
**ATTILA CYBERTECH**

Resilience Beyond **Defense**

Cyber-Resilience for ICS, SCADA & CPS

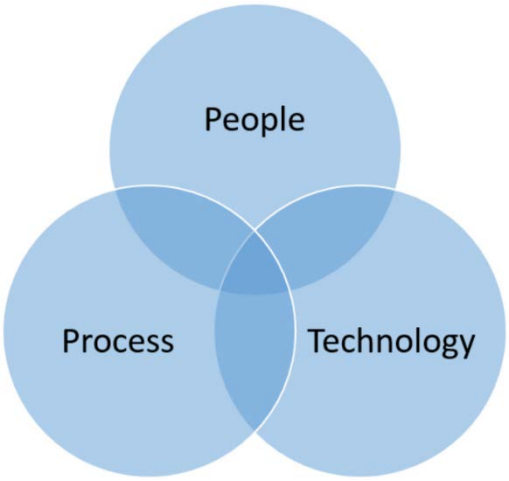
# WHO WE ARE

Attila Cybertech was conceived out of the strong desire to eradicate "insecurity by design" of conventional Industrial Control Systems (ICS), which is now given a newly coined term: Operational Technology (OT). We helped secure our clients' critical assets through a holistic approach with a range of services and solutions ranging from risk assessments to secured network design, industrial firewall selection/deployment and pen-testing for industrial control systems such as SCADA, DCS, PLC and RTU.

Attila's solutions of choice are validated by independent certification bodies and integrate state-of-art OT cybersecurity technology and industrial best practices. We have also supported our clients in attaining certification by fulfilling the requirements of international standard IEC 62443-2-4, a testament to our professionalism in the realm of OT cybersecurity. Such consultation services may include policy and standards development, systems design review, and even executing and implementing cybersecurity solutions for industrial automation and control systems (IACS).

Attila's strength comes from our ability to capitalize on our knowledge in the design, engineering and implementation of industrial control systems that we could be deployed anywhere in industrial assets such as power, water, container ports, maritime vessels/rigs, transportation, chemical, refinery, LNG and so on. No battle to protect our Critical Infrastructures could be fought and won alone. We believe in working alongside with other key stakeholders including automation professionals, process engineering and IT security. Only then can true protection and resiliency be established and more importantly maintain at a high level.

Having well-trained People, good Processes and field-proven Technology is a good beginning. However, maintaining the desired security posture requires constant monitoring and upkeeping. The security lifecycle of ICS can be likened to the growing of a healthy plant that requires consistent sunshine, water and nutrients. Attila can play a vital role in the success of your OT security.




Singapore Cybersecurity Consortium

Attila is one of the founding members of the Singapore Cybersecurity Consortium (SCC). Singapore Cybersecurity Consortium is created for engagement between industry, academia and government agencies to encourage use-inspired research, translation, manpower training and technology awareness in the area of security. The National Research Foundation (NRF) and anchored at the University of Singapore (NUS) funded The Consortium since 1 September 2016.

# WHO WE ARE

## Our competitive advantages


**Strong** Operational Technology (OT) Knowledge

- Our Key Management and Core Team
- Spin-off from Automation System Integration

**Expert OT Cybersecurity** Domain Knowledge and know-how

- Our track records on Critical Control Systems including Safety Instrumentation System

**Deep-dive** in Innovation with an OT element

- Machine learning of data analysis that automates analytical model building.
- Artificial Intelligence

# OUR FOCUS

Our key industry focus is on Operational Technology Cybersecurity in the Critical Information Infrastructure (CII) sector.

Our primary expertise focus is on Cyber-Physical Systems for the following sectors:

- Water and Wastewater
- Transportation
- Oil & Gas
- Power Generation
- Energy
- Critical Manufacturing
- Smart Building
- Maritime & Shipping
- Internet of Things (IoT)

## Market Drivers

- Software Security (or Lack of)
- Digitalization/Industry 4.0
- OT and IT Integration
- IoT/Industrial IoT
- Business Analytics
- Big Data and Cloud Technology
- Hackers
- Sabotage
- Insider Threats

# OUR STRATEGY

We use three basic approaches to building resilience in the Cyber-Physical System (CPS). These approaches are the Security-by-Design, Defence In-Depth Approach and Certification Approach. The diagram below depicts our approaches.

