Applied Risk: Industrial Control Systems cyber security services

Industrial Control Systems (ICS) are now prime targets for dangerous cyber attacks. The risks of security incidents are ever-increasing and the consequences can be severe. Assets, environments, human life and the reputation of asset owners, operators and manufacturers must be protected.

Applied Risk is focussed on critical infrastructure security and combating security breaches that pose a significant threat. Operating on a global scale, we work with a wealth of large organisations that rely on our expertise to safeguard their critical assets.

ICS security is at its core a business enabler, and as such our ICS Cyber Security services are designed to facilitate and deliver robust protection while ensuring that production remains unaffected. Our range of services covers the full spectrum of our clients' requirements, enabling asset owners, operators, government agencies, manufacturers and suppliers to identify appropriate mitigating controls for protecting these systems.

Our services help to:

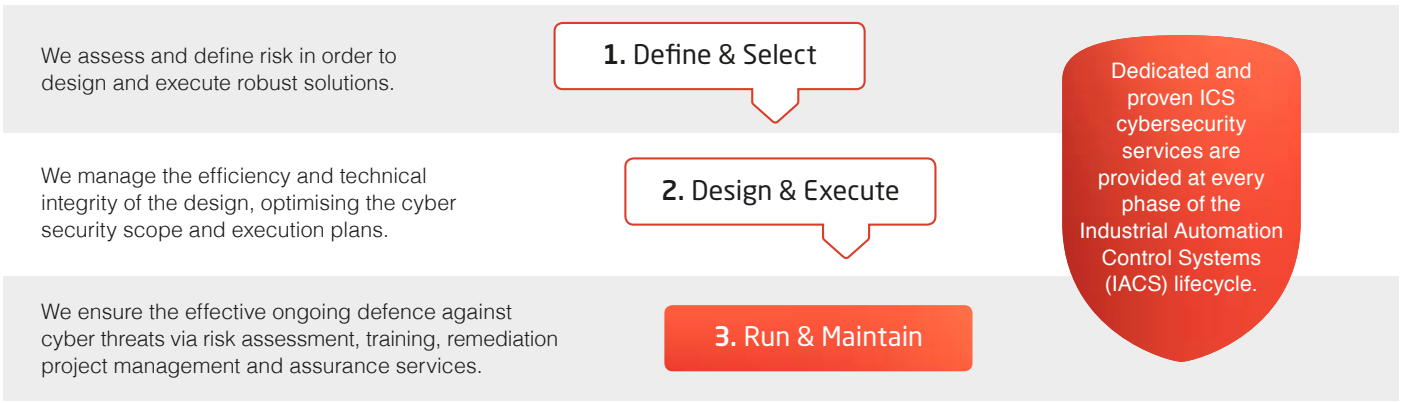
- Identify vulnerabilities and security issues within Industrial Automation Control Systems environments
- Secure critical infrastructures and the industrial assets of companies
- Support specific organisational requirements through the provision of customised security training and expert consultancy.

Key benefits:

- Protection for organisations against the consequences of security breaches, including fatalities; injuries; production continuity; loss or damage of assets; and environmental damage
- Gain the knowledge to mitigate against ever-growing threats targeting Industrial Automation and Process Control Systems environments
- Comply with international standards (IEC 62443) and industry best practices.

Applied Risk

The Industrial Automation Control Systems (IACS) Lifecycle



Industrial automation and control systems security

Confronting the risks and challenges of process control security and design

Applied Risk adds value throughout the Industrial Automation Control Systems lifecycle process, providing comprehensive engineering and consultancy services that harness our broad experience and unique offering as cyber security and engineering specialists. Our approach to IACS security focuses on:

- ICS Security Requirements Specification
- Security Design and Architecture
- Industrial Control Systems Security Frameworks
- Security Factory Acceptance Testing (SFAT) and Security Site Acceptance Testing (SSAT)
- Safety Instrumented Systems (SIS) and Field Devices Security
- Industrial Control Systems Security Assurance
- Network Security and Endpoint Protection
- Staff Augmentation and Remediation Programs.

ICS/SCADA security assessment & penetration testing

Customised testing and assessment to protect assets and mitigate threats

It is essential to identify and validate known security vulnerabilities for both public-facing and internal components in order to protect control systems. With an acute understanding of the sensitive nature of testing systems within live production environments, our comprehensive service includes:

- AMI/Smart Grid Security Assessment
- Infrastructure Assessment and Application Assessment
- Industrial Wireless Assessment and Physical Security Assessment
- Secure Code Review
- Social Engineering
- Targeted Attack Resistance Testing (TART).

