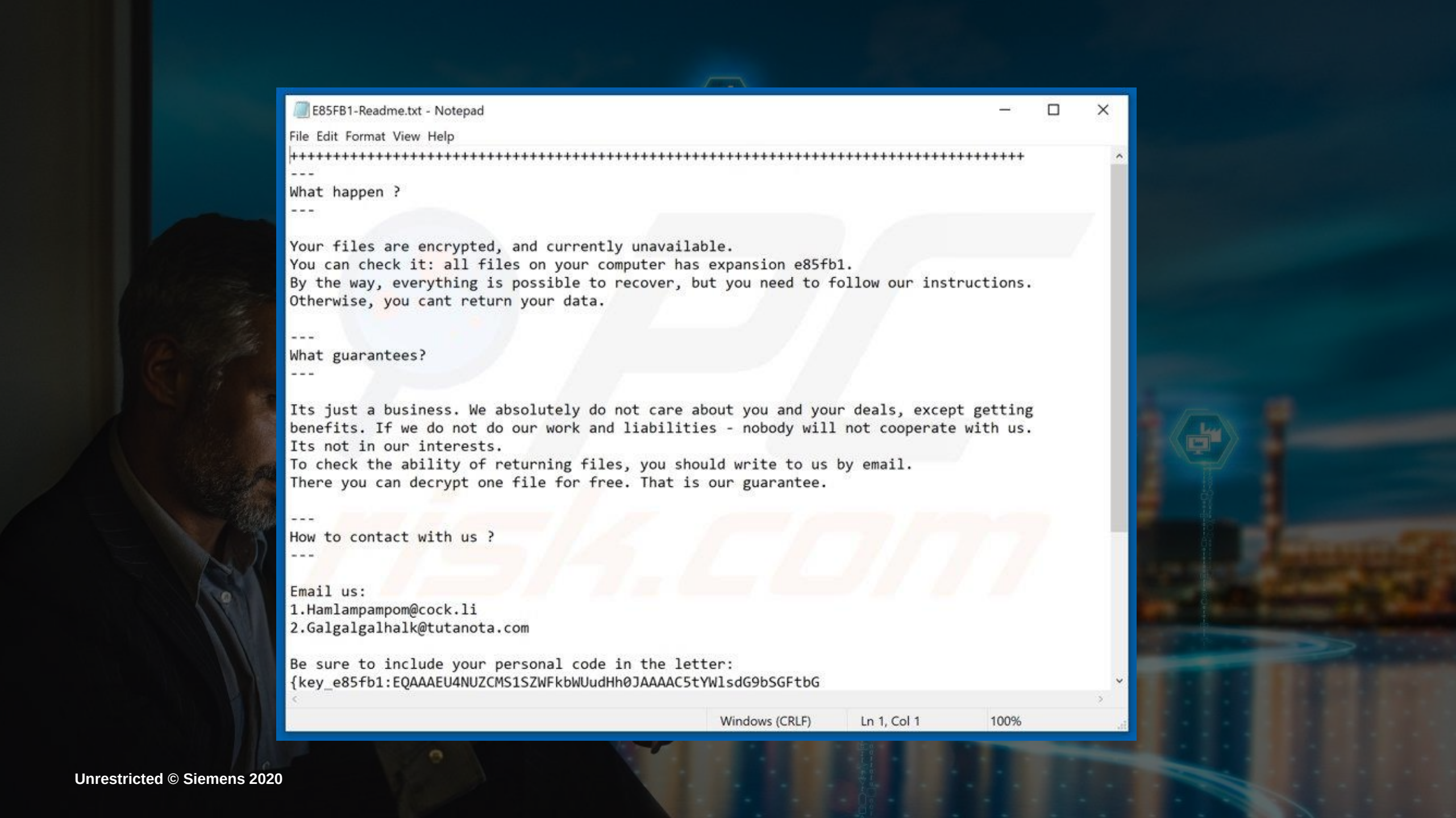
Where:
Toll HQ, Melbourne - Australia

When:
31 January, 2020 (when they became aware)

How**:**
Mailto Ransomware (encrypted file systems)



Outcome:
Hackers demanded AUD $8.5 million in exchange to decrypt of 5GB of data.
(it's believed that Toll decided not to pay the ransom and restore systems)



Update: Toll Group attacked again with ransomware in May 2020.

