EUROPÄISCHER RAHMEN ZUR BEWERTUNG VON CYBER-RISIKEN IM STROMSYSTEM

TAGUNG: WIE WIRD DIE DIGITALE STROMVERSORGUNG RESILIENTER?

10. NOVEMBER 2017

MICHAEL DOERING (ECOFYS)

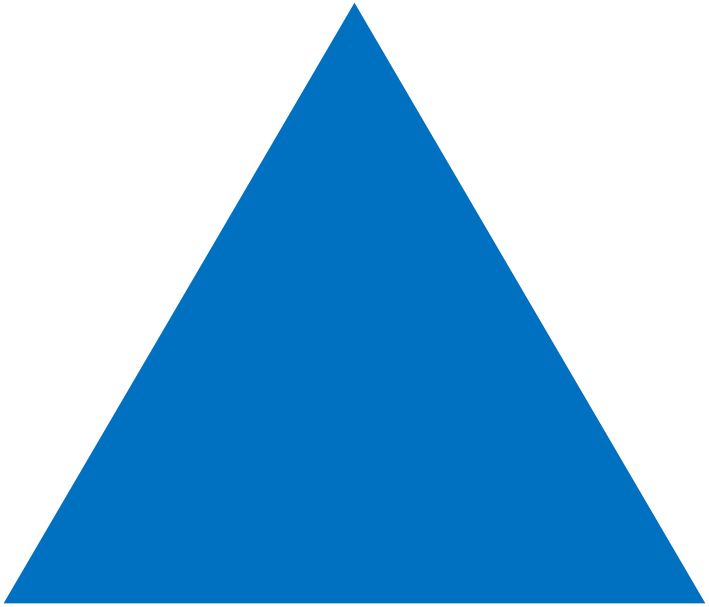
OFFIS

ECOFYS

A Navigant Company

WESENTLICHE TREIBER DER SYSTEMTRANSFORMATION

Digitalisierung

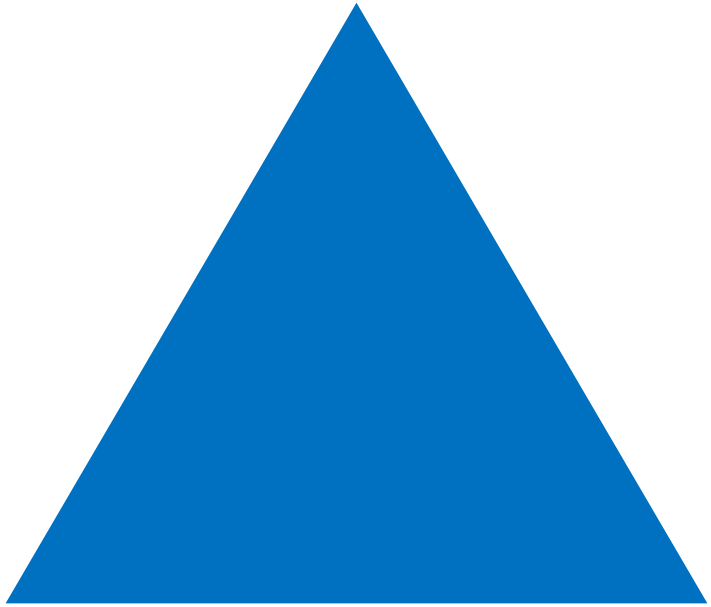


EE-Ausbau

EU Binnenmarkt

WESENTLICHE TREIBER DER SYSTEMTRANSFORMATION

Digitalisierung



EE-Ausbau

EU Binnenmarkt

2006 ZEIGT, DASS IN EINEM GEMEINSAMEN STROMSYSTEM GEMEINSAME REGELN VON VORTEIL SIND

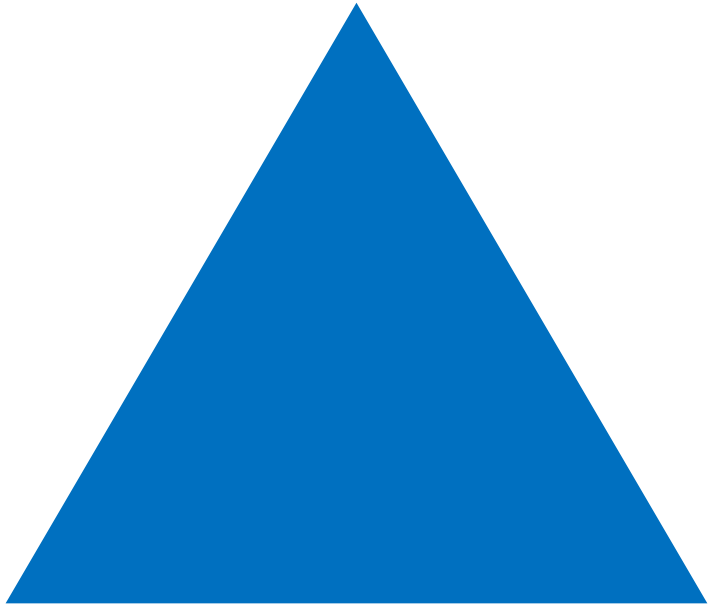
- Stromausfall in 2006 beeinträchtigte mehr als 15 Millionen Netznutzer für rund 2 Stunden

Erkenntnisse / Schluss-folgerungen

- Gründung von ENTSO-E
- Gründung von Koordinationszentren (TSC, Coreso, etc.)
- Entwicklung europäischer Netzkodizes

WESENTLICHE TREIBER DER SYSTEMTRANSFORMATION

Digitalisierung ??



