ICS White Paper

Unbreachable Cyber Security for Oil & Gas Sector

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

Introduction

Terafence Private Limited is an Indian owned entity into R&D and manufacturing of the FPGA based Data Diodes through technology transfer agreement from Terafence Limited Israel. It is focused on providing Cyber Security to IoT and IIoT end-devices.

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.

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 end point cyber security and will highlight the importance, advantages and ease of SEGMENTATION using Terafence technologies in Oil & Gas.

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 or on Oil rigs. 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 critical components of the Oil rigs or onshore critical infrastructure, it could be easy to turn everything down and create large scale damage to revenue, human life and severely hamper the morale of the workforce and hurt the brand image.

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 for 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 pickup 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 Could for analysis. This calls for proper Internet connection and greatly increases the network exposure to external attacks.

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 IT/OT boundaries 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.

Critical Analysis in Oil & Gas Sector

Due to one way dataflow of the device, it allows to monitor drilling operation and BOP (Blowout preventer) and in parallel ensures that all cyber-attacks are unsuccessful.

Preventing rigs from being hacked to protect assets and operation against cyber-attacks, 100% secure transmission and connectivity is of the highest priority for the industry.

In the wake of various cyber breaches, it is becoming essential by every day to maintain regular reporting of health of the equipment, real time working status, maintenance windows, and failure data from blowout preventers (BOPs) and other critical infrastructure elements of the operation along with their associated control systems. The monitoring is essentially done from remote Monitoring operations centers collecting information from many rigs spread across a large geographic area.

The biggest challenge for Oil & Gas Industry is to ensure that BOP systems and other critical elements are protected from external attacks yet maintaining continuous flow of data to the monitoring station without making any change in the routine network topology. Another big challenge is the diversity and ageing of the equipment on rigs which may include legacy products with old, unsupported operating systems.

BOPs and other rig controls are intended to be one time installation and to be used uninterrupted for exceptionally long period of time. FPGA based Terafence data diode is a solution as it require no change in topology for installation, negligible maintenance and the security provided is robust to changes that may occur in the BOP or rig control systems.

Oil and gas exploration and extraction, processing of the raw product, transportation to onshore and through pipelines, and distribution operations are few critical infrastructure requirements that demand 100% cyber secure solution.

An incident can have devastating impacts on people, nations, and the environment. Many Oil and Gas companies already use data diodes to protect the critical infrastructure and it should be looking more use to avoid any attack. Terafence is cost-effective solution that can be used to address a multitude of common industry challenges.

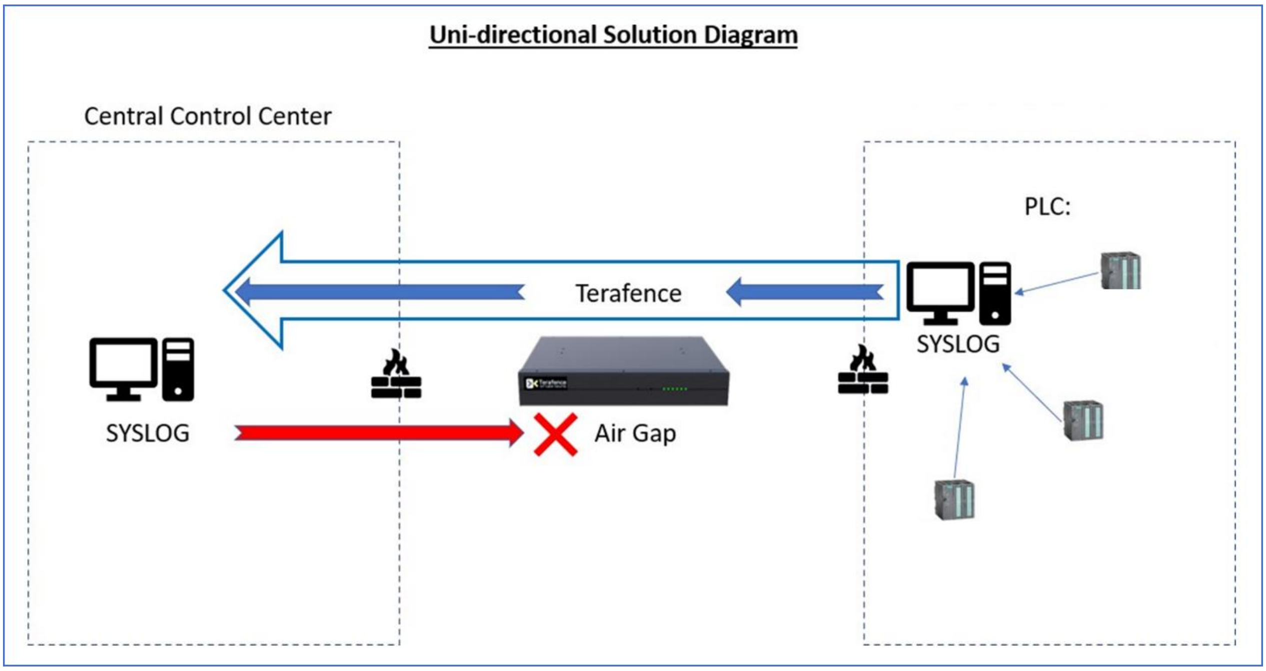
Terafence secures network infrastructure and devices across multiple levels of oil and gas operations, from critical assets to control and safety systems to Industrial IoT-based solutions. Few other important areas that Terafence can protect include terminal automation systems, custody transfer systems, tank farm automation, and oil movement and storage.

