Whitepaper
Industrial Security
based on IEC 62443

TÜViT

TÜV NORD GROUP

Contents

List of Abbreviations 1

Terms & Definitions 2

1. Introduction to Industrial Control Systems Security 4

2. Purpose of this document 7

3. The standard IEC 62443 8

3.1. Structure of IEC 62443 8
3.2. Roles and Scope of IEC 62443 in ICS 10
3.3. Concepts used in IEC 62443 11
3.3.1. Defense-in Depth 11
3.3.2. Zones and Conduits 12
3.3.3. Cybersecurity Life Cycle for IACS using PDCA 14
3.3.4. Security Levels on the basis IEC 62443 3-3 and IEC 624434-2 16
3.3.5. Maturity Levels on the basis of IEC 62443 2-4 and IEC 62443 4-1 17

4. Project Process and Certification 18

Table of Figures 20

Reference 21

5. About TÜViT 22

6. Contact 25

List of Abbreviations

ACL	Access Control List
CR	Component Requirements
DAkkS	German Accreditation Body
DCS	Distributed Control Systems
DMZ	Demilitarized Zone
ESD	Emergency Shutdown System
ES	Engineering Station
FR	Foundational Requirements
FTP	File Transfer Protocol
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commsssion
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ML	Maturity Level
OS	Operator Station
PDCA	Plan Do Check Act
PLC	Programmable Logic Controller
RE	Requirement Enhancement
SCADA	Supervisory Control and Data Acquisition
SR	System Requirements
SL	Security Level
TCP	Transmission Control Protocol
VPN	Virtual Private Network

Terms & Definitions

Asset Owner	An individual or a company owning a physical or a logical object having either a perceived or actual value to Industrial Automation Control system
Attack	Assault on a system that derives from an intelligent act as a deliberate attempt to evade security services and violate the security policy of a system
Authentication	Security measure designed to verify the identity of a user, process or device often as prerequisite to allow access to resource of an information.
Automation Systems	Control systems e.g. DCS, SCADA which are used to operate machines e.g. boilers, turbines and instruments e.g. sensors, pressure transmitters in a plant with minimum human effort.
Authorization	Right or a permission that is granted to a system entity to have access to a system.
Availability	Property of ensuring timely and reliable access and use of control system information and functionality
Component Requirement	Component Requirements are the requirements defined in the standard IEC 62443 that IACS components have to fulfill to attain highest possible security.
Confidentiality	Protection of IACS data and information from an unauthorized access.
Demilitarized Zone	A perimeter network segment that is logically between internal and external networks for controlling data flow between the networks.
Firewall	Inter-network connection device that restricts data communication traffic between two connected networks
Foundational Requirement	Foundational Requirement are the requirements defined in the standard IEC 62443 that every IACS system or component must fulfill to attain security.
Host	Computer that attached to a communication subnetwork or inter-network and can use services provided by the network to exchange data with the other attached systems.
Industrial Automation and Control System	Collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can effect or influence its safe, secure and reliable operation.
Integrity	Measure of assuring the accuracy, consistency and availability of information.
Information	An asset, which is important for an organization’s business. Information can be in digital form, paper form or information can also be in the form of knowledge of organization’s employee.

Maturity Level	Maturity levels are the levels that defines the benchmark, which are required to be met by the requirements defined in the standard IEC 62443.
Product Supplier	Manufacturer of hardware and/or software product
Security gateway	A security relay mechanism that attached two or more computer networks that have similar functions but dissimilar implementation and that enable host computers on one network to communicate with hosts on the other network.
Security Level	Measure of confidence that IACS is free from vulnerabilities and functions in the intended manner.
Service Provider	Organization (internal or external, manufacturer etc.) that has agreed to undertake responsibility for providing a given support service and obtaining, when specified, supplies in accordance with an agreement.
System Integrator	A person or a company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications.
System Requirement	System requirements are the requirements defined in the standard IEC 62443 that IACS system has to fulfill to attain highest possible security.
Vulnerability	Weakness in a system function, procedure, internal control or implementation that could be exploited or triggered by a threat source, intentionally designed into computer components or accidently inserted at any time during its lifecycle.

1. Introduction to Industrial Control Systems Security

Critical infrastructures are becoming a potential target of cyber-attacks as they increasingly connect with other networks. Manufacturers and operators of popular SCADA systems and Industrial Automation and Control Systems report increasing cases of cyber-attacks on their systems. The reason behind this is the more popular a system, the more lucrative the attack is, as it can often be reused.

Interlinking of the enterprise network with the production network and integrating the process control networks with web technologies such as Ethernet and TCP/IP have increased the need for the security in the Industrial Automation Control System (IACS). This cross connection makes the critical system in the process control network open to the vulnerabilities and exploitation of these vulnerabilities (a cyber-attack) can cause the whole system shut down and even affect the safety of the environment. There are several key differences with respect to the security between the traditional IT security environment and IACS security environment as shown in the Table 1.

Security Topic	Office IT Systems	IACS Systems
Antivirus	Widely used and easily updated	complicated and often impossible to implement
Life Cycle	3-5 Years	5-20 Years
Awareness	Good	Not good
Patch Management	Often	Rare, approval from Plant manufacturers
Change Management	Regular and scheduled	Rare
Evaluation of log files	Established practice	Unusual practice
Time Dependency	Delays Accepted	Critical
Availability	Not always available, failures accepted	24*7
IT Security Awareness	Good	Poor
Security tests	Widespread	Rare and problematic
Testing environment	Available	Rarely available

Table 1: Differences between Traditional IT Security and IACS Security

Because of the unusual, rare and poor practice of different measures in the IACS systems as shown in the Table 1 as compared with Traditional IT System, security in IACS environment is challenging as well as important. The security in the IACS is considered to be securing the industrial plants from unauthorized physical and digital attack. The attack in the IACS can be with criminal and intentional motive or through the negligible (unintentional) behavior from an employee, for example when an employee tries to format the plant system during the production process and loses the important data. The objective of the Information security is to fulfill three security objectives i.e. Confidentiality, Integrity and Availability. In IACS, Availability is given the top priority followed by Integrity and Confidentiality. “Confidentiality is given lesser importance because often the data is in raw form and need to be analyzed within context to have any value.” It should be ensured that even during a cyber-attack the production runs although irrespective of an attack or a failure in the system.

