TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag

"IT-Sicherheit im Smart Home und der Gebäudeautomation"

Berlin, 12.11.2014

Standardisierung Datenschutz und Datensicherheit im SmartHome

Michael Staubermann (DKE)

webolution

Kontakt:
Michael Staubermann
Webolution KG
48317 Drensteinfurt
+49-2508-982070
mst@webolution.de

DKE
VDE DIN

Definitionen

- **Smart Home** dient als Oberbegriff für technische Verfahren und Systeme in Wohnräumen und -häusern, in deren Mittelpunkt eine Erhöhung von Wohn- und Lebensqualität, Sicherheit und effizienter Energienutzung auf Basis vernetzter und fernsteuerbarer Geräte und Installationen sowie automatisierbarer Abläufe steht. [Wikipedia, Januar 2014]

Normungs-Themen SmartHome

- Methodik
  - Komplexitätsmanagement in der Normung: Meta-Architekturmodell für Heim+Gebäude
  - Referenzarchitekturen
  - UseCase-basierte Vorgehensweise
- Konzepte
  - Security durch Segmentierung
  - Security Requirements für Schutzzonen
  - Informationsschutzklassen und Zweckbindung
- Normen
  - (Industrial) Automation Security
  - Security Gateways

Methodik

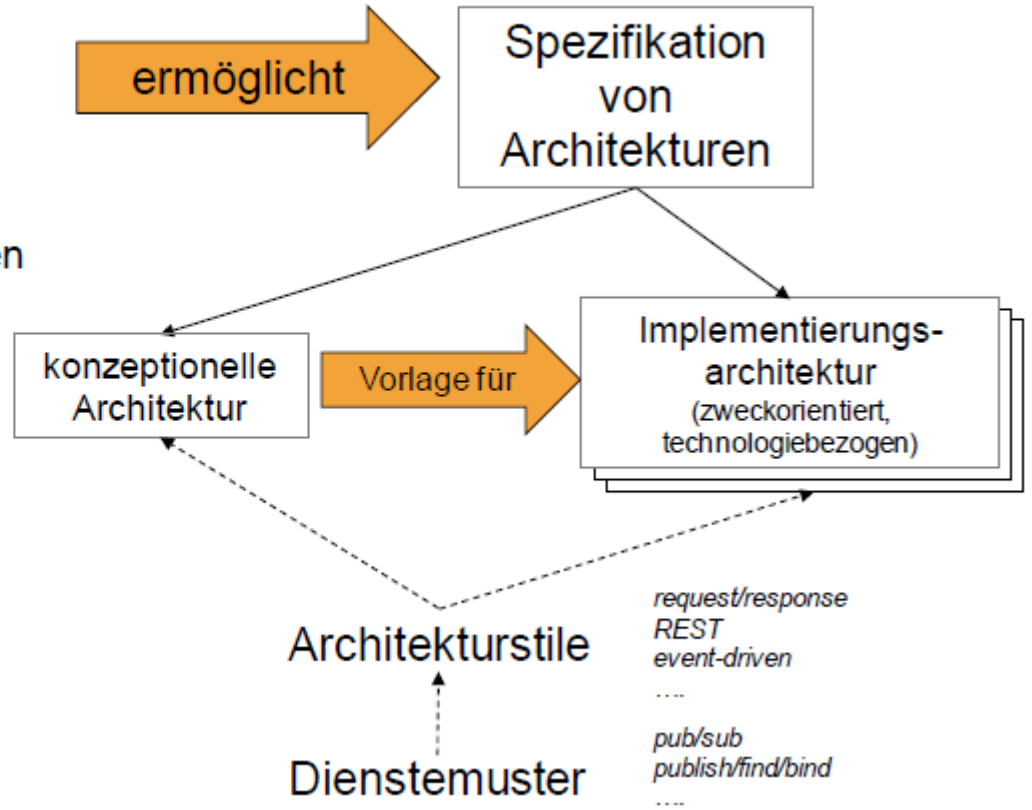
Komplexität in der Normung managen

Meta-Modell für Home+Building Architektur

Meta-Modell für Architektur-beschreibungen für Dienst-systeme

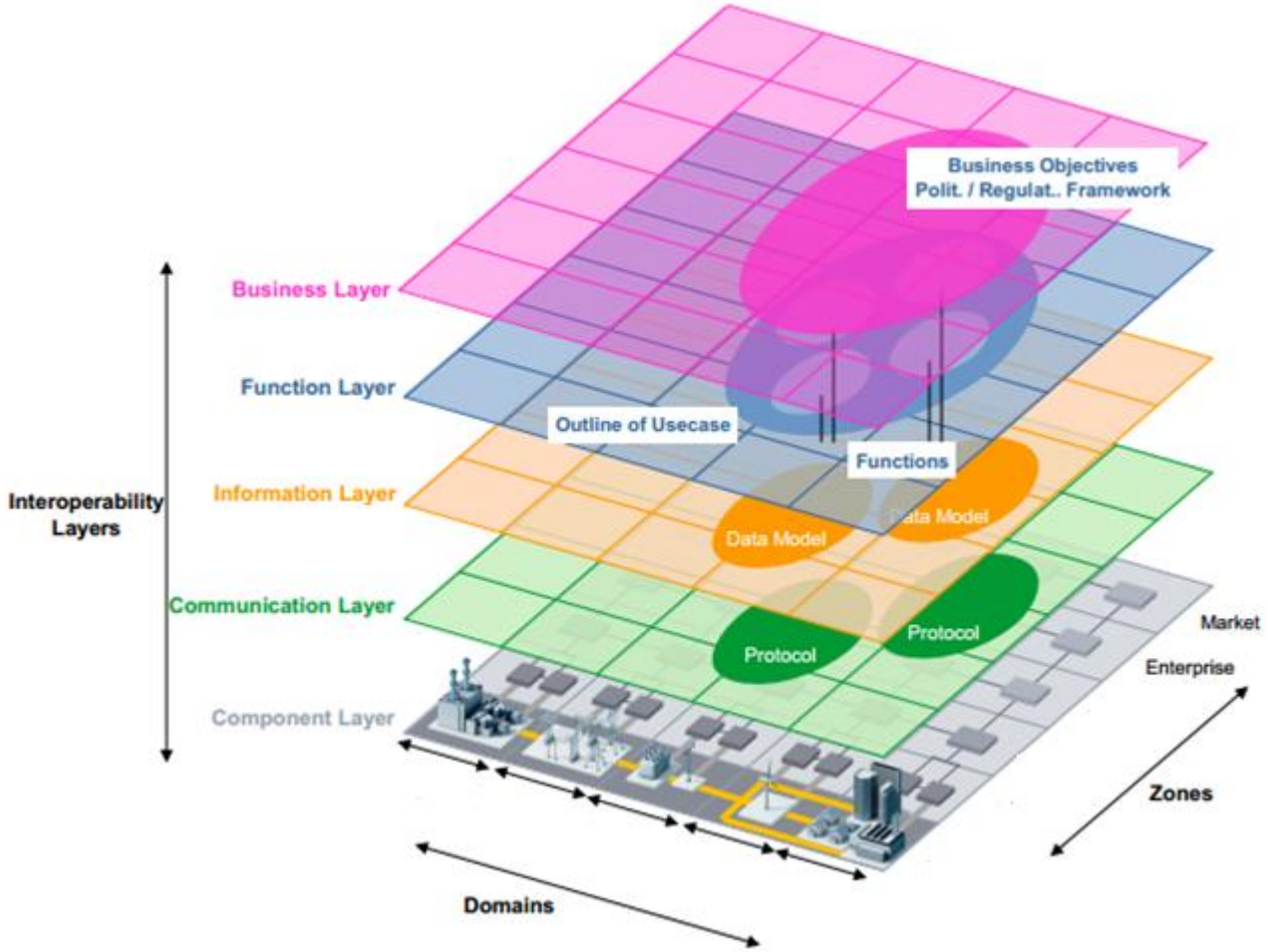
Es definiert insbesondere:

