TeleTrusT
Pioneers in IT security.

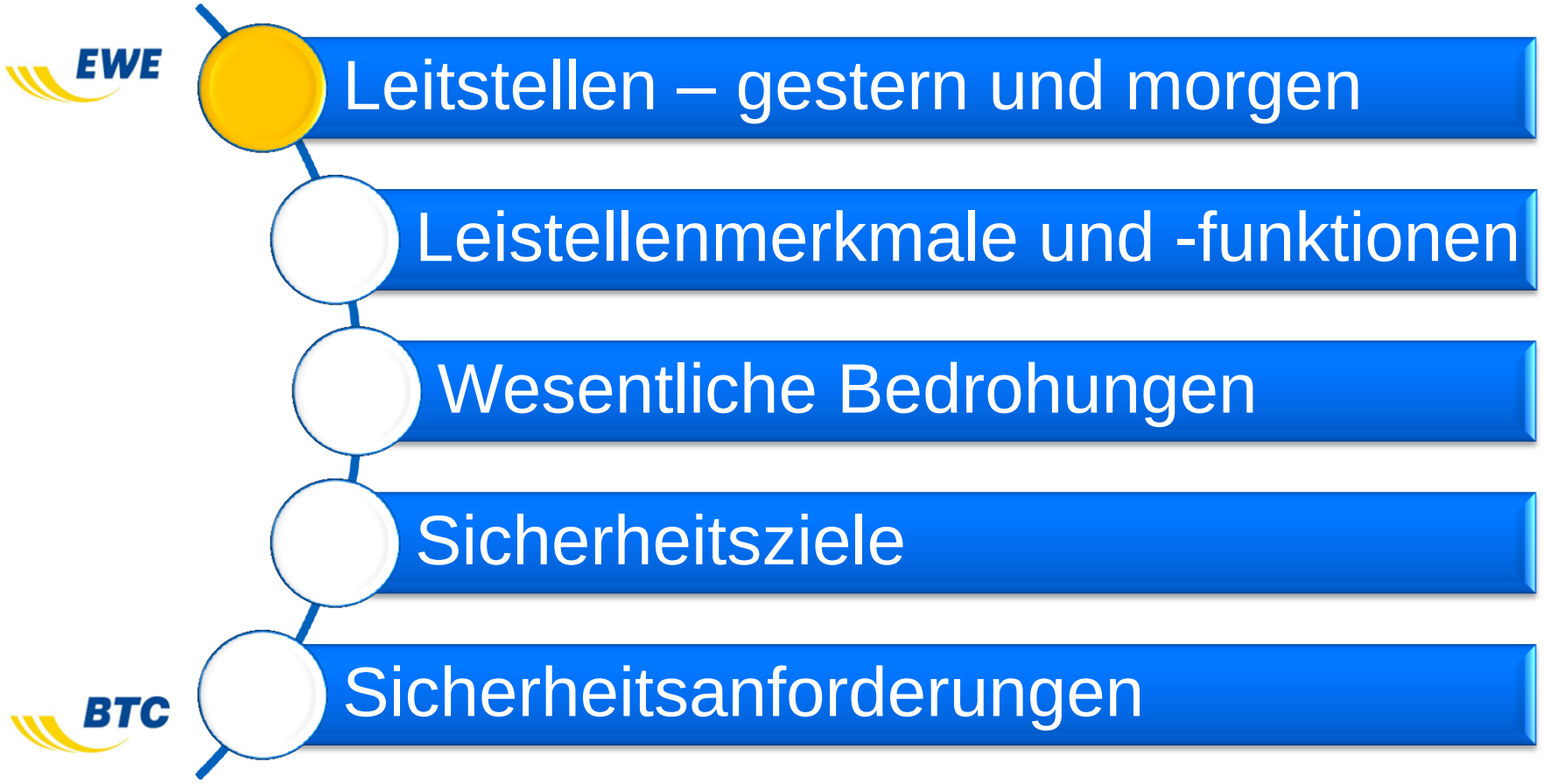
Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 13.06.2013

IT-Sicherheit in und für Leitstellen

Michael Pietsch - BTC AG

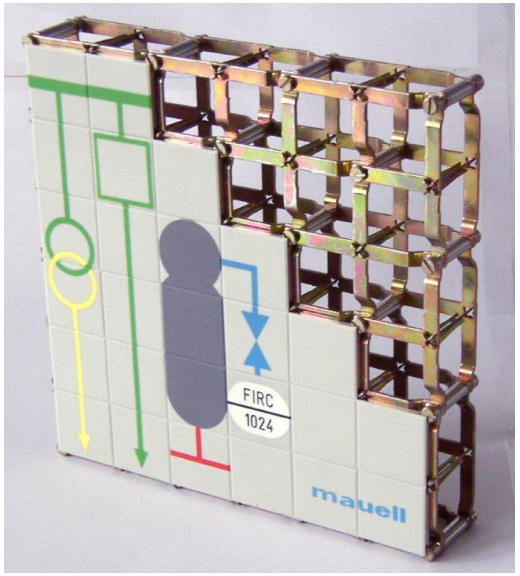
Agenda


EWE
Leitstellen – gestern und morgen
Leistellenmerkmale und -funktionen
Wesentliche Bedrohungen
Sicherheitsziele
BTC
Sicherheitsanforderungen

Leitstellen – gestern und morgen

„Klassische“ SCADA-Systeme

- Ingenieurstechnik mit wenig IT - z.T. 20 Jahre und älter
- Serielle Protokolle und oder einfache Relaissteuerung
- Insellösungen ohne externe Netzkopplung / Büro-IT
- Wenig Abhängigkeiten von Dritten
- Serielle Verbindungen und proprietäre Protokolle