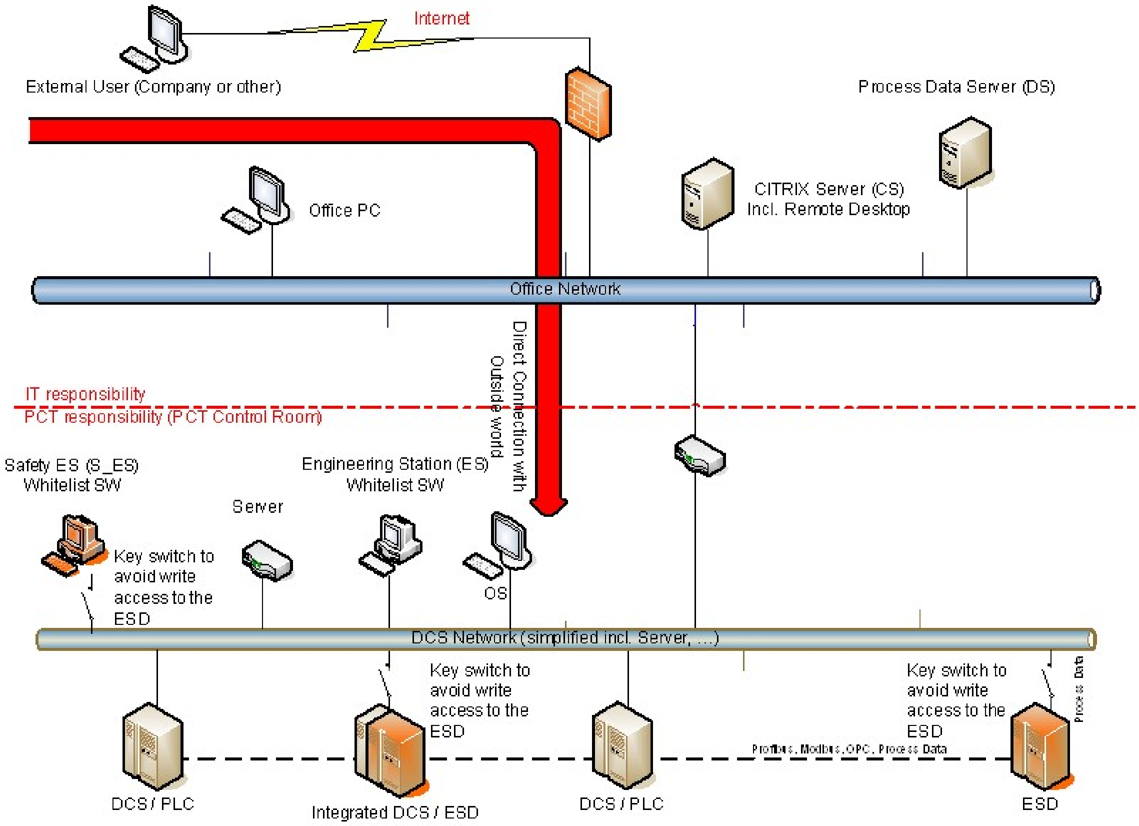


Figure 1: Threat in ICS Network

Figure 1 describes a general architecture of the IACS with division of office network and IACS network. The interconnection between the office network and the IACS network shows how vulnerable (without the security measures) are the critical control systems when interlinked with the office network and connected to the open world (internet).

In the office network, the standard for protecting the information against unauthorized access and unauthorized use is already in practice in the form ISO 27000 series. In IACS network IEC 62443 concentrates on the protection of IACS information, devices and systems.

2. Purpose of this document

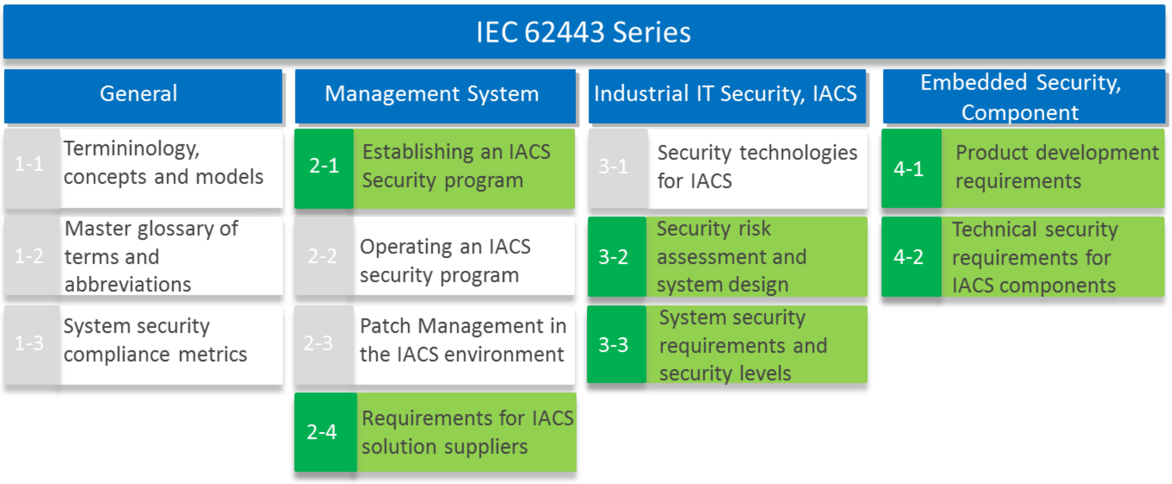
This whitepaper gives a brief explanation about the usage of IEC 62443 in process control and automated systems. The purpose of the whitepaper is to provide a basic understanding about the IEC 62443 standard. The key features in the whitepaper are the different parts of the standard, which focusses on the three major roles in Process Industry i.e. Product Supplier, Integrator and Asset Owner. The basic understanding, implementation and the certification process of the standard are also explained in this whitepaper.

