ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

Austrian Power Grid

INFORMATIONSSICHERHEIT IN DER ENERGIEVERSORGUNG – NIS-G

Oliver Skrbinjek, Manuel Mesgec – Energienetze Steiermark GmbH, Graz
Andreas Stockner, Dr. Georg Achleitner – Austrian Power Grid AG, Wien

Agenda

- Rahmenbedingungen und deren Inhalte
- Assets im Focus von NIS-G
- Ziele und Methoden
- Folgen für Unternehmen
- Zusammenfassung

Kommt ihnen das bekannt vor?

Austrian Power Grid

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

00000000

- Launch-Code für die in den USA stationierten Atomraketen (1962 bis 1977)

Quelle: http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html

Rahmenbedingung und Inhalte

Gesetzliche Rahmenbedingungen

Austrian Power Grid

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

Rahmenbedingung	Geltung	Gültigkeit	Inhalt
NIS – Richtlinie Richtlinie 2016/1148		**07.2016**	Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.
NIS – Gesetz 111. Bundesgesetz		**12.2018**	111. Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz und Informationssystemen (NISG) erlassen und das Telekommunikationsgesetzt 2003 geändert wird.
NIS – Verordnung 215. Verordnung des BM		**07.2019**	Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (NISV).
NIS – Fact-Sheets		**08.2019**	Nähere Erläuterung der genannten Sicherheitsmaßnahmen der NISV, um Betreiber wesentlicher Dienste bei der Umsetzung der Vorgaben aus dem NISG und der NISV zu unterstützen.

Rahmenbedingung und Inhalte

Gesetzliche Rahmenbedingungen – NIS-V

Austrian Power Grid

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

BUNDESGESETZBLATT

FÜR DIE REPUBLI

Jahrgang 2019 Ausgegel

215. Verordnung: Netz- und Informationssyste

215. Verordnung des Bundesministers für EU, von Sicherheitsvorkehrungen und näheren Sicherheitsvorfällen nach dem Netz- und Info Informationssystemsicherheitsverordnung – NI

Auf Grund des § 4 Abs. 2 des Netz- und Infor Nr. 111/2018, wird im Einvernehmen mit dem Bundest

Inhaltsverz

1. Absch Allgemeine Bes

§ 1. Gegenstand der Verordnung
§ 2. Begriffsbestimmungen zu wesentlich
§ 3. Begriffsbestimmungen zu Sicherheits

2. Absch Wesentliche Dienste un

§ 4. Sektor Energie
§ 5. Sektor Verkehr
§ 6. Sektor Bankwesen
§ 7. Sektor Finanzmarktinfrastrukturen
§ 8. Sektor Gesundheitswesen
§ 9. Sektor Trinkwasserversorgung
§ 10. Sektor Digitale Infrastruktur

3. Absch Sicherheitsvor

§ 11. Sicherheitsvorkehrungen

4. Absch Schlussbesti

§ 12. Personenbezogene Bezeichnungen
§ 13. Verweisungen
§ 14. Inkrafttreten

2. Abschnitt

Wesentliche Dienste und Sicherheitsvorfälle

Sektor Ener

§ 4. (1) Wegen ihrer Bedeutung für die Aufrechterh im Sinne des § 16 Abs. 2 NISG sind im Sektor Energie we

1. im Teilsektor Elektrizität
   a) im Bereich der Stromerzeugung
      aa) der Betrieb einer Erzeugungsanlage, die m
      bb) der Betrieb von Systemen zur Steuerung v 340 MW Engpassleistung haben;
   b) im Bereich der Stromverteilung der Betrieb ein als 88 000 Zählpunkte transportiert wird, oder
   c) im Bereich der Stromübertragung der Übertragungsnetzbetreiber;
2. im Teilsektor Erdöl
   a) im Bereich der Erdölförderung der Betrieb vo geförderte Menge mehr als 20% Anteil ar ausmacht;
   b) im Bereich der Erdöllagerung der Betrieb ei Form von Erdöl, Erdölprodukten, Biokraftstof Biokraftstoffen gelagert werden, und die einen
   c) im Bereich des Erdöltransports der Betrieb Menge vier Millionen Tonnen pro Jahr überste
   d) im Bereich der Erdölraffination der Betrieb vo Erdöl, die mehr als acht Millionen Tonnen pro
3. im Teilsektor Erdgas
   a) im Bereich der Gasförderung der Betrieb vo Menge mehr als 20% Anteil am jährlichen Inla
   b) im Bereich der Gasspeicherung der Betrieb ei Arbeitsgasvolumen pro Jahr hat;
   c) im Bereich des Gastransports der Betrieb einer
   d) im Bereich der Gasverteilung der Betrieb ein 88 000 Zählpunkte transportiert wird;
   e) im Bereich des Marktgebietsmanagements Einsatzes von Netzpufferung (Linepack Ausgleichsenergie;
   f) im Bereich des Verteilergebietsmanagements

(2) Im Sektor Energie liegt ein Sicherheitsvorfall im Sinne des § 3 Z 6 NISG vor, wenn

