



Mehr Sicherheit.
Mehr Wert.

Security for Safety in der Industrieautomation

Konzepte und Lösungsansätze
des IEC 62443

**Roadshow
INDUSTRIAL IT SECURITY**

Dr. Thomas Störtkuhl
18. Juni 2013



Einführung: Standard IEC 62443

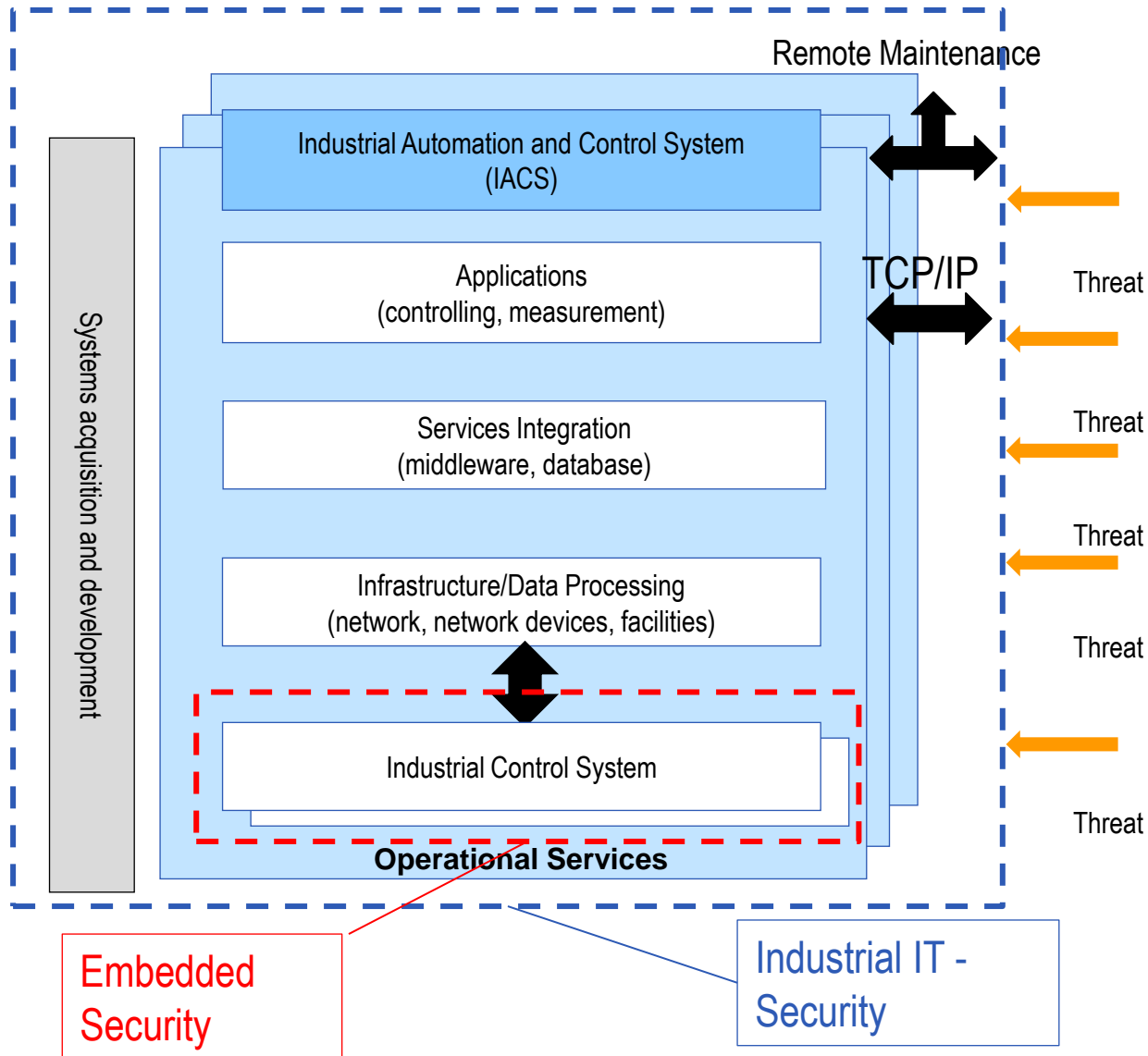
Konzepte und Lösungsansätze

**IEC 62443: Cyber Security
Management System**



industrial automation and control systems IACS

collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process



Documents of the IEC 62443 series

Basis	Management System	Industrial IT Security, IACS	Embedded Security, Component
1-1 Terminology, concepts and models	2-1 Establishing an IACS	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 assurance levels for zones and conduits	4-2 Technical security requirements for IACS products
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security assurance levels	

