SolidRun
Embedded Edge Computing

Whitepaper

DIGITAL TRANSFORMATION IN CRITICAL INFRASTRUCTURE NETWORKS

CRITICAL INFRASTRUCTURE CONCEPT

Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.

Critical Infrastructures include various private and public sectors like energy, power grid, water, as well as health and public transportation just to name a few. Each country has its own definitions as to what sectors are critical in terms of its national infrastructure.

Most of these critical infrastructures have high requirements for the security of digital information and how the information flows within networks. Some governments even impose security guidelines and requirements on the systems like the German BSI.

NATO for example, defines critical infrastructure sectors as Energy, Transport, Water, Public & Legal Order and Safety, Chemical & Nuclear Industry, etc. as shown in Figure 1.

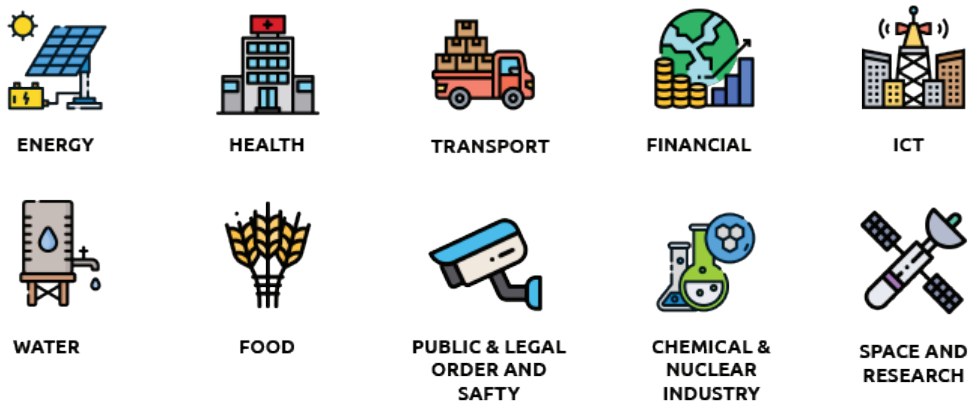

Figure 1: Critical Infrastructure Sectors

Increasing productivity while reducing costs in maintaining and operating system as well as industrial practices, has been the main drive that led to an exponential growth in adoption of the latest smart technologies in the digital transformation of critical infrastructure networks. This integration of increased automation, improved communication and self-monitoring, as well as smart machines that can analyze and diagnose issues without the need for human intervention is what has characterized today's digital transformation.

DIGITAL TRANSFORMATION

To get the most out of the digital transformation, the infrastructure should be designed to support the principles outlined below.

Connectivity: Machines are connected through public or private lines that utilize different technologies like SFP, SHDSL, VDSL, LTE and RJ45.

Security: Critical Systems need a high-security standard to protect against attacks like Denial of Service (DOS) or Distributed Denial of Service (DDOS) as well as hackers.

Maintainability: The systems have the ability to work independently. Management should be fast and centralized as well as continuous updates to maintain a high-security standard.

Protection: Different technologies should be used to protect critical infrastructures like DDOS protection, Intrusion Detection and Protection (IDS/IPS), Firewalls and VPNs.

Digital Transformation – Benefits

The main benefits include:

IMPROVED PRODUCTIVITY AND EFFICIENCY

Digital Transformation enables faster reaction times, while the allocation of resources is done in a more cost-effective and efficient way.

INCREASED DATA SHARING

Machine-to-machine and system-to-system communication, allows data from one entity (like a sensor) to instantly make an improvement across multiple systems located anywhere in the infrastructure without any human intervention.

ENHANCED FLEXIBILITY AND AGILITY

Changes in infrastructure and security risks can be managed faster and more flexible. Maintenance and machine automation can be carried out secure and from remote connections like command centers.

GETTING RETURN ON INVESTMENT (ROI)

Migration to digital networks in critical infrastructures requires investing, so there are upfront costs. However, the cost of maintaining and security will dramatically fall as a result of automation, systems integration, data management, etc.