1. im Teilsektor Elektrizität
   a) im Bereich der Stromerzeugung
      aa) bei dem in Abs. 1 Z 1 lit. a sublit. aa genannten Dienst die Erzeugungsleistung einer Erzeugungsanlage in Summe um mehr als 340 MW verringert ist;
      bb) bei dem in Abs. 1 Z 1 lit. a sublit. bb genannten Dienst die von den Systemen steuerbare Erzeugungsleistung aller Erzeugungsanlagen in Summe um mindestens 340 MW verringert ist;
   b) im Bereich der Stromverteilung der in Abs. 1 Z 1 lit. b genannte Dienst für mehr als 1 056 000 Zählpunktstunden ausfällt oder nur eingeschränkt verfügbar ist;
   c) im Bereich der Stromübertragung der in Abs. 1 Z 1 lit. c genannte Dienst für mehr als drei Stunden ausfällt oder nur eingeschränkt verfügbar ist;
2. im Teilsektor Erdöl
   a) der in Abs. 1 Z 2 lit. a genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;
   b) der in Abs. 1 Z 2 lit. b genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;
   c) bei dem in Abs. 1 Z 2 lit. c genannten Dienst die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet mehr als einen Mitgliedstaat der Europäischen Union betrifft;
   d) der in Abs. 1 Z 2 lit. d genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;
3. im Teilsektor Erdgas
   a) im Bereich der Gasförderung der in Abs. 1 Z 3 lit. a genannte Dienst für mehr als 24 Stunden ausfällt oder nur eingeschränkt verfügbar ist;
   b) im Bereich der Gasspeicherung der in Abs. 1 Z 3 lit. b genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;
   c) im Bereich des Gastransports bei dem in Abs. 1 Z 3 lit. c genannten Dienst die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet mehr als einen Mitgliedstaat der Europäischen Union betrifft;
   d) im Bereich der Gasverteilung der in Abs. 1 Z 3 lit. d genannte Dienst für mehr als 1 056 000 Zählpunktstunden ausfällt oder nur eingeschränkt verfügbar ist;
   e) im Bereich des Marktgebietsmanagements der in Abs. 1 Z 3 lit. e genannte Dienst für mehr als zwölf Stunden ausfällt oder nur eingeschränkt verfügbar ist;
   f) im Bereich des Verteilergebietsmanagements einer der in Abs. 1 Z 3 lit. f genannten Dienste für mehr als zwöf Stunden ausfällt oder nur eingeschränkt verfügbar ist.

Wer ist Betreiber wesentlicher Dienste

Meldewesen (CERT)

Rahmenbedingung und Inhalte

Rahmenbedingungen der Branche / Norm

Austrian Power Grid

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

Rahmenbedingung	Geltung	Inhalt
B3S Österreichs Energie		Definition des Branchen-Focus von relevanten Assets, Segmentierung von Technologien und Zonen mit unterschiedlichem Schutzbedarf.
WhitePaper Österreichs Energie, BDEW	bdew Energie. Wasser. Leben.	Definition von grundsätzlichen Sicherheitsanforderungen für Steuerungs- und Telekommunikationssysteme für die Prozesssteuerung in der Energieversorgung sowie Ausführungshinweise zu deren Umsetzung.
ISO 27001	ISO	Spezifiziert Anforderungen an ein Informations-Sicherheits-Management-System (ISMS) anhand dessen ein Erfüllungsgrad der Konformität nachvollziehbar ist. Daher ist seitens ISO27001 eine Beurteilung und Zertifizierung möglich.
ISO 27002	ISO	Empfehlungen für diverse Kontrollmechanismen für die Informationssicherheit. Aufgabenfelder für Risikoanalyse und –bewältigung sowie Kontrollpunkte und technikneutrale Handlungsanweisungen auf konzeptioneller Ebene.
ISO 27019	ISO	Fachspezifische Subnormen. Richtlinien für das Informationssicherheitsmanagement basierend auf ISO 27002 für energiewirtschaftliche Prozessleit-, Automatisierungs-, Control- und Schutzsysteme.
IEC 62351	IEC	Standard mit den Sicherheitszielen Authentifizierung mit Signatur, Rollbased-Access, Integrität, Vertraulichkeit und Spoofing sowie die Erkennung von Anomalie.
IEC 62443	IEC	Informationssicherheit für Netze und Systeme in der industriellen Kommunikation.