veröffentlicht
 in Arbeit

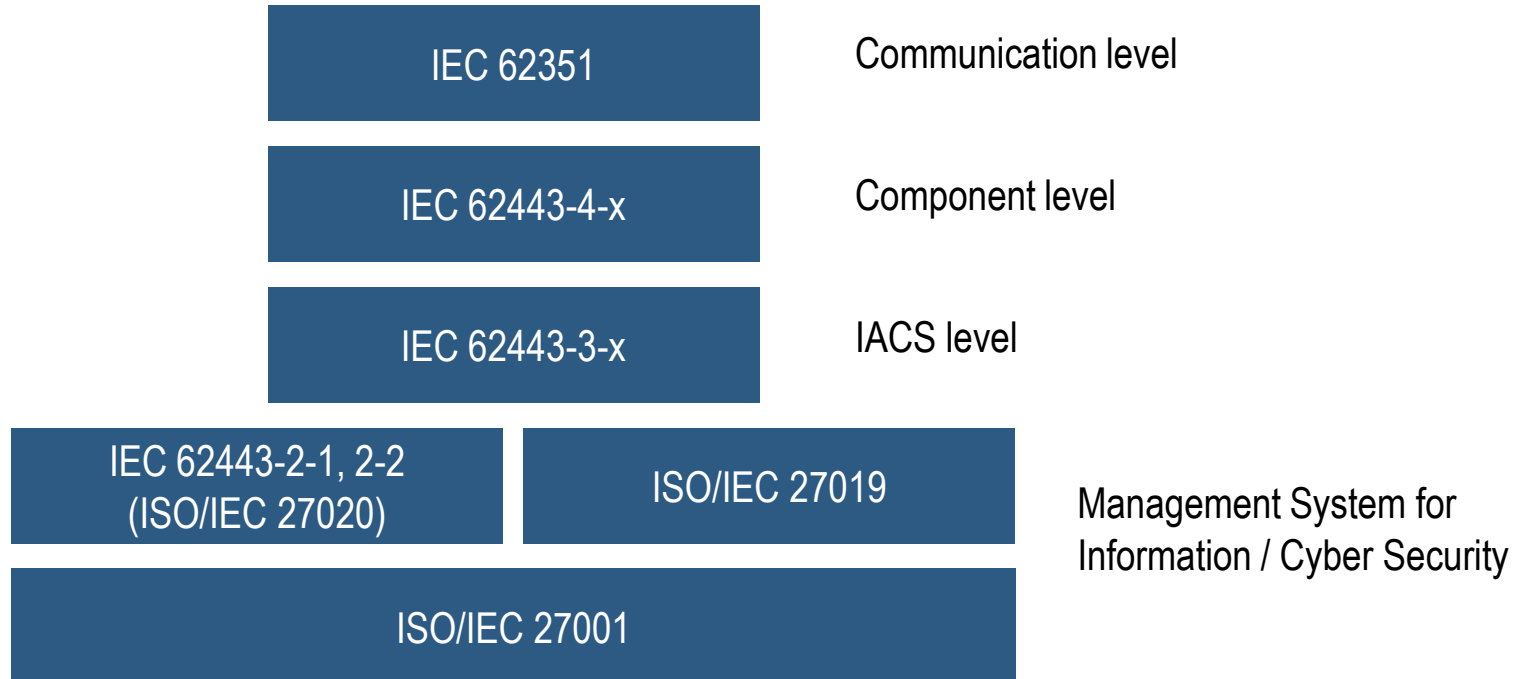
Documents of the IEC 62443 series			
Basis	Management System	Industrial IT Security, IACS	Security, IACS
1-1 Terminology, concepts and models	2-1 Establishing an IACS	3-1 Security technologies for IACS	4-1 Security development requirements
1-2 Master glossary of terms and abbreviations	2-2 Operating an IACS security program	3-2 Security assurance levels for zones and conduits	4-2 Technical security requirements for IACS products
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security assurance levels	