- abstraktes Rahmenwerk
- Sichtweisen auf Architekturen
- Regeln, Notationen, Terminologie, Modellierungssprachen
- ggf. Standard-Vorgaben



www.SOApatterns.org

Architekturmodell mit Interoperabilitäts-Ebenen

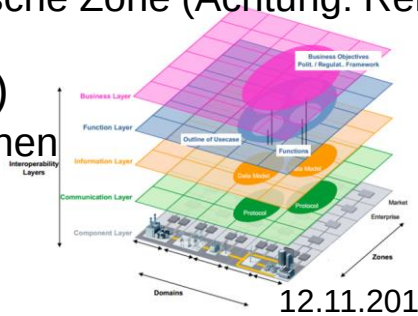


Quelle SG-CG: Normungsmandat M/490

IT-Sicherheit auf allen Ebenen betrachten

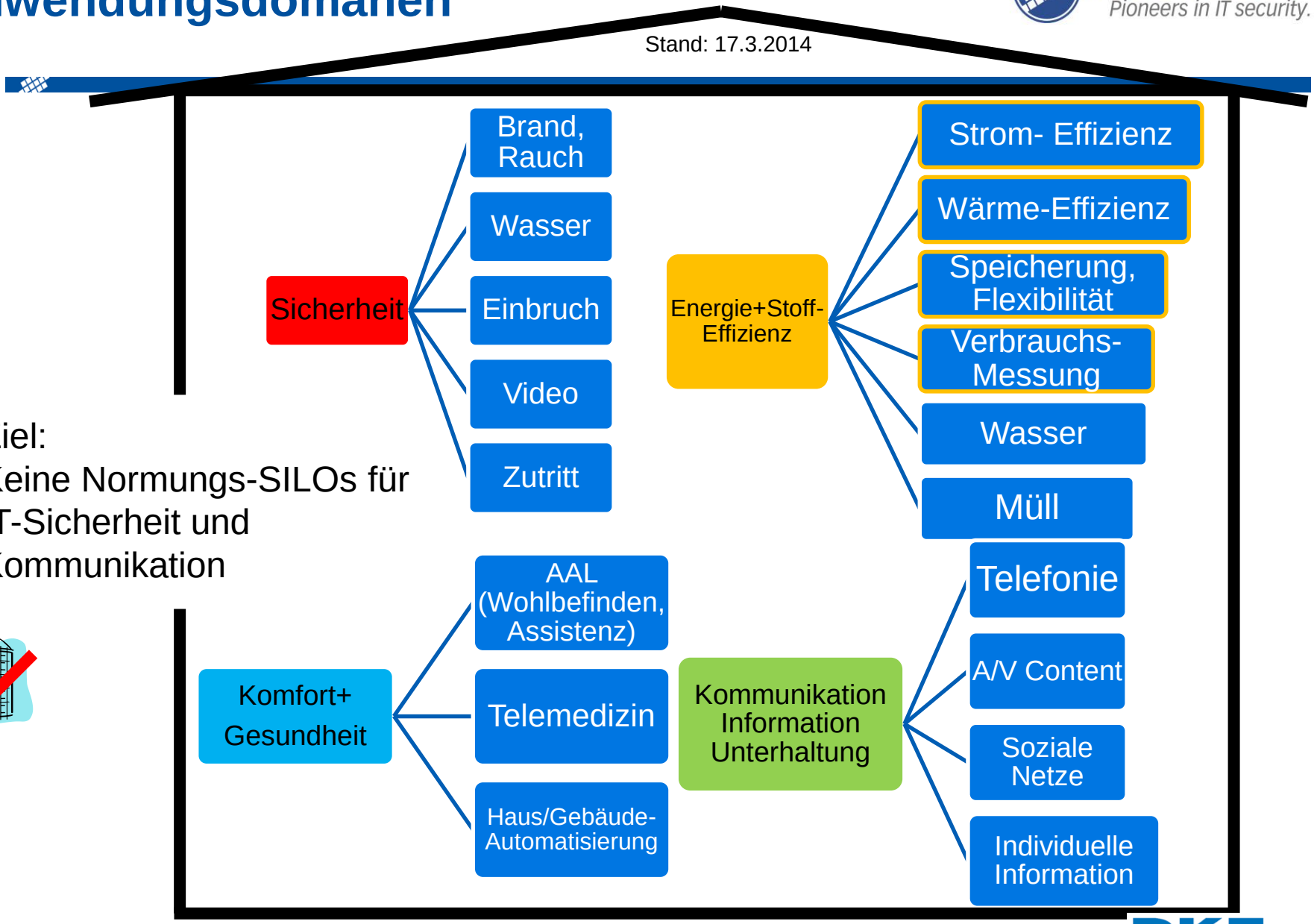
Layered Security Architecture
Beispiele für Standardisierung auf den Ebenen