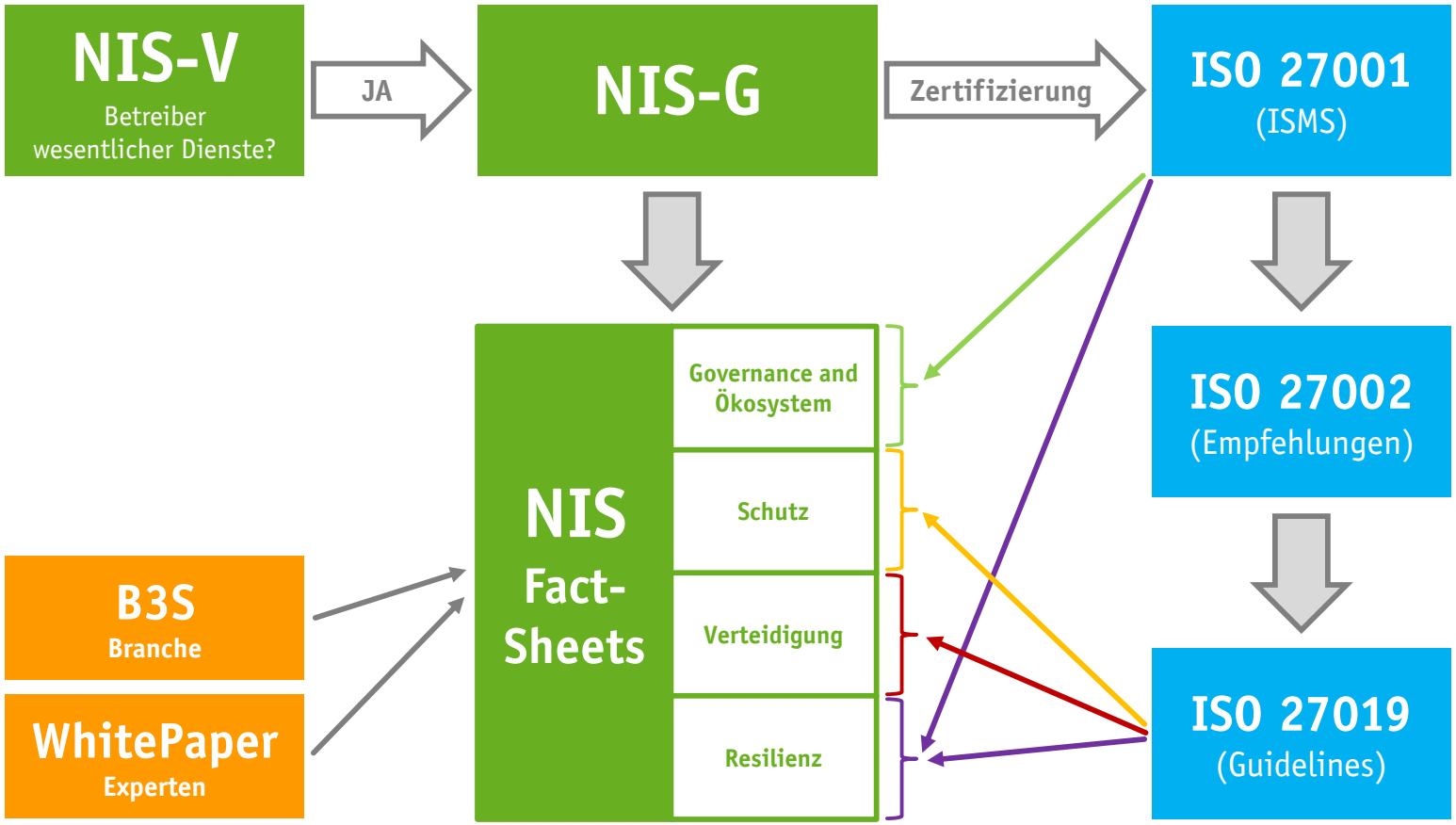
Rahmenbedingungen und Inhalt

Zusammenwirken der Rahmenbedingungen

Austrian Power Grid

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK



Assets im Focus von NIS-G

Definition des Focus

Austrian Power Grid

ENERGIE NETZE STEIERMARK

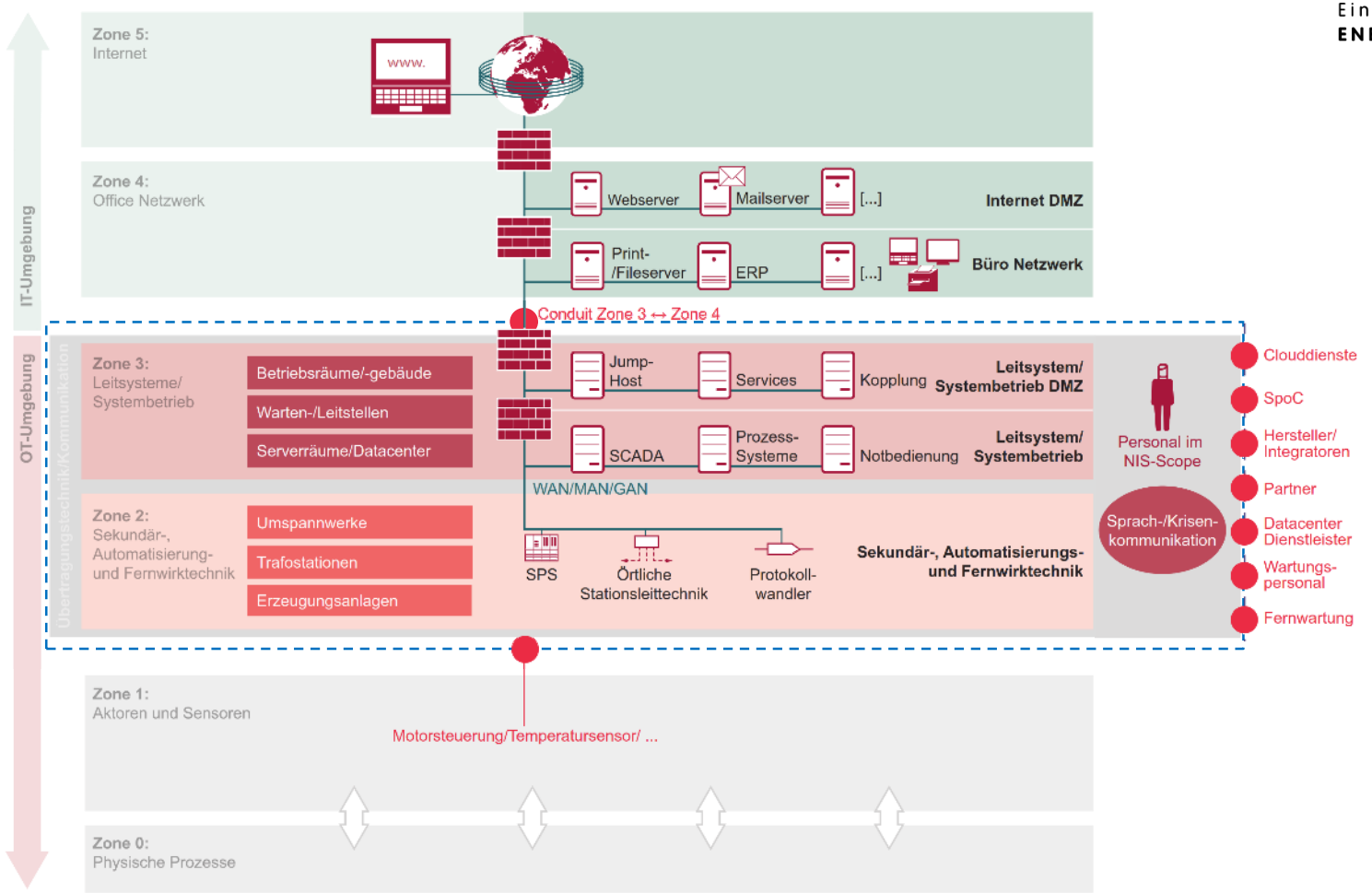
Ein Unternehmen der ENERGIE STEIERMARK

§ 17. (1) Zur Gewährleistung der NIS haben Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist,
angemessen zu sein.

Quelle: BUNDESGESETZBLATT FÜR DIE REPUBLIK ÖSTERREICH, 111. Bundesgesetz: Netz- und Informationssystemsicherheitsgesetz – NISG und Änderung des Telekommunikationsgesetzes 2003

Assets im Focus von NIS-G

Zonen-Modell



Quelle: Österreichs Energie: Entwurf B3S

Ziele und Methoden

Austrian Power Grid

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

Governance und Ökosystem

Schutz

Verteidigung

Resilienz

Ziele und Methoden

Austrian Power Grid

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

Risikoanalyse Ressourcen
Sicherheitsrichtlinie Zyklische Prüfung
Lieferantenbeziehung Personalwesen
Leistungsvereinbarungen

Systemkonfiguration Verantwortung
Filterung Verwaltung relevanter Assets
Vertraulichkeit, Authentizität, Integrität Rollen
Segmentierung nach Schutzbedarf Zweck-Bindung
Autorisierung eindeutige Benutzerkonten
Sichere Fernwartung Minimalrechtprinzip
Wartbarkeit Physischer Schutz

Protokollierung
Erkennung Monitoring
Analyse Vorfallsreaktion
Vorfallsmeldung
Korrelation