RVA risk & vulnerability assessment

Identifying vulnerabilities and risks in the security of physical, IT and ICS/SCADA controls

Applied Risk's extensive RVA assessment is grounded by a robust and proven methodology honed over years of conducting assessments in industrial environments. Our extensive library of recorded IT security risks and vulnerabilities associated with many ICS/SCADA vendors is leveraged in order to establish suitable control measures. This approach is supported by detailed client assessments and clear compliance to industry standards and regulations.

ICS security introduction: instructor-led training course

A fundamental step in ensuring the safe and reliable continuation of production

By empowering employees to incorporate secure working practices in their everyday routines, organisations can ensure security threats against control systems are detected and addressed more efficiently. Our instructor-led 'Introduction to ICS Cyber Security' training course is a service that can be customised to meet specific requirements, providing employees with the necessary knowledge to place security and performance at the heart of business processes.

Embedded security assessment

In-depth security assessment that highlights risks and threats at a device level

Embedded Security has become a vital component of any new embedded product, with the Industrial Internet of Things (IoT) increasingly requiring devices to be connected. The potential detrimental consequences of a security breach are vast, and as such our wide security assessment spanning from Safety Critical Systems to Industrial Devices enables organisations to:

- Understand any vulnerabilities within a device, taking specific operational environments into account
- Eliminate weak entry points early in the product development lifecycle to safeguard against attack
- Increase business resilience through enhanced device security
- Comply with industry best practices and international standards, including IEC 62443
- Reduce vulnerabilities in new products and prevent unexpected costs and brand damage.

Medical devices security assessment

Helping the implementers of new medical device technology to understand the associated risks

Patient safety, data privacy, and intellectual property protection are all now threatened. Medical device manufacturers must adequately anticipate and mitigate the safety, security and business risks that come with the development and delivery of connected medical devices.

Our service measures and improves the security of medical imaging and storage devices; implantable devices, including insulin pumps and cardiac devices; telemedicine devices used for remote health monitoring; and specialised devices used for specific medical procedures.