- Handlungs/Policy-Ebene
  - Verantwortlicher Betreiber (Nutzer=Eigentümer?) der Komponente
  - und der Umgebung (inkl. Infrastruktur)
  - Für jede Phase des Lifecycle der Komponenten (Herstellung, Montage, Inbetriebnahme, Betrieb, Wartung/Reparatur, Abbau, Entsorgung): Anleitungen und Dokumentation
- Funktions/Service-Ebene
  - Rollen/Akteure-Berechtigungen
  - Anwendungsfall-Beschreibungen
  - Application Functional Security Requirements (z.B.Verfügbarkeit, Vertraulichkeit, ...)
- Informationsebene (Information Security Requirements)
  - Content-Security (End2End)
  - Datenschutzklassifizierung (Informationsverarbeitung-, Speicherung, Zweck, Dauer)
- Netzwerk-Ebene (Network Security Requirements)
  - Verbindung: Keine Dienste in offene/unsichere Netze anbieten, Verbindungssicherung
  - Netzwerk: Access Control/Separation of Routing, Netzwerksicherung
  - Link: Access Control/Seperation of Area-Networks and Links, Link-Sicherung
  - Begrenzung der Netzwerk-Reichweite auf die physische Zone (Achtung: Reichweite Shared-Media-Netze: PLC, SRD/WLAN)
- Komponenten-Ebene (Software- und Hardware)
  - Zugangshemmnis (physisch) zu den Netzen und Zonen
  - Rückwirkungsfreiheit von Software auf andere Teile



