CONTEL
BEYOND TECHNOLOGY

Cybersecurity for OT, Infrastructure, and IT

The Cybersecurity Division for OT, Infrastructure, and IT of the Contel Group combines 60 years of expertise in implementing control and automation systems, along with a deep understanding of the needs of Israeli industry.

We support complex and challenging projects across a wide range of industries, including power plants, gas and renewable energy facilities, energy generation and infrastructure sites, petrochemical plants, plastics manufacturing, food production, and pharmaceutical industries.

Among our clients: Etgal Power Station, Halutziot Solar Energy Facility, Dorad, Israel Airports Authority, dozens of solar sites across Israel, EDF, Shikun & Binui, TeraLight, Maxima, Enlight Renewable Energy, Logisticare, Negev Ashalim, and more.

Our vision is to enable operational continuity for our customers by combining decades of experience and control systems integration with the implementation of advanced technologies that ensure availability, reliability, and confidentiality of information in the operational cyber domain.

Our team consists of experts with unique experience in the characterization, integration, and implementation of cybersecurity solutions for OT, tailored to customer and industry needs, regulatory requirements, and the outcomes of risk assessments, penetration testing, or external consultant recommendations.

We operate in compliance with the most stringent standards, such as ISO 27001 and IEC 62443, and work in full cooperation with the Israel National Cyber Directorate, the Ministry of Energy, the Ministry of Environmental Protection, and the Water Authority.

Contel is a member of the Cyber Forum of the Manufacturers Association of Israel (MAI).

Business Partners:

CISCO | GATESCANNER by Sasa Software | OPSWAT | Terafence IoT Cyber Security | WATERFALL Stronger Than Firewalls

CHECK POINT | SIGA Level Zero OT Resilience | FORTINET | veeam | Rockwell Automation

CONTEL
BEYOND TECHNOLOGY

Intrusion Detection Systems (IDS)

Defense-in-Depth for Industrial Networks and Critical Infrastructure

In industrial plants and infrastructure facilities, any deviation in network traffic may impact operational processes,such as changes to controller parameters, shutdown of pumps, unintended equipment activation, or degradation in production quality. Therefore, Contel integrates dedicated IDS solutions for OT environments, capable of detecting intrusion attempts, anomalous traffic, and activities that deviate from normal control network behavior in real time.

These systems are tailored to common industrial protocols and complex network architectures across sectors such as water, energy, advanced manufacturing processes, pharmaceuticals, food production, and national infrastructure. The solutions operate non-intrusively within production environments, provide early alerts on anomalies, and enable plant or site teams to respond before threats escalate into operational incidents.
The result: A detection layer that strengthens the protection of OT networks and ensures continuity, stability, and safety in the most critical environments.

Industrial Switches & Firewalls

Defense-in-Depth for Industrial Networks and Critical Infrastructure

Industrial control networks are required to operate continuously, handle high loads, and function in harsh environments that include heat, vibration, humidity, and other challenging conditions. Any network failure can impact production processes, including energy systems, water supply, and other critical infrastructure. Therefore, selecting industrial switches and firewalls specifically designed for OT environments is essential for operational stability and security.

Contel provides a comprehensive solution that includes the design, implementation, and maintenance of industrial communication switches and firewalls, tailored for SCADA, PLC, HMI, MES systems, and complex network architectures in industrial plants and infrastructure facilities.

Industrial Switches - The Backbone of the OT Network

The industrial switches implemented by Contel are designed for 24/7 continuous operation and built to withstand harsh environmental conditions.

These switches support:
- Stable communication across industrial protocols.
- Full redundancy, including RSTP / DRP / MRP.
- Centralized management and real-time status monitoring.
- Network segmentation to prevent fault propagation.
- Installation in control panels, field environments, or dedicated communication rooms.

The advantage: Building a robust communication network that ensures controllers, field devices, computers, and control rooms operate seamlessly.