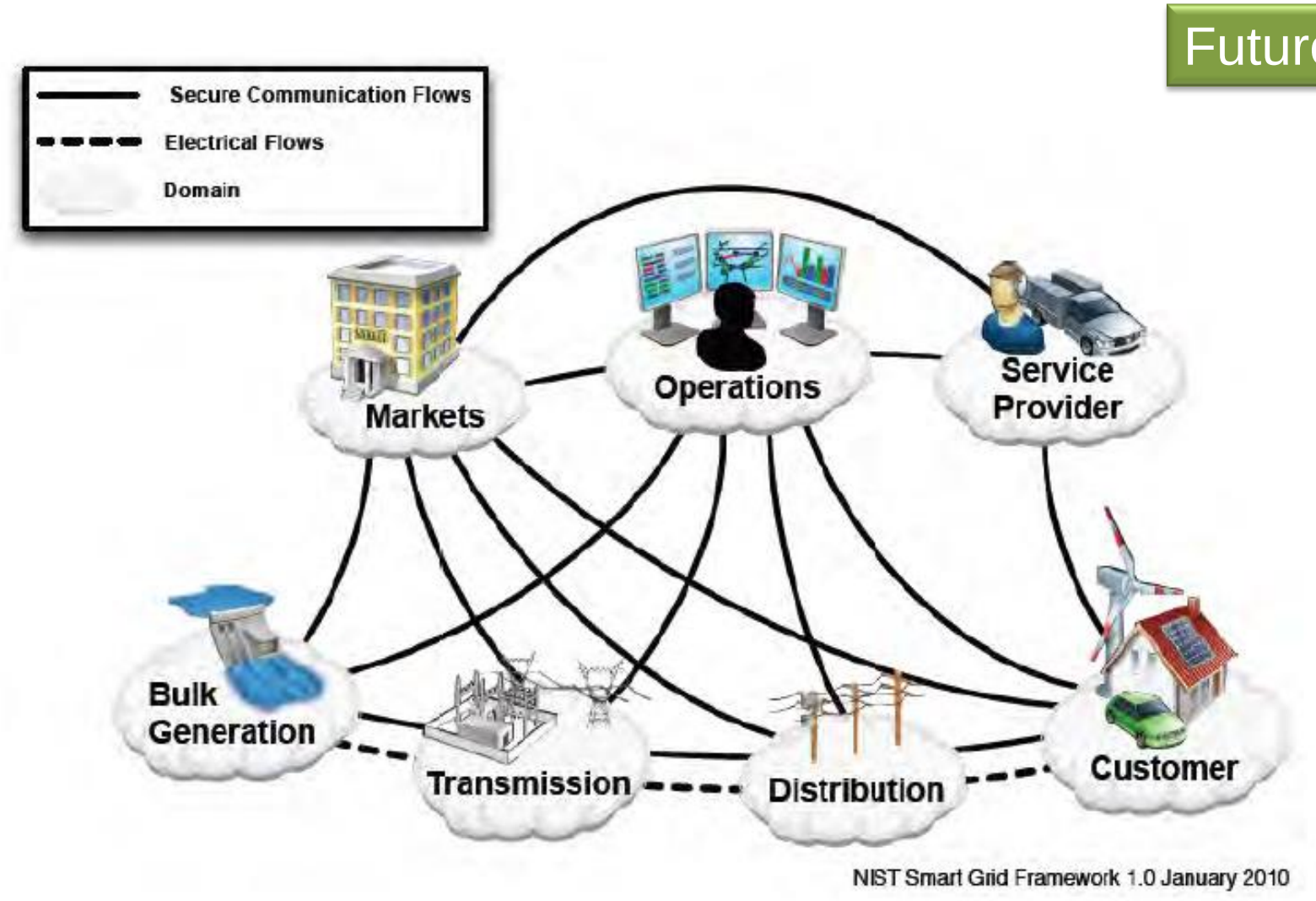
Leitstellen – gestern und morgen

„Moderne“ SCADA-Systeme

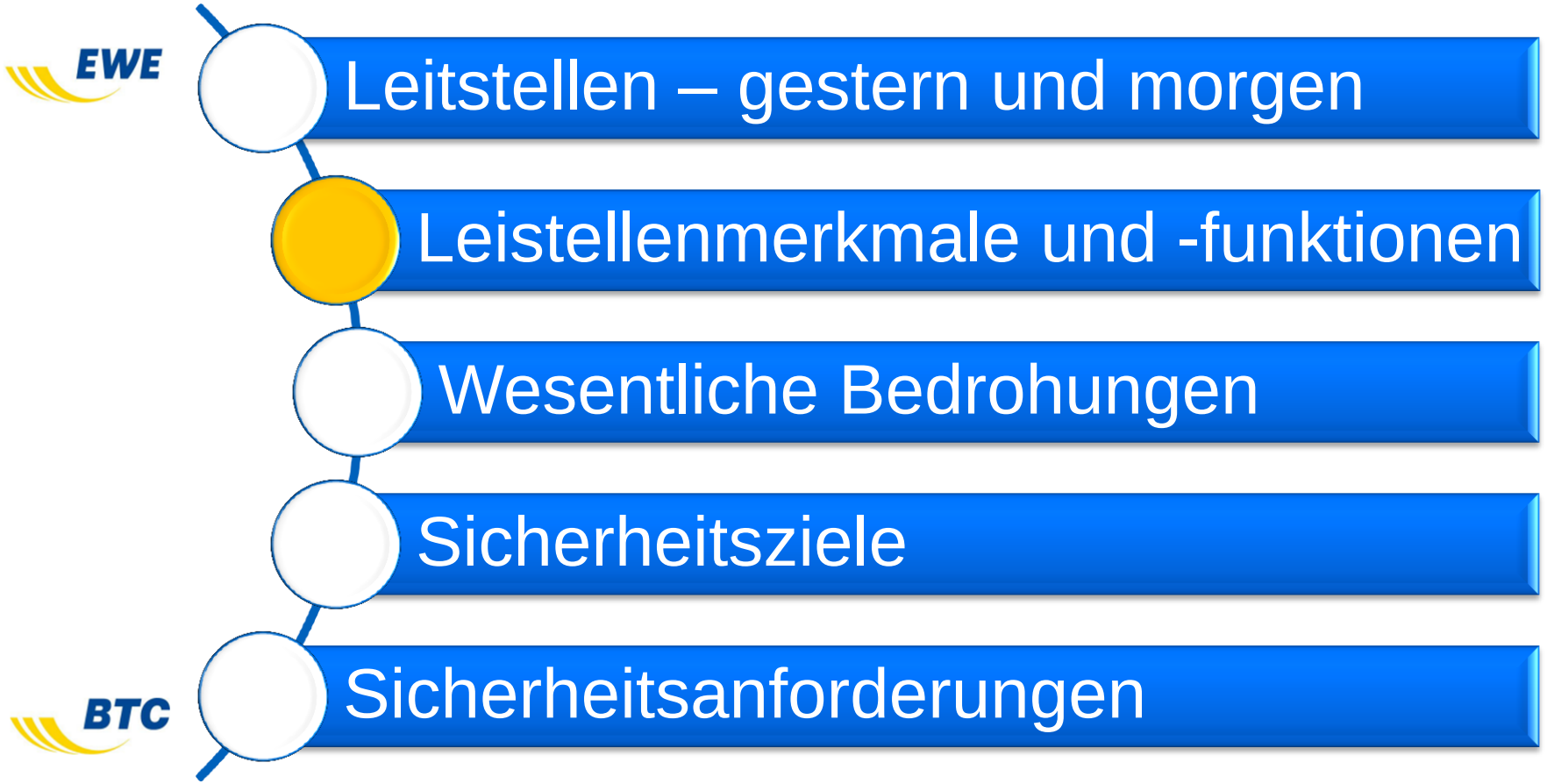
- Erhöhte Funktionalität, z.B. GIS, Grafische Darstellung
- Eine Vielzahl von Schnittstellen und unterschiedliche Protokolle, IP u. Seriell
- Standard „Office“ IT-Systeme (Windows 7, DBMS, Applikationen, WTS…)
- Starke Kopplung zur Büro-IT
- Kommunikation zu externen Komponenten und Drittnetzen

Leitstellen – gestern und morgen

Future Grid



Agenda


EWE
Leitstellen – gestern und morgen
Leistellenmerkmale und -funktionen
Wesentliche Bedrohungen
Sicherheitsziele
Sicherheitsanforderungen
BTC

Leistellenmerkmale und -funktionen

… im Vergleich zur Standard-Büro-IT

	Business IT	Industrial IT
Latency	Limited relevance	Highly critical
Patch management	Often, up to daily	Rarely, needs often additional approval from 3rd party vendor
Management	Centralized	Often standalone
Life time	3 - 5 years	5 - 20 years (unsupported OS like NT and older)
System changes	Often	Rarely
Availability	Reboot is acceptable	24 x 7 x 365
Malware protection	Standard	Complex, often not possible
Awareness	Good	Poor
Vulnerability checks	Standard	Rarely and complex (availability)