Hacked again: **Toll Group** systems hit by fresh ransomware ...
The Australian Financial Review - 4 May 2020
But this second attack against **Toll**, which is such a crucial component of Australia's **logistics**, is beyond criminal." Head of the **cyber security** ...

Toll Group suffers second ransomware **attack** this year
iTnews - 4 May 2020

News / **Toll Group** resists ransom demands from hackers after ...
theloadstar.com - 12 May 2020
However internal sources do point to a **cyber attack**." Mr Jensen added that, following a webinar on **cyber security**, he came away with "the clear ...

Toll Group's corporate data stolen by attackers
iTnews - 11 May 2020

Toll Group may have lost over 200GB of data in ransomware ...
iTnews - 14 hours ago
"**Toll Group** failed to secure their network even after the first **attack**. ... Given the **attacks** on Toll have been by two different ransomware groups ...

Toll Group Data Leaked Following Second Ransomware ...
BankInfoSecurity.com (blog) - 10 hours ago

Toll customer data stolen in its second **cyber attack** of 2020
Inside Retail - 12 May 2020
Toll Group managing director Thomas Knudsen said the **attack** was unscrupulous, and that the business is working with the Australian **Cyber** ...

Toll Group reveals stolen data may show up on dark web
CRN Australia - 12 May 2020

Top 5 Vulnerabilities, Risks and Exposures for Digital Industry

SIEMENS
Ingenuity for life

1. Industrial Control Systems (ICS) software applications and operating systems are outdated and vulnerable to CVEs.
2. Industrial networks are ineffectively segregated.
3. Poor system and operating system hardening and patch management.
4. Weak physical and logical access control.
5. Insufficient logging and monitoring of mission-critical systems.

The advanced persistent threats targeting industry are emerging and evolving.

Industrial Cybersecurity as a top priority for today and tomorrow

SIEMENS
Ingenuity for life

Security by Default

- Architect and design security from the start
- Security-measures are implemented by default

Secure Access

- All functions require Authentication and Authorisation
- Least-Privilege security principles
- 2-Factor Authentication (2FA)

Central Administration

- Transparency on configured Security settings
- Ease of Administration to maintain Protection-Level over the plant lifecyle

Security by Design

- Communication security based on certificates
- IEC 62443-conform development process

Defense in Depth

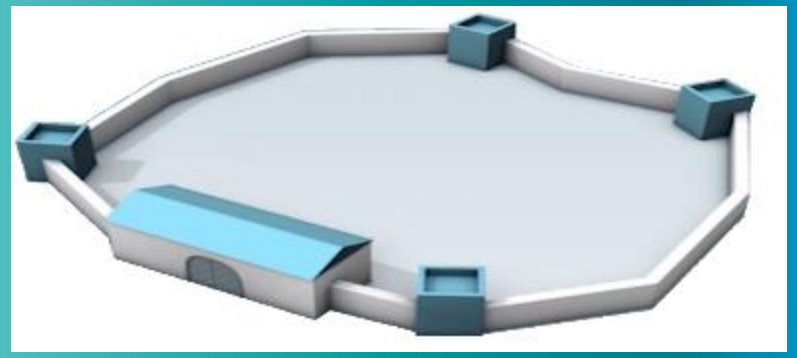
- Firewalls, Network Devices, Virus Scanners, Application Whitelisting, Intrusion Detection/Prevention.