Digital Transformation – Vulnerabilities

Although the digital transformation of critical infrastructure networks provides clear business advantages, the most challenging aspect of implementing these techniques is the security risk. The operational technologies driving operations until now were relatively isolated or even non digital. The integration / convergence of IT (Information Technology) and OT (Operational Technology), which is essential for the digital transformation, resulted among others, in Machine systems and Industrial Control Systems (ICSs) being exposed to the majority of cyber-attacks.

Industrial Control System (ICS) is a general term that includes supervisory control & data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations like programmable logic controllers (PLC). ICSs can be found in manufacturing, processing facilities and critical infrastructures, such as nuclear and thermal plants, water treatment facilities, power generation, heavy industries, smart cities and distribution systems. This makes them very attractive targets for attackers, who are often motivated by financial gain, political cause, or even a military objective. Attacks may be state-sponsored, or they could also come from competitors, insiders with a malicious goal, and even hackers. Most ICS devices are inherently less secure against advanced attacks due to vulnerabilities in hardware, operating systems and ICS applications as well as in the ICS networks.

However, all devices are subject to cyber threats. Researchers at cybersecurity company Trend Micro and experts at the Milan Polytechnic University examined how hackers can exploit security flaws in IIoT equipment to break into networks as a gateway for deploying malware, conducting espionage or even sabotage. Also, the JSOF research lab has discovered a series of zero-day vulnerabilities in a widely used low-level TCP/IP software library developed by Track, Inc. The 19 vulnerabilities, given the name 'Ripple20' (https://www.jsof-tech.com/ripple20/), affect hundreds of millions of devices (or more) and include multiple remote code execution vulnerabilities.

The risks inherent in this situation are high. Just a few examples: data could be stolen off of a printer, an infusion pump behavior changed, or industrial control devices could be made to malfunction. An attacker could hide malicious code within embedded devices for years. One of the vulnerabilities could enable entry from outside into the network boundaries; and this is only a small taste of the potential risks. Such findings have become one of the main reasons, which hold digital transformation in critical infrastructures initiatives back.

CYBER SECURITY RISK MITIGATION

The backend systems of Critical Infrastructure Networks are responsible for routing various types of data between devices and applications. One way to mitigate the risk of cyber-attacks that may cause significant damage is by designing a simple, smart and expandable network infrastructure. A typical network functions in a decentralized and distributed way. It consists of separate backend networks that are linked to the public internet. Each backend network requires gateways to bridge between specific wireline and wireless protocols and the Internet.

These gateways have to forward packets to the Internet as well as carry out routing and processing before data can be delivered to an application. In addition, next-generation routers should be used as gateways. These routers are suitable for industrial environment and provide both, high flexibility in network design due to various interface types and protection against cyber-attacks by incorporated firewall software. Since Critical Infrastructure networks are normally not operated by communication experts or IT teams, the routers should be easy to configure and simple to operate and maintain.

INTRODUCING THE ADVANCED INDUSTRIAL ROUTER VT AIR 300

Voleatech GmbH, a German leading provider of advanced networking technology (https://www.voleatech.de/), has launched in October 2019 the VT AIR 300 (https://www.voleatech.de/en/product/vtair300/) – an innovative next-generation, compact, robust and flexible industrial router shown in Figure 2.

Figure 2: VT AIR 300

VT AIR 300 was specially developed for a demanding industrial environment and its requirements. Due to its modern technology (SHDSL, VDSL, LTE, SFP, RJ45) and its numerous innovative solutions, the VT AIR 300 is the next generation of industrial routers based on the most advanced ClearFog GT-8K family from SolidRun Ltd. (https://www.solid-run.com/), a global leading developer of IIoT and networking embedded systems, and the feature rich VT AIR state-of-the-art firewall software from Voleatech.

The VT AIR 300 is tailor-made for critical infrastructures and complex industrial environments that have to be renewed or even completely repositioned due to the digital change. In network technology, the intelligent router marks the logical step into the digital age of Critical Infrastructures and 5G technology – thus the beginning of modern network technology.

The VT AIR 300 offers the following major advantages:

Modular hardware: Various types of optional physical interfaces and features to match the exact needs of customers and implementations. The modular structure also allows to change the device configuration after deployment.