Betriebskontinuität
Notfallmanagement
Kriesenmanagement

Ziele und Methoden

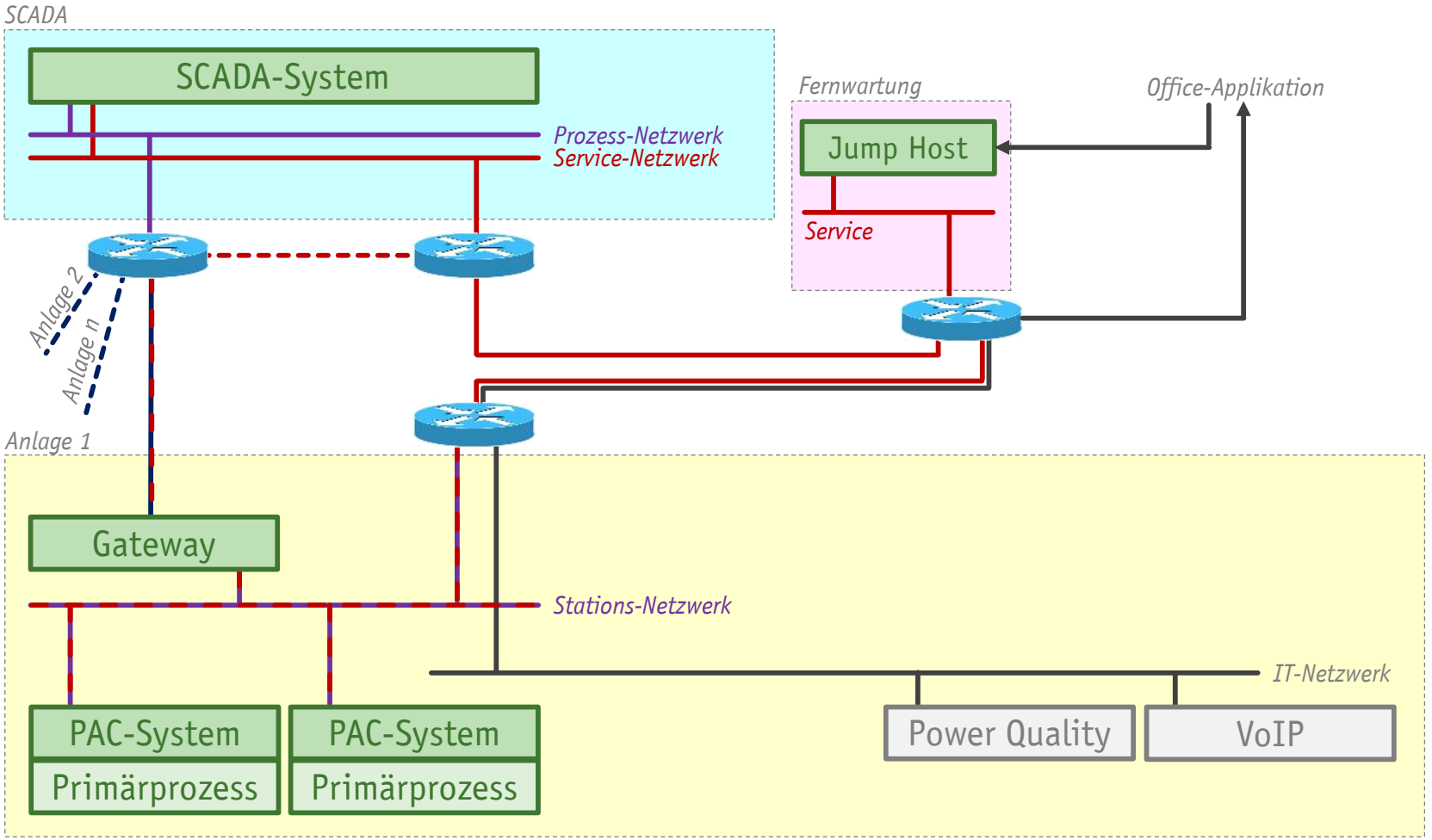
Maßnahmen zur Zielerreichung

- Domänentrennung IT/OT (Office-Netze/technische-Netze)
  → *AD, DNS, Radius/LDAP, SIEM - Syslog/SNMP, PKI, WSUS, …*
- Vertikale Segmentierung innerhalb der OT-Domäne
  → *SCADA/Leitsystem, zentrale Management-/Serviceanwendungen und Stationen/Anlagen (Level 3 - 1 gemäß ICS Security Reference Architecture)*
  ggf. IP-Stack-Bruch zwischen Schutzzonen, (Application-) Firewall, Datendiode, …
- Horizontale Segmentierung innerhalb eines Segments
  → *Redesign von dezentralen Netzwerkssegmenten, segmentieren von Diensten und Services*
- Horizontale Segmentierung nicht relevanter Assets
  → *VoIP, Zählwerterfassung, Objektschutz, Power Quality, …*
- Härtung von Systemkomponenten und Netzen
- Patch-Management, …, und noch viele weitere

