Agenda

Teil I Vorstellung und Motivationen

Teil II Vorgehensweise Risikoanalyse

Teil III PPD-Prozess E-Wirtschaft

Teil IV Diskussion

RELEASE TO PUBLIC

Teil I Grundsätze und Ziele (1)

Ziele und **Vorgehensweise** der Arbeitsgruppe:

- Gemeinsame **Erhöhung der Sicherheit** in der Energiewirtschaft
- **Gemeinschaftliche, abgestimmte, harmonische Erarbeitung** von Mindestsicherheitsstandards durch die Energiebranche

- **Großflächige, langanhaltende Störungen** der IKT-Infrastruktur mit Auswirkungen auf die Stromversorgung erfassen, bewerten und Empfehlungen erstellen

Nicht-Ziele:

» Sicherheitsvorschriften von „außen" abwarten

RELEASE TO PUBLIC

Teil I Einführung und Hintergründe

» Schaffung von Strukturen und Prozessen für den **Informationsaustausch zwischen Betreibern kritischer Infrastruktur, Behörden und Gesellschaft**

» Diskussionen über einen **adäquaten ordnungspolitischen Rahmen:**
- Meldeverpflichtungen
- regulatorische Maßnahmen
- freiwillige Selbstverpflichtungen
- Definition von allgemeinen **Mindeststandards**

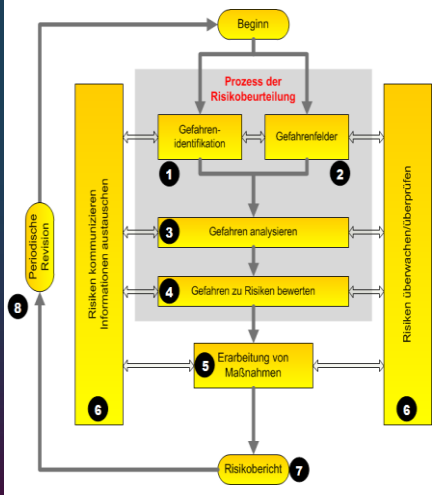
» **Sensibilisierung und Ausbildung von Sicherheitsbewusstsein**

» **Internationale Zusammenarbeit und branchenübergreifender Wissensaustausch**

» **Schutz kritischer Infrastruktur:**
- Krisenkommunikation inkl. Meldepflicht bei Cyber-Attacken
- laufende Aktualisierung einer umfassenden Sicherheitsarchitektur bei systemrelevanten EVUs

RELEASE TO PUBLIC

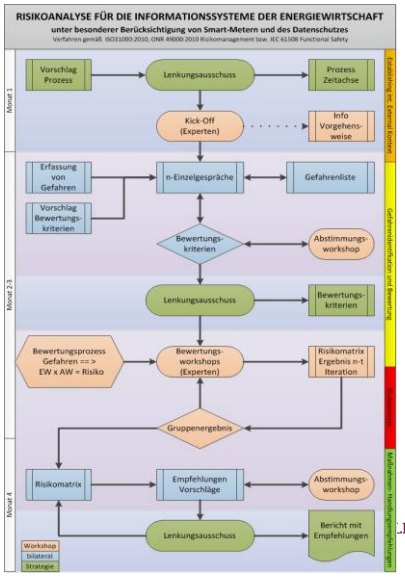
Teil II Der Prozess RM-Allgemein



- ISO 31.000 risk management
- ISO 31.010 risk assessment techniques
- ONR 49.002-1-3
- ÖNORM S2410
- ISO 27.XXXX

RELEASE TO PUBLIC

Teil II Der Gesamtprozess



- Lenkungsausschuss:
  - Ressorts
- Fachexperten: (nicht abgeschlossen)
- Verbund
- APG
- WES
- CERT
- BKA/SKI
- BMI
- KNG
- BMLVS
- LAG
- Energie AG
- Energie Institut
- IKB
- EXTERNE inkl. Si-Dienstleister
- Hersteller&Lieferanten

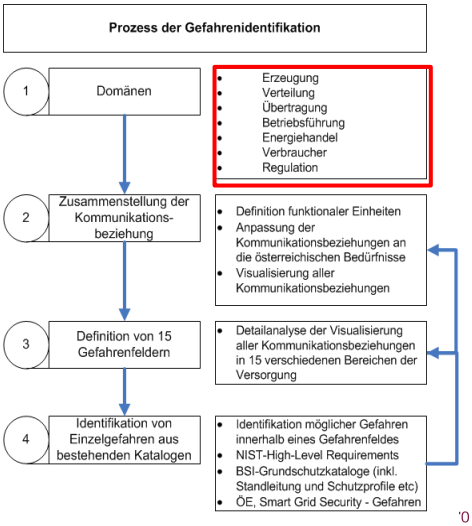
LEASE TO PUBLIC

Teil II Gefahrenkatalog aus ALLEN !

