Industrial Robotics and Cybersecurity.

www.tuv.com/fscs

TÜVRheinland®
Precisely Right.

Contents

INDUSTRIAL ROBOTICS AND CYBERSECURITY

Executive Summary.

Industrial robots are improving in terms of capability and performance, and their use across manufacturing and associated industries where fast, accurate and repetitive work is required is rapidly increasing.

The need for safety in such systems has been recognized for many years, and the increasing proximity of collaborative robots with human workers continues the need for safe working practices. As industrial robots become smarter, better connected and linked to the internet, there are now increased risks of cybersecurity related threats that can undermine the safe use and deployment of robots, lead to intellectual property loss, production delays and possibly effect physical damage.

The good news is that with an appropriate cybersecurity risk review, followed by product testing and the implementation of proportionate controls, an organization can be assured that their industrial robots are operating in a safe and secure way.

INTRODUCTION

Undoubtedly robots have transformed the world of manufacturing and are set to impact the provision of other services and medical care in the same way. Industry 4.0 will continue to drive the adoption of robots in manufacturing, service robots will gain increasing usage around the home in support of aging populations, and remote telemedicine robots will enable complex surgery to be undertaken in remote and maybe hostile environments.

Like any complex electromechanical system robots are subject to cybersecurity threats that can impact their safe and secure functioning. No longer can a robot be considered safe if its cybersecurity risks haven't been evaluated and addressed. Interconnected robots using common but unsecured internet protocols coupled with vulnerable operating systems that are rarely patched provide a huge surface area for attackers and a significant challenge for defenders.

This paper discusses the cybersecurity aspects of industrial robots and provides a way forward for manufacturers, system implementers and operators. It will bring together best practices from other industries and the broad experience from across TÜV Rheinland.

WHAT IS A ROBOT?

The term robot was derived in the early 20th century from the Czech word *robota*, which means a serf or laborer. Originally meant as an anti-technology jibe, the word has entered our current language to mean anything from a science fiction robot such as *The Terminator* through to the myriad of mechanical machines performing repetitive tasks on a production line. With such use in factories and facilities across the world humans have been freed from many mundane and often dangerous tasks.

A robot is defined as "a reprogrammable, multifunctional manipulator, designed to move materials, parts, tools or devices by means of variable programmed movements, with the purpose of accomplishing different tasks" (Mark W. Spong, 2004).

Definitions and a standard classification of robots is still emerging. The International Standards Organisation (ISO) (ISO-Standard 8373:2012) groups robots into following classifications:

- Industrial. Defined as an automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes, that can be either fixed in place or mobile for use in industrial applications
- Service. Defined as a robot that performs useful tasks for humans or equipment excluding industrial automation applications. Includes personal care robots such as mobile servants, physical assistants and person carriers (European Robotics Association, 2017).
- Additionally, medical robots have been defined as a "robot or robotic device intended to be used as medical electrical equipment" (VIRK, 2017).

It is accepted that further refinement in terminology is ongoing; for example a robot has no end effector but a robotic system does. Further discussion of this is outside the scope of this paper.

One of the first uses of robots in manufacturing was in the early 1960s when General Motors used the Unimate robot to assist in vehicle production. Since then we have seen an ever-increasing use of robots across different areas of society beyond industry and manufacturing. It has been estimated that there are almost 2 million industrial robots in use across the world (Hagerty, 2015).

ROBOTICS AND CYBERSECURITY

As with many products cybersecurity may often be an afterthought in the minds of robotic manufacturers. Cybersecurity may come low down on a list of important areas to be considered, inevitably being eclipsed by new features, reduced cost and safety issues. The notion of designing in cybersecurity at the beginning of robot product development has not gained traction in many places, and indeed many users and consumers are more interested in product features, cost and functionality than cybersecurity.

Unfortunately, many people get seduced by the anthropomorphic nature of some robotic systems and start to "over think" the nature of robotic cybersecurity risk. Robots are a combination of mechanical structures, sensors, actuators, and computer software that manages and controls these devices like any other machinery (Morante, 2015) and need to be considered in such a way when evaluating cybersecurity risk.