Ziele und Methoden

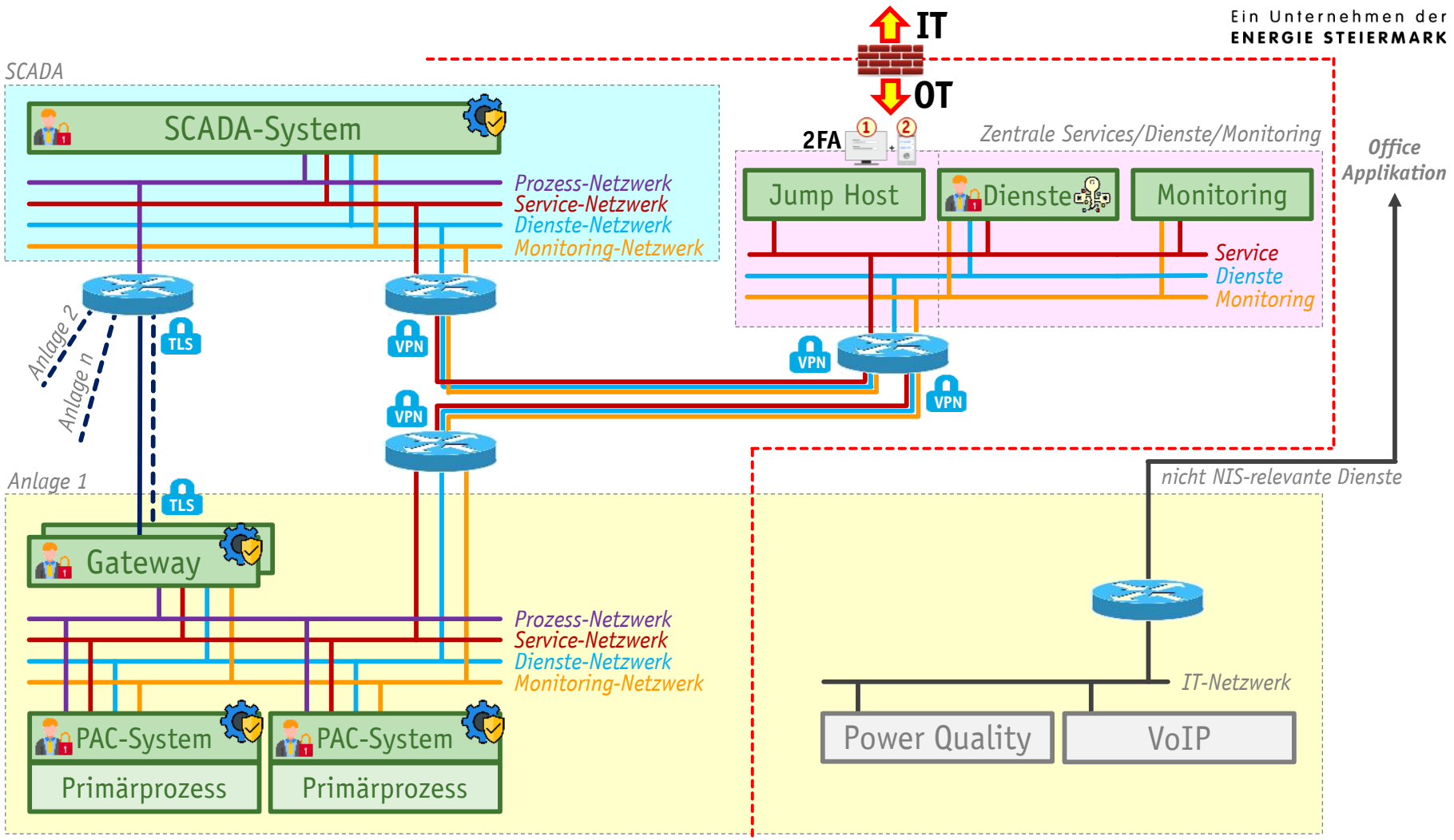
Folgen für Unternehmen

Legacy vs. neues Systemdesign



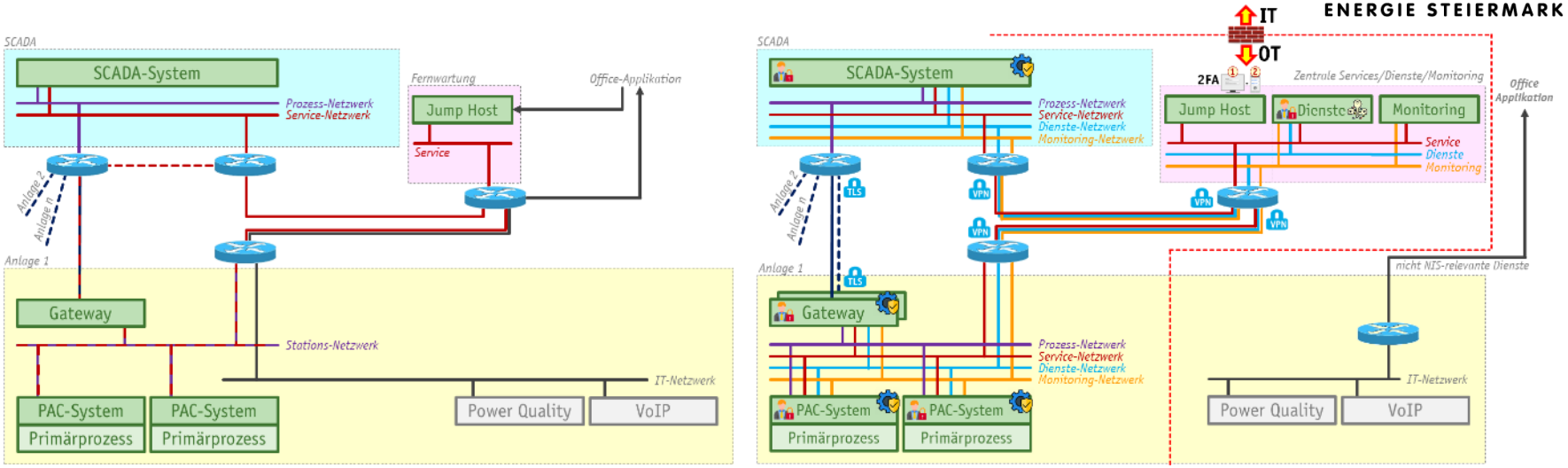
Folgen für Unternehmen

Legacy vs. neues Systemdesign



Folgen für Unternehmen

Legacy vs. neues Systemdesign

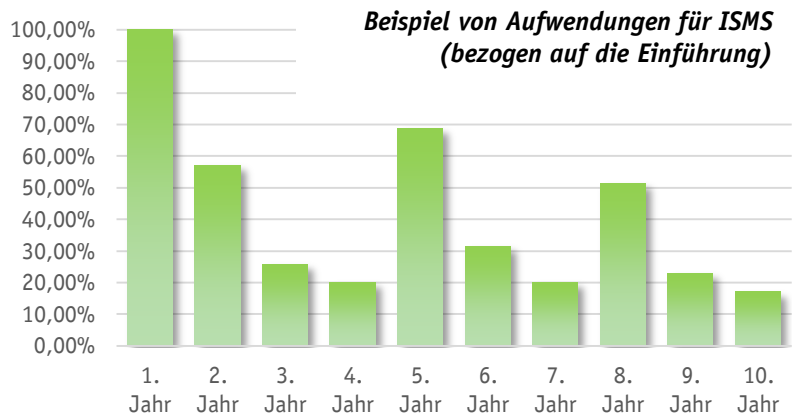


- Konzeption erstreckt sich über viele Know-How-Bereiche → Know-How / Ressourcen
- Bestehende Datenstrukturen können meist nicht weiter genutzt werden → Investition
- Legacy-Systeme technisch ungeeignet (EoL: 15 – 20 Jahre) → Risikoverlagerung
- Neue Schnittstellen eröffnen neue Risiken → Standardisierung
- Managen des Übertragungs- oder Verteilernetzes und eines Datennetzwerks → Focus