Nr.	Gefahrenbeschreibung	
GF V.1	Gefahr einer absichtlichen, aber nicht autorisierten Auslösung von Aktionen, die keine User Identifizierung oder Authentifizierung benötigt	AC-14 A1.13
GF V.2	Gefahr, dass Unbefugte Zugang zu nicht privilegierten Remote-Access-Accounts, LAN-Accounts mit Privilegien oder Remote Access LAN Accounts mit Privilegien erhalten	IA-04 A1.13
GF V.3	Gefahr, dass Maschinen/Equipment ohne organisatorische eineindeutige Identifikation im LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem in Betrieb genommen werden können (Organisatorisch - MAC, oder Maschinenzertifikate)	IA-05 A1.3 A1.22

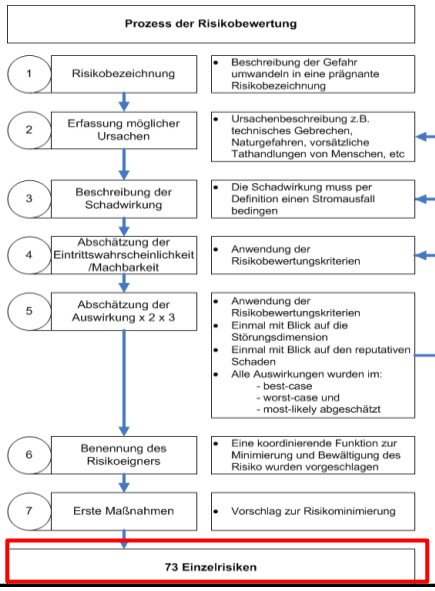
Gefahrenkatalog gesamt		Gefahrenzuordnung zu den Gefahrenfeldern															
Nr.	Gefahrenbeschreibung	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Häufigkeit
1	Gefahr einer absichtlichen, aber nicht autorisierten Auslösung von Schalthandlungen, die keine User Identifizierung oder Authentifizierung benötigen	0	0	0													3
2	Gefahr, dass Unbefugte Zugang zu nicht privilegierten Remote-Access-Accounts, LAN-Accounts mit Privilegien oder Remote- Access- LAN- Accounts mit Privilegien erhalten	0	0	0	0	0	0		0	0	0	0	0		0	0	13
3	Gefahr, dass Maschinen/Equipment ohne organisatorische eineindeutige Identifikation im LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem in Betrieb genommen werden können (Organisatorisch - MAC, oder Maschinenzertifikate)	0	0	0	0	0	0	0				0		0	0	0	11
4	Gefahr, dass während der Authentifizierung Authentifizierungsinformationen an unbefugte Dritte zurückgegeben werden (Bsp. Maskieren der Passwortinformationen)	0		0	0			0						0	0	0	7
5	Gefahr, dass im abgeschotteten LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem DDoS-Angriffe durchgeführt werden können	0	0	0	0												4
6	Gefahr, dass konzeptionelle Schwachstellen bei der Trennung von LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem zu anderen LAN/Netzwerk/Fernwirksystem/Netzleitsystem/Prozessleitsystem übersehen wurden	0	0	0	0	0	0	0	0	0	0		0	0	0	0	14
7	Gefahr, dass die Integrität eingeführter und abgesicherter Kommunikation kompromittiert wird	0	0	0	0		0	0	0	0	0		0	0	0	0	13