Outsourcing	Often	Rarely
Physical security	Safeguarded and closed areas	Unmanned and white areas

Quelle: Symantec

Leistellenmerkmale und -funktionen

Existierende Schnittstellen

- CRM- und ERM-Systeme, Abrechnungssysteme
- Verbrauchs- / Einspeisungs-Datenbanken
- Kommunikation zu Transportnetzbetreiber sowie Leitstellen-Kopplungen (z.B. TASE.2)
- Schnittstellen zu Handelssystemen

- Ortsnetz-Stationen
- Sensorik (Umspannwerke, …)
- Steuer- / Regeleinheiten (Fernwirksysteme)
- Wartungssysteme

Leistellenmerkmale und -funktionen

Protokolle und Schnittstellen

- Kaum oder keine Verschlüsselung
- Transparent und keine Sicherheitsfeatures

Beliebte Protokolle u.a.

- IEC 60870–5–104 Anwendungsbezogene Norm für Fernwirkaufgaben in ***IP-Netzen***
- IEC 60870–5–101 Anwendungsbezogene Norm für Fernwirkaufgaben ***serielle Kommunikation***
- OPC Protokoll

Leistellenmerkmale und -funktionen

- Versorgungsüberwachung
- Steuern / Regeln / Schalten
- Störungsbeseitigung und Koordination
- Instandhaltung und Wartung

… in der Zukunft:

- mehr Prognosen, Steuerung, Management-Funktionen - Energiemanagement
- mehr Komplexität, mehr Kommunikation und
- mehr Schnittstellen