Industrial Firewalls - Protection for Control Networks

In OT environments, standard IT firewalls are not sufficient.
Contel implements industrial-grade firewalls designed specifically for OT, including:

• Industrial protocol awareness (DPI – Deep Packet Inspection).
• Blocking of unsafe or unauthorized commands to controllers.
• Secure remote access management for vendors and third parties.
• Segmentation between IT and OT networks with an Industrial DMZ.
• Security segmentation based on Zones & Conduits.
• Prevention of malicious code infiltration and anomalous traffic

These capabilities provide a critical layer of protection, preventing manipulation of production processes and reducing the risk of cyberattacks.

Contel’s Solution - Seamless Integration Between Networking and Control

Contel delivers full integration between communication switches, firewalls, and existing control systems, based on a deep understanding of plant architecture and operational needs.

The solution includes:

1. OT/IT Network Design & Engineering
Creating a stable, secure architecture aligned with production processes.

2. On-Site Implementation & System Hardening
Installation in control cabinets, in communication rooms, or in an open environment, all according to the structure of the site.

3. Segmentation & Security Management
Dividing the network into zones, defining authorized data flows, and blocking unwanted traffic.

4. Monitoring, Maintenance & Continuous Upgrades
Preventive maintenance, periodic testing, security updates, and ongoing network performance monitoring.

With Contel, everything integrates precisely into the site’s control and operational systems-enabling secure, efficient, and reliable operations over time.

CONTEL
BEYOND TECHNOLOGY

Cybersecurity Assessments

Defense-in-Depth for Industrial Networks and Critical Infrastructure

In a world where production systems, energy, water, and critical infrastructure are increasingly connected to IT networks, cloud services, and smart systems, risks are growing accordingly. Therefore, having an accurate understanding of the actual security posture has become essential. A cybersecurity assessment is the first step in building a robust defense layer-identifying vulnerabilities, analyzing risks, and providing a detailed action plan for improvement.

Contel conducts dedicated cybersecurity assessments for industrial and OT environments, with a strong emphasis on maintaining availability, safety, and operational stability.

What Does Contel's Cybersecurity Assessment Include?

1. Comprehensive Asset and Network Mapping.

Identification of servers, workstations, controllers, communication equipment, SCADA systems, subnetworks, and third-party connections-ensuring a complete and accurate view of the environment.

2. Vulnerability and Cyber Risk Analysis

Identification of weaknesses such as:

- Uncontrolled remote access
- Connections between IT and OT networks
- Unencrypted protocols
- Missing updates and patches
- Insecure network configurations
- Excessive user permissions

3. Review of Operational Processes and Management.

Evaluation of procedures, maintenance methodologies, user management, configuration documentation, and compliance with internal and regulatory standards.

4. Scenario Analysis and Risk Evaluation (if required, without impacting production)
Assessment of whether events may be cyber incidents or network faults that could affect processes, product quality, or overall system stability.

5. Comprehensive Report with Findings, Priorities, and Action Plan
Providing a clear picture of:
• What is urgent?
• What is high-risk?
• What can be quickly remediated?
• Which processes require changes or adjustments?
• Which controls should be added to achieve optimal protection?

Why Choose Contel for Cybersecurity Assessments?

Deep Expertise in OT & ICS Environments.
Unlike general cybersecurity providers, Contel has in-depth knowledge of control systems,

PLCs, SCADA, and industrial communications-ensuring assessments are aligned with operational reality, not just IT considerations.

No Impact on Production Processes.
Assessments are conducted using safe methodologies that prevent downtime, overload, or disruptions to production lines.

Integration of Cybersecurity, Engineering, and Control.
Contel’s teams combine engineering and operational experience, ensuring a comprehensive understanding of how risks impact both digital and physical processes.

Compliance with International Security Standards.
Assessments are aligned with standards such as IEC 62443, NIST, and relevant regulatory requirements.