EE-Ausbau

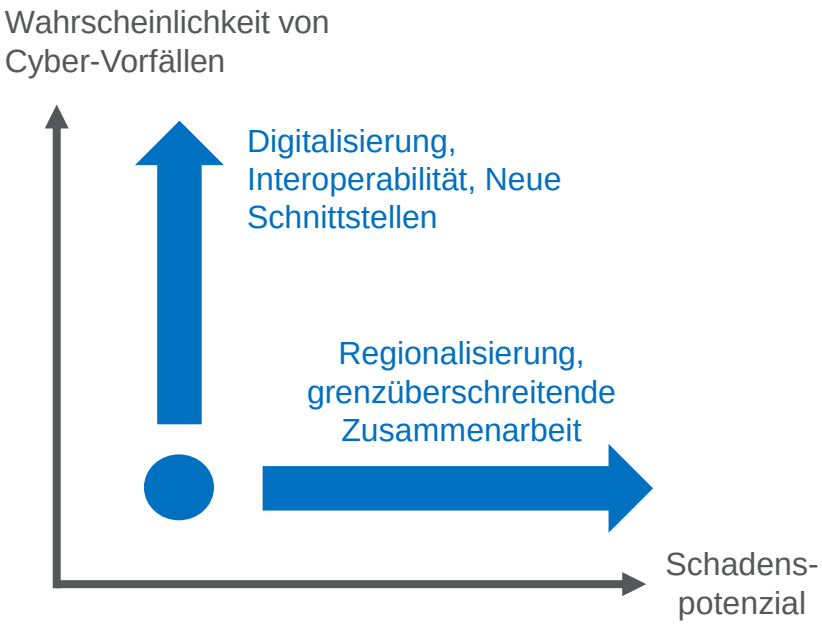
EU Binnenmarkt

ZUKÜNFTIG LÄSST SICH SYSTEMSICHERHEIT NICHT OHNE EINBEZIEHUNG DER CYBER-RISIKEN BEWERTEN

- Anzahl und Relevanz der Cyber-Ereignisse steigt in den letzten Jahren stetig an

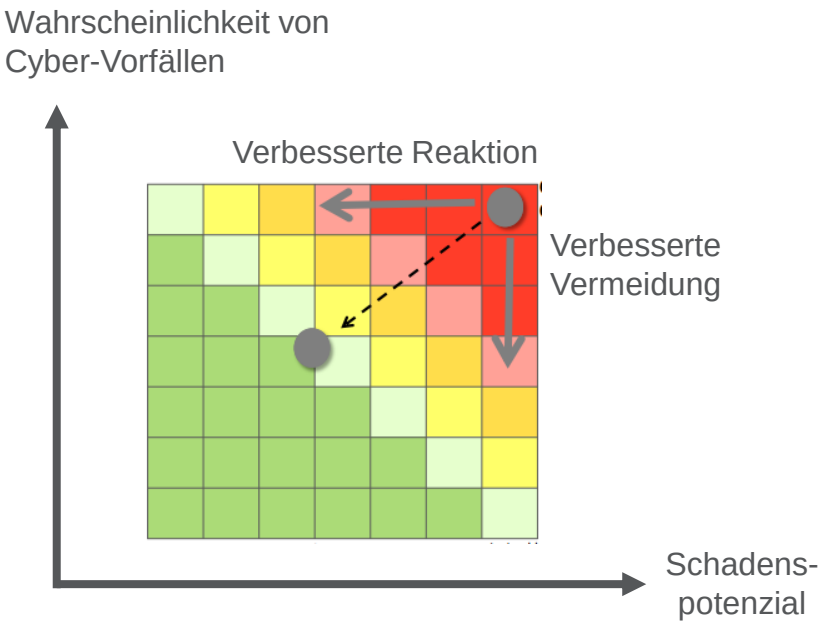
ZUKÜNFTIG LÄSST SICH SYSTEMSICHERHEIT NICHT OHNE EINBEZIEHUNG DER CYBER-RISIKEN BEWERTEN

- Anzahl und Relevanz der Cyber-Ereignisse steigt in den letzten Jahren stetig an



ZUKÜNFTIG LÄSST SICH SYSTEMSICHERHEIT NICHT OHNE EINBEZIEHUNG DER CYBER-RISIKEN BEWERTEN

- Anzahl und Relevanz der Cyber-Ereignisse steigt in den letzten Jahren stetig an



DIE AKTIVITÄTEN UND AKTEURE IM BEREICH CYBER-SECURITY SIND SEHR VIELFÄLTIG

Comm. on Digital Single Market
"Reinforcing trust and security in digital services and in the handling of personal data"

European Agenda on Security
"…cybercrime with a strong cross-border dimension, where EU action can make a real difference

Directive on "Network and Information Systems" (NIS)

Data Protection Directive

- Agency (enisa, ACER – Agency for the Cooperation of Energy Regulators)
- CERTS
- Energy Expert Cyber Security Platform (EECSP)
- SysOps guideline obligation on TSOs
- Public-private partnership
- DSOs (ENCS)

Dedicated NC on cyber security

DER AKTUELLE EU-RAHMEN REGELT IT-SICHERHEITS-ANFORDERUNGEN SEHR RUDIMENTÄR

- Vor 2016 fokussierte sich Cyber-Security auf kritische Infrastruktur.

