


ICS White Paper

Cyber Security for Industry 4.0 Era.

Making Industrial IoT (IIoT) end-devices safe & secure from malicious network based attacks



A Technical Report from Terafence Research Lab

Contents

INTRODUCTION 3

ICS THREAT ANALYSIS..... 4

EXAMPLE-1: SMART BUILDING REFERENCE ARCHITECTURE 6

 TERAFENCE MICRO-SEGMENTATION CONCEPT:7

EXAMPLE-2: INDUSTRY 4.0 IMPLEMENTATION..... 8

 THREAT ANALYSIS:8

SECURITY– FIREWALL VS. TERA FENCE 9

SYSLOG STUDY CASE: 10

TERAFENCE MBSECURE+ TECHNICAL INFO:..... 11

Introduction

Terafence Ltd. Is focused on providing Cyber Security to IoT and IIoT end-devices.

We consider IoT devices as a potential security threat as most of IoT/IIoT devices do not have any security built into them, currently. Estimated number of IoT devices in service today is around 20 Billion, if none are truly secure, it is only a matter of time before hackers find how to exploit these devices.

“A chain is as strong as its weakest link” (idiom by Thomas Reid’s “Essays on the Intellectual Powers of Man”, 1868). At Terafence we believe that unsecured end-devices pose a real security threat in networked environments.

At Terafence, we witnessed the DDoS attack on DNS servers in 2015 in the USA and set out to provide a secure solution that will deny attempts to gain control over unsecured end-devices such as CCTV cameras and Industrial Programmable Logic Controllers (PLC).

Terafence is now introducing an innovative, secure, bullet-proof and cost-effective solution that denies access by hardware while maintaining end-device functionality unhindered.

Terafence core technology allows full control over Data Flow through the solution offering near Air-Gap segmentation between networks at the hardware level. No signals go across. At the same time, we maintain the functionality of the end-device without allowing access.

The accelerated growth of IoT/NoT (Network of Things) applications and devices brings new dimensions of risk and vulnerability from cyber-attack and hackers, especially in critical areas such as medical, industrial infrastructure and transportation. Unprotected IoT/NoT systems may lead to substantial economic damage, injury and even loss of life.

Terafence suggests that one measure of security for such devices is by ISOLATION and SEGMENTATION, simply remove these devices from the reach of attackers, by hardware, at the lowest possible (OSI) layer as possible without degrading their functionality or performance.

This paper reviews common approaches to IIoT cyber security and will highlight the importance, advantages and ease of SEGMENTATION using Terafence technologies.

ICS Threat Analysis

Programmable Logic Controllers (PLC) often cost little compared to the potential damage caused if misused, either maliciously or by simple human error. A 150\$ controller may cause \$10M damage to a power generator in a power plant, for example. Ransom attacks are common today and we can only expect the trend to strengthen. One can assume that someday someone will take control over PLC/HMI system and demand ransom to free them. If a PLC is controlling HVAC, it could be easy to turn everything down and change username/ passwords so rightful owners may no longer have accesses to the system.

It is commonly accepted that only 20% of attacks come from the outside (Internet) and 80% come from internal sources. One can have the state of the art network IDS/IPS/FireWall but an infected USB-Disk-on-Key inserted on the HMI server bypassing everything and possibly infecting the entire network or worse, allowing external control over the HMI and the PLC process. A laptop that traveled outside the network may have picked up malicious code on someone else's network, on an open WiFi link in a café, on the train or at the Airport.

Security needs to address such threats and essential assets should be secured from internal and external threats.

Industry 4.0 is calling for uploading as much as possible data to the Cloud for analysis. This calls for proper Internet connection and greatly increases the network exposure to external attacks and may require connecting the TO network to the internet directly or merge with the IT network...

As technology advances, more and more control become essential as it drives productivity and eventually profit, and everything needs to be connected, monitored, controlled and processes must be continuously updated. Connecting everything together becomes critical and the classical IO/OT boundaries can need to be removed to allow constant data flow between services, servers and the Cloud.