Evolution of Cybersecurity Frameworks

SIEMENS
Ingenuity for life

Security measures in the past

- Simple protection systems
- One gate / single access point
- Simple overcoming of security measures possible



Defense in Depth security measures

- Deep graded security architecture / protection systems
- Several different security measures
- Difficult access for an attacker
- An attacker has to invest a lot of efforts and time against each measure adopted

Defense-in-Depth
Security Architecture based on IEC-62443

SIEMENS
Ingenuity for life

Defense in Depth

Security threats demand action

Plant Security
- Physical access protection
- Processes and guidelines
- Holistic security monitoring

Network Security
- Cell protection and perimeter network
- Firewalls and VPN

System Integrity
- System hardening
- Patch management
- Detection of attacks
- Authentication and access protection

Industrial Cybersecurity
Essential for secure industrial automation

SIEMENS
Ingenuity for life

Information technologies are used in industrial automation

Horizontal and vertical integration

- **Open standards**
- **PC-based systems**

Increased security threats demand action

Loss of intellectual property, trade secrets, recipes …

Plant standstill, e.g. due to viruses or malware

Sabotage in the production plant

Manipulation of data or application software

Unauthorised use of system functions

Compliance with standards and regulations is required

Industrial Cybersecurity
Essential for secure industrial automation

SIEMENS
Ingenuity for life

Communication

Encryption and monitoring of the communication

Access

Access control for networks and automation systems

Integrity

Protection of transmitted and stored data against unwanted changes

Identification

Authentication and Authorisation of devices and users

Basis for a continuous, reliable operation of production plants

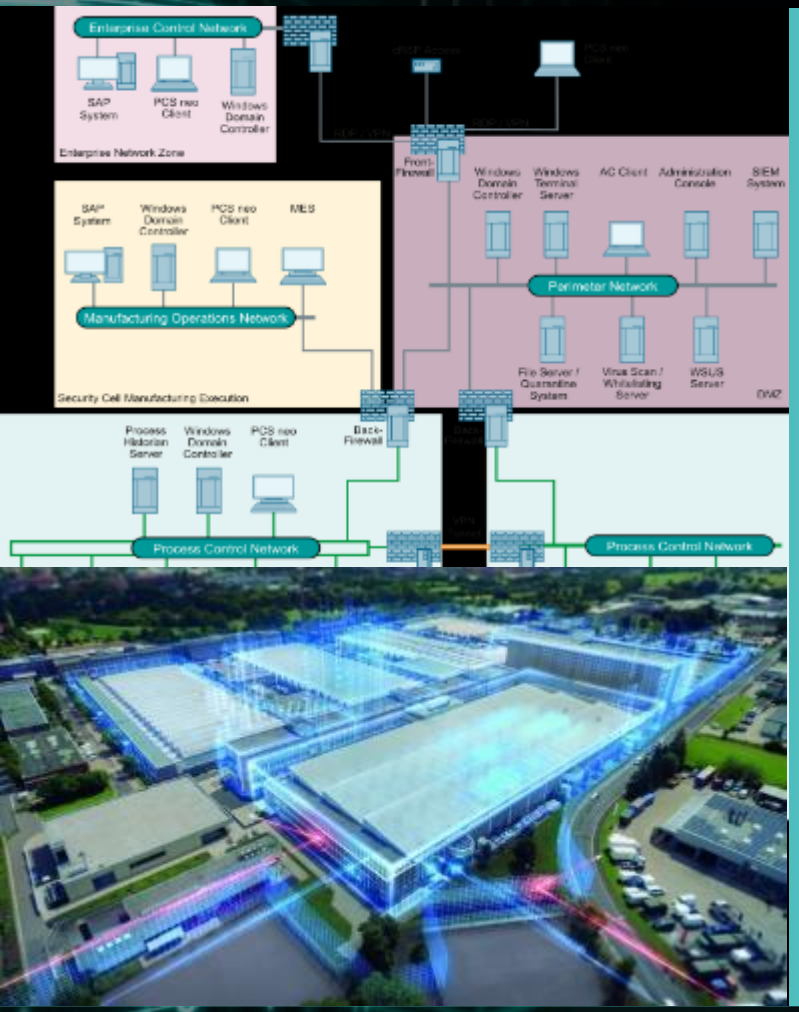
High Availability: Avoiding disturbances caused by attacks