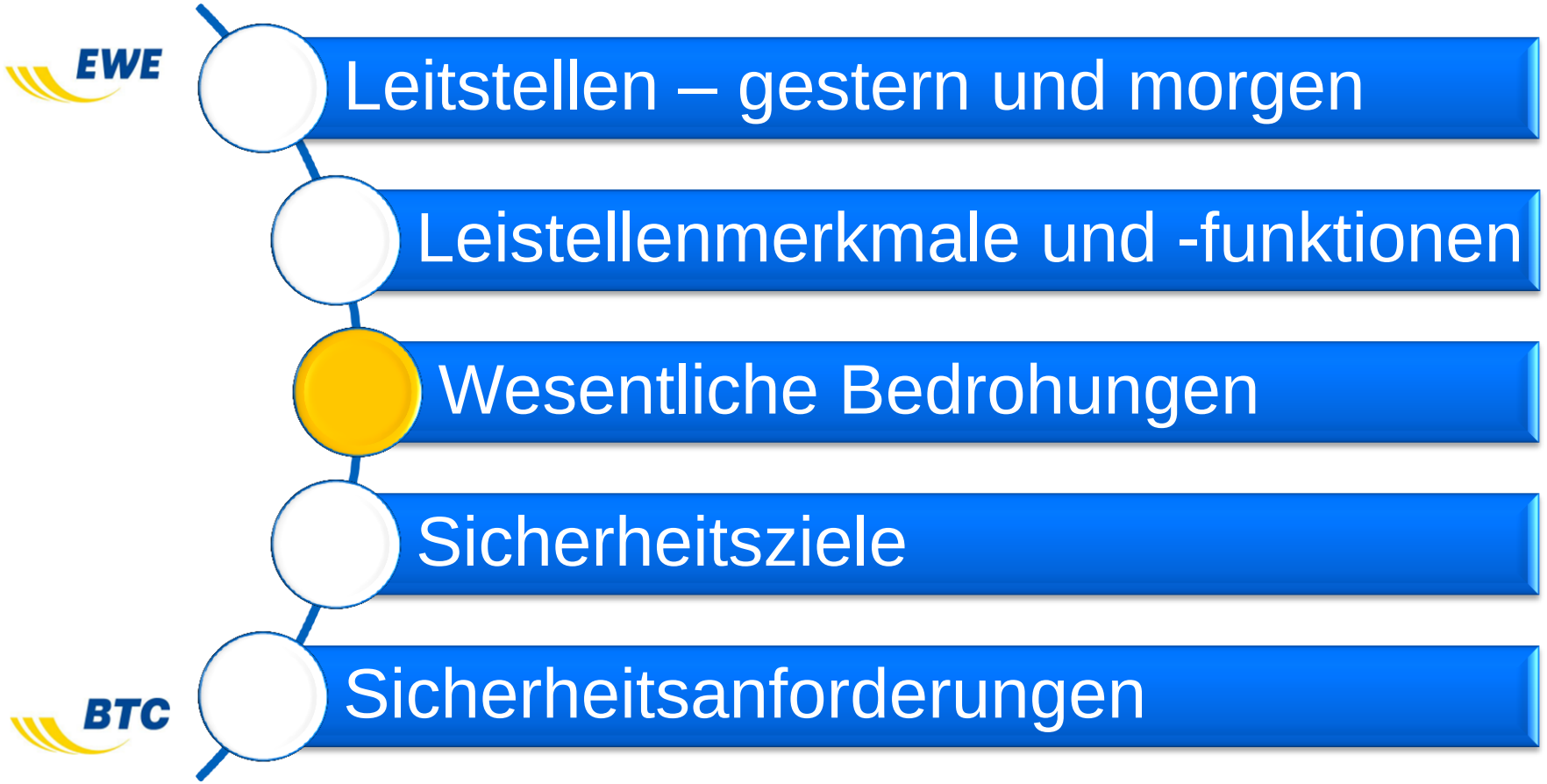
.. bei gleicher Technologie ….

Leistellenmerkmale und -funktionen

Besondere Anforderungen an

- Physikalische Umgebungen
- Technische Komponenten und Schnittstellen
  - „Safety and Security“
- Aufbau- und Ablauforganisation
- Personal
  - Geschultes und sensibles Personal
- ……

Agenda


EWE
Leitstellen – gestern und morgen
Leistellenmerkmale und -funktionen
Wesentliche Bedrohungen
Sicherheitsziele
BTC
Sicherheitsanforderungen

Wesentliche Bedrohungen

- Datenmanipulation (Messdaten)
- DDoS Attacken
- Schadsoftware durch Datenträger
- Man-in-the-Middle (Protokolle)
- Büro-IT
- Menschliches Fehlverhalten
- Fernwartungszugänge
- Komplexität neuer Systeme
- Externe Dienstleister

Wesentliche Bedrohungen

15.04.2013 13:00 « Vorige | Nächste »

Vaillant-Heizungen mit Sicherheits-Leck

Quelle: Heise.de

vorlesen / MP3-Download

Die Vaillant-Heizungsanlagen des Typs ecoPower 1.0 enthalten ein hochkritisches Sicherheitsloch, durch das ein Angreifer die Anlage über das Internet ausschalten und potenziell beschädigen kann. In einem Informationsschreiben rät der Hersteller seinen Kunden daher zu einem drastischen Schritt: Sie sollen den Netzwerkstecker ziehen und auf den Besuch eines Servicetechnikers warten.