Security Always up to date: Thanks to modular software structure, different components of the system can be modified individually, and security gaps can be updated immediately! Tools like Firewall, DDOS Protection and Deep Package Inspection IDS/IPS can be deployed to secure the infrastructure. VPNs can be deployed to encrypt traffic on public lines (IPSec, OpenVPN, Wireguard).

VT AIR Software: A Feature rich firewall Linux-based system that includes a modern, user-friendly, easy-to-understand and dynamic web interface in multiple languages allowing users to carry out all settings easily and conveniently. A central management system can be used to easily configure a magnitude of VT AIR devices.

The VT AIR 300 is already successfully deployed by energy companies in Germany to secure and manage highly critical network infrastructures.

USE CASES

The following subsections include descriptions of a few use cases.

PUBLIC AND PRIVATE UTILITIES (FIGURE 3)

VT AIR – DSL and VPN for fast and secure networks:

Critical infrastructures require modern as well as innovative network technologies in order to be up to date within the context of the digital transformation and meet the increasing security requirements. The VT AIR 300 not only offers SHDSL, VDSL, SFP and LTE, but also provides high level encryption technology. The innovative firewall technology can also be retrofitted at any time and, thanks to over-the-air updates, is always up to date with the latest security standards.

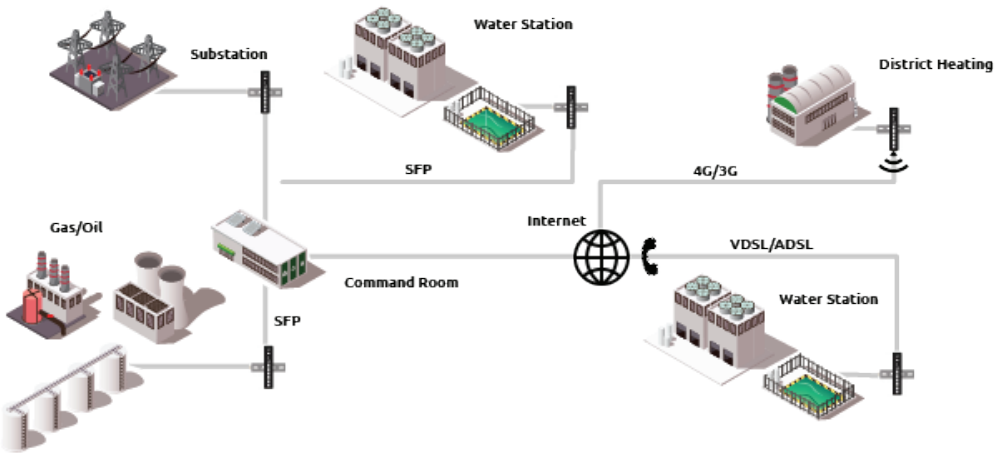

Figure 3: Energy Supplier and Public Utility Implementation

WIND ENERGY SUPPLIER (FIGURE 4)

VT AIR – modular and retrofittable for the highest requirements:

Wind energy is an important part of the renewable energy transition that is developing steadily and quickly. Particularly in such an environment, it is important to use innovative network technologies that not only meet the highest security requirements but also have a modular structure and can be retrofitted at any time. This is guaranteed with the VT AIR 300. Thanks to the modular software structure, individual components can be updated, and any security vulnerabilities closed immediately. The Docker applications also allow you to use your own applications and control software.

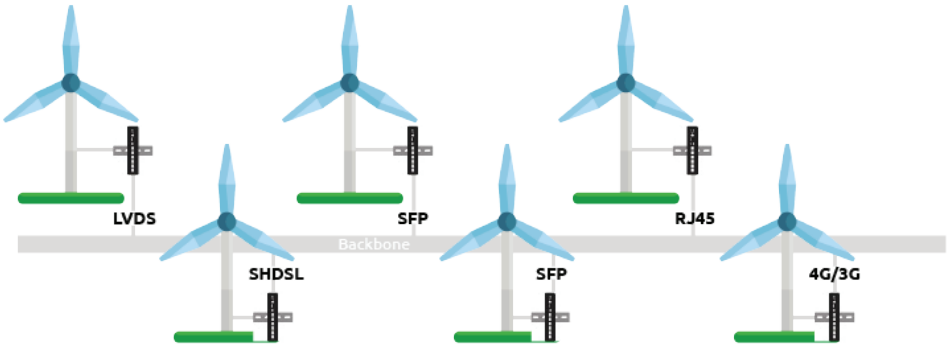

Figure 4: Wind Energy Supplier

SMART CITY (FIGURE 5)