When considering robotics and cybersecurity the information security triad of confidentiality, integrity and availability is likely to be replaced with focused attention on availability and machine safety. Shutting down systems for security patches and updates, even if they are provided by manufacturers, takes planning and effort especially as industrial robots are assets to be fully utilized as any other.

Of course confidentiality should not be ignored. The robotic process employed in a factory or the complex control software used to guide an autonomous or semi-autonomous robot has value – to both hackers and competitors and should be protected as such.

THREATS AND RISKS TO ROBOTS

Robots and their associated supporting software and firmware can be undermined by attackers much as in any other system. Unfortunately, in many cases, and certainly in the industrial context, such an attack could have implications for the safe operation of the robot in question.

As manufacturers strive to implement innovative features, for example allowing control of an industrial robot by using a smartphone instead of the teaching pendant (the hand-held device used to instruct a robot) (Control Engineering Europe, 2011), there is an ever-growing need to build cyber-security into the robot design and development phase.

For a committed and well-funded attacker, such as a nation state actor, access to industrial robot hardware and software for research purposes is easy. It is unlikely that a hobbyist hacker would have access to industrial robot hardware unless they can enter a manufacturing facility, vendor's premises or gain remote access via Wi-Fi. Second hand industrial robots are available for purchase but this would need funding. Whilst not exceptionally expensive this provides another barrier to the hobbyist hacker, as does the size and weight of many industrial robots.

Industrial robot controller firmware is made freely available by some manufacturers from their websites (notably others will only provide supporting software to known customers). At the least this will enable a potential hacker to review software code and understand weaknesses without needing access to the associated hardware.

In contrast, medical robots deployed in a clinical setting are often poorly secured physically as many hospitals are often open sites with 24-hour access to members of the public. And of course, service robots sold to members of the public are a prime target due to their physical accessibility.

FIRMWARE AND SOFTWARE ATTACKS

Industrial robot firmware and supporting software may be loaded onto a local flash drive, hard drive or solid state media. Like all software it is susceptible to malware and poor coding practices that can lead to unforeseen cyber-security issues.

Software and firmware deployed on robots are often left in an accessible state for engineering maintenance and support. This could be in the form of an open USB or RJ-45 port or maybe an open wireless connection weakly protected by a manufacturer's default password. Access could be gained on the factory floor or in the deployed environment as physical security is often poor or non-existent. Traveling maintenance technicians will usually have a supporting laptop for accessing a robot and to provide diagnostics or software updates. These laptops may not be securely configured and could access other websites or resources that could provide a route in for malware or an attack.

ROBOT SOFTWARE DEVELOPMENT

There are many languages that can be used to program a robot, ranging from proprietary languages used by industrial robot manufacturers to C#, .NET (as used by the Microsoft Robotics Developer Studio), Python (as used in Robot Operating System (ROS) main client libraries) and C++.

In addition, ROS provides open source software that can be shared and propagated through the commercial and hobbyist robot community. Whilst the sharing and reuse of software code is a massive boon to developers it also means that security flaws and issues can be copied and inadvertently used repeatedly across the ecosystem. As ROS does not have any security features, by default solutions based on the platform need to be secured in other ways. Recognizing this, the development of SROS, a secure variant, is in progress.

ROBOT COMMUNICATIONS

Many robots are configured to provide communications to external parties such as a factory control system, a local ecosystem of co-robots, smartphones or a vendor's cloud hosted monitoring solution.

Remote access via a manufacturer's service box often uses wireless communications including cellular networks enabling remote access by the vendor. In some cases, this access may be without the operator's knowledge. Although undoubtedly designed to improve the customer experience, such hidden connections can present a risk that has not been captured or considered by a manufacturing plant operator.

As we have seen data confidentiality may not have been a consideration in the design of the robot, resulting in plain text, weakly encrypted or unsecured communications between systems. Data security, during an ephemeral task, may not be a major concern. In some cases, the fact that an industrial robot may have rotated 27 degrees rather than 30 degrees may not matter. What does matter is that the communication channel is insecure such that it could act as a conduit for delivering an attack on other systems or production logic could be interfered with.

On the other hand, tampering with closed-loop controls or open-loop parameters that result in a robotic arm moving from 27 degrees to 30 degrees could have a huge impact on manufacturing quality or even injure a nearby worker.