Integrity: Reduction of malfunctions, production errors and downtimes

Confidentiality: Protection of confidential data, information and intellectual property

Network Security
Network Cells, Firewalls and VPN

SIEMENS
Ingenuity for life



Logical Segregation in network cells

- Architect ICS assets to operate in separated network cells via network segmentation.

Multiple firewall layers

- Front firewall to control and restrict the data exchange with the office (IT) enterprise network and the production (OT) network.
- Perimeter network (DMZ) to allow service and support access to the plant with controlled and restricted data exchange with the process control network.
- On every host Operating System (e.g. Windows) install or implement a firewall to protect critical ICS application services.

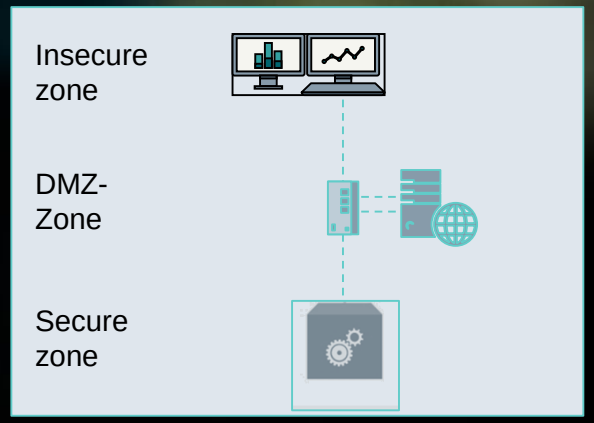
Network Security – Use Cases

SIEMENS
Ingenuity for life

DMZ

Increased protection through data exchange via DMZ by preventing direct access to the automation network

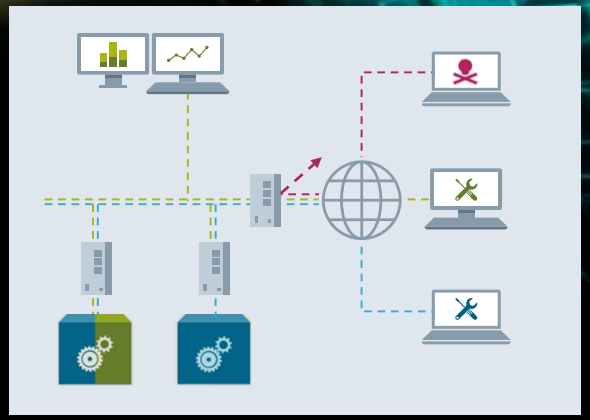
A firewall controls all data traffic between the different networks and DMZ



Remote access

Secured remote access via the Internet or mobile networks preventing espionage and sabotage

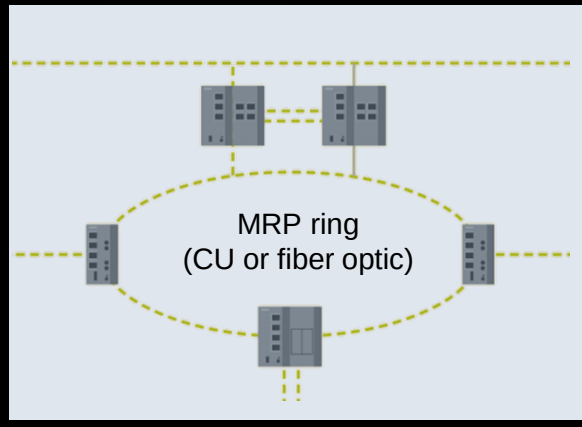
Encryption of data transmission and access control via security modules or Internet - and mobile wireless routers