wird ISO 27020 werden

- veröffentlicht
- in Arbeit
- im Umbruch



- IEC 62443 Security for Industrial Process Measurement and Control – Network and System Security
- IEC 62351 Power systems management and associated information exchange – Data and communications security
- ISO 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements
- VDI/VDE 2182 Informationssicherheit in der industriellen Automatisierung
- ISA S99 Manufacturing and Control System Security
- NIST, Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, June 2011
- BDEW Whitepaper (wird ISO/IEC 27009 werden)

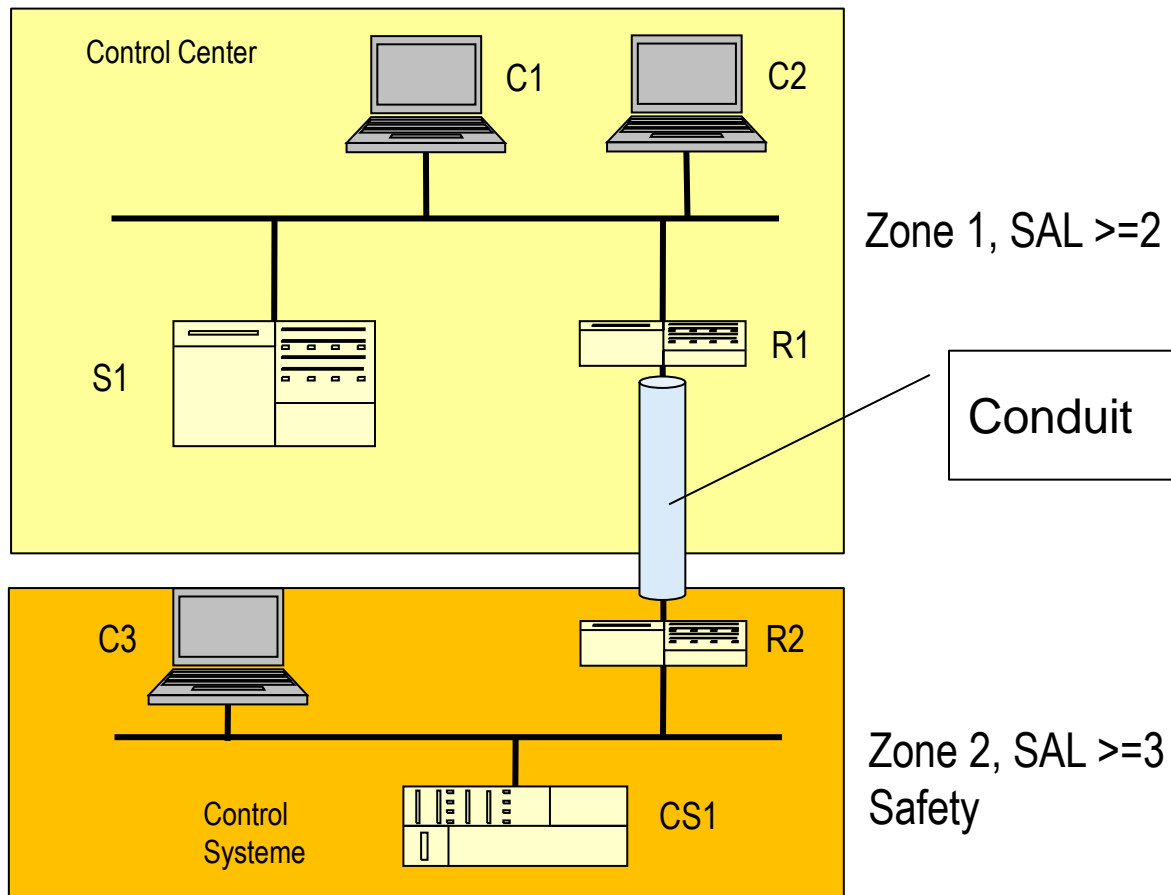




Definitionen der SALs

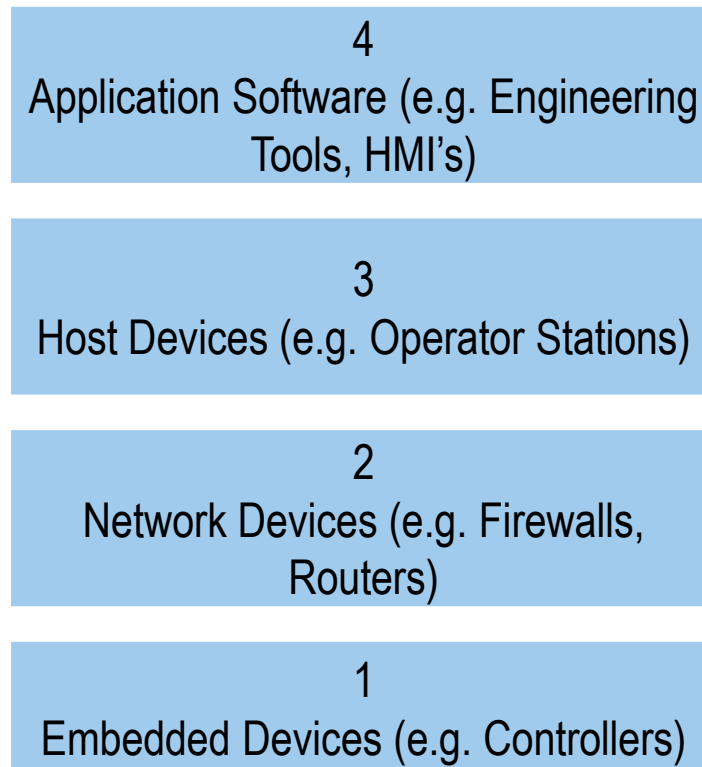
- SAL 1: Protection against casual or coincidental violation
- SAL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation
- SAL 3: Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation
- SAL 4: Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation

Konzept: **zones** und **conduits**

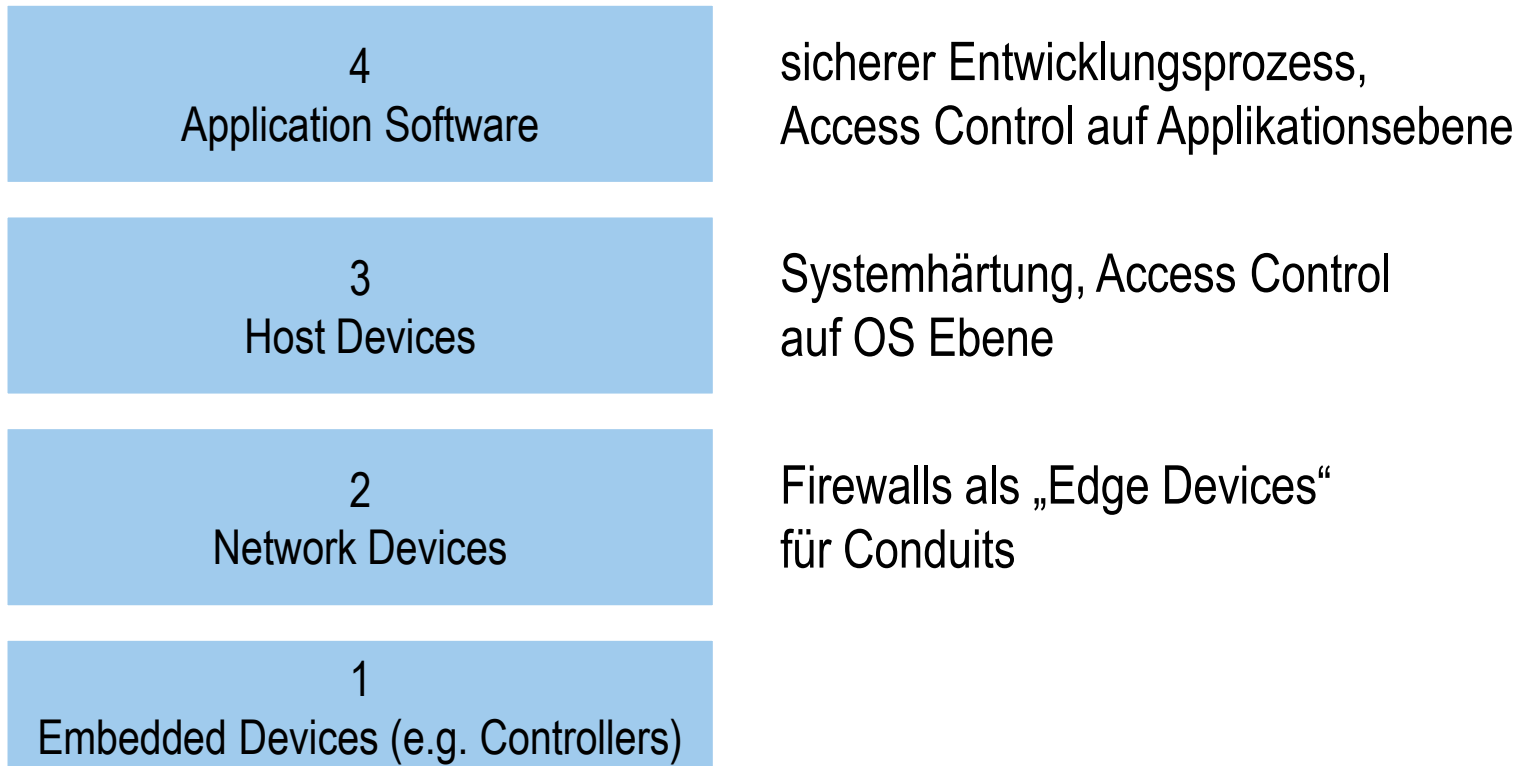




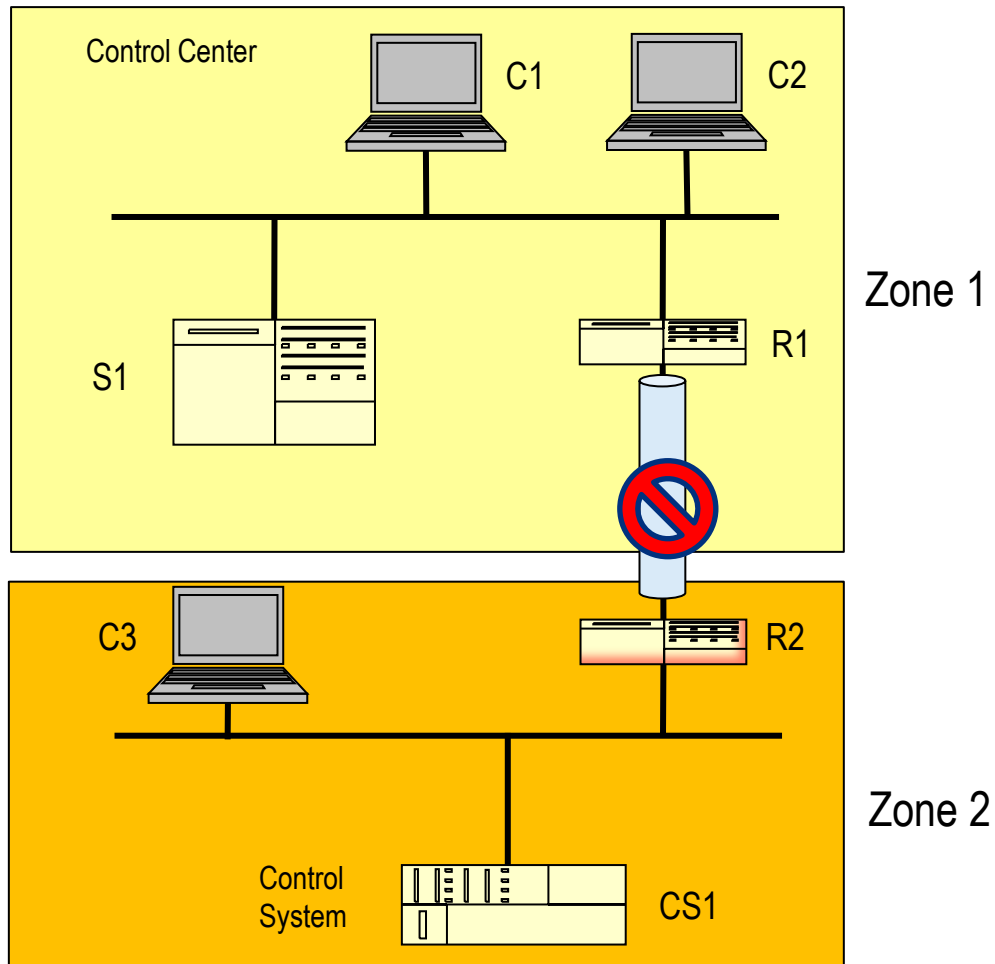