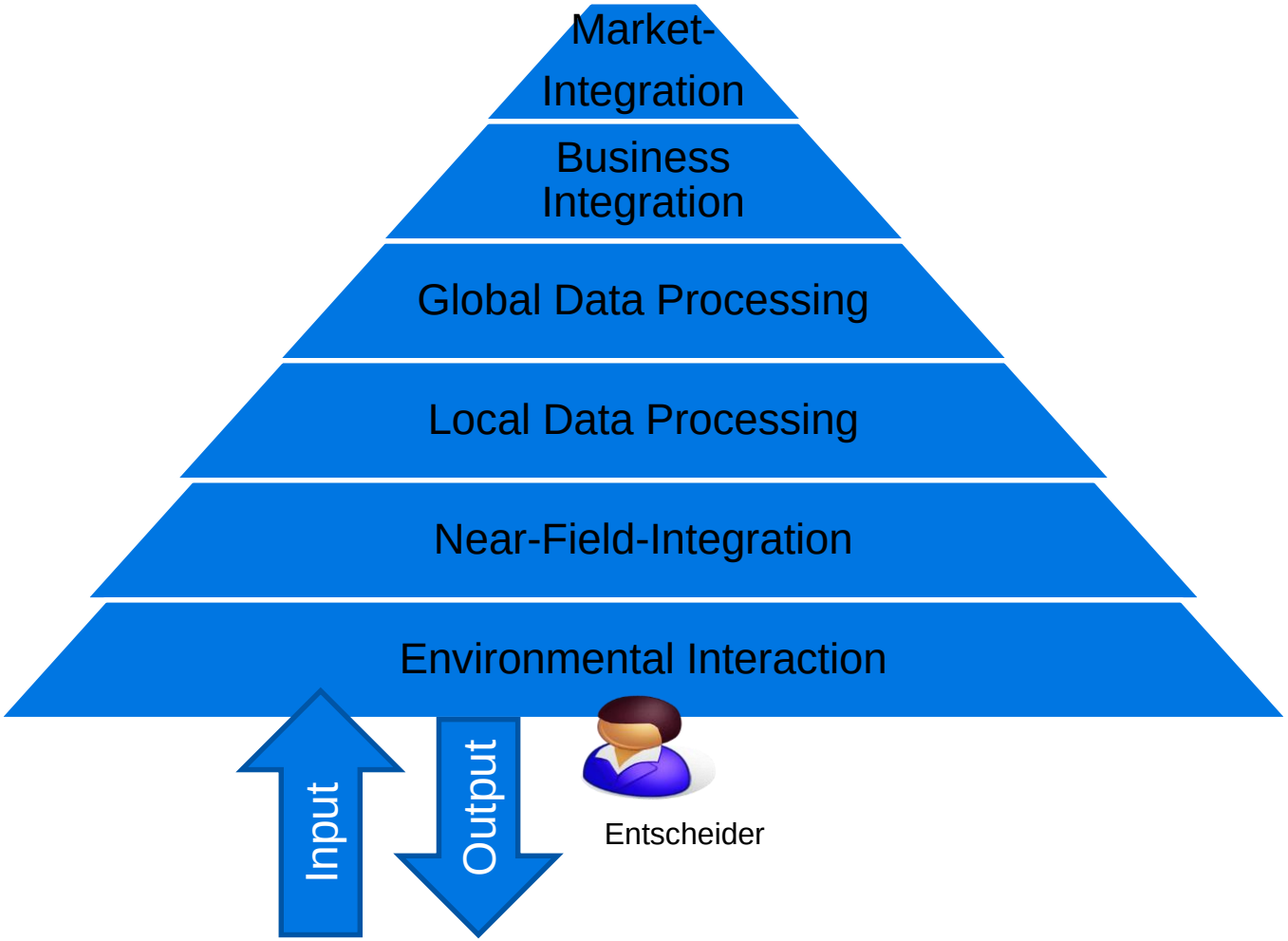
Komplexität managen: Anwendungsdomänen

Stand: 17.3.2014



Ziel:
Keine Normungs-SILOs für IT-Sicherheit und Kommunikation

Komplexität managen: Unterteilung Integrationszonen

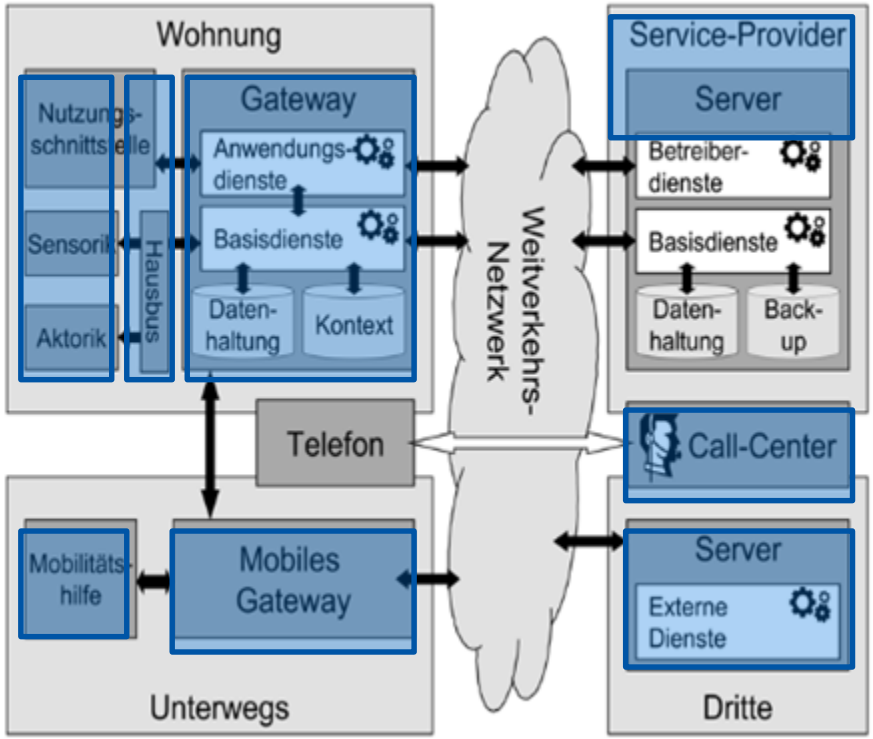


Referenz-Architekturen

Datensicherheit und Datenschutz
im SmartHome+Building

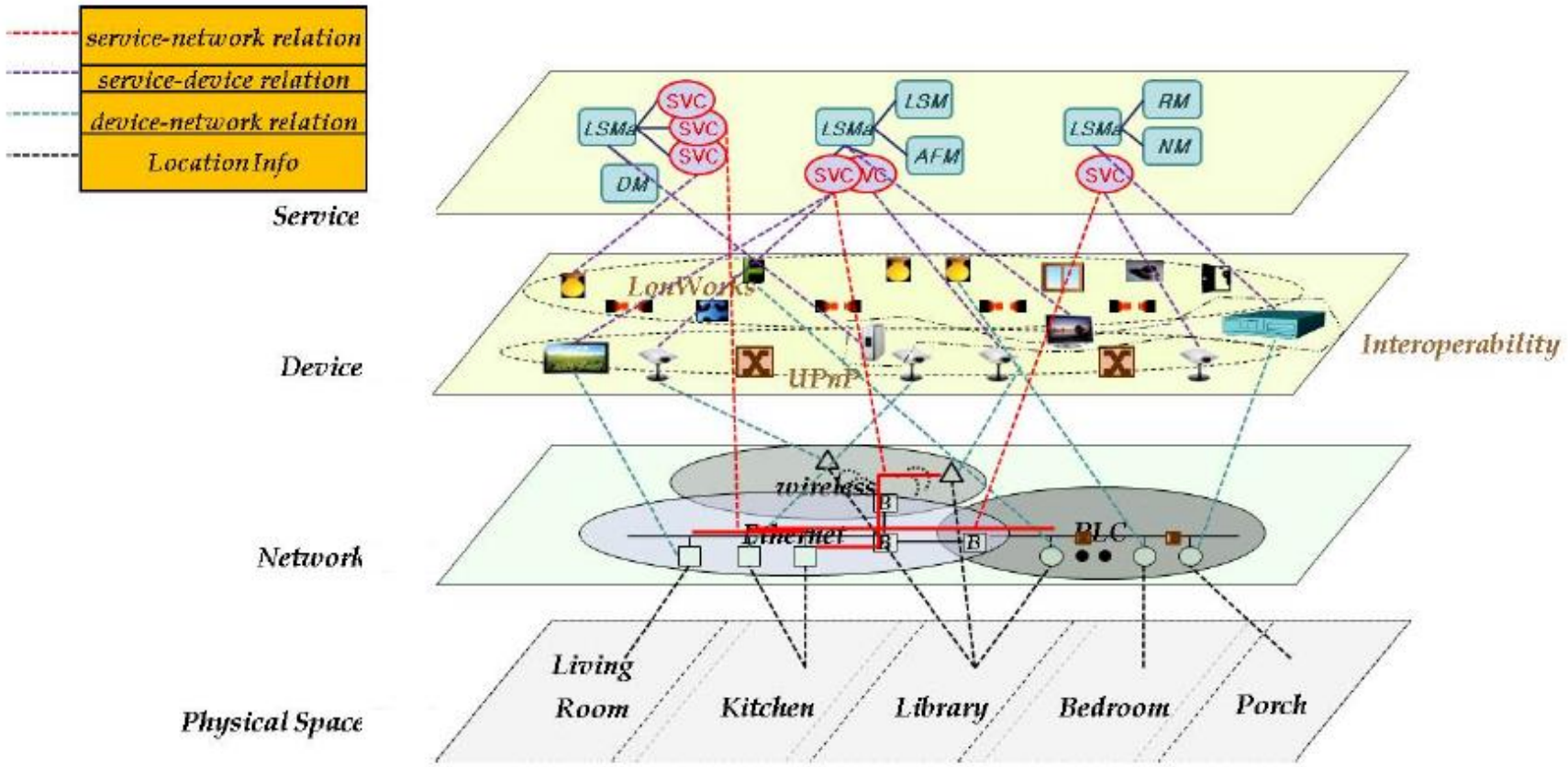
Beispiel: Domäne AAL

Umwelt – Nahfeld – Lokale – Globale – Business - Markt



Quelle: Offis/DKE AAL Roadmap

ISO/IEC DIS 30100-2:2013 (JTC 1/SC 25)
Home Network Ressource Management



Weitere Referenzarchitekturen

- [RA-IOT] www.iot-a.eu Internet of Things Architecture (EU H7 Projekt)
- [RA-I4.0] www.vdi.de - Auf dem Weg zu einem Referenzmodell für Industrie 4.0
- [SGCG-RA] SmartGrid Coordination Group Reference Architecture
- [ETSI-M2M] – ETSI M2M/OneM2M Reference Architecture