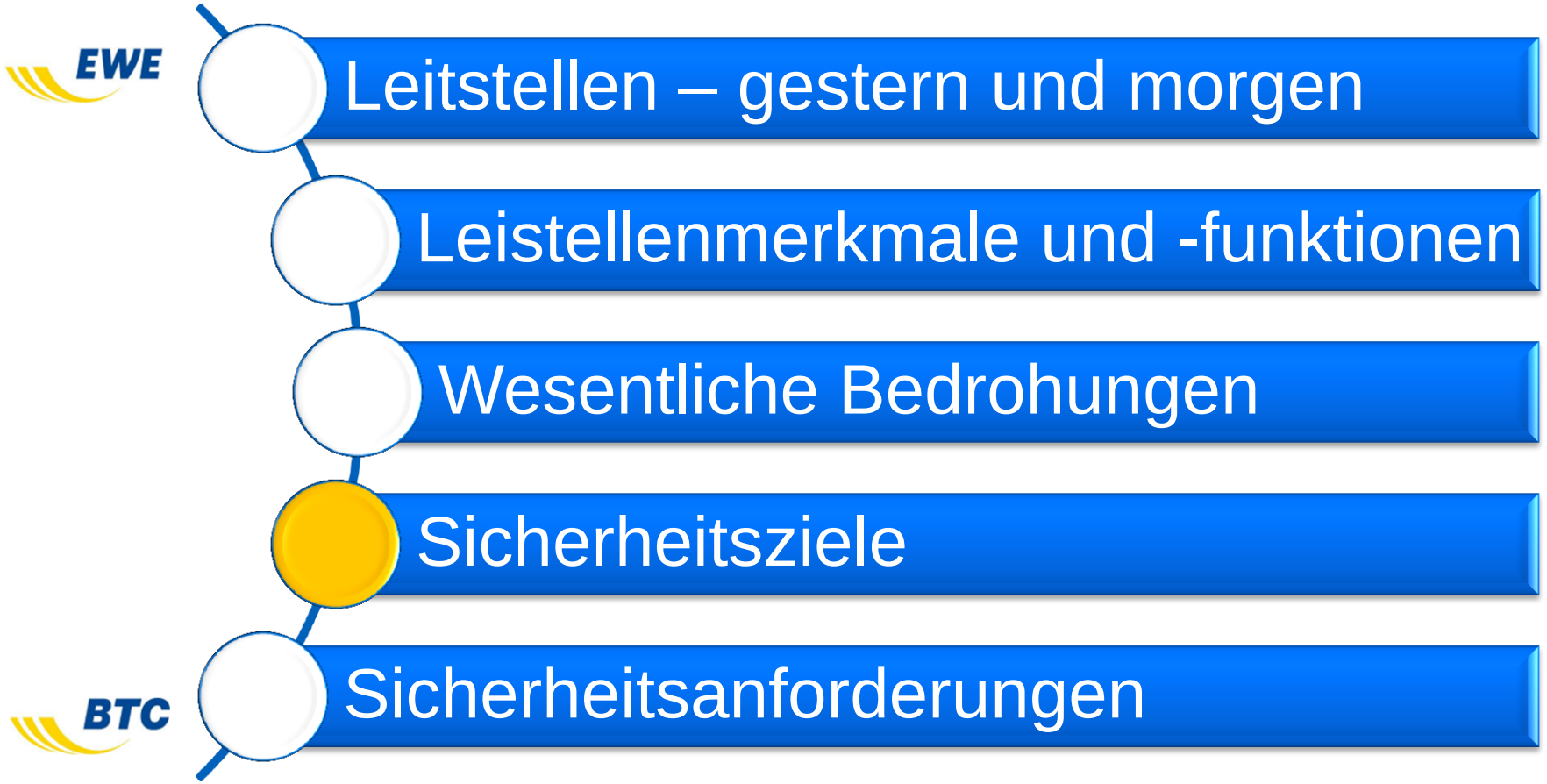
Vaillant ecoPOWER 1.0

Bild: BHKW-Infothek

Bei den für Ein- und Zweifamilienhäuser ausgelegten ecoPower-Anlagen handelt es sich um sogenannte Nano-Blockheizkraftwerke, die aus Gas nicht nur Wärme, sondern gleichzeitig auch Strom produzieren. Die Anlagen sind mit dem Internet verbunden und über ein Webinterface fernsteuerbar – sowohl von ihren Besitzern als auch von Service-Technikern. Allerdings schlummert in diesen Webinterface ein erhebliches Sicherheitsproblem, wodurch man sehr einfach an die Klartext-Passwörter für den Fernzugriff kommt.

Neben dem Kundenpasswort geben die Anlagen auf Zuruf auch das sogenannte Experten- und das Entwicklerpasswort aus; man kann also mit höchstmöglichen Rechten auf das System zugreifen und so etwa die Anlage im Winter ausschalten, wodurch es zu Frostschäden kommen kann. Durch das Erhöhen der Vorlauftemperatur kann es auch im Sommer zu Schäden kommen, sofern angeschlossene Flächenheizungen nicht über einen unabhängigen Temperaturbegrenzer verfügen.