Evidently, this opens multiple opportunities for malicious attacks on the organization, production process and end-devices in use slowing down adoption on Industry 4.0 until IT/OT convergence can be done in a secure and safe manner.

Recent events, shown in the table, are a clear evidence that attacks may come from various sources and utilize different methods to create havoc, damage and possibly threaten human health and life.

| Date | Target | Method |
|------|---|-----------------------|
| 2000 | Australian Sewage Plant | Insider |
| 2010 | Iran Uranium Enrichment | Stuxnet |
| 2013 | ICS Supply Chain attack | Havex |
| 2014 | German Steel Mill | |
| 2015 | Ukraine Power Grid | BlackEnergy, KillDisk |
| 2016 | Ukraine Substation | CrashOverride |
| 2017 | Global shipping company | NotPetya |
| 2017 | IoT DDos attack | BrickerBot |
| 2017 | Health care, Automotive, many others | WannaCry |
| 2017 | Saudi Arabia Petrochemical | TRITON/TRISIS |
| 2019 | Norwegian Aluminum Company | LockerGaga |

Source: www.awa.csis.org/programs/technology-policy-program/significant-cyber-incidents

Example-1: Smart Building Reference Architecture

Devices in a smart building network need to communicate to share information about their status and to send commands to each other. For instance, a sensor reads the temperature of a room and provides it to a controller, which decides to switch a fan on or off, according to a setpoint configured by a management workstation.

These devices are typically grouped into subsystems according to their functionalities. For example, smoke detectors are part of the fire alarm system, whereas badge readers are part of the access control system. Ideally, these subsystem networks should be segregated from each other, and especially from the IT network, although that is rarely the case in practice, as confirmed by our daily experience with securing production networks. Sometimes different subsystems are configured in different VLANs for network segmentation, but misconfigurations allowing cross-VLAN communication (VLAN hopping) are common.

The architecture of a typical smart building network is shown in Figure 1, where systems including Video Surveillance, Access Control, IoT, HVAC, and Smart Lighting are connected. Besides residential and commercial buildings, the reference architecture shown in Figure 1 can also represent the networks found in critical or sensitive facilities such as hospitals, factories, airports, stadiums, schools, data centers, and many other types of buildings with a large number of occupants.