ROBOTS AND IDENTITY AND ACCESS MANAGEMENT

Identity and access management, where the correct user is given the correct access to a system at the correct time, is a key foundation of cybersecurity. Well implemented, it provides a capability for auditing and accountability for users, processes and other systems. Poor implementation of IAM could result in untrained, inexperienced operators making changes to an industrial robot that could introduce manufacturing or safety issues. This is often seen in poor practices such as sharing and displaying access credentials (username and password) on a sticky note attached to a robot, or worse, still removing all need for users to submit appropriate credentials. And of course this is not helped by poor implementation of basic access controls by manufacturers.

The use of default passwords by manufacturers, not changed when a robot has been installed, will often provide an easy route for attackers.

With the growth in Internet of Things (IoT – the myriad of devices and hardware that connects to the internet) hackers have already corralled devices into a „botnet", something that could have been largely prevented by forcing users to change the default administration password on setup (Newman, 2016).

DATA PRIVACY AND ROBOTS

Industrial robots are unlikely to contain personal data. In contrast with the growing interest in robots for medical care and surgery, it is inevitable that these devices will process personal and sensitive data such as health-related details. In most jurisdictions both personal and healthcare data is protected under local, national or sector specific laws due to their sensitive nature. Special attention will need to be paid by manufacturers and users of this equipment to ensure they do not breach patient confidentiality requirements. In some countries such robot manufacturers would not be able to enroll into nationalized healthcare networks, share patient data or provide a service until they meet stringent information security requirements.

SAFE DISPOSAL AND RECYCLING

Disposal of industrial robots or control equipment that contain sensitive data should be thought through. During robot decommissioning any resident non-volatile memory should be destroyed or forensically overwritten in cases where such sensitive data may be present and the risk warrants it. Simply deleting such data will not provide an effective defence against criminals who can easily recover this data for their own use. G-code (a numerical control (NC) programming language) left on a decommissioned robot may tell a competitor something about a process used by the previous owner.

FUNCTIONAL SAFETY AND ROBOTICS

The worlds of functional safety, robots and cybersecurity are now inextricably linked as an industrial robot can no longer be deemed safe if it is not secure. But how does functional safety compare to cybersecurity?

- Functional safety is the defence against random and systematic technical failure to protect life and the environment.
- Cybersecurity is the defence against negligent and willful actions to protect devices, facilities and data.

Industrial robots are often physically separated in a cage or work cell, away from their human co-workers. Protected by various safety interlocks, such cages provide a physical or light curtain safety barrier between humans and machines. The development of collaborative industrial robots (co-bots) has seen this separation diminish, increasing the chances of safety failings directly resulting in worker injuries. For example, if a robot work cell uses software to implement a cage safety zone, then this could be tampered with to impact its operation. In 2015, a worker entered a robot safety cage in a car manufacturing plant and was killed (Byrant, 2015).

Service and medical robots are normally in close proximity to their human operators or human clients and patients. The need for exceptional functional safety in these cases is necessarily paramount.

A robot that meets an appropriate safety integrity level (SIL) due to a rigorous functional safety design and implementation could still be compromised by a cyber attack or negligent actions. Industrial robot control systems may be well designed and implemented, but if the controller is not secured using basic measures, it could be tampered with or runtime control loop parameters could be altered, potentially resulting in safety measures being bypassed.

ANALYSIS OF CYBERSECURITY – THREATS

Unlike threats to safety, cybersecurity threats are developing, evolving and morphing continuously. In this context, a threat is anything – either originating from a technical software bug or human criminal gang – that can compromise the availability and safety of an industrial robot system. As hackers of all types take an increased interest in robotics, these threats need to be understood and then processed in a way that identifies the most important issues based on their risk to the business.

This is cyberthreat analysis and for many operating in the world of industrial robotics, as either a vendor or operator, could be a major change to the way they manage business related risk.

Most cyberthreat analysis processes include many steps. Initially, a scope is established that defines what information is needed to improve an understanding of threats. For example, is there a particular make of robot that is deployed in a plant? If so, threats to these would be of interest. Data can then be collected from a variety of places including open source information on industry and government security forums. This data then needs to be analyzed to further draw out relevant information that impacts business risk.