Folgen für Unternehmen

ISMS

- Risikoanalyse für NIS-relevante Assets und Domänen
  (betriebliche Auswirkungen von Vorfällen hinsichtlich Funktion des Gemeinwesen bewerten)
- Erstellen und aktualisieren von Sicherheitsrichtlinien
  (strategische Ziele, Dokumentation Risikomanagement, Verweis auf Richtlinien u. Guidlines)



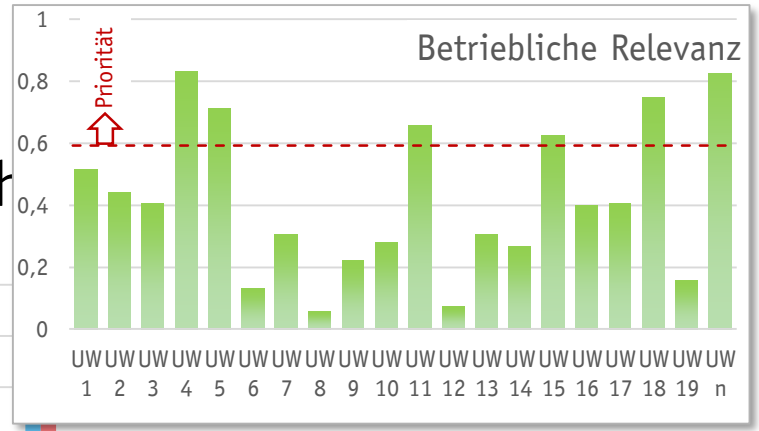
Im ersten Jahr Einführung, gefolgt von Perioden der Nachjustierung und der Kontrollen

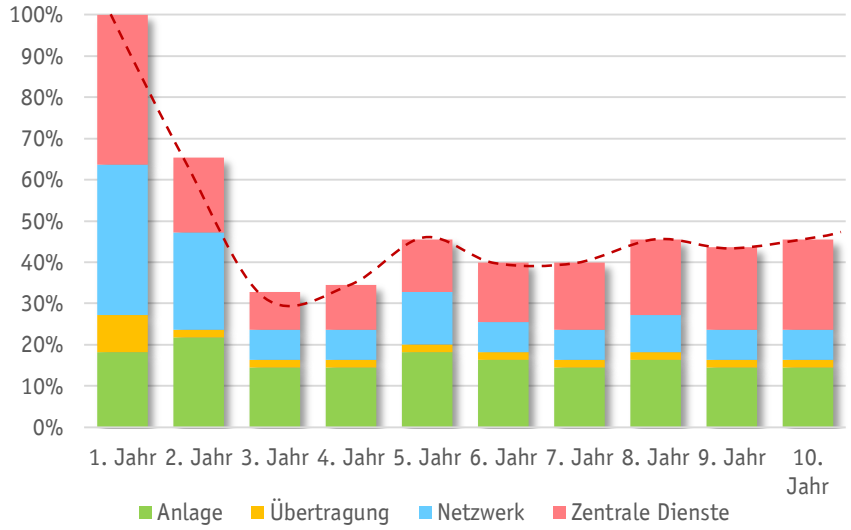
- Überprüfung der Netz und Informationssysteme
- Ressourcen- und Personalplanung und Management
- Definition von Lieferantenbeziehungen und Vereinbarungen

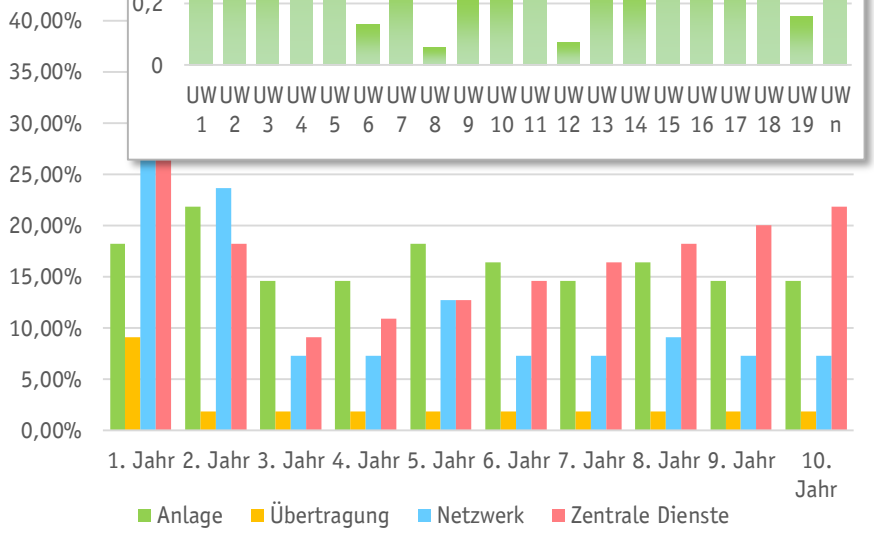
Folgen für Unternehmen

Integration und Betrieb – „Schutz“

- Schutz entsprechend Klassifizierung
  (Auswirkung, Betriebsführungsrelevanz, …)
- Standardisiertes Design mit Rücksich