Actionable Implementation Plan.
The final report goes beyond listing issues-it provides a clear, structured roadmap translated into practical projects, procedures, and improvements.

In summary, Contel’s cybersecurity assessment provides organizations with a clear, accurate, and up-to-date understanding of their security posture, forming a solid foundation for strengthening defense layers, improving processes, and preparing for cyber threats- while maintaining the operational stability of core industrial activities.

CONTEL
BEYOND TECHNOLOGY

Protection of OT Networks

Defense-in-Depth for Industrial Networks and Critical Infrastructure

OT networks have become a primary target for cyberattacks because they connect critical control systems-such as SCADA, PLCs, field instrumentation, and energy systems-with IT environments and the cloud. This increased connectivity, driven by the need for real-time data analysis and process optimization, creates more entry points for attackers. Additionally, OT systems were historically designed for stability and availability-not cybersecurity-often operating without encryption, advanced access controls, or regular updates.

This combination of exposed networks, legacy operational technologies, and high dependence on real-time data means that any attack can have immediate and tangible consequences, including production line shutdowns, manipulation of process parameters, or safety incidents. As a result, OT networks are now at the forefront of ransomware attacks and industrial cyber threats.

Why Do OT Networks Require Specialized Protection?

Based on extensive field experience, OT networks:

- Require high availability and typically cannot be taken offline for maintenance.
- Rely on legacy, often unencrypted industrial protocols.
- Operate for many years without software updates.
- Are highly sensitive-any small change may impact safety, quality, and production.

Therefore, OT security requires a different approach-more cautious, process-oriented, and grounded in a deep understanding of control environments.

How Can OT Networks Be Protected?

Contel combines decades of experience in control systems, energy, and automation with advanced cybersecurity capabilities. Our approach is based on four key layers:

1. Full Visibility of the Control Network
Creating a complete picture of all OT assets, including controllers, engineering stations, SCADA servers, switches, communication systems, operational applications, and more. Goal: Know “who talks to whom” and detect anomalies before they escalate.

2. Secure Network Architecture Tailored to the Plant
Segmentation between IT and OT, creation of industrial security zones, controlled remote access, and secure integration between SCADA, PLCs, MES systems, and cloud platforms. Architecture is always designed according to operational needs-not generic templates.

3. Real-Time Protection of Production Processes
Monitoring OT traffic, detecting changes in process parameters, alerting on abnormal control commands, protecting industrial protocols, and identifying early signs of abnormal behavior in controllers and operator stations.

4. Operational Resilience and Rapid Recovery
Configuration backups, structured recovery procedures, and training for production, maintenance, and control teams-ensuring rapid recovery in the event of a cyber incident or system failure.

What Sets Contel Apart?

- Proven field experience across hundreds of industrial plants and infrastructure sites.
- Full integration of control, electrical, ICS, and cybersecurity domains-without disconnect between IT and OT.
- Deep process knowledge enabling precise understanding of how risks impact production.
- Seamless integration with existing systems: SCADA, MES, ERP, energy systems, cloud, and more.
- End-to-end support: assessment, design, implementation, monitoring, and training.

In Summary

Protecting OT networks is not a one-time project-it is a foundational capability that enables industry to safely advance toward cloud, automation, and smart technologies.

With Contel, organizations gain a protection layer precisely tailored to their operational environment - ensuring stability, production continuity, and true organizational peace of mind.

Unidirectional Data Transfer Solutions (Data Diodes)

Protecting Control Networks Without Compromising Data Flow

In an era where industrial control networks (OT) must connect to enterprise systems, cloud services, and external data providers, exposure to cyber risks is increasing daily. In practice, any bidirectional connection can serve as a pathway back into production systems-potentially leading to line shutdowns, process quality issues, and even safety risks.
Therefore, unidirectional data transfer solutions (data diodes) have become essential-enabling secure outbound data flow while completely preventing any return traffic.

How It Works?