Tying together disparate snippets of data to produce actionable threat intelligence can be complex but will help identify areas that the business needs to act upon. It is only by efficiently and effectively processing threat data that cost effective and proportionate action can be taken to protect an industrial robot.

The NIST Cybersecurity Framework (CSF) is based on 5 areas of functionality: Identify, Protect, Detect, Respond and Recover. It was originally created for industrial control systems and critical national infrastructures but provides a model to understand the contextual risk of using a process or system such as a robot. It enables the overall risk, governance and compliance model to be viewed (i.e. the overall factory/company/deployed security posture) as well as addressing issues such as how a security incident could be managed, such as in the case of IP theft.

Manufacturers should consider providing a Risk Traceability Matrix to customers and integrators to provide transparency about the threats that were (and were not) considered. The integrator or operator can then position additional layered controls that address threats in the use context of the industrial robot.

SAFETY AND SECURITY TESTING OF AN INDUSTRIAL ROBOT

As seen, it is no longer possible for a complex electro-mechanical system such as an industrial robot to be considered safe if appropriate controls have not been implemented to ensure that it is suitably secured against cyber risk.

The generic standard for functional safety, IEC 61508:2010, states that:

- "If the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out."(7.4.2.3)

In addition:

- "If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements."(7.5.2.2)

The standard further goes on to recommend using the guidance given in the IEC 62443 series.

IEC 62443 (previously ANSI/ISA-99) is a set of standards that relates to procedures for securing industrial control systems and can be equally applied to industrial robots. The guidance is applicable to those that create products, integrate systems and run industrial control systems and robotics.

Within IEC 62443 there are seven foundational requirements (FR):

- FR 1 Identification and authentication control (IAC). Protect the device by verifying the identity of and authenticating any user requesting access;
- FR 2 User control. Protect against unauthorized actions on the device resources by verifying that the necessary privileges have been granted before allowing a user to perform the actions;
- FR 3 System integrity. Ensure the integrity of the application to prevent unauthorized manipulation;
- FR 4 Data confidentiality. Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure;
- FR 5 Restricted data flow. Segment the control system via zones and conduits to limit the unnecessary flow of data;
- FR 6 Timely response to events. Respond to security violations by notifying the proper authority, reporting required evidence of the violation and taking timely corrective action when incidents are discovered; and
- FR 7 Resource availability. Ensure the availability of the application or device against the degradation or denial of essential services.

If properly addressed, these requirements will reduce many cybersecurity risks across an industrial robot system. An industrial robot can be tested against the foundational requirements of IEC 62443-3-3. A security level (SL) can then be applied to the system, based on the following definitions:

- SL 1 - Protection against casual or coincidental violation
- SL 2 - Protection against intentional violation using simple means
- SL 3 - Protection against intentional violation using sophisticated means
- SL4 - Protection against intentional violation using sophisticated means with extended resources

Level 4 requires significant investment to prevent a nation state actor type attack, something that may not be considered proportionate in most industrial robot settings.

TÜV Rheinland suggests that the best approach is to design in safety and security at the initial development of an industrial robot. For product testing a combination of traditional vulnerability and penetration testing with those tests for IEC 62443-3-3 will likely provide the best level of coverage. These tests will additionally cover issues such as outdated software components, use of poor authentication or default credentials, poor transport encryption using outdated cryptographic techniques, insecure web interfaces and poor software protection.

YOUR ACTIONS

Industrial robot manufacturers and operators need to review the cybersecurity risks of their products based on the function, performance and context in which they are used.

Once reviewed, a set of proportionate controls should be implemented so that risks are reduced to an acceptable level. By undertaking this process, manufacturers are able to continue product research, development and innovation with the knowledge that such risk has been managed.

Manufacturers should undertake a:

- Review of robot security design
- Hazard analysis and threat modeling
- Creation of a Traceability Risk Matrix
- Secure code review
- Penetration and dynamic test to identify vulnerabilities
- Review of components for potential cybersecurity weaknesses
- Review of appropriate key security controls

- Security incident response plan review
- Legal and regulatory assessment
- Software update and patch process review
- Review of vulnerable design intersections within the device architecture

Industrial robot systems integrators face the complex task of integrating complex robotic systems in a production, manufacturing or process plant. A systems integrator linking together insecure industrial robots can compound any cybersecurity issues manyfold, as risks multiply across multiple platforms. Systems integrators need to understand the security risks of their products and work with manufacturers to reduce such risks in a deployed facility.