VT AIR – modern encryption algorithms for better security:

Cities keep changing their characteristics. Many cities will transform themselves into smart cities in the coming years and will therefore be completely networked. As a result, operators will be dependent on the most modern network technology, if they want to secure the associated and presumably rapidly increasing data transfers. VT AIR stands for high encryption, security and offers hardware that can be used in complex environments with high temperatures and consequently forms the backend of modern cities.

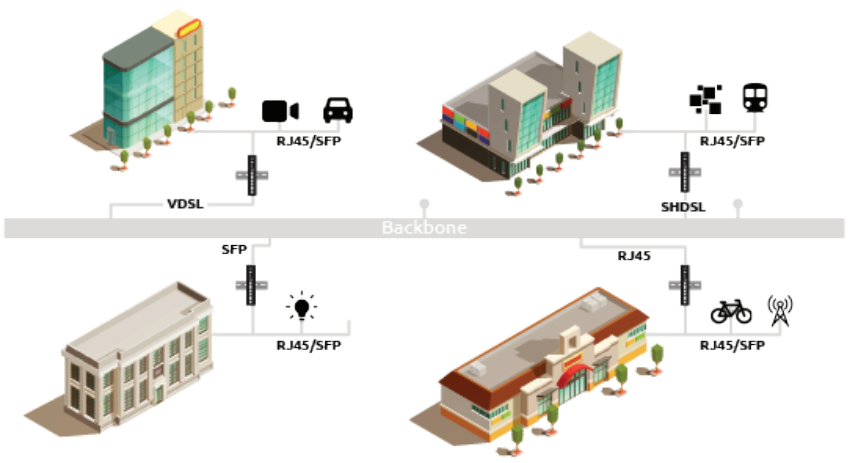

Figure 5: Smart City Implementation

SUMMARY

Critical infrastructures such as Energy, Transport, Water, Public & Legal Order and Safety, Chemical & Nuclear Industry, etc., are of vital importance to society and economy and their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences. Increasing productivity while reducing costs in maintaining and operating system as well as industrial practices led to an exponential growth in the adoption of the latest smart

technologies in the digital transformation of critical infrastructure networks. Along with the clear business advantages, the most challenging aspect of implementing these techniques is the security risk, due to IT and OT integration in the industrial control systems. As a result, the critical infrastructures, including all 'smart' devices, are exposed to cyber-attacks.

The risk of cyber-attacks can be mitigated by simple, smart and expandable network infrastructures based on next-generation routing gateways that are suitable for industrial environment and provide both, high flexibility in network design due to various interface types and protection against cyber-attacks by incorporated firewall software. Voleatech's recently launched VT AIR 300 Advanced Industrial Router based on SolidRun's most advanced ClearFog GT□8K family, is tailor-made for critical infrastructures and complex industrial environments. Its modular hardware and feature-rich always up to date firewall software make it the ideal building block in public and private utilities requiring DSL and VPN for fast and secure networks, wind energy suppliers requiring modular and retrofittable systems, smart cities that need modern encryption algorithms for better security and more.

Learn more about SolidRun's networking products offering:

Marvell based OCTEON CN913x Family

NXP based Layerscape LX2160A family

ABOUT VOLEATECH GMBH

Voleatech has evolved from a classic startup to a leading provider of advanced networking technology. The philosophy of the developers is clearly defined: For the engineers of Voleatech GmbH, the focus is on the customers. This is expressed in two principles: on the one hand, technology has to be innovative, on the other hand it has to be intelligent and intuitive – only then will the customer have the maximum benefit. Voleatech therefore invests specifically in innovative future technologies.

https://www.voleatech.de/

VOLEATECH
NETWORKING LINUX COMPANY