3. The standard IEC 62443

IEC 62443 deals with security of the industrial control system, popularly known as the “Industrial Automation and Control System”. The term IACS includes control systems used in the manufacturing and processing facilities, geographically distributed operations such as electricity, gas and water using automated, remote controlled or monitored assets. The aim of the standard is to ensure that a product supplier, integrator or an asset owner follows an efficient method for secured process with a key aspect on safety of the personnel and the production, availability, efficiency and quality of the production of the IACS as well as the safety of the environment.

3.1. Structure of IEC 62443

IEC 62443 standard family is divided into four parts i.e. General, Management System (policies and procedures), Industrial IT Security, IACS (System requirements) and Embedded Security, Component as shown in the Figure 2.



IEC 62443 Series

General	Management System	Industrial IT Security, IACS	Embedded Security, Component
1-1 Termininology, concepts and models	2-1 Establishing an IACS Security program	3-1 Security technologies for IACS	4-1 Product development requirements
1-2 Master glossary of terms and abbreviations	2-2 Operating an IACS security program	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch Management in the IACS environment	3-3 System security requirements and security levels	
	2-4 Requirements for IACS solution suppliers		

Figure 2: IEC 62443 Series

General: explains the basic terminologies, concepts, and abbreviations used in the series.

- Standard 62443-1-1 presents the concepts and models of the series.
    - The technical report 62443-1-2 contains a glossary of terms and abbreviations used throughout the series.
    - The standard 62443-1-3 describes a series of metrics derived from the basic requirements (FR) and system requirements (SR).
- Management System (Policies and procedures): describes the policies and procedures that are required and used to implement a cyber-security management system.
    - Standard 62443-2-1 describes what is required to define and implement an effective IACS Cyber Security Management System. This standard is aligned with the ISO 27000 series.
    - The standard 62443-2-2 provides specific guidance on what is required to operate an effective IACS Cyber Security Management System.
    - Technical Report 62443-2-3 provides guidance on the specific topic of Patch Management for IACS.
    - Standard 62443-2-4 specifies requirements for suppliers of IACS.
- Industrial IT Security, IACS (System requirements): describes the security requirements for a system in an IACS environment.
    - The technical report 62443-3-1 describes the application for different safety technologies to an IACS environment.
    - The standard 62443-3-2 addresses the risk assessment and the system design for IACS.
    - Standard 62443-3-3 describes the basics of the security requirements and the Security Assurance level (SL).
- Embedded Security, Component (Component Requirement): describes the security requirement of a component in an IACS environment.
    - Standard 62443-4-1 describes requirements that apply to the development of products.
    - The standard 62443-4-2 contains requirements, which allow a detailed mapping of the system requirements (SR) to subsystems and components of the system under scope.

3.2. Roles and Scope of IEC 62443 in ICS

The IEC 62443 standard defines three different roles i.e.

1. The Product Supplier
2. The System Integrator and
3. The Asset Owner

These roles plays the basis for defining and connecting the different parts in series of IEC 62443 explained in the next figure:

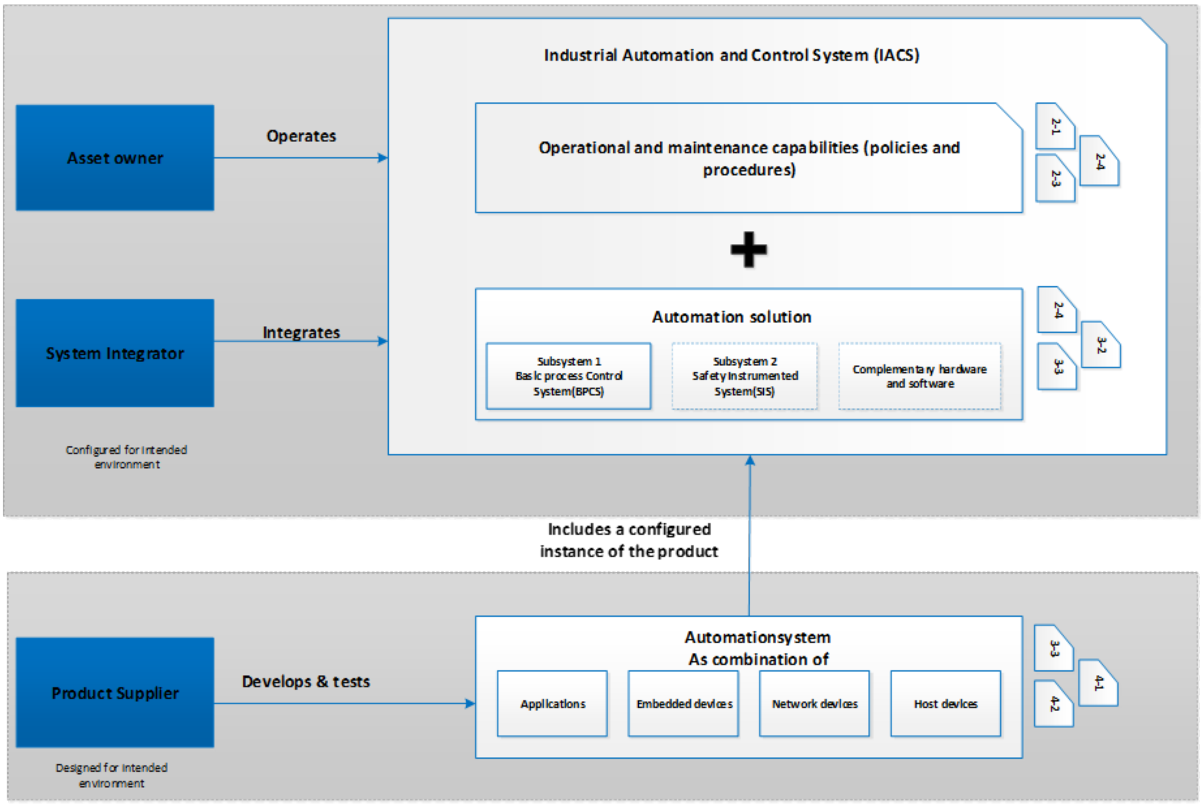

Industrial Automation and Control System (IACS)
Asset owner
Operates
Operational and maintenance capabilities (policies and procedures)
2-1
2-4
2-3
System Integrator
Integrates
Automation solution
Subsystem 1 Basic process Control System(BPCS)
Subsystem 2 Safety Instrumented System(SIS)
Complementary hardware and software
2-4
3-2
3-3
Configured for intended environment
Includes a configured instance of the product
Product Supplier
Develops & tests
Automationsystem As combination of
Applications
Embedded devices
Network devices
Host devices
3-3
4-1
4-2
Designed for intended environment

Figure 3: Roles in IEC 62443

Figure 3 illustrates how a product developed by the product supplier relates to the maintenance and an integration capability by system integrator and to its operation by the asset owner. It also illustrates the role and relationship between the product supplier, system integrator and asset owner.