Integrators should undertake a:

- Review of vulnerable design intersections within the system architecture
- Review of the device source code across the system
- Development of a Traceability Risk Matrix
- Secure code review of other associated systems
- Penetration and dynamic test to identify software vulnerabilities
- Review of other components for potential cybersecurity weaknesses.
- Review of and suggest appropriate security controls

Operators need to ensure that their production plant robots are configured in a way to address cyber risks. Other systems will need to interact with a production or processing plant, therefore a holistic approach should be taken, as each implementation is likely to be highly customized with a special set of cybersecurity risks. A cybersecurity risk assessment of the plant along with any robot systems should be undertaken on a regular basis, dependent on the nature and type of work being performed.

Operators should:

- Develop a security incident response plan
- Review software update and patch management processes
- Undertake a cybersecurity risk review of the plant facility and review vulnerable design intersections

CONCLUSION

We have seen that industrial robots can bring significant productivity gains and cost savings. New and emerging cyber-related threats give manufacturers, integrators and robot operators a new set of challenges to confront. By using a cyber threat driven risk-based approach to these issues it is possible to ensure the successful growth of a business that is safe, secure and profitable.

BIBLIOGRAPHY

Byrant, C. (July 1, 2015). Worker at Volkswagen plant killed in robot accident. Retrieved from Financial Times: https://www.ft.com/content/0c8034a6-200f-11e5-aa5a-398b2169cf79

Control Engineering Europe. (September 11, 2011). iPhone used to program and control industrial robot. Retrieved from Control Engineering Europe: http://www.controlengeurope.com/article/44966/iPhone-used-to-programme-and-control-industrial-robot.aspx

European Robotics Association. (April 26, 2017). Definition of Robot (industrial and service) according to ISO-Standard 8373:2012. Retrieved from Eu-nited.net: http://www.eu-nited.net/robotics/market/introduction/index.html

Hagerty, J. R. (June 2, 2015). Meet the New Generation of Robots for Manufacturing. Retrieved from Wall Street Journal: https://www.wsj.com/articles/meet-the-new-generation-of-robots-for-manufacturing-1433300884

Mark W. Spong, S. H. (2004). Robot Dynamics and Control. In S. H. Mark W. Spong, Robot Dynamics and Control. smpp.northwestern.edu/savedLiterature/Spong_Textbook.pdf.

Morante, S. (September 29, 2015). Cryptobotics: why robots need cyber safety. Retrieved from Frontiers in Robotics and AI: http://journal.frontiersin.org/article/10.3389/frobt.2015.00023/full

Newman, L. H. (December 9, 2016). The Botnet That Broke the Internet Isn't Going Away. Retrieved from Wired.com: https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

Virk, G. S. (April 26, 2017). CHALLENGES OF THE CHANGING ROBOT MARKETS. Retrieved from Nist.gov: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913708

Appendix 1 Industrial robot threat actors

Threat actors have a range of motivations for attacking a robot or robot installation. Many of these motivations don't differ from those of attackers targeting other systems, be they corporate IT or operational technology/industrial Internet of Things.

THREAT GROUP	MOTIVATION	OBJECTIVE
Disgruntled employees	▪ Get back at an employer ▪ Show the employer up in a bad light ▪ Steal data for use in a new job	▪ Damage employer reputation ▪ Deliver a "what they deserve" message to an employer ▪ Delay a production line
Criminals	▪ Financial gain	▪ Insert ransomware that could impact production ▪ Steal financial and transactional data
Opportunists and cyber hacker wannabes	▪ The challenge ▪ „Fun" of an attack	▪ To prove they can access a „secure" site ▪ Bragging rights/bravado
Nation states	▪ Political gain ▪ Advance national technology capability ▪ Espionage ▪ Prepare the „intelligent battlefield" for possible future conflicts	▪ Get intellectual property (plans, processes, methods,…) ▪ Target individuals for blackmail ▪ Stop or reduce the effectiveness of a process or manufacturing plant ▪ Infiltrate a supply chain

In addition, there is always the potential for accidental data loss via incompetent/non-malicious means such as lost or stolen employee laptops and memory sticks.