Secure redundancy

Higher reliability and availability, and securing of redundant network structures

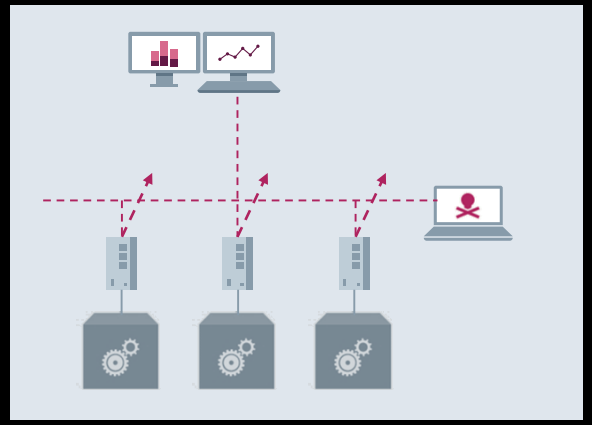
Security modules in synchronized standby mode and integrated in redundant rings



Cell protection

Devices without own network security functionality can be protected within the automation cells

Access to cell is secured by firewall mechanisms



Siemens Vision 2020+

SIEMENS
Ingenuity for life

Operating Companies

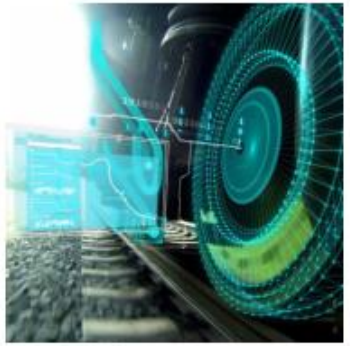
Gas and Power*

Smart Infrastructure

Digital Industries

Strategic Companies

Siemens Mobility

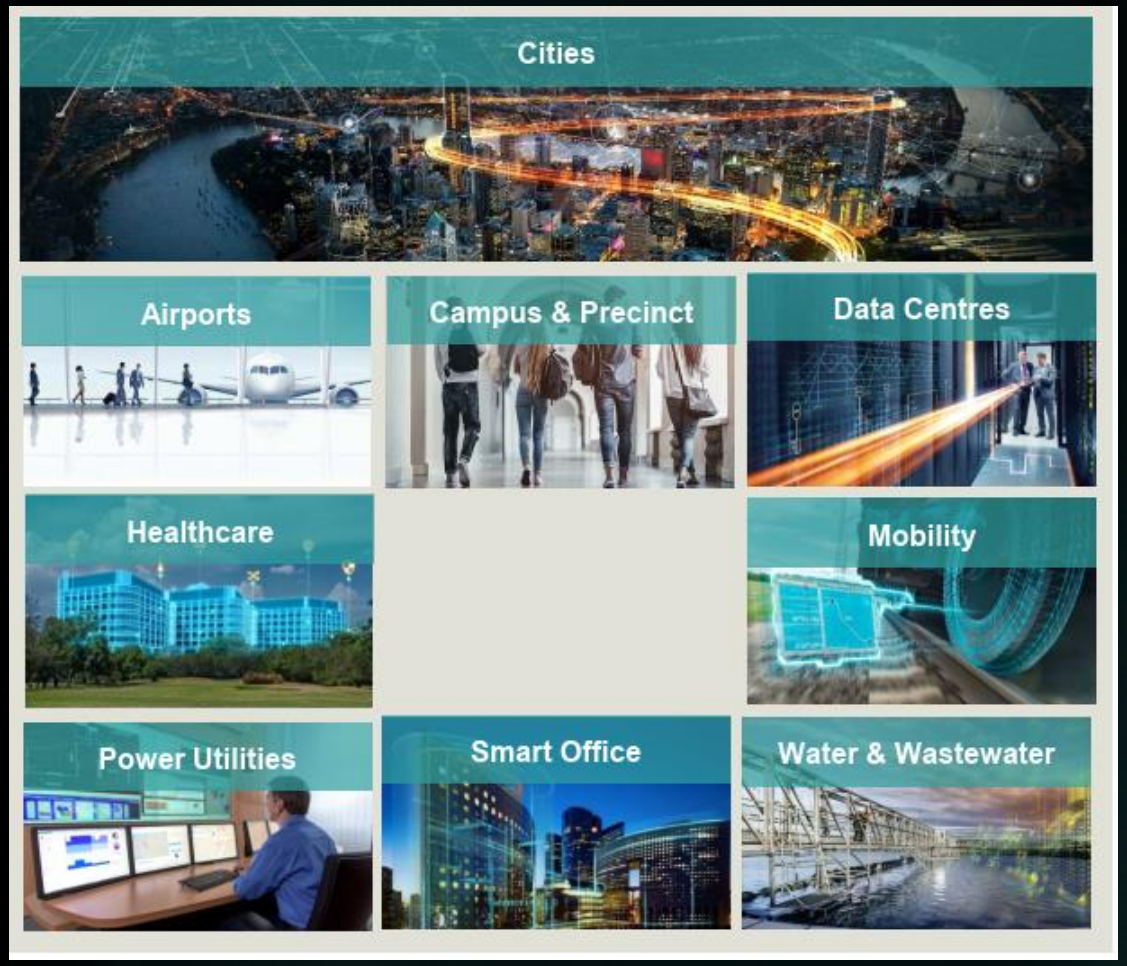


SIEMENS Gamesa* RENEWABLE ENERGY

SIEMENS Healthineers

Siemens Australia – Key Vertical Market Segments

SIEMENS
Ingenuity for life



Siemens Australia – Operating Regions

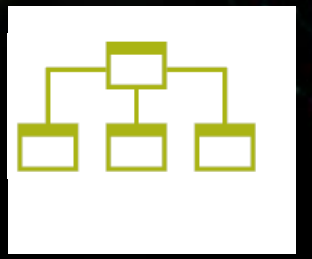
SIEMENS
Ingenuity for life

Siemens Industrial Security Services (ISS)
Concepts, Products, Services

SIEMENS
Ingenuity for life

Authentication and User Management

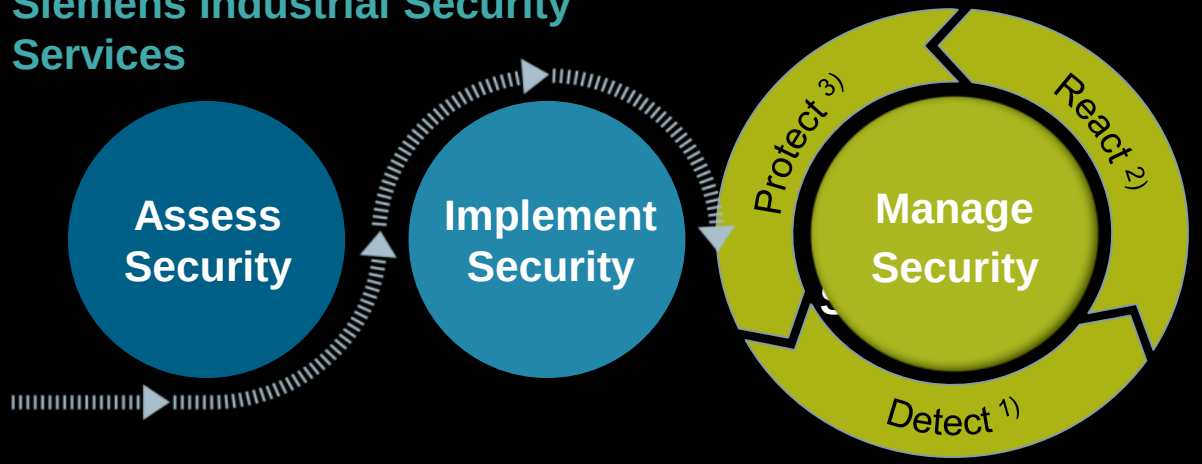
Access – know how & copy protection



Firewalls IDS/IPS VPN

System hardening & continuous monitoring

Siemens Industrial Security Services



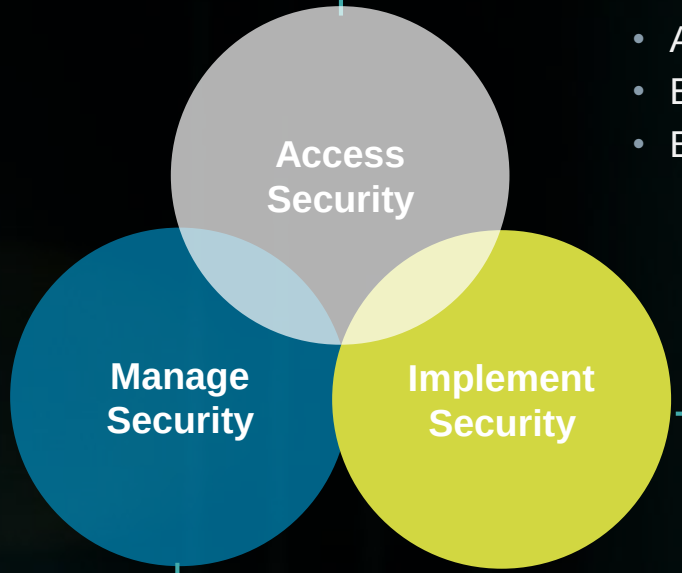