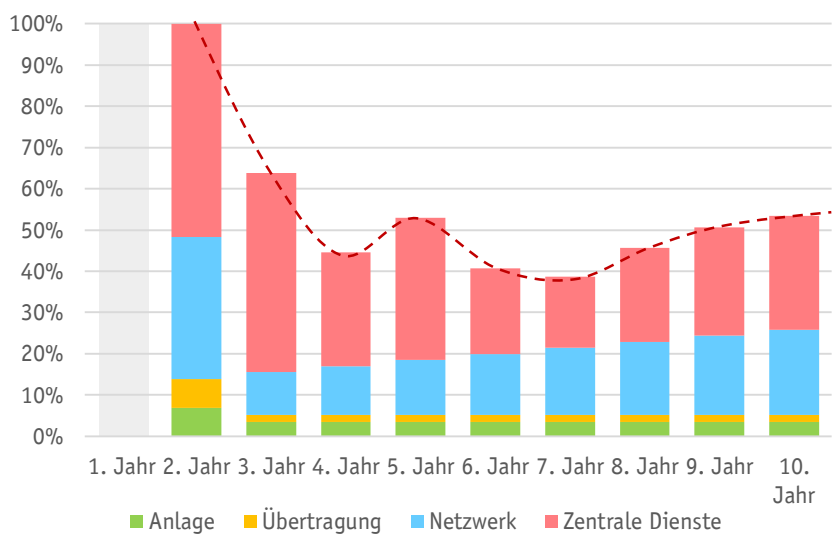


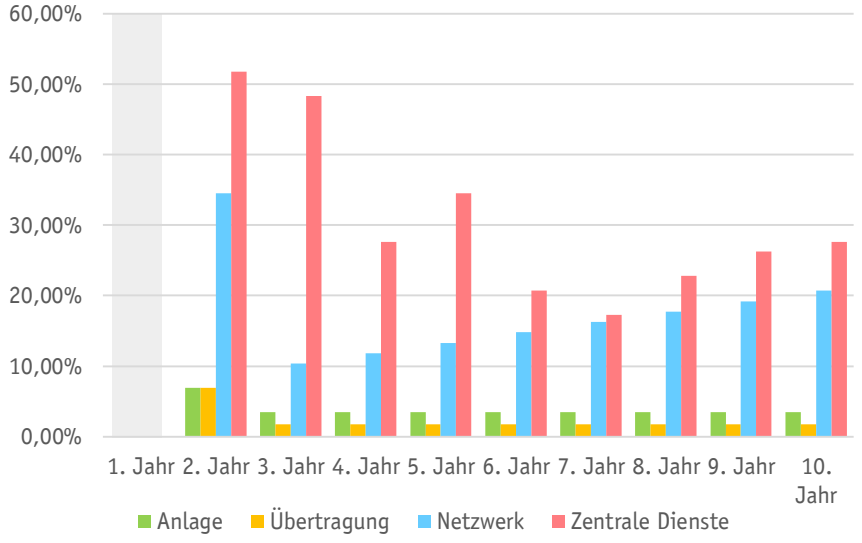
Beispiel von personellen Aufwendungen für den „Schutz“ auf Basis der NIS-Fact-Sheets (bezogen auf die Einführung)

Folgen für Unternehmen

Integration und Betrieb – „Verteidigung“

- Für die Verteidigung sollte ein Basissystem vorhanden sein
- Geeignetes Systemdesign (Netzwerk, zentrale Dienste)





Beispiel von personellen Aufwendungen für die „Verteidigung“ auf Basis der NIS-Fact-Sheets (bezogen auf die Einführung)

Zusammenfassung

Austrian Power Grid

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

- Neue Rahmenbedingungen = neue Konzepte
- Aufwände durch NIS-G = zusätzliche Ressourcen
- Operativer Betrieb der Asset wird komplexer
- Integration wirtschaftlich über EoL-Zyklus

- Ist morgen nicht schon heute?
- Berufsbild: Energie- bzw. Sekundärtechnikers?

ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

Austrian Power Grid

INFORMATIONSSICHERHEIT (NIS-G)

Oliver Skrbinjek, oliver.skrbinjek@e-steiermark.com, Energienetze Steiermark GmbH, Graz
Andreas Stockner, andreas.stockner@apg.at, Austrian Power Grid AG, Wien
Manuel Mesgec, manuel.mesgec@e-steiermark.com, Energienetze Steiermark GmbH, Graz
Dr. Georg Achleitner, georg.achleitner@apg.at, Austrian Power Grid AG, Wien