Appendix 2 Selected key standards in industrial robotics

STANDARD REFERENCE	STANDARD NAME	APPLICABLE ROBOTIC DOMAIN	COMMENTS
ISO 10218-1:2011	Robots and robotic devices -- Safety requirements for industrial robots -- Part 1: Robots	Industrial robots	Specifies requirements and guidelines for the inherent safe design, protective measures and information for use of industrial robots. It describes basic hazards associated with robots and provides requirements to eliminate, or adequately reduce, the risks associated with these hazards.
ISO 10218-2:2011	Robots and robotic devices -- Safety requirements for industrial robots -- Part 2: Robot systems and integration	Industrial robots	Specifies safety requirements for the integration of industrial robots and industrial robot systems as defined in ISO 10218-1, and industrial robot cell(s).
ISO/TS 15066	Robots and robotic devices -- Collaborative robots	Collaborative industrial robots	Specifies safety requirements for collaborative industrial robot systems and the work environment, and supplements the requirements and guidance on collaborative industrial robot operation given in ISO 10218-1 and ISO 10218-2.
ISO/NP TR 20218-1	Robots and robotic devices -- Safety requirements for industrial robots -- Part 1: Industrial robot system end of arm tooling (end-effector)	Industrial robots	Under development
ISO 8373:2012	Robots and robotic devices -- Vocabulary	Industrial and non-industrial robots	Defines terms used in relation to robots and robotic devices operating in both industrial and non-industrial environments.
ANSI/RIA R15. 06-2012		Industrial robots	An adoption of ISO 10218:2011 Parts 1 and 2, provides industry with guidance on the proper use of the safety features embedded into robots, as well as how to safely integrate robots into factories and work areas.

Appendix 3 Other standards of interest

STANDARD REFERENCE	STANDARD NAME	APPLICABLE ROBOTIC DOMAIN	COMMENTS
IEC 61508	Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems	Functional Safety	Basic functional safety standard applicable to all kinds of industry
IEC 62443	Industrial network and system security	Industrial systems including robots	Provides a set of foundational requirements to address cyber-security risks

About TÜV Rheinland.

Safety and quality in almost all areas of business and life: That's what TÜV Rheinland stands for. With more than 20,000 employees and annual sales of 2 billion euros, the company, which was founded around 150 years ago, is one of the world's leading testing service providers. TÜV Rheinland's highly qualified experts test technical systems and products around the globe, support innovations in technology and business, train people in numerous professions and certify management systems in accordance with international standards. In this way, the independent experts ensure trust along global flows of goods and value chains. Since 2006, TÜV Rheinland has been a member of the United Nations Global Compact for more sustainability and against corruption.

Our services portfolio spans innovative solutions for digitalization with smart data, critical infrastructure and connected solutions delivered by highly experienced consultants. Our approach to cybersecurity solutions offers a unique fusion of security, privacy and safety in an increasingly more vulnerable world of interconnected cyber-physical systems and devices, with pragmatic solutions for mastering enterprise risk, analytics-based threat detection, automated and manual cybersecurity testing, industrial security, IoT data privacy, and secure cloud infrastructures.

With a team of nearly 1,000 consultants around the globe, we deliver advisory, consulting, testing and managed services to our clients across all industry segments as well as public safety authorities, government organizations and public institutions. TÜV Rheinland runs a worldwide network of more than 100 advanced testing laboratories offering our clients a one-stop-shop for all their testing needs from product safety to cybersecurity and privacy protection.

We help enterprises with:

- Managing cybersecurity risks.
- Planning for IT optimization initiatives.
- Shifting computing to virtual and cloud based infrastructures.
- Developing next generation applications and data centers requiring next generation security and application security.
- Managing and securing the proliferation of BYOD and mobile devices.
- Compliance and mitigating risk across the organization.
- Developing highly functioning IT organizations while reducing costs.

For more information about TÜV Rheinland, please visit www.tuv.com

For more information about OpenSky, please visit www.openskycorp.com

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne
service@i-sec.tuv.com

www.tuv.com/fscs

TÜVRheinland®
Precisely Right.