The product supplier is responsible for the development and testing of the control system comprising of the application (antivirus, whitelisting etc.), embedded device (PLC, DCS etc.), network device (firewalls, routers, switches etc.), host devices (operator stations, engineering stations etc.) working together as system or a subsystem defined in IEC 62443 3-3, IEC 62443 4-1, IEC 62443 4-2.

- The system integrator is responsible for the integration and commissioning of the product into an automation solution1 using a process compliant with IEC 62443 2-4, IEC 62443 3-2, IEC 62443 3-3.
- The asset owner is responsible for the operational and maintenance capabilities with the help of the policies and procedures defined in IEC 62443 2-1, IEC 62443 2-3 and IEC 62443 2-4 of the automation system developed by installation of the automation solution at a particular site.

3.3. Concepts used in IEC 62443

3.3.1. Defense-in Depth

Defense in Depth is a layered security mechanism enhancing security of the whole system. The benefit of this mechanism is that during an attack if one layer gets affected, other layers can still hold on assisting to protect against, detect and react to as many attacks. The layers can be described as

- Data Layer is the inner most layer and can be used for ACL and encryption of data.
- Application Layer is the next layer used for installing antivirus software and application hardening.
- Host Layer is the layer after application layer and is used for the patch implementation of vulnerability detected, authentication of the users.
- Internal Network Layer is the following layer and is used for IPsec (Internet Protocol Security) for IP communications, authentication and encryption of the packet which takes part in a communication system, IDS (Intrusion Detection System) detecting the intrusion of every user (authorized or unauthorized).
- Perimeter Layer is the next layer and is used for implementing the firewalls and VPN quarantining.
- Physical Layer is the layer after perimeter layer where the useful guards, switches, locks, ports, physical access are employed.
- Policies, Procedures Layer are the outermost and the last layer where the security policies and procedures for the IACS networks are defined.

[1] “An automation solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (for example, continuous or manufacturing) as defined by the asset owner”.

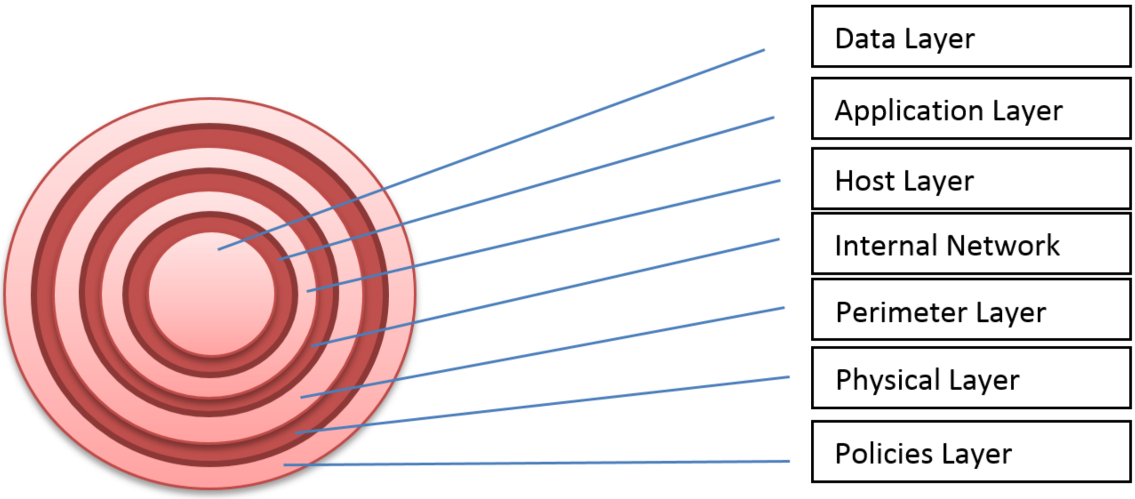


Figure 4: Defense in Depth

3.3.2. Zones and Conduits

Security zones are physical or logical grouping of assets that share common security requirements and isolating the critical control systems components. A special type of security zone is the Demilitarized Zone (DMZ), which segments the external network with the internal (IACS) network with help of security components for e.g. Firewall. This concept provides a layered security approach with "Defense- in- Depth" approach being taken into account.

"Conduits are the special type of security zone that groups communications that can be logically organized into a grouping of information flows within and also external to a zone. It can be a single service (i.e. Ethernet network) or be a multiple data carrier." [1-1]. Conduits controls the access to the zone by resisting several attacks like Denial of Service, malware attacks and protects the integrity and confidentiality of the network traffic.