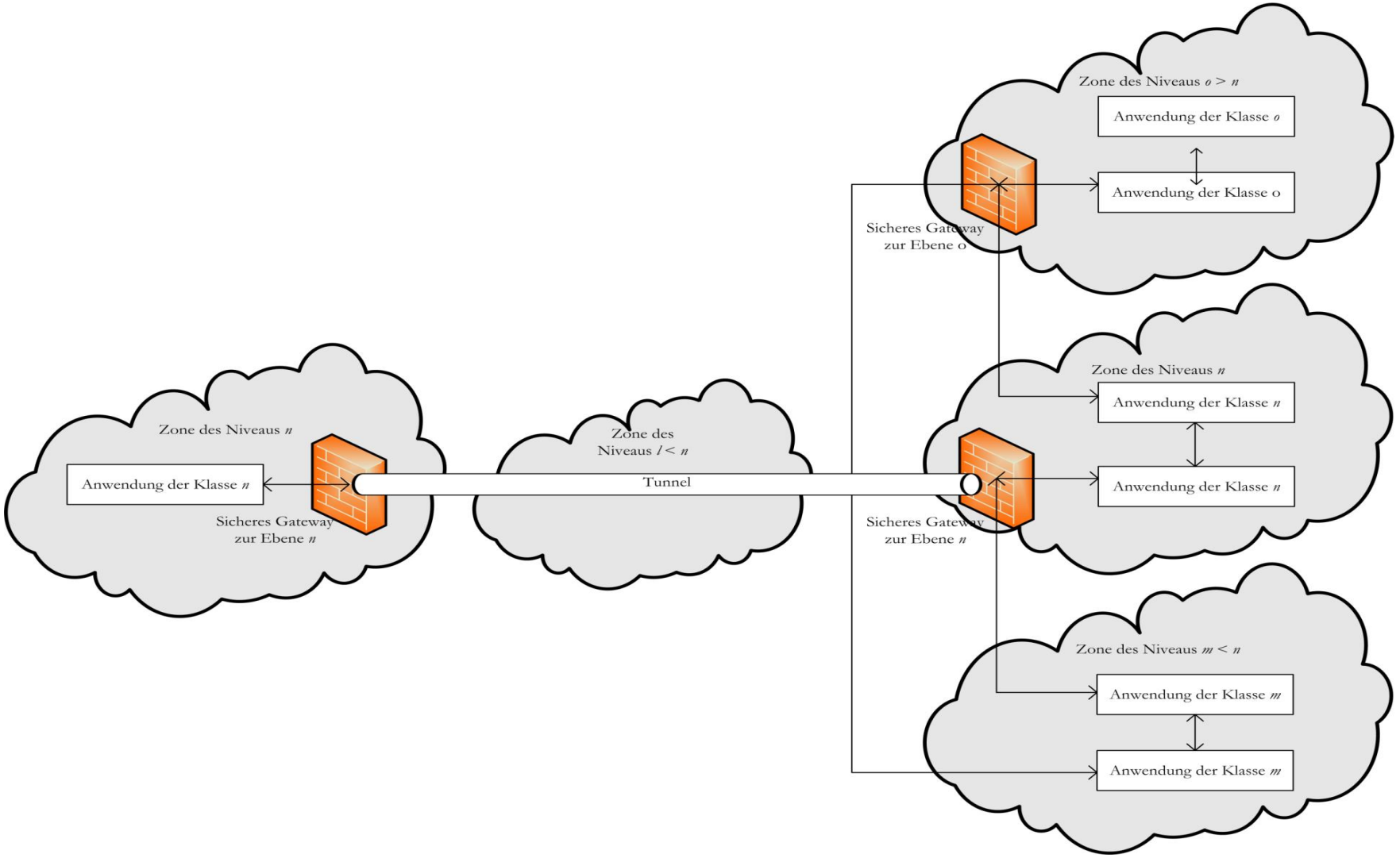
Security durch Segmentierung

K716.0.1

IEC62443 - Zones

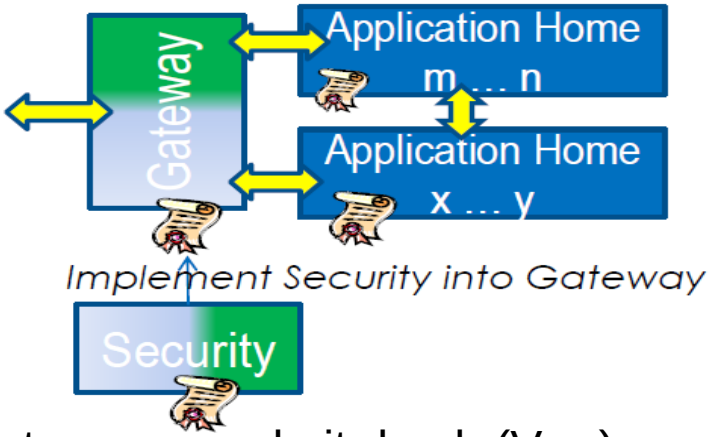
- Each zone has a set of characteristics and security requirements that are its attributes.
  - security policies
  - asset inventory
  - access requirements and controls
  - threats and vulnerabilities
  - consequences of a security breach
  - authorized technology
- Sinnvoll auch für SmartHome?!

Security durch Segmentierung
Sicherheitszonen (K716.0.1 AG4)



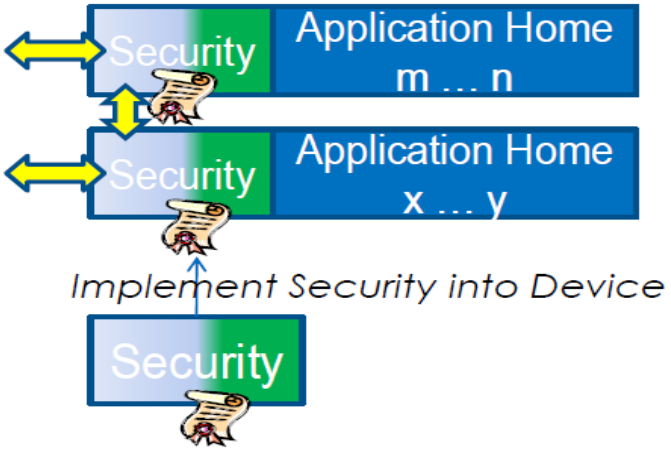
Architekturvarianten mit/ohne Gateway

Architektur mit Gateway



- Datensparsamkeit durch (Vor-) Verarbeitung und Speicherung im Gateway
- Widerstandsfähigkeit durch geringere WAN-Verfügbarkeitsabhängigkeit
- Vertrauen in lokalen Kommunikationspartner
- Segmentierung auf Netz- und Verbindungsebene
- Beispiele: SmartMeterGW, HomeGateway

Architektur ohne Gateway



- Weniger Kontrolle über Datenflüsse
- Stärkere Abhängigkeit von WAN-Kommunikation
- Vertrauen in globalen Kommunikationspartner
- Segmentierung durch Router auf Netzebene, nicht auf Verbindungsebene
- Beispiele: Consumer/Entertainment (SmartTV, FitenessTracker)