A data diode is based on a mechanism that allows data to flow in one direction only-for example, from operational systems such as SCADA, PLCs, MES, and historian servers to IT networks or external systems.
There is no technical capability for reverse communication, ensuring that the control network remains isolated and fully protected.

Contel's Solution

Contel implements unidirectional solutions as part of a comprehensive OT cybersecurity framework tailored for industrial plants and infrastructure facilities:

1. Custom Network Architecture & Design
Defining the data to be transferred, analyzing protocols, determining connection points, and selecting the optimal environment for integration.

2. Full Integration with Production Systems
Seamless integration with systems such as SCADA, MES, historians, energy systems, and other control solutions-without altering processes or impacting performance.

3. Secure Deployment & Infrastructure Hardening
Controlled physical installation, network hardening, configuration of data paths, and ensuring complete isolation between networks.

4. Ongoing Maintenance, Monitoring & Upgrades
Periodic monitoring, system validation, configuration updates, and integration into a broader OT protection strategy.

Key Advantages

- Complete protection against intrusion into OT networks.
- Preservation of operational continuity and process stability.
- Secure transfer of real-time data to IT, BI, and cloud environments without risking production.
- Hardware-based solution independent of software updates.
- Compliance with industrial cybersecurity standards and regulatory requirements.

In Summary

Unidirectional data transfer solutions provide industrial plants and infrastructure with a unique combination of data accessibility and absolute protection of control networks.

Contel delivers these solutions with precision, security, and seamless integration into production processes.

Servers & Workstations

The Infrastructure That Powers Industrial Operations and Control Systems

Servers and workstations are the core components of any industrial control, production, and management environment. In domains where availability, reliability, and response time determine an organization's ability to produce, monitor, and manage processes in real time, the quality of the computing infrastructure has a direct impact on performance and operational stability.

In environments where every second of downtime translates into significant financial loss, a stable, secure, and well-maintained IT infrastructure is essential for business continuity and operational efficiency.

Contel specializes in the design, supply, implementation, and maintenance of servers and workstations tailored specifically to the needs of SCADA, PLC, MES, operational reporting, energy systems, industrial communications, and OT/IT applications.

What Does the Infrastructure Include?

1. Dedicated Industrial Servers

Robust and reliable servers designed for 24/7 operation and high workloads.

These servers are optimized for control systems, data management, historians, communications, and cybersecurity solutions.

ensuring complete isolation between networks.

2. Workstations for Operations, Engineering, and Control.

Workstations designed for industrial environments, including:

- HMI stations
- Engineering stations for PLC/RTU programming.
- Central control room operator stations.
- Operational stations for SCADA systems and production processes.

These systems provide a stable and user-friendly interface for operators, engineers, and operations managers.

3. Architecture Design & Full Implementation.
Establishing a complete computing infrastructure including servers, storage, virtualization, communications, backups, and site synchronization.
All designed according to performance requirements, number of users, system types, and relevant regulatory standards.

4. Secure Connectivity Between OT and IT.
Servers and workstations are securely and systematically connected to production and control networks, with managed interfaces to MES, ERP, BI, and cloud systems.

Our Advantages

Tailored for Industrial Control & Production Systems
Servers and workstations are designed to meet SCADA/PLC requirements and the needs of critical OT environments.

High Reliability and Long-Term Durability
Quality components, system hardening, proper network design, and redundancy solutions ensure maximum availability.

Centralized Management & Backup
All configurations, HMI screens, and project files are securely backed up and centrally managed.

Expert Support & Service
Contel's teams combine expertise in IT, communications, OT, and control systems—providing a significant advantage in environments where every component must work in harmony.

Servers, workstations, and professional maintenance services form the foundation for stable, secure, and efficient operations.
Contel delivers a comprehensive solution-from architecture and design to ongoing maintenance-ensuring that critical systems operate exactly as required.