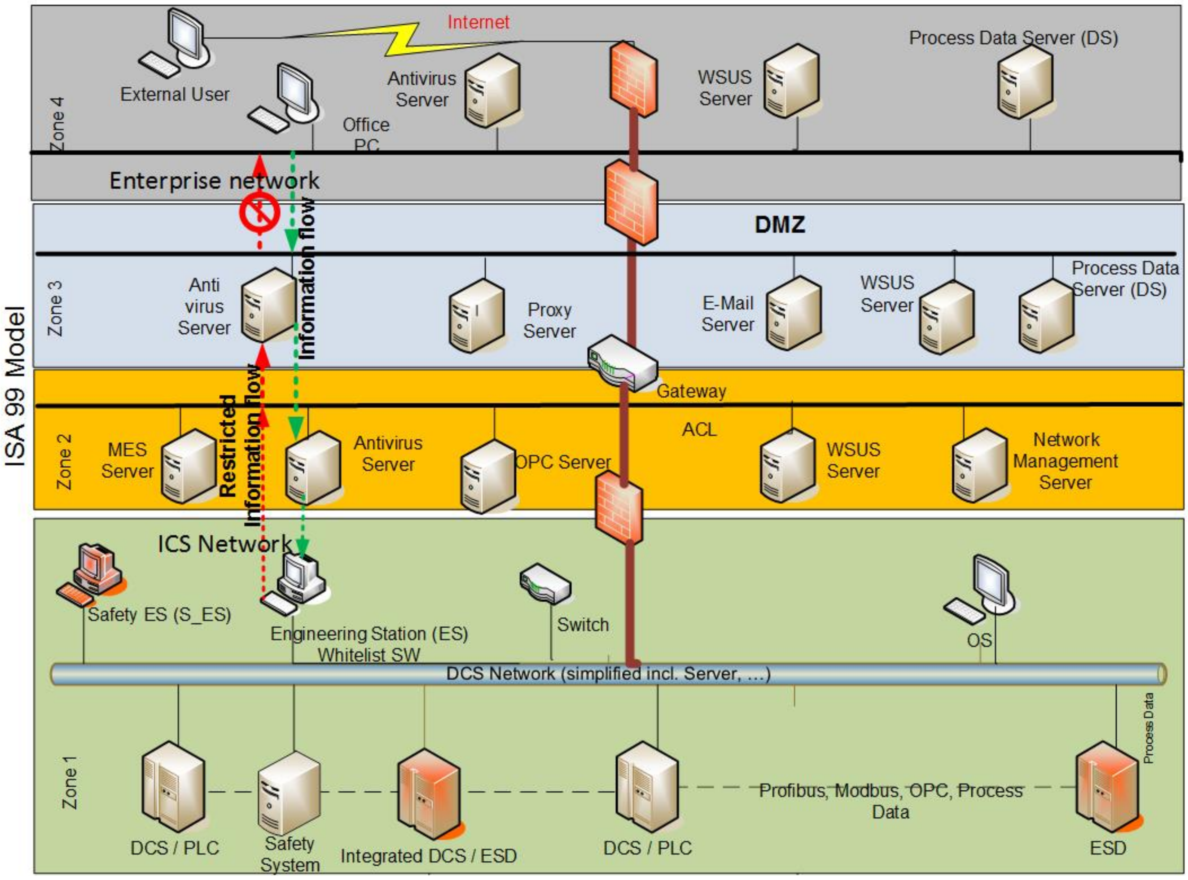


Figure 5: Zones and Conduits in ICS Architecture

Figure 5 illustrates the network architecture of an IACS network with zones and conduits. The network is segmented into four zones and each zone has a firewall or gateway protection. The zoning concept in an IACS network have to be in a such a manner that the information transfer from the enterprise network should be step wise (Zone4 to Zone3, Zone3 to Zone2, Zone2 to Zone1) process. The information can be antivirus pattern updates, patch updates etc. The flow of information from zone 1 to the other zones has to be restricted (read only function) and should be transferred only through proper authentication method. For example, process data of the production network is only transferred to a process data server in the DMZ in Zone 3. Access to the Process Data server should be limited to authorized employees.

3.3.3. Cybersecurity Life Cycle for IACS using PDCA

The Plan, Do, Check and Act method of security measure has been effectively followed in the ISO 27000 series. In IEC 62443 PDCA life cycle is based on the basic roles defined by the standard i.e. the product developer, system integrator and asset owner. The PDCA cycle includes the following step:

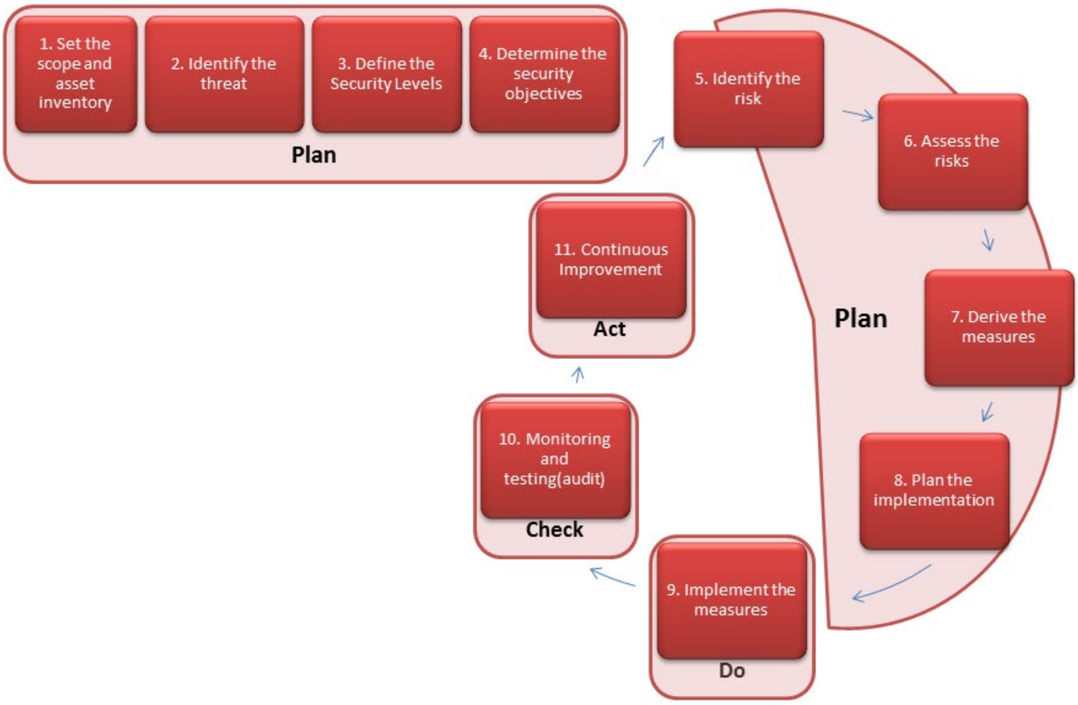

1. Set the scope and asset inventory
2. Identify the threat
3. Define the Security Levels
4. Determine the security objectives
Plan
5. Identify the risk
6. Assess the risks
7. Derive the measures
Plan
8. Plan the implementation
9. Implement the measures
Do
10. Monitoring and testing(audit)
Check
11. Continuous Improvement
Act

Figure 6: PDCA Cycle

Figure 6 illustrates the PDCA cycle that can be implemented in ICS with reference to IEC 62443. Each of the three roles defined in the standard i.e. product supplier, system integrator and asset owner have to follow the PDCA cycle. The PDCA cycle for the product supplier is the product life cycle as it is product/devices specific and for the integrator and asset owner is the plant life cycle as it concentrates on the entire plant.