Konzepte des SMGW-PP und der SMGW-TR für Security Gateways im SmartHome

- In Netze unbekannten oder niedrigen Security-Levels werden keine Kommunikations-Dienste angeboten, d.h. keine offenen Ports, nur abgehende Verbindungen
- Zusätzliche Ende-zu-Ende Inhaltssicherung für Verbindungen mit personenbeziehbaren Daten zwischen Home+Gebäude Zone und externen Akteuren im WAN
- Transportsicherung mindestens mit TLS1.2 mit ECDHE/ECDSA beidseitig Zertifikatsauthentifiziert für Datenflüsse zwischen Gateway und angeschlossenen Geräten
- PublicKey-Verfahren für Authentifizierung und Verschlüsselung nur noch ECC-basiert
- Unidirektionale Constrained (Sensor-)Networks Devices (Wireless Meter) begrenzter Ausdehnung verwenden individuelle Schlüssel und AES-basiertes Encrypt-than-MAC mit Counter-KDF
- Bidirektionale Constrained (Sensor-)Networks verwenden TLS1.2
- Geräteindividuelle Schlüssel (Wired-Meters, Controllable Devices)
- Alle Datenflüsse auf Netzwerk- Transport- oder Anwendungsebene werden durch ein Security Gateway kontrolliert und für den Nutzer transparent gemacht
- Beschreibung von Kommunikationsszenarien/-Patterns (Gleichartige Rollen, Datenfluss-Richtungen, Request/Response und Sicherheits-Protokolle)
- Gateways die Netze verbinden, sollen bzgl. Umsetzung der IT-Sicherheitsanforderungen vertrauenswürdig, geprüft und zertifiziert sein
- Mindestens TLS1.2 mit gegenseitiger Authentifizierung für alle bidirektionalen Schnittstellen (auch nicht IP-basierte)
- IT-Security Administration:
  - Schlüssel/Zertifikatswechsel
  - Schwachstellenbeseitigung
  - Konfiguration der Erlaubnisvon Datenflüssen zwischen den Kommunikationspartnern an den Schnittstellen
  - Log-Abfrage durch einen authorisierten Administrator.
- Nachweis eines Flaw-Remediation Prozess („Patches“ für Sicherheits-Exploits, Durchsetzen des Updates) für bidirektional kommunizierende Komponenten

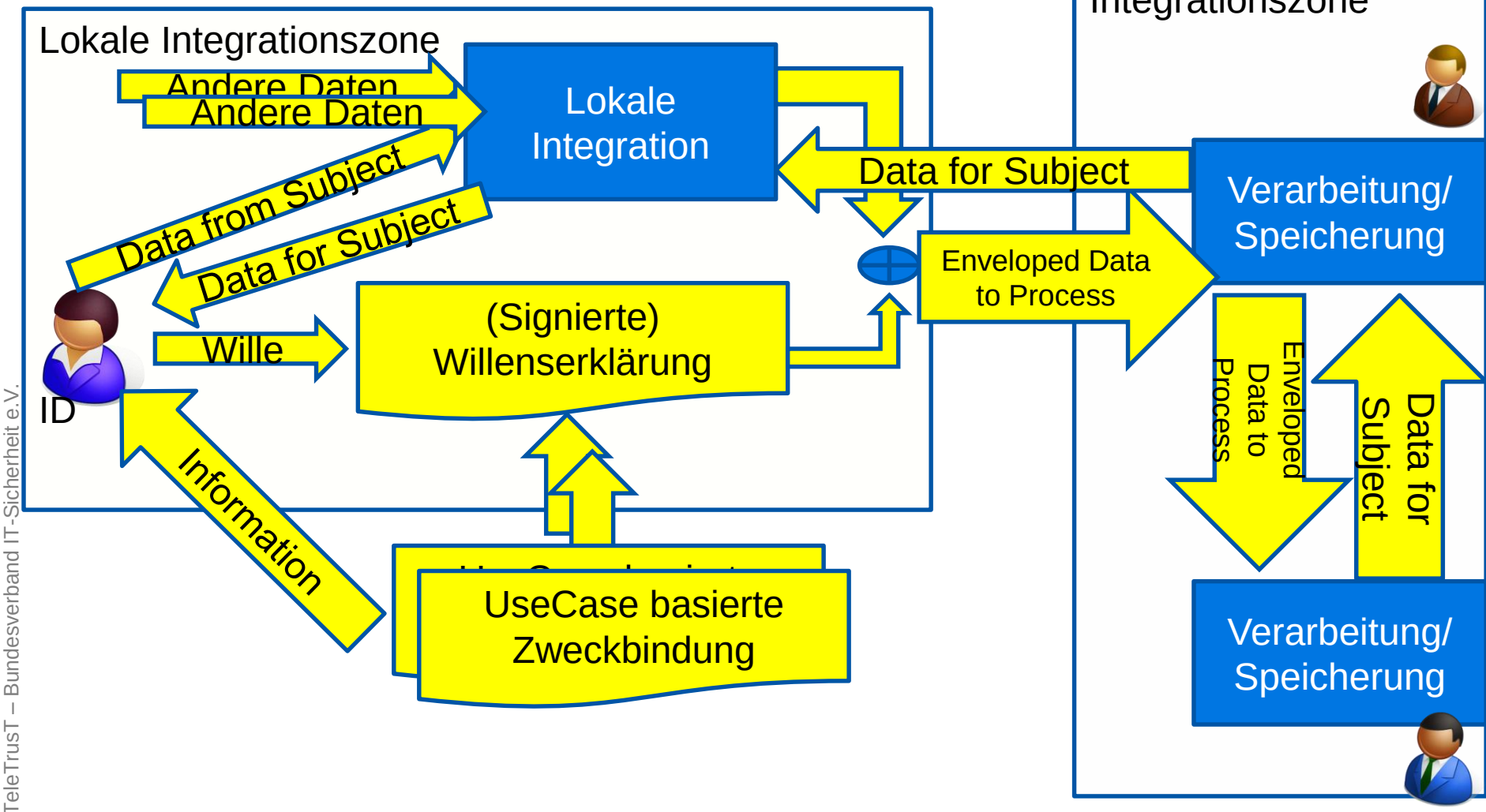
UseCase-Methodik in der IT-Sicherheit

IT-Security SmartHome+Building

UseCase-Beschreibung für Datenschutz und Datensicherheit

- Anwendungsfall beschreibt, welche Daten welchen für welchen Zweck von welcher Rolle verarbeitet oder gespeichert werden
- Katalog von (High-Level) Anwendungsfall-Beschreibungen oder Freitext (Siehe TR03109 TAF1-13, WAF, HAF...)
- Anwendungsfälle beschreiben welche Informationen im Rahmen der Transparenz an den Nutzer bereitzustellen sind (z.B. Wann, welche Daten weitergeleitet werden)
- Anwendungsfälle beschreiben die minimalen (z.B. Rechtlich notwendigen) Fristen zur Speicherung