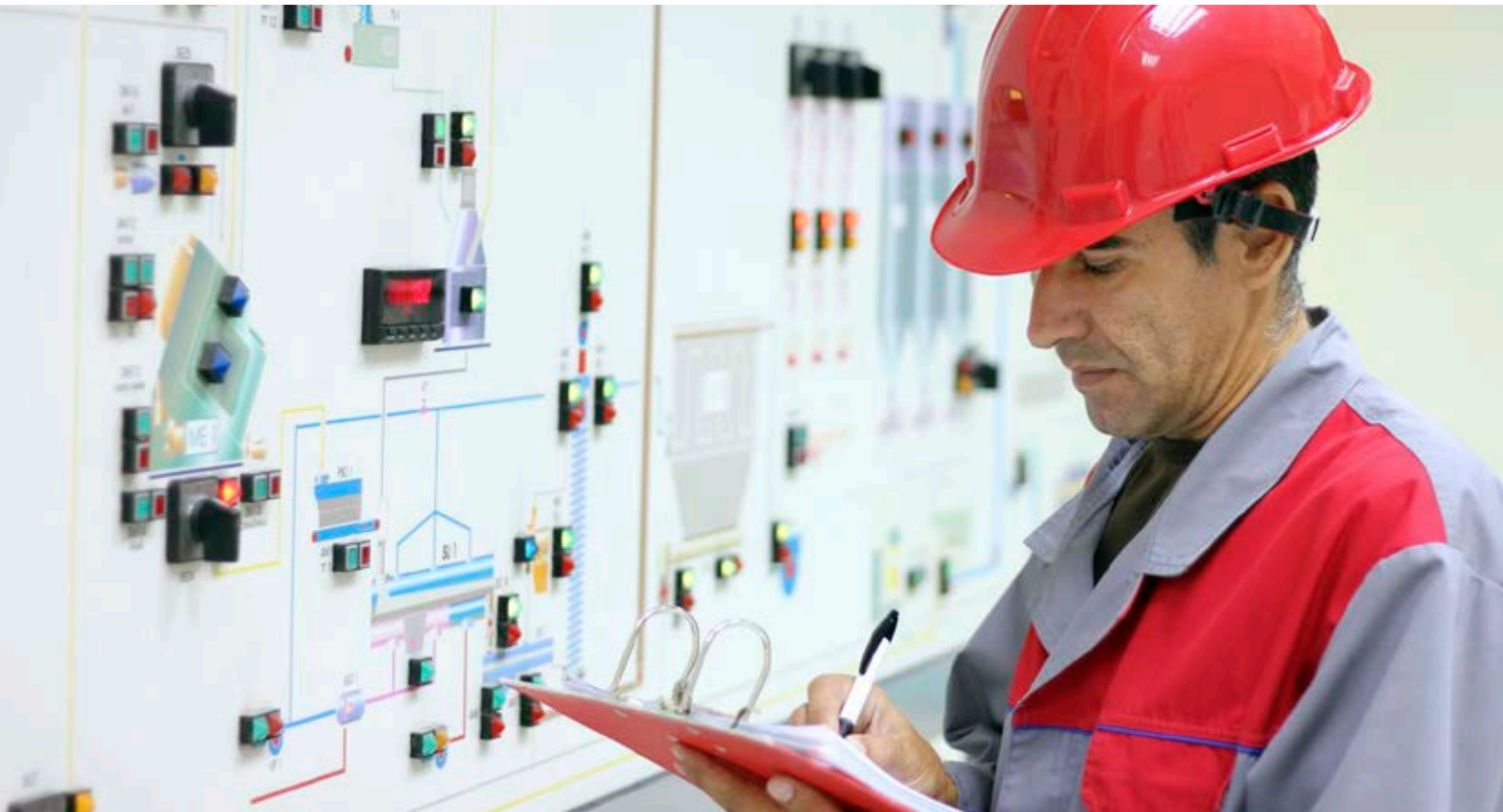
ICS security lab

Independent analysis of industrial control systems and critical infrastructure security

The new Applied Risk ICS Security Lab tests industrial control systems and critical infrastructure's resilience from cyber attacks. Our Amsterdam-based lab includes a team of ICS security researchers, dedicated to delivering unique market and threat analysis.

The lab is experienced in applying reverse-engineering, protocol analysis, and source code analysis techniques to a variety of ICS security threats. Our services deliver key information including:

- Early warning of the emergence of new ICS threats and confirmation of threat legitimacy
- Conclusive confirmation of affected code bases, products, versions and configurations
- Details necessary for conclusive identification of vulnerable and infected ICS systems
- Details necessary for detection of exploit attempts or malware activity
- Detailed remediation advice, including workarounds and configuration changes to safeguard systems.



Security threats are ever present in today's business landscape

Industrial environments are becoming increasingly exposed to costly and dangerous attacks. Growing levels of interconnectivity mean that cyber attacks will continue to expand in scope and increase in volume.

The security of Industrial Control Systems is an engineering-based problem that requires an engineering-focused solution. We uniquely combine extensive cybersecurity knowledge with broad engineering expertise to support organisations operating within the Industrial Automation and Process Control field.

Our proven experience is integral to securing the critical infrastructures and industrial assets of companies in the **Oil & Gas**; **Chemical**; **Manufacturing**; **Pharmaceutical** plus **Power** and **Water** sectors.

Understanding Industrial Control Systems cyber security risks – sector by sector

OIL & GAS

"New technologies are enabling companies to implement agile, cost-effective business practices. Unfortunately, they also come at a cost - many of the same security vulnerabilities that have plagued business systems now appear in SCADA systems. Pipeline control systems are now exposed to cybersecurity threats they were never designed for." **PipelineAndGasJournal.com**

CHEMICAL

"Chemical companies are not immune from cyber attacks. Both targeted and non-targeted attacks can cost companies millions of dollars in lost business and proprietary information. Yet many companies are woefully unprepared when it comes to protecting their industrial control systems from viruses and other cyber intrusions." **The U.S. Department of Homeland Security**

MANUFACTURING

"Automation comes with potential threats, as many manufacturing companies have had their industrial networks attacked and usually don't learn about it until significantly after the fact." **IndustryTap.com**

PHARMACEUTICAL

"Pharmaceutical companies do not view cyber security as a strategic business issue. They do not spend enough resources to protect their data, in part because cyber security has not received the executive level attention it deserves." **FT.com**

POWER

"Cyber threats, unlike traditional threats to electric grid reliability such as extreme weather, are less predictable in their timing … experts agree that the risk of a successful attack is significant, and that the system and its operators must be prepared." **BPC Electric Grid Cybersecurity Initiative**

WATER

"The Water and Wastewater Systems Sector is vulnerable to a variety of attacks, including contamination with deadly agents, physical attacks such as the release of toxic gaseous chemicals and cyber attacks." **The U.S. Department of Homeland Security**

Industrial Control Systems security is a rising global concern where targeted threats are now impacting multiple critical sectors. Applied Risk's holistic approach to security and our delivery of Industrial Control Systems Cyber Security Services is designed to specifically address our client's unique risk requirements with proven solutions.

Contact us to find out how Applied Risk can empower your organisation's cyber security defences.

Applied Risk BV
Joop Geesinkweg 901-999, 1114 AB, Amsterdam
The Netherlands

T: +31 (020) 561 6018
E: info@applied-risk.com
W: applied-risk.com

Applied Risk