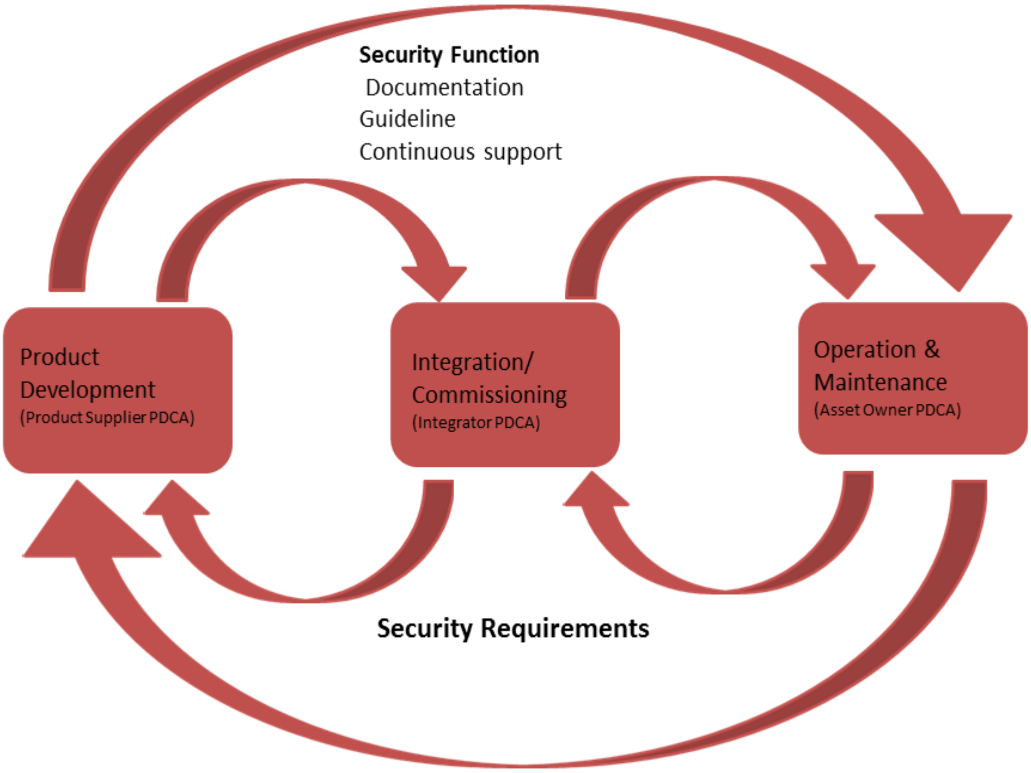


Figure 7: Products and Plant Life Cycle

Figure 7 illustrates life cycle process and the interactions of product and plant in the form of product development by product supplier, integration or commissioning by system integrator and operation and maintenance by asset owner. It is a continuous process and is fulfilled by the PDCA cycle.

3.3.4. Security Levels on the basis IEC 62443 3-3 and IEC 624434-2

Security Level (SL) concept focus on the zones of the ICS. SLs provide a frame of reference for making decisions on the use of countermeasures and devices with different inherent security capabilities. The concept can be used to select the ICS devices and countermeasures to be used within a zone and provides the ability to categorize risks for zone or conduits. The SL may also be used to identify layered Defense-in-Depth strategy for a zone that includes hardware and software base technical countermeasures. The security levels defined for components are based on the four types of device categories defines in the standard i.e. embedded device, host devices, network devices and application software. The security levels in the standard are defines as:

- SL 1- Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2- Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3- Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

Security Level	Description	Target	Skills	Motivation	Means
SL1	Capability to protect against casual or coincidental violation	Misconfiguration	No awareness	Confusion	No ojective
SL2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation	No security measures implemented, hacker	Basic	Low	Straight forward
SL3	Capability to protect against intentional violations using sophisticated means with moderate resources, IACS specific skills and moderate motivation	Only moderate security measures implemented, high level hacker	Industrial specific	Average	Intentional
SL4	Capability to protect against intentional violations using sophisticated means with extended resources, IACS specific skills and high motivation	Economical Damage	Industrial specific	High	Aggressive

Table 2: Security Levels Categorization

Table 2 shows a summary of each security level with characterization of target, skills, motivation and means of attacks that can occur in each security level

3.3.5. Maturity Levels on the basis of IEC 62443 2-4 and IEC 62443 4-1

Maturity Levels are based on the CMMI-SVC model. These levels define the benchmark which are required to be met by the requirements defined the standards IEC 62443 2-4 and IEC 62443 4-1. Each level is progressively advanced than the previous level. The service providers and the asset owners are required to identify the maturity level associated with the implementation of each requirement.

Maturity Level	Category	Description
ML 1	Initial	Capability of performing a service without a documented process that is poorly controlled
ML 2	Managed	Capability of performing a service in a formal documented characterized process with evidence of expertise and trained personnel
ML 3	Defined	Capability of performing ML2 level including evidence of practicing the process e.g. Documented process plus list of participants in the training of personnel
ML 4	Improved	Capability of performing ML3 level including demonstration of continuous improvement e.g. internal audit report

Table 3: Maturity Levels Categorization and description

Table 3 shows the summary of each maturity levels with categorization and description about each level.

4. Project Process and Certification

The certification body is a DAkkS or an international (e.g. IEC) accreditated body; testing center is approved by the certification body for the performance of tests according to IEC 62443.