defense-in-depth Strategie



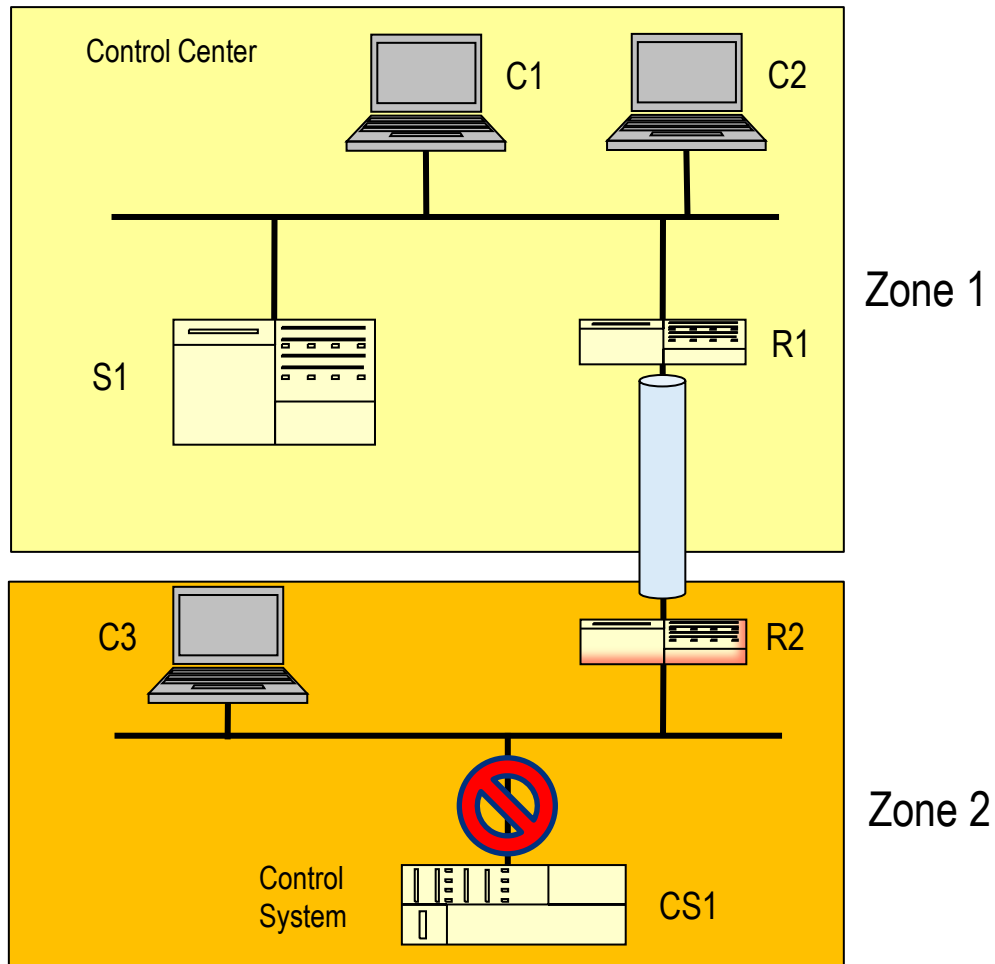
according to information of source: IEC-62443-04-1, Security for industrial automation and control systems, Product Development Requirements