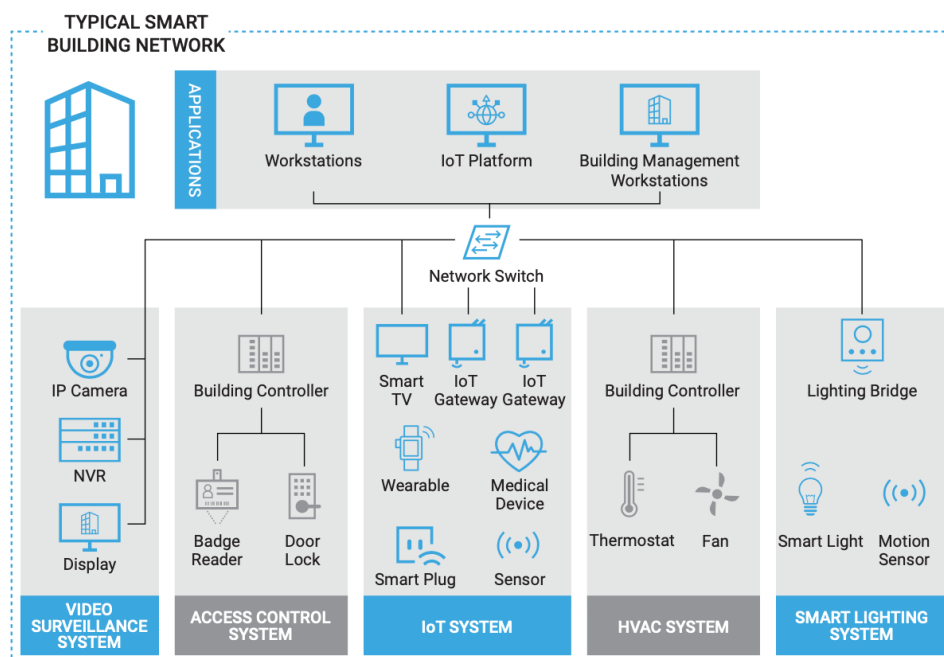
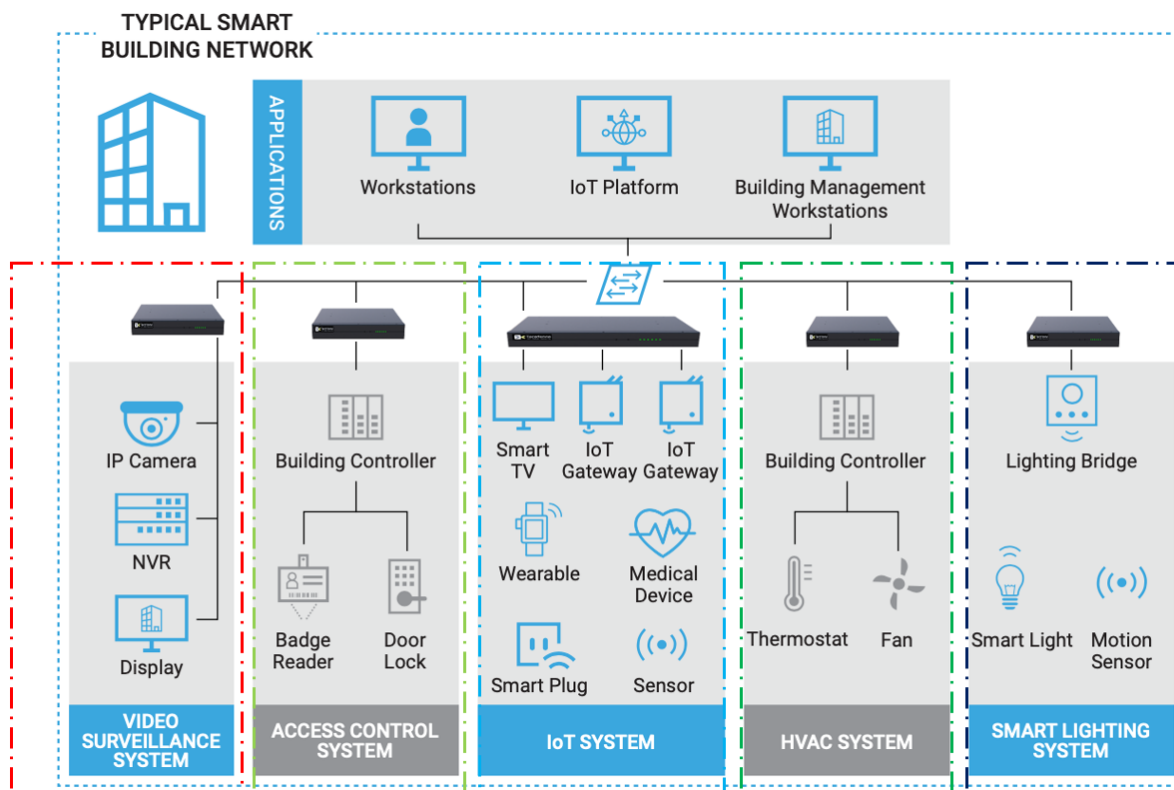


Figure 1 - Building automation network with IoT devices

The OT devices in the different subsystems use either proprietary or standard domain-specific protocols such as BACnet, DNP3, and RTSP to communicate. More recently, IoT devices like smart lights, smart locks, smart electrical plugs, and other sensors and actuators started being deployed alongside building automation systems using protocols such as Message Queue Telemetry Transport (MQTT) and the Constrained Application Protocol (CoAP) to achieve machine-to-machine (M2M) communication

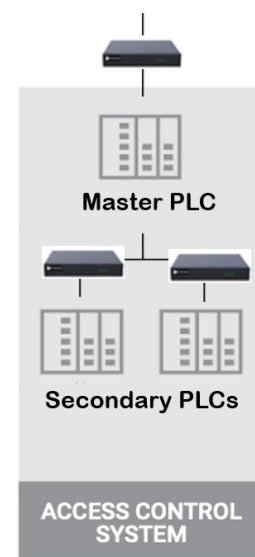
and establish a common message bus (see modern building automation controllers adopting MQTT for data exchange).