If a customer is interested in testing and certification of its component or system, then the customer sends an offer request to a test center or certification body. After agreement of cost and offer between the certification and offer between the testing center and certification body, the will receive an offer from the test center about the execution of the test and a separate offer from the certification body about the certification activities, after clarifying the necessary details.

If the customer agrees with the offers, he / she submit a test order to the inspection body in the form of the acceptance of the offer and the certification body a certification order. The testing center then carries out the tests and documents its results in a certification report.

This will be forwarded to the certification body. The report is verified there and the certificate is issued if the result is positive. The certificate is handed over to the customer by the certification body.

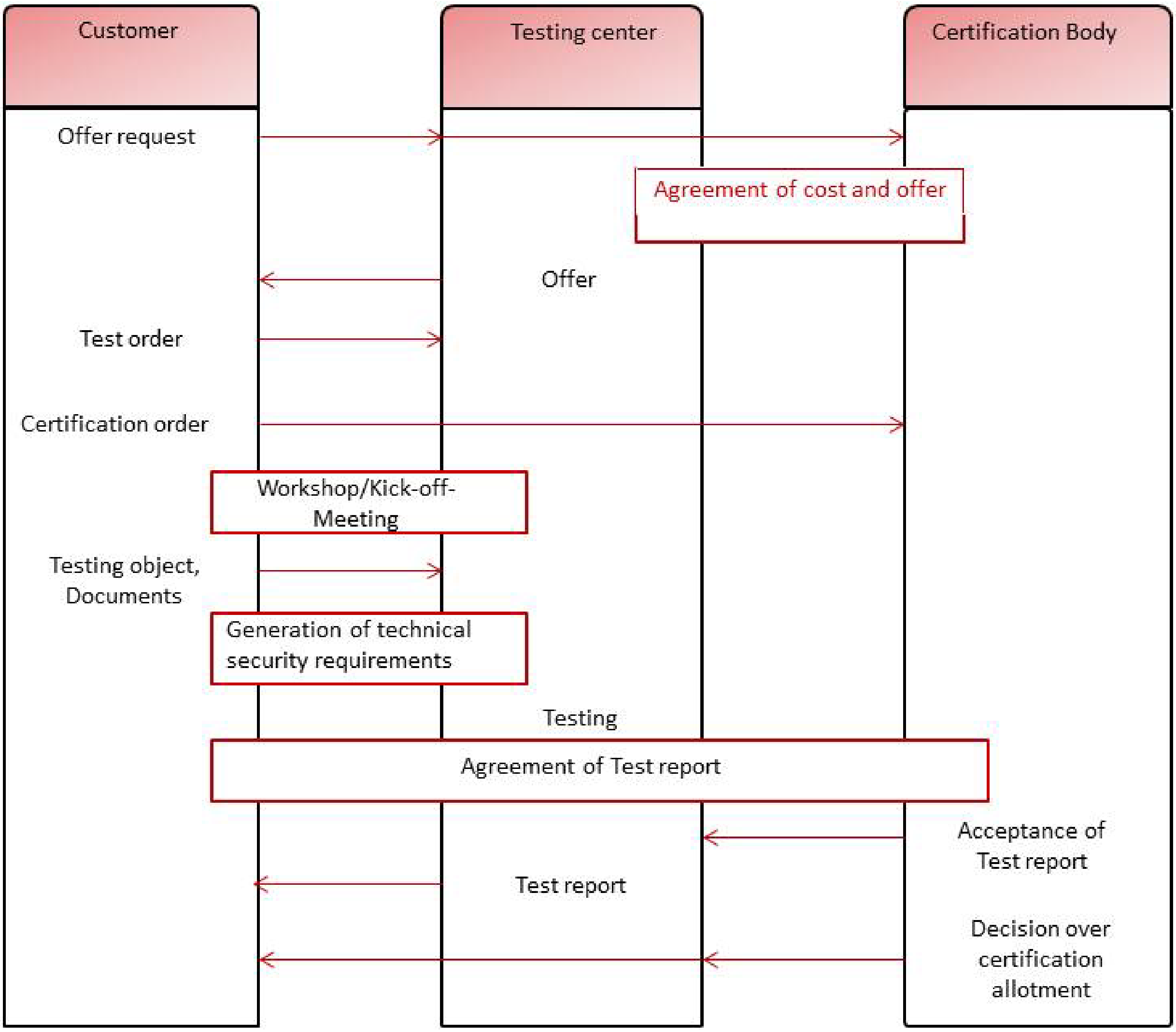

Customer
Testing center
Certification Body
Offer request
Agreement of cost and offer
Offer
Test order
Certification order
Workshop/Kick-off-Meeting
Testing object, Documents
Generation of technical security requirements
Testing
Agreement of Test report
Acceptance of Test report
Test report
Decision over certification allotment

Figure 8: Project Process in IEC 62443

Table of Figures

Figure 1: Threat in ICS Network 5
Figure 2: IEC 62443 Series 8
Figure 3: Roles in IEC 62443 10
Figure 4: Defense in Depth 12
Figure 5: Zones and Conduits in ICS Architecture 13
Figure 6: PDCA Cycle 14
Figure 7: Products and Plant Life Cycle 15
Figure 8: Project Process in IEC 62443 19

Reference

(1) IEC 62443-1-1: Industrial communication networks- Network and system security-Part 1-1: Terminology, concepts and models (IEC/TR 62443-1-1:2009)

(2) ISA- 62443-1-2: Security for industrial automation and control systems- Master Glossary, Draft 1, Edit 5, August 2014 (ISA-TR62443-1-2)

(3) ISA-62443-1-3: Security for industrial automation and control systems.- Part 1-3: Cyber security system conformance metrics, Draft 1, Edit 19, October 2015

(4) ISA-62443-2-1: Security for industrial automation and control systems- Part 2-1: Industrial automation and control system security management system, draft 7, Edit5, November 9,2015

(5) ISA-62443-2-2: Security for industrial automation and control systems: Implementation Guidance for and IACS Security Management System, Draft 1, Edit 4, April 2013

(6) IEC 62443-2-3:Security for industrial automation and control systems- Part 2-3: Patch Management inn IACS environment (IEC /TR 62443-2-3:2015)