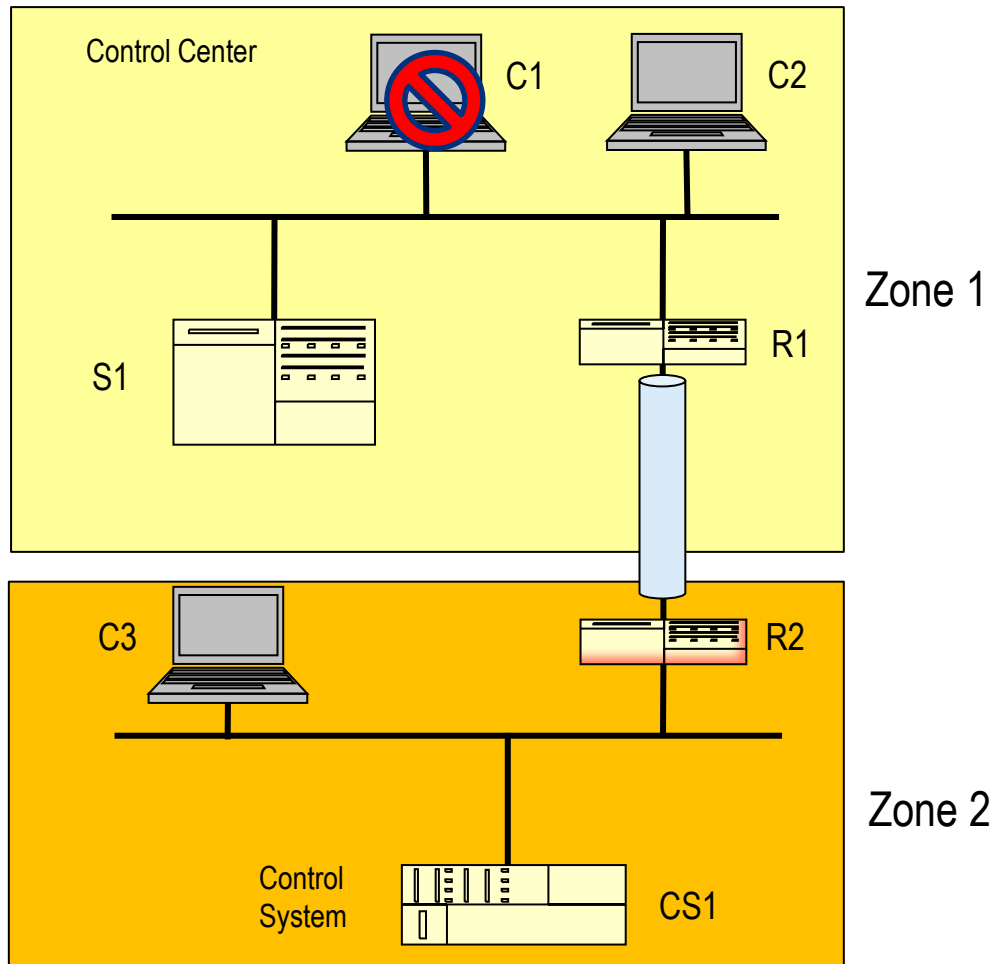
Ebene 2 : R1/R2 Regeln für Zugriffskontrolle auf Zone 2