### Security-by-Design

- Design phase
- Implementation Phase
- Maintenance Phase

### Certified Solution

- Achilles Practices Certification
- Align to IEC 62443-2-4
- CREST

### Defence in Depth

- Security Management (Cybersecurity Program, Risk Management)
- Physical Security (Protection of Physical Locations, Physical Access Control, Access Monitoring System, People and Asset Tracking)
- Network Security (Architecture, Logging, Monitoring, Zero-Trust)
- Hardware Security (Trusted Platform, Hardware Encryption Implementation)
- Software Security (Application White Listing, Patching, Secure Coding, Hardening)

# OUR SERVICES & PRODUCTS

We adhere closely to the National Institute of Standards Technology (NIST) Framework for Improving Critical Information Infrastructure Cybersecurity which advocates an Identify, Protect, Detect, Respond, Recover model. Attila Cybertech strives for the coherent integration of this model alongside the process safety measures that are already in place.

Our Services modernise and integrate disparate legacy systems across a broad base and facilities to increase productivity. We are the Operational Technology (OT) cybersecurity domain experts in Industrial Control Systems (ICS), Safety Instrumented System (SIS), SCADA, DCS, PLC, RTU and etc. Unlike the conventional IT security companies in the region, our domain knowledge and expertise in implementing cybersecurity solutions make us a unique player.

# OUR SERVICES & PRODUCTS

## ATTILA CYBERTECH CONSULTING

With our years of experience in industrial automation, we coupled state-of-the-art technology and best practices in managing security risk. Our cybersecurity consultants are capable of providing practical advice to help our clients minimize risk and establish a cyber-hardened industrial control environment.

Our Consulting Services include:

- Security Policy & Architecture Review
- Security Gap Analysis and Solution
- Security Audit
- Risk Assessment
- Vulnerability Assessment
- Penetration Testing
- Security Remediation

## ATTILA CYBERTECH SOLUTION

We provide comprehensive solutions that include secured network design, through the implementation of DMZ, rationalizing zone and segmentation according to Purdue level while balancing the need for communication versus segmentation via firewalls. Our solution also includes routine maintenance services for the Asset Owner.

Some of our Solutions offered are:

- Secure Network Design Implementation
- System Hardening
- Domain Controller Set-up
- Multi-Factor Authentication (MFA) for ICS/SCADA
- Unidirectional Security Gateway/Data Diode
- Industrial Graded Firewall
- Application Whitelisting
- Secure Sanitization of Storage
- Intrusion Detection Systems
- Anomaly Detection System
- Audit Logs System

## ATTILA CYBERTECH MAINTENANCE

We believe that service does not stop at just the end of implementation. We continue to engage with our clients by providing premium after-sales services such as continuous system health checks and monitoring, provide system patches and software/firmware updates and an extra helping hand in times of cyber crisis.

## ATTILA CYBERTECH TRAINING

Education is one of the key successes of cybersecurity. It is important to educate and inform every stakeholder on cyber hygiene, mitigation and threats. Our Customisable Training Solution ranges from basic to advance in ICS cybersecurity. This training solution can be adjusted to suit various levels, ranging from operator to senior management.

# OUR SERVICES & PRODUCTS

## ADPICS® Data Diode

Attila introduces ADPICS® Data Diode as a cybersecurity tool for the protection of Critical Information Infrastructure. It is designed to protect critical assets against manipulation, protect classified and sensitive data, and prevent data leakage, using solely unidirectional communications.