SYSLOG Case Study in Oil & Gas Industry:

Industry needs a fool-proof barrier between local IT infrastructure and the network from the Governmental Resource Management or data transfer between onshore critical infrastructure and offshore monitoring stations to continuously collect SYSLOG messages from networked devices and servers regarding functionality and operational status.

Generally, the two networks are connected via 2 firewalls, each at the edge of it’s network.

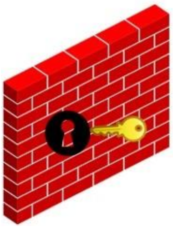
Terafence can provide a 100% secure barrier between the two networks to ensure no leakage of Cyber events happen from either end. Terafence SYSLOG product creates a total barrier between the two networks. SYSLOG data can be sent real time to the original destination as before with zero chance of cyber-attack. This will ensure no change of network connectivity topology and no operational impact during or after the installation.



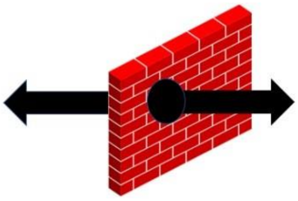
Security– Firewall vs. Terafence

“I can do this with a Firewall…"

Yes, you can configure a Firewall to deny any access from the outside… but:



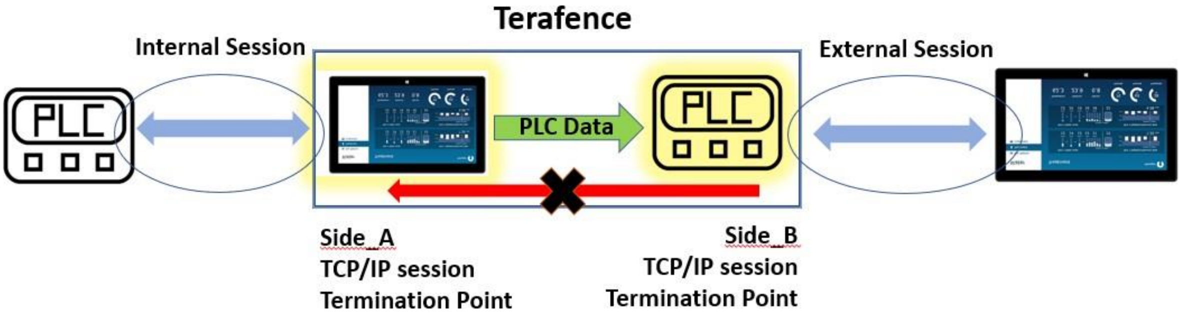
A firewall is a mainly system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules / keys. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate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

Latest technology deployment reference

14 Feb 2021 **...** Aramco begins using latest Data **Diode** against cyber threats

Terafence iTF-SecureOT Technical:

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) *****

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

For more information:

Chandra Shekhar Misra
Founder & CEO
Terafence Private Limited
chandra@terafence.in
+91 98113 23448