AG2 - Souveränität mit UseCase basierter Informierter Einwilligung



Anwendungsfallbasierte Zweckbindung

1	Anwendungsfall-ID und Version	Anhand der ID und Version ist in einem öffentlichen Webservice die Anwendungsfallbeschreibung zu finden.
2	Name des Anwendungsfalles	(Max. 80 Zeichen)
3	Zweck (nach BDSG)	Eine Verständliche Beschreibung über den Verwendungszweck. Z.B. Konkretisierung von „Erfüllung eines Vertrages nach BDSG §4c(2) (Abrechnung)“. Hier könnten Textblöcke referenziert werden die mehrsprachig semantisch identisch vorformuliert sind. So dass sie Bestandteil von Verträgen werden können.
4	Beschreibung	Eine Beschreibung des Verarbeitungsprozesses. Dies kann in formaler Form z.B. durch MUSS/KANN Anforderungen geschehen.
5	Beeinflussende Parameter	Welche Beeinflussenden Parameter bei der Verarbeitung verwendet werden
6	Verarbeitete Personenbezogene Informationen	Welche Informationen zur Zweckerfüllung verarbeitet werden
7	Bereitgestellte Informationen	Welche Informationen dem/den berechtigten Empfänger(n) bereitgestellt werden
8	Dem Datensubjekt bereitzustellende Transparenz Informationen	z.B. Nennung der Beeinflussende Parameter, Verarbeitete Informationen und Bereitgestellten Informationen
9	Für den Zweck notwendige Speicherdauer der Verarbeiteten Informationen	Relative Zeit (Zeitdauer)

Willenserklärung

1	Anwendungsfall-ID	Anwendungsfall-ID (s.o.)
2	Subjekt-ID	Leer, Pseudonym oder iD des Datensubjektes (Absenders)
3	Berechtigte Empfänger	Leer oder Liste von berechtigten Empfängern. Eine Identifikation einer natürlichen oder Juristischen Person. Alternativ eine technische Adresse die einer verantwortlichen natürlichen oder juristischen Person zugeordnet ist.
4	Über den Zweck hinausgehende Speicherdauer der Bereitgestellten oder Verarbeiteten Informationen	Danach dürfen die Daten nicht mehr verwendet werden. Absolutes Datum/Zeit
...	Weitere	
N	Signatur	Signiert vom Datensubjekt (Absender) (zu konkretisieren)

Verbunden mit den übermittelten Daten

Anwendungsfälle aus einer anderen Sicht (Mis-)UseCases des Angreifers

- (Bad-)Business-Cases
  - Erschleichen von Geheimnissen (Identitäten, Schlüssel, Schwachstellen) zwecks Verkauf
  - Erschleichen von Dienstleistung (Kryptopower/Bitcoin-Hashing) zwecks Verkauf
  - Unterdrückung von Informationen Zwecks Verminderung von Nutzungsentgelten für in Anspruch genommene Dienste
  - Erfassung und Auswertung der Nutzereigenschaften zwecks personalisierter Werbung oder anderem wirtschaftlichem Vorteil
  - Verknüpfen von Daten zwecks Nutzung außerhalb der ursprünglichen Zweckbindung zum wirtschaftlichen Vorteil
- Communication-(Mis-)UseCases
  - Erlangung von Administratorrechten zwecks Anonymisierung und Fernsteuerung anderer Systeme (Botnets)
  - Nutzung des Systems für Reflection/Amplification-Attacks
- Schwachstellenerforschung und Exploit-Entwicklung
  - zwecks Veröffentlichung und Reputationsgewinn
  - zwecks Verkauf
- Destabilisierung von Infrastrukturen zur Durchsetzung von Interessen (DoS Attacken)

Informations-Schutzklassen

IT-Security SmartHome+Building

Schutzbedarfs-Klassifizierung für Informationen

- Ziel 1: VDE Anwendungsregel „Datenschutzklassifizierung“
- Sondierung von Anforderungen aus unterschiedlichen Normen, um diese für die Schutzklassen zu berücksichtigen.
- Identifizierung und Definition von sinnvollen Schutzklassen
- Schutzklassen sollen eine einfache Identifizierung der Security Anforderungen für einen Use-Case ermöglichen
- Damit soll eine differenzierte Sicherheitsbetrachtung unterstützt werden. BDSG §9: Technische Maßnahmen: „wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

Bestehende Normen und Normentwürfe (z.B. ISO/IEC 62443-3-3, DPR, CC)
Zusammentragen von Schutzanforderungen aus dem Bereich IT-Security, Privacy und Safety

Schutzklassen

Klassifizierung des Schutzbedarfs von Informationen und den daraus resultierenden Anforderungen

Verfügbarkeitsanforderungen aus Brand- und Einbruchsschutz (Abfrage K716.0.1, Beispiele)

Norm	Typ	Erkennung Kommunikations-verlust	Alarmierungs-verzögerung
EN54-25	Brandalarm (Funk)	(4.2.6): <=100s	(4.2.2/4.2.5) 1.Msg <=10s, 10.Msg <=100s No Loss
EN50131-1 EN50131-5-3 (4.5.1, Table 9, 5.1.7.1)	Einbruch/ Sabotage (Funk)	(8.8.4.1) Grad 1: <=4h... Grad 4: <=10s	(8.8.1) <=10s von Quelle bis Ziel

Wirkungsklassen für Wohngebäude

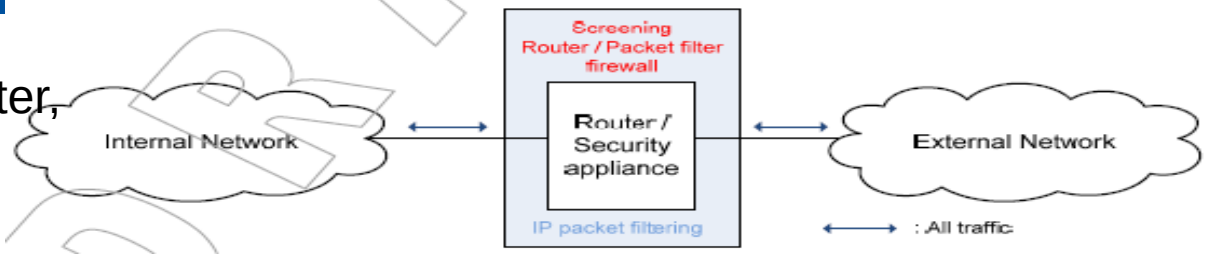
- Differenzierung der Wirkungsklasse(WK) 0:
  - Im Wohnbereich können Eigentümer und Privater Nutzer unterschiedlich sein (z.B. wenn die IKT im Vertrags/Rechtsverhältnis mit Dritten verwendet wird)
  - Abhängig davon kann WK 0 auch WK1 Kriterien erfüllen.
- Der in WK0 realisierte IT-Schutzlevel wird durch eine Analyse bestimmt (Checkliste)
- Passt der realisierte IT-Schutzlevel nicht zum notwendigen IT-Schutzlevel:
  - Level durch Maßnahmen erhöhen
  - Risiko trägt der Nutzer (nur wenn kein Rechtsverhältnis mit Dritten)
  - Risiko trägt der Dritte (z.B. Dienstanbieter, Eigentümer)
  - Risiko versichern (Delta zwischen Required and Realised)
- Offen: Nutzung von IKT-Diensten des Privaten Bereiches (WK 0) die im Fokus des Datenschutzes liegen, z.B. Fitness-Tracking, HBB-TV Dienste aber in einer WK 1 o. 2 terminieren (z.B. Organisation die sensitive Daten verarbeitet).