*Ethernet Data Diode (above) catered for seamless integration into existing architecture in the server rack.*

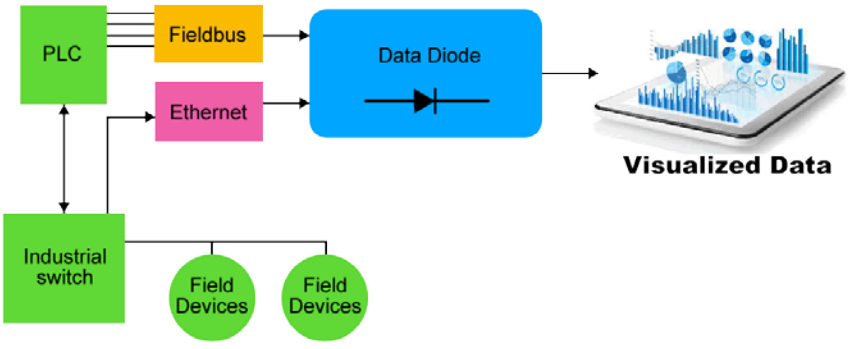
### Key Features of ADPICS® Data Diode

- Hardware-Enforced One-Directional Data Flow
- Air-Gapped between ICS & Corporate IT Networks
- Certified with Common Criteria, the International Standard for Security Evaluation

Using a state-of-the-art PROFIBUS and Ethernet data diode, operational data is kept flowing in one direction, thus protecting the availability and integrity of the critical infrastructure while preventing any intrusion efforts.

## ADPICS® Commander

Attila ADPICS® Commander makes use of ingressed data to understand the process behaviour of the monitored OT assets. Enhancing cyber situational awareness with AI real-time monitoring and alert triggering. Coupled with domain knowledge, it is capable of reducing false alarms and pinpointing the process tag in which the anomaly had occurred.




### Key Features of ADPICS® Commander

- Real-time monitoring of the Industrial Control System (ICS) process data
- Ability to predict potential instrument/equipment failure
- Notification Alerts sent to Operators on detected anomalies

# OUR SERVICES & PRODUCTS

## Prediction Engine

- Continuous machine learning algorithm to provide up-to-date anomaly detection and prevention
- AI-powered, giving rise to speedier response times and correlated incident identification increases the accuracy of detection

With machine learning algorithms, predicted data are generated using real-time process data. These data together with its mathematical statistics are compared with its historical brandmark.