[1] z.B. Industrial Security Monitoring; [2] z.B. Incident Response; [3] z.B. Patch Management

Siemens Industrial Security Services Portfolio

SIEMENS
Ingenuity for life

Evaluation of current Security Status

- Analysis of threats and vulnerabilities to identify, evaluate and classify risks.
- Assessment of business and operational impacts.
- Execution from process engineering and automation view.
- Basis for the establishment of a security program.



Comprehensive security through monitoring and pro-active protection

- Close security gaps with continuous updates and backups.
- Identify and handle security incidents thanks to continuous security monitoring.
- Early adaption to changing threat scenarios.

Risk mitigation through implementation of security measures

- Design and implement technical security measures.
- Develop and deploy security relevant processes.
- Enhance security awareness with specific training.

Charter of Trust

SIEMENS
Ingenuity for life

In February 2018, Siemens teamed up with the Munich Security Conference (MSC) and six other governmental and business partners to create the Charter of Trust.

The Charter of Trust contains ten principles that should make the digital world more secure and also sets three important goals:

- Protect the data of individuals and companies
- Prevent damage to people, companies and infrastructures
- Create a reliable foundation for instilling trust in a networked, digital world.

The Charter's aims is to set minimum general standards for cybersecurity that are in alignment with the requirements of state-of-the-art technology.

Siemens RUGGEDCOM

SIEMENS
Ingenuity for life

The Siemens RUGGEDCOM family of modular Layer 2 and Layer 3 switches, and intelligent IoT nodes offers WAN, serial or Ethernet connectivity options with embedded security.

RUGGEDCOM RX1500

Field-proven industrial network devices coupled with security applications to offer customized solutions for various security levels. Field-swappable modules for flexibility and easy maintenance for critical applications.

RUGGEDCOM APE

Industrial Application Processing Engine provides a powerful industrial application platform that lets you tap into a range of Siemens and leading 3rd party security applications in mission-critical environments.

RUGGEDCOM RX1400 IN

Industrial Intelligent Node (IoT) with advanced security features including ML user passwords, SSH/SSL (128-bit encryption), port security, firewall & IDS, VLAN (802.1Q), RADIUS, SNMPv3 and 56-bit encryption.