Ongoing Maintenance Services for IT & Cyber Infrastructure

Operational Stability Starts with Proper Maintenance

In every industrial plant and infrastructure facility, IT and cybersecurity systems form a critical operational layer-servers, control systems, engineering stations, communication systems, databases, network equipment, security systems, and OT–IT integration. Any cyber threat, infrastructure failure, or poorly timed update can directly impact production lines, energy systems, water facilities, storage sites, control rooms, and command centers. Contel provides ongoing maintenance services that ensure operational continuity, high security, and peace of mind-fully tailored to the unique characteristics of industrial environments.

What Does the Service Include?

1. Controlled Patch & Update Management

Security and software updates are implemented with great care, following compatibility testing and without unnecessary downtime that could lead to revenue loss.
Our methodology is tailored for industrial environments, where every change must be coordinated with plant operations and the production floor.

2. Incident Response & Rapid Recovery

Contel follows structured protocols for handling cyber incidents and operational failures, including:

• Root cause identification.

• Rapid isolation of affected components.

• System recovery and implementation of preventive controls.

• Lessons learned and continuous improvement processes.

3. Backup, Recovery & Operational Resilience.

Regular backups of control configurations, HMI screens, PLC/RTU setups, databases, and more.

Periodic recovery tests ensure systems can be restored quickly and reliably.

4. Cybersecurity as a Routine Practice

Implementation of access policies, user privilege management, control of third-party connections, network hardening, and employee training.

All with an emphasis on establishing proper work practices in environments where mistakes can impact safety and productivity.

Why Choose Contel?

Deep Expertise in OT, Control Systems & Infrastructure

With decades of experience in SCADA, PLC, energy, and infrastructure projects, Contel understands the difference between an “IT issue” and an “operational failure” that can stop a physical process.

Unified IT & OT Approach

Managing IT and OT under one expert provider simplifies risk prevention, improves detection, and ensures systems operate securely and seamlessly together.

High Availability & Rapid Response

Contel’s teams are available for real-time issue resolution-especially in environments where downtime is not an option.

End-to-End Solution

From monitoring to backup, from network hardening to recovery testing-all IT and cybersecurity layers are managed under a single service framework.

Who Is This Service For?

- Process industries.
- Food & pharmaceutical manufacturing.
- Industrial production & automation.
- Energy & electricity sectors.
- Water, wastewater, and desalination facilities.
- Transportation, supply, and storage infrastructure.
- Industrial campuses and sensitive facilities.

Contel’s maintenance services ensure that both IT and OT systems remain stable, secure, and aligned with operational processes-so your plant or facility can continue to operate safely, efficiently, and without interruption.

About Contel Group

Operational Stability Starts with Proper Maintenance

Contel delivers projects and provides systems and equipment in industrial automation, electrical systems, process control, building management systems (BMS), energy management, and HVAC control.

The company is headquartered in Deniv Park, Kiryat Aryeh, Petach Tikva. An additional branch in the Omer Industrial Park provides technical support and engineering services to industry and engineering companies in southern Israel. Another branch in the Mevo Carmel Industrial Park also provides engineering services and serves as the location of the company's advanced electrical and control panel manufacturing facility.

An additional branch in Afula delivers end-of-line (packaging) solutions and robotics systems. A new branch in Sha'ar HaNegev supports the company's engineers in the Gaza envelope region, enhancing service capabilities in the area while contributing to recovery and support efforts.

Contel's activities cover nearly all market requirements in automation, control, and process control. As a system integrator, Contel offers comprehensive solutions that include hardware and equipment, system analysis, software development and implementation, electrical and control panels, engineering and installation, as well as training and services-all tailored to the specific needs of each customer. Much of the equipment is sourced from Contel's global business partners, leading manufacturers in their respective fields.

Professional Courses

Cybersecurity in Practice - Fundamentals of Cybersecurity for OT Networks, Industrial Plants, and National Infrastructure Facilities

https://contel.co.il/course/cyber-security-course-online/