Agenda


EWE
Leitstellen – gestern und morgen
Leistellenmerkmale und -funktionen
Wesentliche Bedrohungen
Sicherheitsziele
Sicherheitsanforderungen
BTC

Sicherheitsziele

Bei klassischer IT:

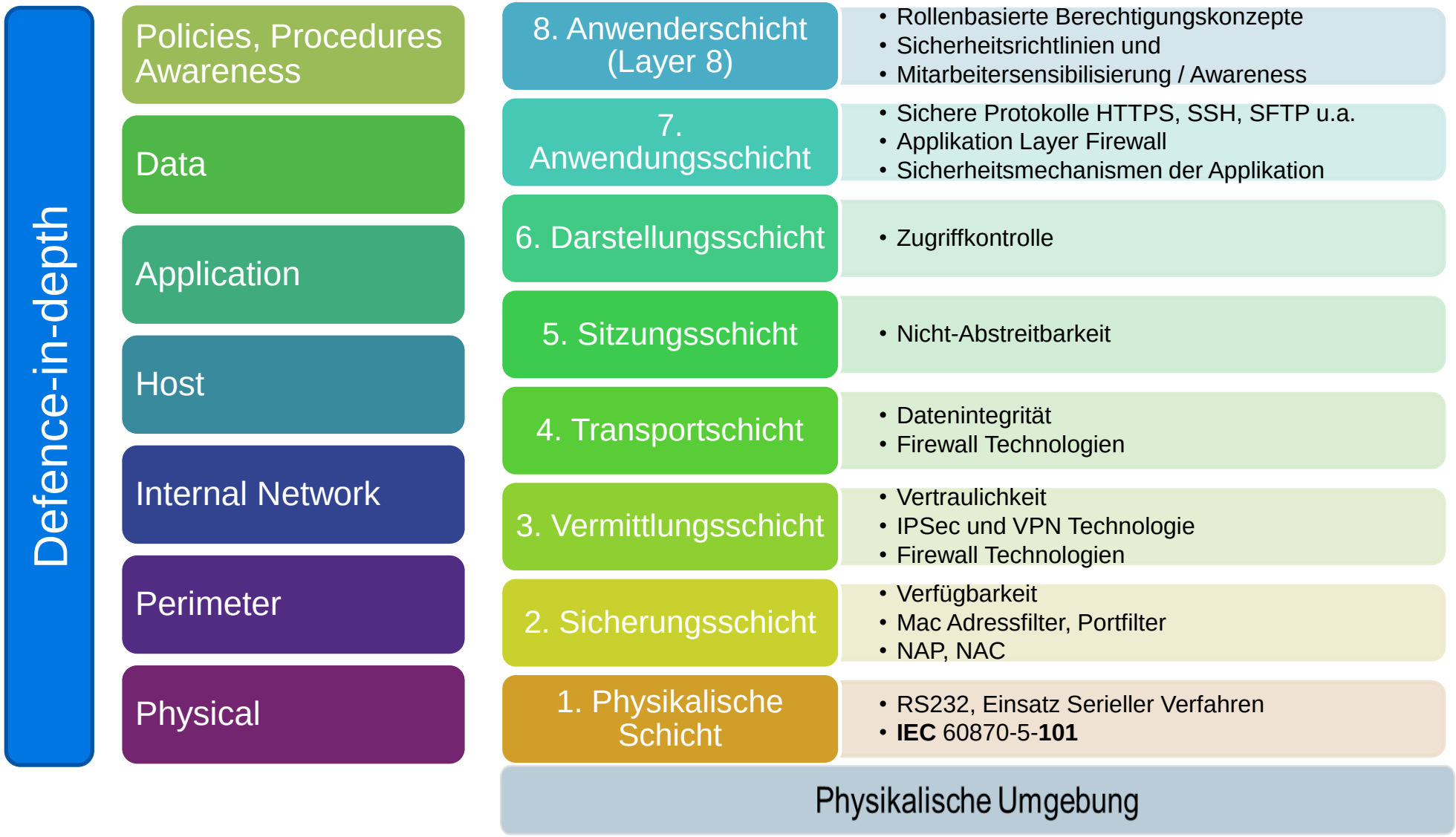
- Fokus: Vertraulichkeit, Verfügbarkeit, Integrität