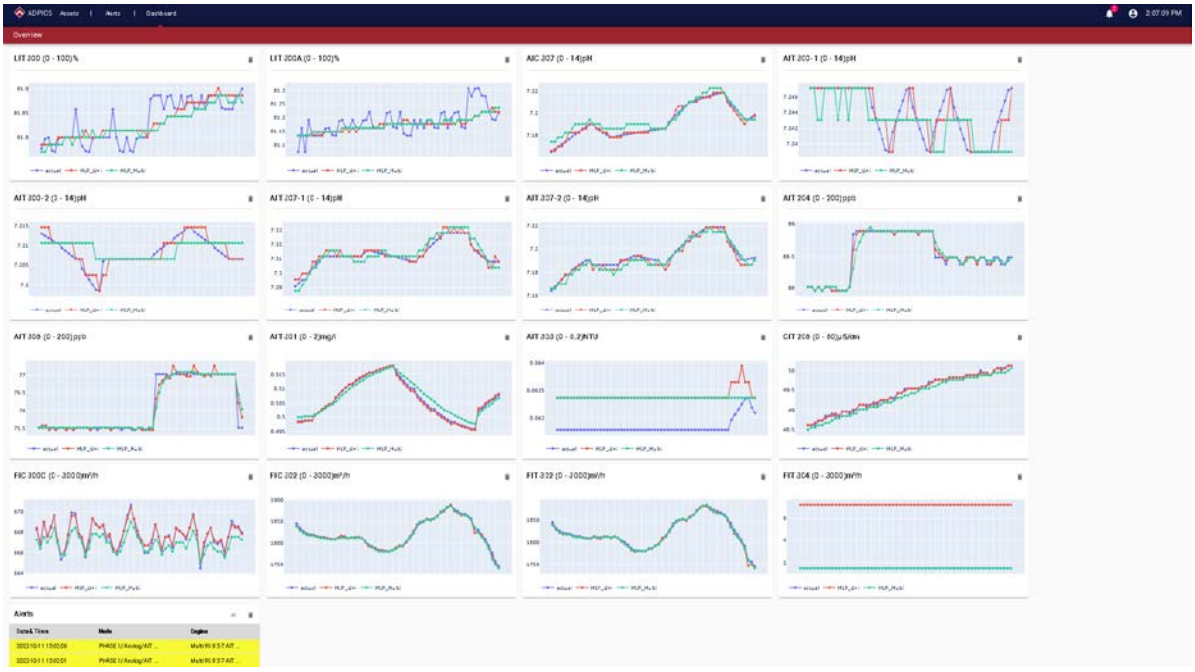
## Domain Knowledge Correlation

- Reducing the false alarm
- Pinpointing anomaly source

Alert accuracy plays a critical part in any detection system, to avoid overwhelming the operator with alerts. Domain knowledge is incorporated into the system to improve its accuracy.

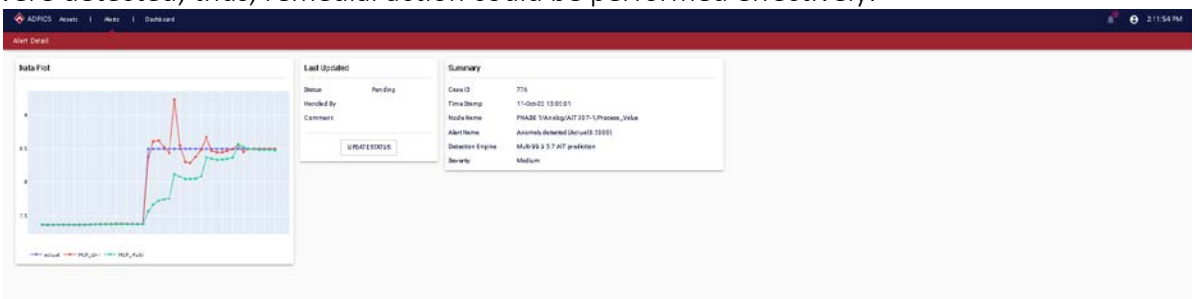
## Command Dashboard

The dashboard provides insight into the overall threat landscape of the monitored environment.



## Alert Manager

An anomaly could happen anytime and without a real-time alerting system, these critical assets would be at risk. The Alert Manager provides the operator with first-hand information on all probable anomalies that were detected; thus, remedial action could be performed effectively.



# OUR SERVICES & PRODUCTS

ATTILA CYBERTECH
INNOVATION

Cyber threats are continually evolving. We strongly believe that innovation is one of the key strategies to counter these incessant threats. We strive for innovation through collaboration with our customers, institutions of higher learning and technology partners by sharing ideas, concepts and domain knowledge to develop the most resilient protections for critical infrastructure and operational technology assets. We continuously seek out innovative research areas and market opportunities in advanced cybersecurity that go beyond existing product offerings.

Below are some of the research areas:

- Advanced threat management through machine learning
- Industry protocol and Fieldbus analysis
- Advanced data analytics on existing network
- Trusted network for high-security system

# CUSTOMERS

We have worked with various public and private corporations in securing their critical infrastructure. Some of our customers (in alphabetical order) include:

- BW Offshore/Omega Integration
- ExxonMobil Singapore
- Jurong Port Pte Ltd
- Maritime and Port Authority of Singapore
- PacificLight Power Pte Ltd
- PSA Corporation Ltd
- PUB (Public Utilities Board)
- Sembcorp Marine Ltd
- ST Engineering Electronics Ltd
- Tuas Power Generation Pte Ltd
- UOB Bank Limited
- UST Global
- YTL PowerSeraya Pte Ltd

# CONTACT US

**Attila Cybertech Pte. Ltd.**
39 Ubi Road 1, #05-01
World Publications Building
Singapore 408695

Tel: +65 6747 6116
Email: sales@attilatech.com
Website: www.attilatech.com

ATTILA
CYBERTECH