Terafence micro-SEGMENTATION concept:



Terafence suggests that each sub-system should be micro-SEGMENTED and physically ISOLATED from other sub-systems in general. This creates micro-segmentation and “Process Islands” of each process. Attacks, of any sort, can not spread between processes and TCP/IP access to the end-devices is prevented.

Further segmentation, where critically required, is also possible by introducing Terafence within each process Island:

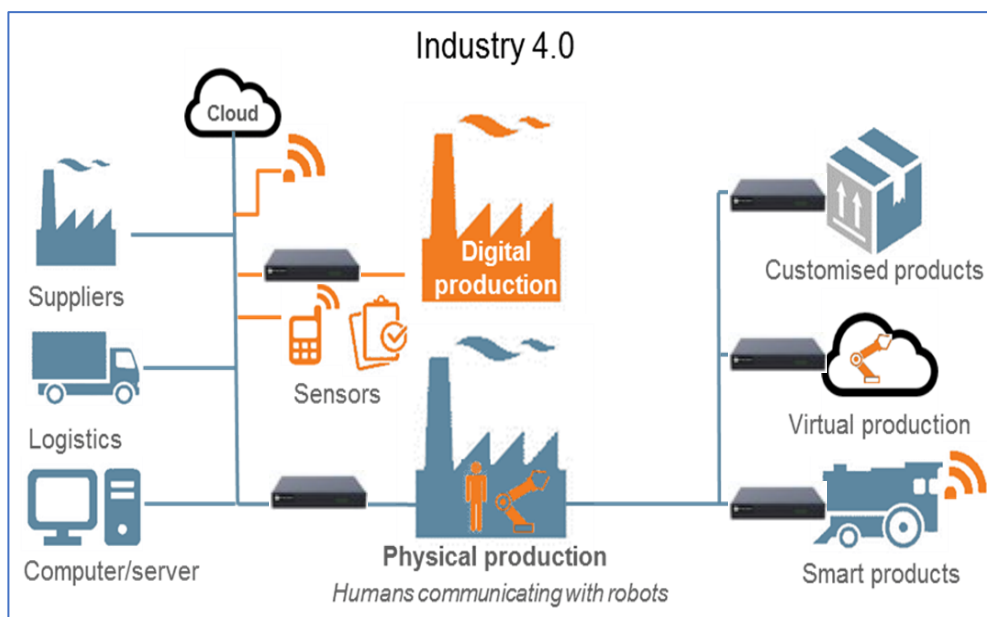


Example-2: Industry 4.0 implementation

The diagram below illustrates the complexity of Industry 4.0 in protecting the industrial environments from Cyber / Network attacks and threats.

Having external entities connected to the network (Firewalled obviously) poses tremendous security burden on IT, OT and Security departments to ensure continuous control and production continuity.

By micro-segmentation, Terafence offers peace of mind to both IT and OT knowing that assets are isolated from attacks and only relevant data flows out from the process to the Cloud or other IT services.



Threat Analysis:

| | Perception layer | Network layer | Service layer | Application layer |
|------------------------------------|--|---|---|---|
| Components | <ul style="list-style-type: none">• Barcodes• RFID tags• RFID reader-writers• Intelligent sensors, GPS• BLE devices | <ul style="list-style-type: none">• Wireless sensor networks (WSNs)• WLAN• Social networks• Cloud network | <ul style="list-style-type: none">• Service management• Database• Service APIs | <ul style="list-style-type: none">• Smart applications and management• Interfaces |
| Security threats & vulnerabilities | <ul style="list-style-type: none">• Unauthorized access• Confidentiality• Availability• Noisy data• Malicious code attacks | <ul style="list-style-type: none">• Denial of Services (DoS)• Routing attack• Transmission threats• Data breach• Network congestion | <ul style="list-style-type: none">• Manipulation• Spoofing• Unauthorized access• Malicious information• DoS attacks | <ul style="list-style-type: none">• Configuration threats• Malicious code (Malware) attacks• Phishing Attacks |