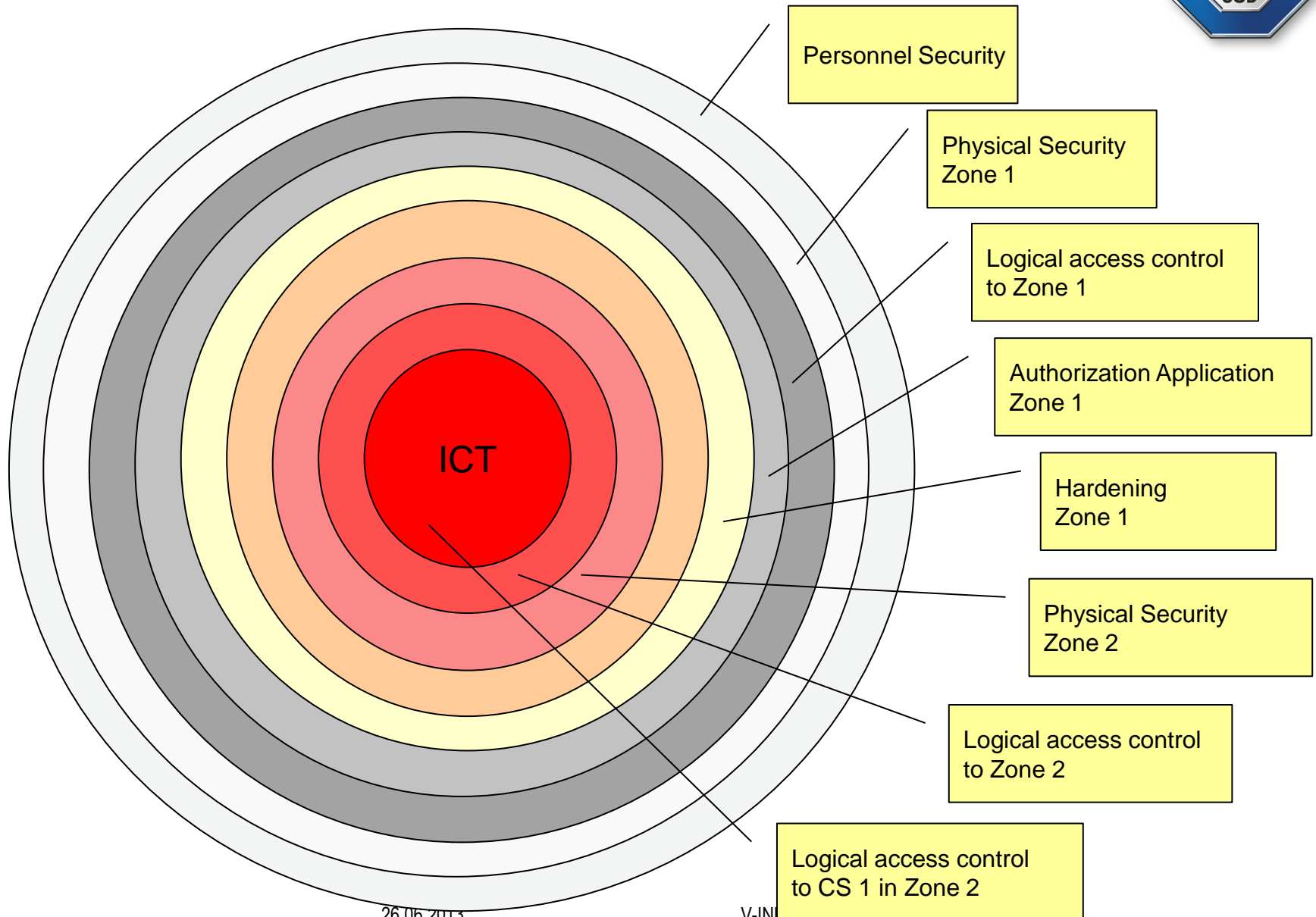
Ebene 2: R2 Regeln für Zugriffskontrolle auf CS1



Ebene 4: Authorisierung für Zugriffskontrolle auf Applikation



Defense-in-depth Strategie durch Zonierung



26.06.2013

V-IN



- führt ganzheitliche Sicht ein: Management, System, Komponente
- erläutert Konzepte wie Zonierung und SAL
- gibt Antworten auf Anforderungen der industriellen Umgebungen
- kann als Standard für Zertifizierungen verwendet werden

Embedded Systems Team:

embedded@tuev-sued.de
www.tuev-sued.com/embedded

Dr. Thomas Störtkuhl
Product Manager Industrial IT Security

thomas.stoertkuhl@tuev-sued.de

Phone: +49 89 5791-1930
Fax: +49 89 5190-3933
Mobil: +49 151 2764 5644

TÜV SÜD AG
Embedded Systems V-INM
Barthstr. 16
80339 Munich
Germany