Teil II Gefahrenkatalog



- GF I: M2M- Kommunikation
- GF II: Steuerungs-Kontrollsysteme i.d. Organisation
- GF III: Steuerungs-Kontrollsysteme zw. Organisationen
- GF IV: Backoffice Systeme
- GF V: Intraorganisatorische Kommunikation
- GF VI: Steuerungssysteme Verwaltungssysteme
- GF VII: Sensoren und Sensorennetzwerk
- GF VIII: Smart Meter Transaktionskommunikation
- GF IX: HAN/BAN/NAN
- GF X: Externe Systeme mit „direkter" Beziehung zum Verbraucher
- GF XI: Service und Wartungsschnittstellen
- GF XII: Schnittstellen am Smart Meter
- GF XIII: Decision Support Systeme
- GF XIV/XV: Entwicklung und Wartung
- GF XVI: Überwachung/Sicherheitssysteme

Teil II Risikobewertungskriterien



» Technische Gefahren und Naturgefahren

» Intentionale Gefahren

» R= E (M) X A

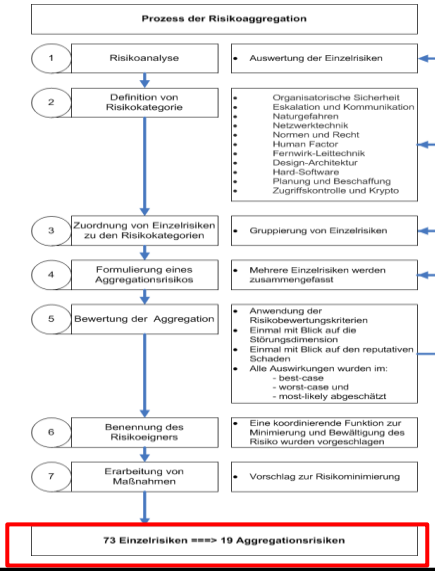
» Auswirkung (Ausfall von)
- Netzlast
- Anzahl Anschlüsse
- Zeit

» Eintrittswahrscheinlichkeit

» Machbarkeit

'O PUBLIC

Teil II Risikoaggregation



» Aggregation

» Risikokategorien:
- Eskalation und Kommunikation
- Design und Architektur
- Human Factor
- Organisatorische Sicherheit
- Hard- und Software
- Normung und Recht
- Zugriffskontrolle und Kryptographie

'O PUBLIC

Teil II Zahlen Daten Fakten

- Risikoanalyse Strom 1.0 inkl. umfassenden Bericht
  - Dauer ca. ¾ Jahr je 8x WS a 6-7h
  - 28 externe Gespräche inkl. Hersteller nat. und international
- Risikoanalyse Strom 2.0 Update
  - Dauer ca. 1/2 Jahr 4WS a 6-7h Review und Update/ Ergänzung
- Risikoanalyse Gaswirtschaft 1.0
  - Dauer ca. ¾ Jahr je 14 x WS a 4h
- Zusammenführung der Arbeitsgruppen und Risikoanalysen