There is no single solution to solve such a complex environment, and it is common knowledge that security is made of layer upon layers. Terafence is offering yet another layer, the only solution acting on OSI Layers 1&2, the physical network layer. One can even say that Terafence is offering the last line of defence, protecting the end-device itself from network-based attacks.

Security– FireWall vs. Terafence

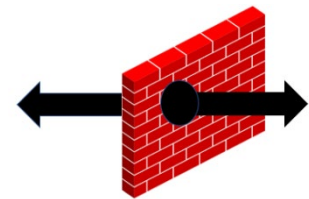
“I can do this with a FireWall...”

Yes, you can configure a FireWall to deny any access from the outside... but:

A firewall is a mainly system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules / keys. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate (with the correct key) communication to flow freely.

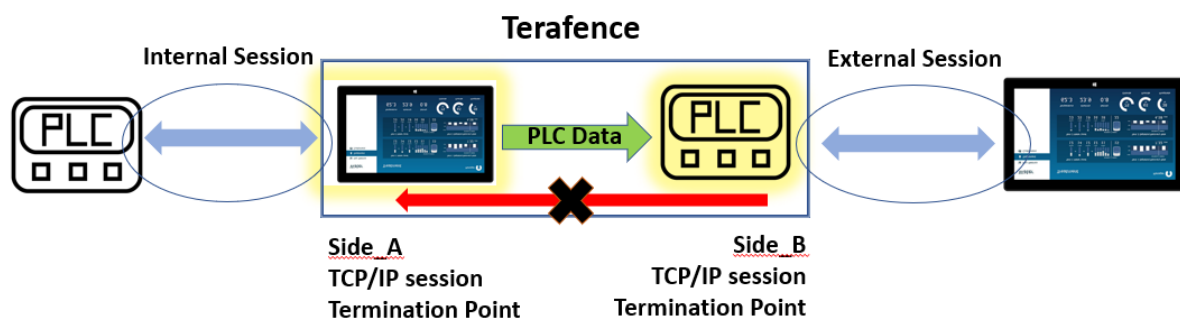


A FireWall will, eventually, ***will*** grant access to an entity that fits the FireWall rule (key) configuration, the problem is that once access is granted, that entity gains full access to the end-device and the FireWall is no longer in effect (unless it's a Layer_7 firewall). In other words, the FireWall will grant a live session between the end-device and the someone. This is exactly what a hacker needs to gain access and manipulate the end-device.



Still, preventing all inbound traffic will make the FireWall “a unidirectional” device but this will prevent the protocol integrity and functionality between the IIoT device and the HMI. These two need to communicate in order to properly work, the HMI sends a POLL/READ command to obtain parameters (as in ModBus), the PLC will reply with the requested information. *Without a mediator, this will not work, and no FireWall will mediate such protocols.*

With Terafence, no entity will ever gain full access to the end-device. Terafence will take an active (Internal Session) role as a mediator between the PLC and HMI, unlike any FireWall.



In special applications, Terafence may allow a heavily filtered commands (only) to be accepted, filtered, disassembled, and coded and then forwarded to the end-device via a secure, out-of-band channel. The actual TCP/IP session will terminate on the Terafence side next to the sending device (External Session). At no time live sessions will become available, thus manipulation avoided.