Bei Leitstellen / Automatisierungstechnik

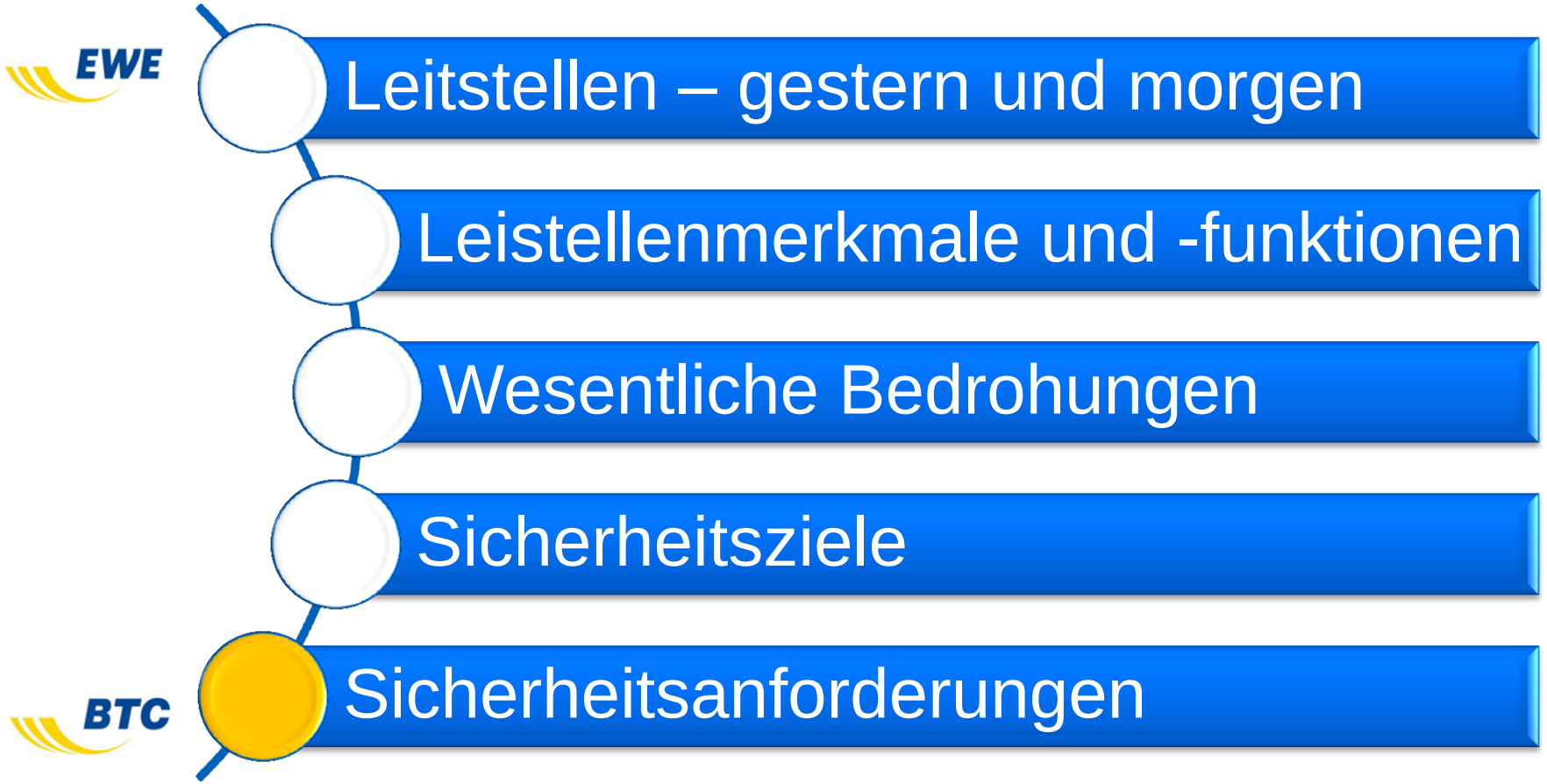
- Fokus: Vertraulichkeit, Verfügbarkeit, Integrität

- zusätzlich Authentizität, Nachvollziehbarkeit etc.

Sicherheitsziele



Agenda


EWE
Leitstellen – gestern und morgen
Leistellenmerkmale und -funktionen
Wesentliche Bedrohungen
Sicherheitsziele
BTC
Sicherheitsanforderungen

Sicherheitsanforderungen

Anforderungen an Hersteller / Lösungsanbieter

- Sichere Entwicklungsumgebung
- Sicherheitskonzepte für Lösungen / Produkte
- Sicherheits-Analysen, Tests der Sicherheitsfunktionen aus Hersteller-Sicht
- Robuste und gehärtete Systeme
- Betriebskonzept

Vertrauenswürdige Komponenten

- Gesicherte Installation / Konfiguration einschließlich Herkunftsprüfung und Härtung
- Getestete / zertifizierte Funktionalität (Politische Würdigung des Herstellers)

Sicherheitsanforderungen

Sichere Schnittstellen

- Gegenseitige Authentisierung / Authentifizierung
- Vertrauliche Kommunikation
- Integritätsgeschütze Kommunikation
- E2E-Sicherheit
- Schutz vor DDoS

Klassische Sicherheitsmechanismen

- Schadsoftware-Prüfung
- Sichere Protokollierung / Archivierung
- Patchmanagement / 3rd. Party Patchmanagement

Sicherheitsanforderungen

Sichere Protokolle / Protokollerweiterungen

- IEC 62351
- IEC 61968
- …..

Redundante Auslegung

- Hard- / Software
- Georedundanz

Wartungszugänge und Fernzugriffe

- Anforderungen an den Client
- Anforderungen an die Authentisierung / Autorisierung
- Anforderungen an Netzwerksicherheit

Sicherheitsanforderungen

Bedienung

- Sichere Authentisierung / Autorisierung
- Nutzer / Berechtigungssysteme
- PKI bzw. Token-Administration für sichere Authentisierungen
- Ggf. sichere Single-Sign-On-Systeme

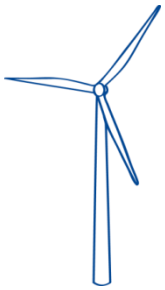
Sichere Netze und Netzübergänge

- Authentisierung / Autorisierung der Komponenten im Leitstellen Netz
- Firewalls, Gateways, Schleusen-PCs, IDRS, VPN
- Trennung Administrations- und Wirksystem-Netze
- Trennung von Büro-IT und Leistellen-IT
- System- und netzwerktechnische Trennung unterschiedlich kritischer Systeme
- Zonenmodelle

Sicherheitsanforderungen

Manipulationsgeschützte Komponenten / Software / Daten

- „Safety and Security“
- Gehärtete und geschützte Systeme
- Mögliche Zertifizierung



Hochverfügbarkeit

- Systeme / internes Netz
- Telekommunikationsnetz kritischer Komponenten
- Telefonnetz (ggf. dedizierte Kanäle zu Polizei/ Feuerwehr – Tetra / Satellitentelefone)

Sicherheitsanforderungen

Informationssicherheitsmanagement

- ISMS (Schaffung einer IT-Sicherheitsorganisation / Sicherheitsbeauftragten / PDCA-Zyklus)
- Standards und Best Practices wie ISO/IEC 2700x, NIST SP800

