GLOBAL TRANSIT SOLUTIONS

CYBER SECURITY

Security is trust in action

+966502466700(KSA)
+966500627589(KSA)
+923215588000(PAK)
www.gtsconnects.com
Block C, Sec B-17 Islamabad, Pakistan

SECURE YOUR VITAL OPERATIONS

The complexity and interconnection of IT and OT systems mean that cyberattacks can lead to significant operational, safety, reputational, and financial impacts. In brownfield environments, it is the responsibility of organizations and operators to inventory existing assets, perform comprehensive risk assessments including safety critical incidents, operational disruptions, and data breaches to implement both organizational and technical controls to mitigate these risks.

The main challenges include:

- Wide geographic distribution of assets across multiple sites and remote locations.
- Integrating legacy systems with modern connected technologies such as COTS, open-source platforms, remote ICS, and IoT devices.
- Challenges in patch management and securing outdated or unsupported components due to system lifecycle and warranty constraints.
- The requirement to comply with both cybersecurity standards and operational safety regulations concurrently.

In the development of new IT and OT systems, it is essential to integrate cybersecurity considerations into the design and planning phases and to implement adaptive processes that address evolving threat landscapes. Cybersecurity plays a fundamental role in ensuring connected, resilient, and safe operations across critical infrastructures. Many such systems are designated as critical assets by national authorities and are governed by regulatory frameworks such as the NIS Directive in Europe.

SECURITY LEVELS

IEC 62443 defines four Security Levels for OT systems, while NIST and ISO/IEC 27001 offer complementary risk-based frameworks for securing both IT and OT environments.

Level 1 $

Basic defense against casual or opportunistic threats

Level 2 $ $

Protection against intentional cybercriminals with improved detection and recovery.

Level 3 $ $ $

Defense against skilled attackers requiring centralized management and monitoring.

Level 4 $ $ $ $

Advanced protection against highly sophisticated, state-sponsored adversaries

Organizations managing IT and OT infrastructure remain significantly vulnerable to cyber threats. While some governance and protection measures are in place, detection and response capabilities are often limited. Most known cyberattacks are opportunistic in nature; however, the absence of effective logging and monitoring hampers incident investigation. Additionally, critical infrastructure systems are increasingly exposed to Advanced Persistent Threats (APTs) that target both IT networks and Operational Technology (OT) environments.

TAKEAWAY RECOMMENDATIONS

1	Assess and prioritize critical IT/OT assets based on business and operational impact.
2	Evaluate risks by analyzing potential threat scenarios and their likelihood.
3	Harden system configurations and enforce segmentation with firewalls and gateways.
4	Apply backup, recovery, and continuity practices to OT and legacy systems.
5	Implement unified physical/logical access using RBAC and least privilege.
6	Deploy host/network IDPS and centralize log collection for threat visibility.
7	Use a SOC for event correlation, real-time monitoring, and incident response.
8	Provide ongoing cybersecurity training to reduce human and insider risks.

These recommendations follow standards like ISO/IEC 27001, IEC 62443, and TS 50701, and are guided by NIST, ENISA, and ANSSI. Both IT and OT require tailored security, with IT focusing on Confidentiality, and OT prioritizing Integrity and Availability. OT security also incorporates safety standards such as IEC 61508 and ERA's CSM.

WHAT WE PROVIDE

Security Governance & Risk Management

Deliver strategic alignment and risk visibility across IT and OT environments.

- Governance & Strategy Development (ISO 27001, NIST CSF, IEC 62443)
- Risk & Compliance Audits (ISO 31000, NIST RMF, NIST 800-53)
- Cybersecurity Policy & Standards Development
- Security Awareness & Training Programs

Communication & Network Security

Protect critical infrastructure and data through secure network.

- Network Security Architecture Design (Cisco SecureX, Palo Alto NGFWs)
- Firewall, IDS/IPS & Perimeter Defense (Fortinet, Suricata, Palo Alto)
- VPN & Secure Remote Access (Zscaler ZPA, Cisco AnyConnect, OpenVPN)
- ICS/SCADA Network Protection (Nozomi Networks, Dragos)

Security Assessment & Testing

Identify vulnerabilities and validate defenses across enterprise systems.

- Vulnerability & Penetration Testing (Nessus, Qualys, Burp Suite)
- Red, Blue & Purple Team Exercises (Cobalt Strike, Caldera, MITRE ATT&CK)
- OT/ICS Cybersecurity Assessments (GRASSMARLIN, Tenable.ot)
- Threat Modeling & Risk Analysis (IriusRisk, Microsoft TMT)

Data Security & Privacy

Safeguard sensitive data and maintain operational continuity.

- Data Classification & Encryption (at rest/in transit)
- Secure Storage & Backup Strategies (Ransomware Resilience)
- Data Loss Prevention (DLP) for IT and Industrial Networks
- Secure Protocol Implementation for OT (e.g., TLS for Modbus/TCP, OPC-UA)

Security Operations & Threat Management

Detect, respond, and recover from cyber threats across IT/OT in real time.

- SIEM & SOAR Implementation (Splunk, Cortex XSOAR, QRadar SOAR)
- Threat Hunting & Malware Analysis (CrowdStrike, Mandiant, YARA)
- Incident Response & Digital Forensics (TheHive, EnCase, Velociraptor)

HIGHLIGHTED REFERENCES

Project Services in Public / Private Sectors of Pakistan

Provided cybersecurity services for critical infrastructure in both the Government of Pakistan and private sectors, covering IT and OT aspects, including power plants.

- **Standard compliance:**
  ISO 27001, IEC 62443, IEC 62645, USNRC 10 CFR 73, USNRC RG 5.71
- **Risk management**:
  Risk assessment and management of IT and OT infrastructure.
- **Enterprise Network Protection**:
  Securing administrative systems (email, databases,file servers) against cyber threats.
- **Access Control & Identity Management**:
  Implementing least privilege access, MFA, and secure authentication for corporate users.
- **Patch and Vulnerability Management:**
  Timely updates of OS and software to manage known vulnerabilities.
- **Incident Detection & Response:**
  Use of SIEM solutions, EDR, and threat intelligence platforms to detect, analyze, and respond to cyber incidents.
- **Data Governance and Backups:**
  Enforcing data protection policies, encryption, and secure offsite backup for business continuity.
- **ICS/SCADA System Security**:
  Protection of control systems (PLCs, DCS, RTUs) against unauthorized access and manipulation.
- **Network Segmentation**:
  Strong separation between IT and OT networks using firewalls and demilitarized zones (DMZs).
- **Legacy System Risks:**
  Addressing vulnerabilities in outdated OT devices that lack built-in security features.
- **Physical-Cyber Interface Protection**:
  Ensuring that physical access controls (e.g., to control rooms, cabinets) are integrated with cyber defenses.
- **Secure Remote Access**:
  Controlled and monitored remote access for maintenance teams, particularly during emergencies or outages.

Collaborators:

Nextreme Techno Solutions	EMOS Engineering Services	Data Hawk Enterprises	Premier Data Systems

CONTACT US

GLOBAL TRANSIT SOLUTIONS

info@gtsconnects.com
sales@gtsconnects.com