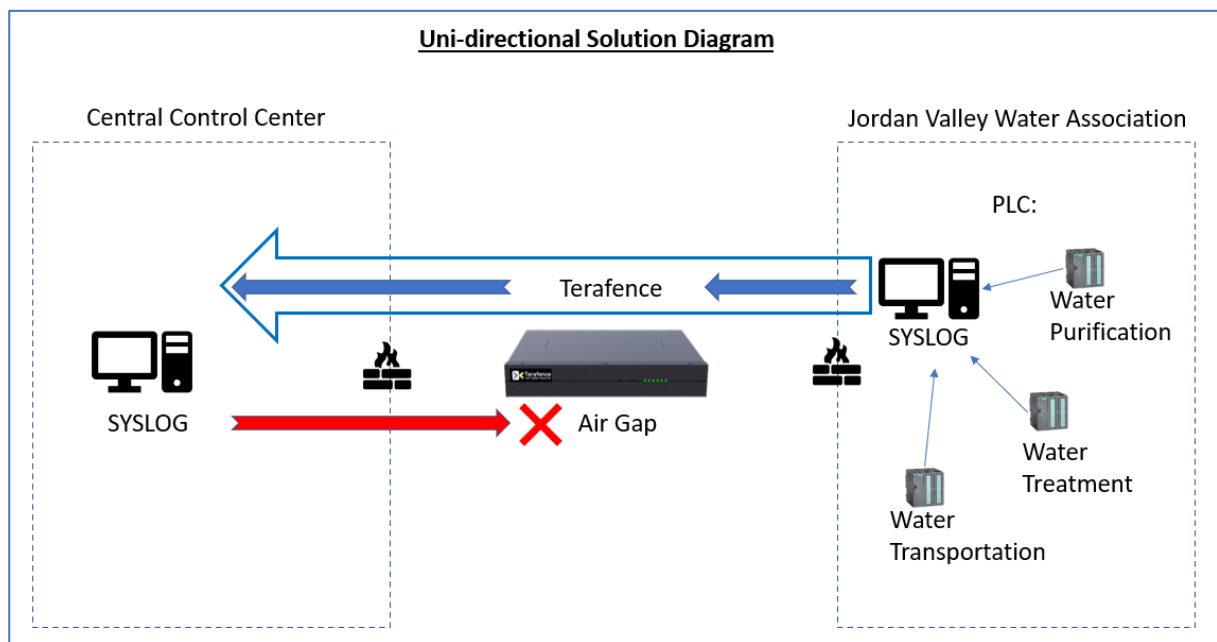
SYSLOG Study Case:

A Water Association needed to create a full-proof barrier between local IT infrastructure and the network from the Governmental Resource Management which continuously collects SYSLOG messages from networked devices and servers regarding functionality and operational status.

Initially, the two networks were connected via 2 firewalls, each at the edge of it's network.

The Water Association requested Terafence to provide a super-strong barrier between the two networks to ensure no leakage of Cyber events happen from either end.

Terafence installed the SYSLOG product and created a total barrier between the two networks. SYSLOG data was actively sent to the original destination as before. No operational impact was observed after the installation.



The solution described above is now evaluated throughout the country between local Water Associations and the Governmental Controlling body.

Terafence MBsecure+ Technical Info:

Basic Features

- Full Modbus RTU support
- Up to 247 MODBUS devices supported per network segment
- OPC DA/UA Support
- Syslog Support
- MQTT Support
- SMTP Support
- DNP3 Support*
- BACnet Support*
- Multiple HMI units support
- Hardware Reset to factory defaults
- High Availability (unit redundancy) *

* Future release

Security Features:

- Physical ISOLATION at OSI Layer-1
- Logical ISOLATION at OSI Layer-2
- Secure unit access (HTTPS) with encryption keys
- Configurable HMI list to provide access restriction

Management:

- Unit configuration via Web based GUI

Hardware Specifications

- Data bandwidth = 1 Gbps
- Power – 5VDC / 8AMP
- No FANs, no disk drives no moving parts
- 2xRJ-45 CAT6 connectors STP/UTP
- Physical ports – 2x1Gbps LAN ports
- Measurements: Wx290 , Hx50 , Dx230 (mm)
- Power consumption: max-40W
- Mounting options:
 - Desktop / 19” Rack Shelf
 - IEC/EN 60715 DIN Rail

Operating System for accompanying CPU's – Linux

Contact information:

Web site : www.terafence.com

Email: info@terafence.com