RELEASE TO PUBLIC

Agenda

Teil I Vorstellung und Motivationen

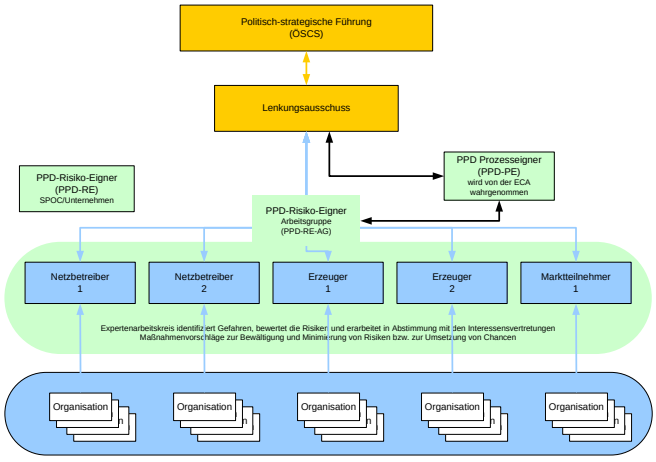
Teil II Vorgehensweise Risikoanalyse

Teil III PPD-Prozess E-Wirtschaft

Teil IV Diskussion

RELEASE TO PUBLIC

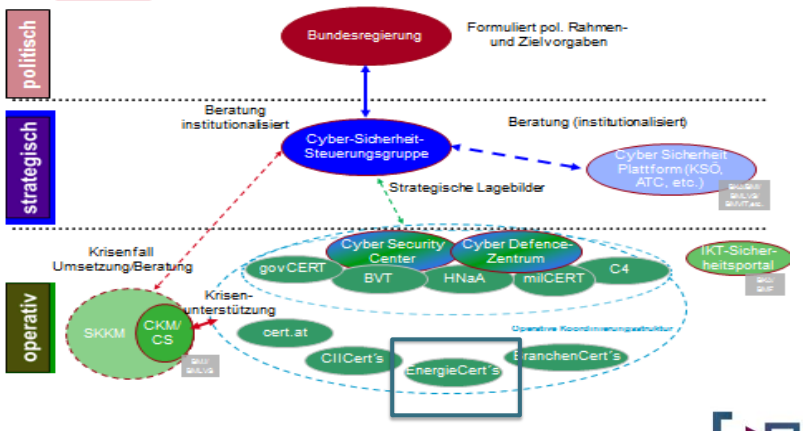
Teil III Aufbau eines PPD-Prozesses Vorschlag



RELEASE TO PUBLIC

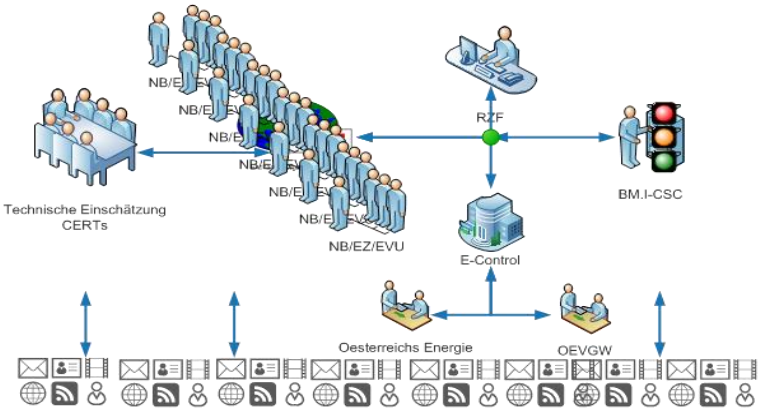
Teil III Aufbau eines Eskalationsprozesses

Funktioneller Aufbau der Beziehungsstrukturen zur permanenten Koordination auf operativer Ebene



RELEASE TO PUBLIC

Teil III Aufbau eines Eskalationsprozesses



RELEASE TO PUBLIC

Agenda

Teil I Vorstellung und Motivationen

Teil II Vorgehensweise Risikoanalyse

Teil III PPD-Prozess E-Wirtschaft

Teil IV Diskussion

RELEASE TO PUBLIC

Teil IV Branchen und Risikoanalysen

- **Österreichische Strategie für Cybersicherheit:**
  - „Krisenmanagement- und Kontinuitätspläne werden auf Basis von Risikoanalysen für sektorspezifische und sektorübergreifende Cyber Bedrohungen in Zusammenarbeit von öffentlichen Einrichtungen und den Betreibern von kritischen Infrastrukturen ausgearbeitet und laufend aktualisiert."
- **Masterplan zum Schutz Kritischer Infrastruktur:**
  - 1. Teilziel des Aktionsplanes: Punkt 3: Risikoanalyse im Wirkungsbereich der Bundesministerien
  - „PPP: Die Einbindung der ACI - Betreiber in den gesamtstaatlichen Lagebildprozess und in die Risikoanalyse ist dabei ein wichtiger Schritt."

RELEASE TO PUBLIC

Teil IV Branchen und Risikoanalysen

- **NIS-Richtlinie**
  - „The national NIS strategy shall address in particular the following issues: (a) The definition of the objectives and priorities of the strategy *based on an up-to-date risk and incident analysis*;"
  - "2. The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements: A risk assessment plan to identify **possible**-risks"

RELEASE TO PUBLIC

Persönliche Bemerkung

» Austausch von HOPPLA's ! (CIRS)

RELEASE TO PUBLIC

Dipl. Ing. Wolfgang Czerni, MBA
INFRAPROTECT GMBH

Gesellschaft für Risikoanalyse,
Notfall- und Krisenmanagement

www.infraprotect.com

RELEASE TO PUBLIC