Organisatorische Prozesse

- Rollentrennung (Need-to-know)
- Geklärte Abbildungen für Personalführung / Aufsicht
- Sichere Prozessabbildungen für Betriebsvorgänge
- Sicherer Lifecycle für Nutzer- / Access-Management
- Schalt- und Steuerungsfunktionen
- Bei kritischen Prozessen: Mehr-Augen-Prinzipien

Sicherheitsanforderungen

Prozessbeschreibungen und Dokumentation

- Betriebshandbücher
- Notfallhandbücher

Personal

- Betroffen sind: Personal für Bedienung, Management und auch Hersteller /Zulieferer:
- Fachkundenachweis und Awareness
  - Vertrauenswürdigkeit / Polizeiliches Führungszeugnis
  - Regelmäßige Prüfung
- Mehr-Augen-Prinzipien
- Verfügbarkeit einschl. Bereitschaft, Wohnort-Nähe, Überwachung der "Funktionsfähigkeit / Lebendigkeit"

Sicherheitsanforderungen

Physikalische Sicherheit

- Schutz vor unberechtigtem Zutritt / Zugang (Zutritt-Kontroll-Systeme)
- Gebäude und Geländesicherung
- Schließsysteme
- Videoüberwachung
- Notstrom-Stromversorgung (USV, Batterie / Dieselaggregate etc.)
- Schutz vor Feuer / Wasser
- Sichere Notöffnungen
- Ggf. Tierabbildungen
- Ggf. Nutzung von biometrischen Merkmale
- Ggf. Personenschleusen
- Zertifizierungen der Technik / Rechenzentren

Sicherheitsanforderungen

Umgang mit Sicherheitsereignissen

- Fehlerhafter Software / Sicherheitslücken
- Sicherstellung rechtzeitiger Lieferung von Patches
- Software-Subscription
- Integration in den CERT Verbund
- Sicherstellung rechtzeitiger Lieferung von Patches / Wartungsverträge

Nachschlagen

- ISO/IEC 2700x
- ISO/IEC TR 27019 – DIN SPEC 27009
- BDEW Whitepaper
- BDEW WP Umsetzungsempfehlung (Österreich / Deutschland)
- NIST SP 800-82, -53, -39
- IEC 62351Netzführungssysteme und ihr Informationsaustausch – Daten- und Kommunikationssicherheit
- IEC 62443 IT-Sicherheit in der Automatisierungstechnik
- Allianz für Cybersicherheit
- VDI/VDE, BSI
- ……

Vielen Dank für Ihre Aufmerksamkeit.

BTC Business Technology Consulting AG
Escherweg 5
26121 Oldenburg
Tel. 0441 / 36 12-0
www.btc-ag.com

Fragen?

Die Standorte der BTC AG

Hauptsitz:

Escherweg 5
26121 Oldenburg
Fon: + 49 441 3612-0
Fax: + 49 441 3612-3999
E-Mail: office-ol@btc-ag.com
www.btc-ag.com

Kurfürstendamm 33
10719 Berlin
Fon: + 49 30 88096-5
Fax: + 49 30 88096-777
E-Mail: office-b@btc-ag.com

Weser Tower
Am Weser-Terminal 1
28217 Bremen
Fon: +49 421 33039-0
Fax: +49 421 33039-399
E-Mail: office-hb@btc-ag.com

Wittekindstraße 32
44139 Dortmund
Fon: +49 231 981288-0
Fax: +49 231 981288-12
E-Mail: office-do@btc-ag.com

Bartholomäusweg 32
33334 Gütersloh
Fon: +49 5241 9463-0
Fax: +49 5241 9463-55
E-Mail: office-gt@btc-ag.com

Willy-Brandt-Str. 51
20457 Hamburg
Fon: +49 40 210098-0
Fax: +49 40 210098-76
E-Mail: office-hh@btc-ag.com

Klostergasse 5
04109 Leipzig
Fon: +49 341 350558-0
Fax: +49 341 350558-59
E-Mail: office-l@btc-ag.com

Wilh.-Th.-Römheld-Str. 24
55130 Mainz
Fon: + 49 6131 88087-0
Fax: + 49 6131 88087-99
E-Mail: office-mz@btc-ag.com

Türkenstraße 55
80799 München
Fon: +49 89 3603539-0
Fax: +49 89 3603539-59
E-Mail: office-m@btc-ag.com

An der Alten Ziegelei 1
48157 Münster
Fon: +49 251 14132-0
Fax: +49 251 14132-11
E-Mail: office-ms@btc-ag.com

Konrad-Zuse-Straße 3
74172 Neckarsulm
Fon: +49 (7132 380-0
Fax: +49 7132 380-29
E-Mail: office-nsu@btc-ag.com

Çayiryolu 1, Partaş Center Kat: 11-12
Içerenköy, 34752 Istanbul
Türkei
Fon: +90 (216) 5754590
Fax: +90 (216) 5754595
E-Mail: office-ist@btc-ag.com

ul. Małe Garbary 9
61-756 Poznań
Polen
Fon: +48 (0) 61 8560970
Fax: +48 (0) 61 8501870
E-Mail: biuro-poz@btc-ag.com

Hasebe Build.11F,
4-22-3 Sendagi, Bunkyo-Ku,
113-0022 Tokyo
Japan
Fon: +81 (3) 5832 7020
Fax: +81 (3) 5832 7021
E-Mail: Info.OSCJapan@btc-es.de

Bäulerstraße 20
CH-8152 Glattbrugg
Schweiz
Fon: +41 (0) 44 874 3000
Fax: +41 (0) 44 874 3010
E-Mail: office-zh@btc-ag.com