BONNER

STANDARDS YOU CAN TRUST

CyberSecurity Partners

TOSIBOX

ABB B&R

ISA

bonner.ie

Head Office
35 Western Parkway Business Centre
Ballymount Drive, Dublin 12
D12 X542, Ireland

T +353 1 450 5050

contact@bonner.ie

Cork Office
Mitchelstown Enterprise Centre
Mitchelstown, Co. Cork
P67 X660, Ireland

T +353 21 242 7197

BONNER
STANDARDS YOU CAN TRUST

bonner.ie

Industrial CyberSecurity

CyberSecurity + Bonner

For clients installing new Industrial Automation and Control Systems (IACS) or updating to modern systems for factory digitisation, concerns about system security and safeguards are paramount.

At BONNER, our innovative approach to Cybersecurity and tailored solutions are designed to fortify the integrity of operations with security as the linchpin of our IACS solutions, every facet of the infrastructure is equipped with robust built-in measures, ensuring a meticulously documented approach from project inception and a seamless transition post-handover. Recognising the potential vulnerabilities within the architecture, both in the cyber and physical domains, we've integrated a range of adaptable features. This enables you to scale security measures up or down as required, providing a comprehensive life-cycle approach to safeguarding your operations. We prioritise not only the functionality but also the security of our solutions, ensuring a seamless and fortified digital factory experience.

Risk Assessment and Management

We work with the client to discuss these securities from a risk based approach and plan any system hardening most suited to their IACS from protecting endpoints to securing WIFi networks.

Security by Design

Incorporating a structured approach to security measures into the design and development phases of project delivery is essential, rather than adding them as an afterthought. We use ISA/IEC 62443 to define foundational requirements to organise technical requirements for the management of IACS and include secure network design at each stage of project design. We assist clients in establishing security policies, procedures and guidelines, for maintaining security within your industrial environment and complete Security Development Lifecycle management.

Incident Response

In the event of a cybersecurity incident, BONNER can help define the Incidence Response plan to be initiated. This plan may include roles and responsibilities, recovery objectives, and any recovery time objectives (RTO). We also include a comprehensive backup and restoration plan which is essential in the event of an incident and each element in the system should have a defined backup method and recovery procedure including PLC's, DCS or SCADA Servers and Network Devices.

Secure Remote Access

We use cutting-edge technology that enables seamless and highly protected connectivity to industrial systems, networks, and IoT devices. Users can confidently manage and monitor assets from a distance, knowing that their connections benefit from state-of-the-art encryption and security features. Using secure VPN's in IACS, guarantees reliable and safe access to vital infrastructure from anywhere in the world.

Reporting + Root Cause Analysis

We design our clients' systems to utilise processed data, presenting it in user-friendly reports and Key Performance Indicators (KPIs) for Cybersecurity. Additionally, our expertise extends to identifying incidents and pinpointing their underlying causes through root cause analysis. This approach empowers you with a thorough understanding of potential risks, their impact, and a clear roadmap for effective remediation to bring risk levels back to an acceptable threshold.

System Features

Projects delivered by BONNER use advanced cybersecurity measures including:

- **Electronic and Physical Access Control**
- **Network Intrusion Detection System (NIDS)**
- **Host Intrusion Detection System (HIDS)**
- **Network Segmentation + Monitoring**
- **Threat Modelling**