(7) IEC 62443-2-4: Security for industrial automation and control systems-Part 2-4: Security program requirements for IACS providers (IEC 62443-2-4:2015)

(8) ISA-62443-3-2: Security for industrial automation and control systems: Security risk assessment for system design, Draft 6, Edit 3, August 5, 2015

(9) IEC 62443-3-3: Industrial communication networks- Network and system security- Part 3-3: System security requirements and security levels(IEC 62443-3-3: 2013)

(10) IEC/NP 62443-4-1 Industrial communication networks- Network and system security- part -4-1: Product development requirements based on ISA-62443-04-01, Draft 1, Edit 9, April 2013

(11) ISA-62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development life- cycle requirements Draft 3, Edit 11, March 2016

(12) ISA -62443-4-2 Security for industrial automation and control systems Technical security requirements for IACS components Draft 2, Edit 4 July 2,2015

(13) ISO/IEC 27001 Information technology- Security techniques- Information security management systems- requirements (ISO/IEC 27001:2013)

(14) ISO/IEC 27002 Information technology- Security techniques- Code of practice for information security controls(ISO/IEC 27002:2013)

(15) VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung- Blatt 1: Allgemeines Vorgehensmodell

(16) Leitfaden Industrial Security IEC 62443 einfach erklärt- Pierre Kobes (VDE Verlag 2016)

5. About TÜViT

TÜV Informationstechnik GmbH (TÜViT) was founded in 1995 and is a company of TÜV NORD GROUP, which is one of the largest technical service providers with more than 10,000 employees and business activities in 70 countries worldwide.

TÜViT is one of the leading testing service providers for IT security and is completely focused on security in information technology. Many international companies already benefit from TÜViT-tested security. The Company focuses on subjects such as cyber security, hardware and software evaluation, IoT, data protection audits, evaluation of information security management systems in accordance with ISO/IEC 27001, smart energy, mobile security, automotive security as well as eID and trust service providers. In addition, TÜViT audits and certifies data centers with regard to their physical security and high availability.

TÜViT participates actively in developing the state of technology in national and international research projects and committees.

TÜViT meets its customers' high expectations with an active and responsive quality and environmental management system certified according to ISO 9001:2015 respectively ISO 14001:2015.

Numerous accreditations and approvals by national and international organisations and public authorities prove TÜViT's competence in testing and certification.

German Federal Office for Information Security

- Recognition persuant to § 9 (3) BSIG for conducting evaluations according to ITSEC/ITSEM/CC/CEM
- Recognition persuant to § 9 (3) BSIG for conducting evaluations according to BSI-TR 01201, BSI-TR 03105 Teil 3 und Teil 5, BSI-TR 03121, BSI-TR 03132 und BSI-TR 03133
- Certified IT Security Service Provider in the specified scope of application IS-Revision and IS-Consulting, Penetrationtesting
- Licensed auditors for IT-Grundschutz and ISO/IEC 27001 on the basis of IT-Grundschutz
- Licensed auditors for De-Mail

German Accreditation Body

- Testing Laboratory for IT Quality: Competence according to DIN EN ISO/IEC 17025 for evaluations in the field of IT Security
  - Evaluation Body for IT Security: Accreditation for evaluations according to Common Criteria, ITSEC/ITSEM
- Certification Body: Competence for certifications of products in the field of IT Security (ITSEC, Common Criteria, ETSI EN 319 401 / 319 411-1 / 319 411-2 / 319 421, ETSI TS 101 456 / 102 042 / 102 023, DIN EN 50518-1:2014 / -2:2014 / -3:2014), accredited according to DIN EN ISO/IEC 17065:2013
- Certification Body: Competence for certifications of products, processes and services in accordance with EN ISO/IEC 17065:2013 and ETSI EN 319 403 V2.2.2 in the scope qualified trust service providers and the qualified trust services provided by them in the scope of application REGULATION (EU) No 910/2014 (eIDAS)

German Federal Network Agency

- Confirmation Body according to Signatures Act/Signatures Ordinance for the confirmation of products for qualified electronic signatures
- Confirmation Body according to Signatures Act/Signatures Ordinance for the confirmation of the implementation of security concepts for certification service providers

German Banking Industry Committee

- Listed Testing Body for Electronic Payment Transactions

Independent Center for Privacy Protection Schleswig-Holstein

- Test Center for Privacy (legal/technical)

European Privacy Seal (EuroPriSe)

- Legal and technical experts

TeleTrusT Deutschland e.V.

- IT Security made in Germany

Swiss Association for Quality and Management Systems SQS

- Certification according to ISO 9001:2015 (Quality Management System) and ISO 14001:2015 (Environmental Management System)

Information-technology Promotion Agency, Japan

- IT Security Evaluation Facility: Competence for evaluations according to CC/CEM

National Institute of Technology and Evaluation, Japan

- Evaluation Body for IT Security: Accreditation according to DIN EN ISO/IEC 17025 in the field of IT / Common Criteria evaluations (Lab Code: ASNITE0019T)

National Institute of Standards and Technology, USA
National Voluntary Laboratory Accreditation Program, USA

- Evaluation Body for IT Security (NVLAP Lab Code: 200636-0) for Cryptographic Module Testing (scopes 17BCS, 17CAV/01, 17CMH1/01, 17CMH1/02, 17CMH2/01, 17CMH2/02, 17CMS1/01, 17CMS1/02, 17CMS2/01, 17CMS2/02) and Biometrics Testing

Europay, MasterCard and Visa, USA/United Kingdom/Japan

- Full Service Laboratory for evaluations of ICs and IC cards according to EMVCo Security Guidelines
- Modular Label Auditor

Visa, USA

- Test House for performing Visa Chip Product security evaluations

MasterCard, United Kingdom

- Accredited to perform CAST (Compliance Assessment and Security Testing) evaluations

Betaalvereniging Nederland, The Netherlands

- Evaluation Laboratory

6. Contact

Michelle Michael

TÜV Informationstechnik GmbH

TÜV NORD GROUP

Langemarckstraße 20

45141 Essen

Tel.: +49 201 8999-629

Fax: +49 201 8999-666

m.michael@tuvit.de

www.tuvit.de