Siemens SCALANCE S

SIEMENS
Ingenuity for life

The Siemens SCALANCE S Industrial Security Appliances as a part of network security support the “Defense in Depth” industrial security concept. They protect automation networks, and seamlessly connect to the security structures of the Office and IT world.

Industrial Firewall Appliances

High-performance Industrial Firewall Appliances offer you versatile firewall mechanisms you can use to protect even flat networks with a throughput of 600 Mbit/s and up to 1,000 firewall rules.

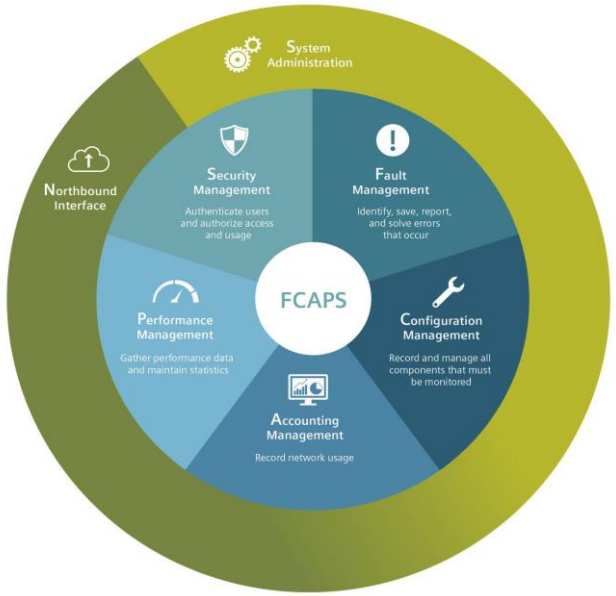
Industrial VPN Appliances

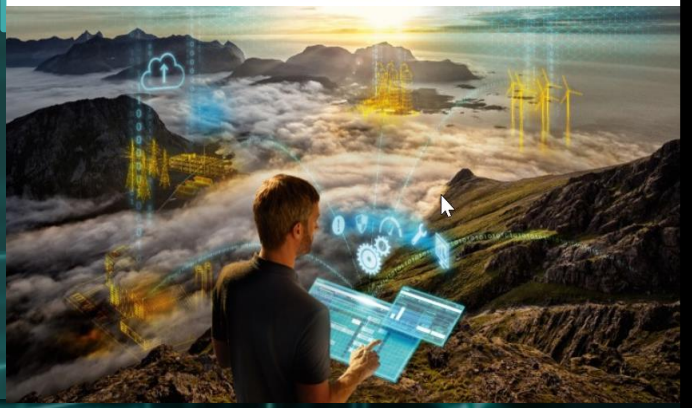
In addition to the firewall mechanisms offered by the Industrial Firewall Appliances, powerful Industrial VPN Appliances also permit up to 200 VPN connections with a data throughput of up to 120 Mbit/s.

SCALANCE S is developed in accordance with the provisions of the Industrial Security Standard IEC 62443-4-1, as certified by the TÜV. These provide for the implementation of a flexible security zone concept and be used in a temperature range of -40 to +70c.

Siemens SINEC NMS

SIEMENS
Ingenuity for life





The Siemens SINEC NMS is the all-around Network Management System (NMS) for industrial networks. SINEC NMS supports the five pillars defined in the FCAPS model.

Fault Management
Identify, save, report, and solve any error status that occur.

Configuration Management
Record and manage all OT network components that must be monitored.

Accounting Management
Record network usage.

Performance Management
Gather performance data and maintain statistics.

Security Management
Authenticate users and authorize access and usage.

SINEC NMS fulfills process-based and technical security requirements according to IEC 62443 framework.

Siemens Industrial Security Information

SIEMENS
Ingenuity for life

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit **http://www.siemens.com/industrialsecurity**.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under **http://www.siemens.com/industrialsecurity**.


SIEMENS
Ingenuity for life

Disclaimer

SIEMENS
Ingenuity for life

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.