ISO/IEC Standards

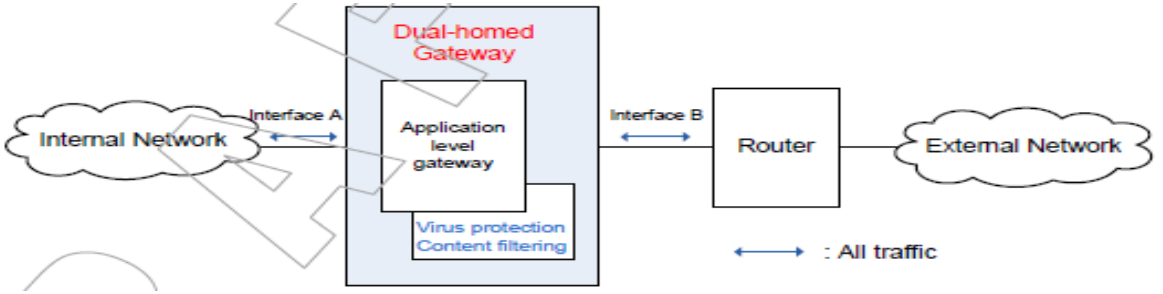
IT-Security in
SmartHome+Building

ISO/IEC 27033-4 Security Gateways (3/2014 1st ed)

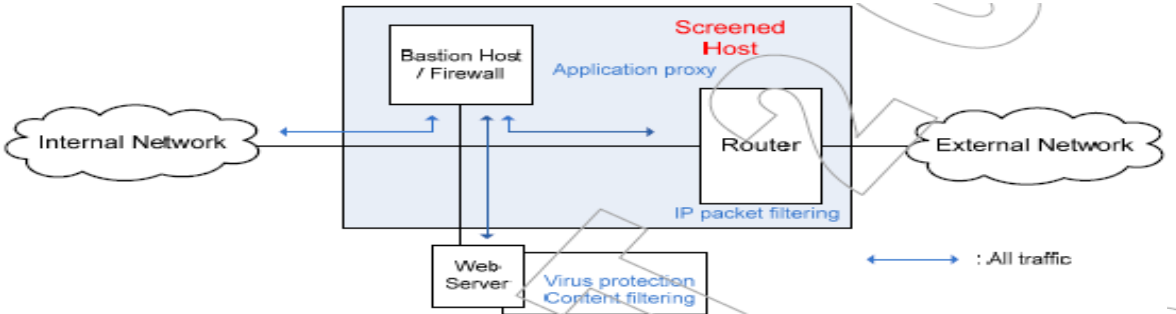
1. Screening Router, Packet Filter FW



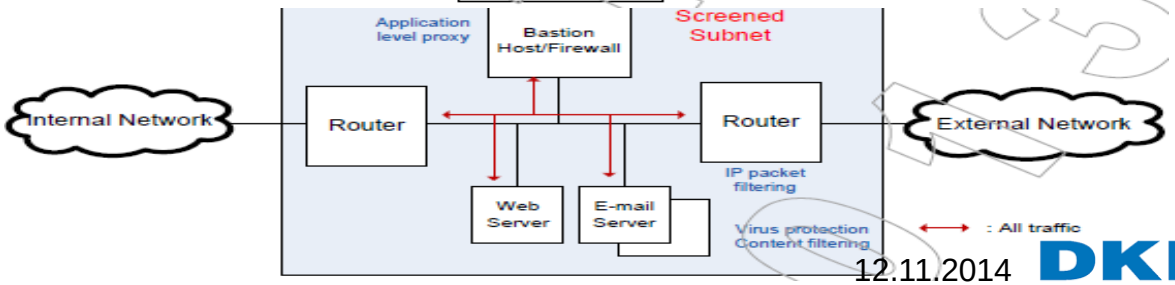
2. Dual-homed Gateway breaks End2End connectivity



3. Screened Host



4. Screened Subnet



IEC 62443 - Industrial Communication Networks Network and system security

- -1-1: Terminology, concepts and models
- -1-2: Master Glossary Terms+Abbreviations
- -1-3: Security Compliance
- -2-1: Establishing an industrial automation and control system security program
- -2-2: Operating an industrial automation and control system's security program
- -2-3: Patch management in the IACS environment
- -2-4: Certification of IACS supplier security policies and practices
- -3-1: Security technologies for industrial automation and control systems
- -3-2: Security assurance levels for zones and conduits
- -3-3: System security requirements and security levels
- -3-4: Technical requirements: Protection of data at rest
- -4-1: Product development requirements
- -4-2: Technical Security requirements for IACS components

Gebäudeautomatisierung=Industrie?
Privacy wird nicht berücksichtigt (aber wettbewerblicher Datenschutz).

IEC 60335-1 Ed5.1– Additional requirements for household and similar appliances used in network connected and/or smart environments

- Gerätebedienung hat Vorrang vor Fernsteuerung
- Verschlüsselung, und Verifikation müssen für Sicherheits-Relevante Funktionen implementiert sein
- Nur freigegebene (Approved and accepted) Methoden für Verschlüsselung und Integritätsschutz dürfen implementiert werden
- Remote-Software download muss verschlüsselt sein
- Remote-Software download muss *gegenseitig* authentifziert sein
- Jede Installation von Software muss durch einen lokalen Benutzer authorisiert werden
- ...

Weitere

- [EU-DPR] Europäische Datenschutzgrundverordnung
- [PP-0073] SMGW-PP - Security Functional Requirements, Threats, Objects, Assumptions
- [TR-03116-3] Kryptografische Anforderungen an das Intelligente Messsystem
- [CC] Common Criteria 3.1 – Security Functional Requirements, Assurance Requirements und CEM
- [ETSI-TVRA] TS102165-1 - Thread, Vulnerability, Risk Analysis for Communication Systems
- [BDSG] Bundesdatenschutzgesetz
- [TR03109-1] SMGW-TR – Insbesondere Kapitel Kommunikationsprofile und –Szenarien
- [ISO29182-7] ISO/IEC FDIS 29182-7:2014 Sensor Network Architecture

Normungsroadmaps

www.dke.de/SmartHomeBuilding

http://www.dke.de/de/std/informationssicherheit/documents/nr_it-sicherheit_de_version%201.0.pdf

Kapitel 5.1 Informationssicherheit im Smart Home

Ed.2 folgt bald

Kontakt:
Michael Staubermann
Webolution KG
48317 Drensteinfurt
+49-2508-982070
mst@webolution.de