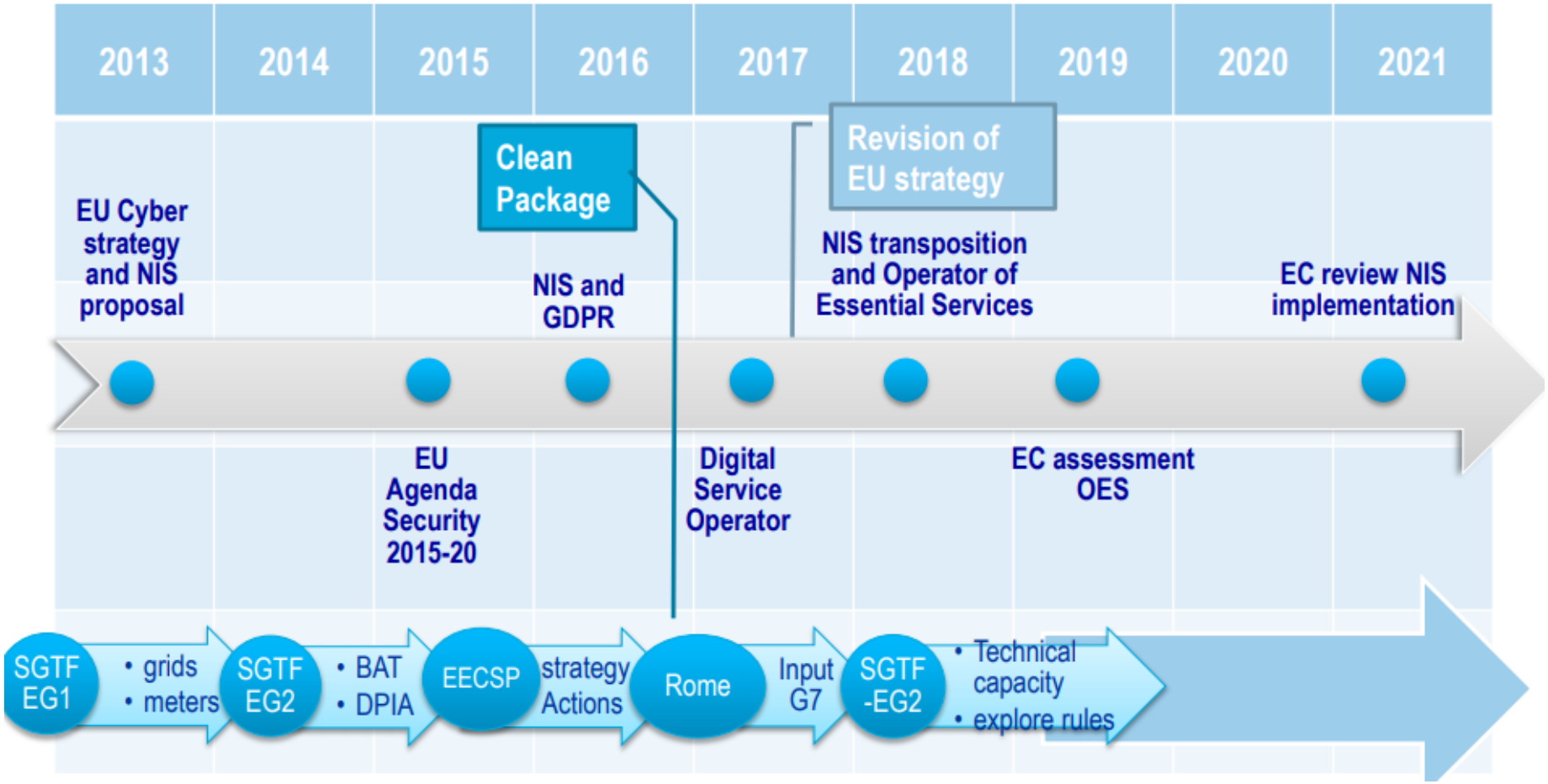
- Seit 2016 gibt die **NIS Richtlinie** (Directive on security of Network and Information Systems) einen ersten allgemeinen EU-Rahmen für Cyber-Security vor. Umfang und Tiefe der Ausgestaltung der IT-Sicherheitsanforderungen für die nationale Implementierung werden aber weitestgehend den einzelnen Mitgliedsstaaten überlassen.
- Erste spezifische Anforderungen sind in den aktuellen europäischen **Netzkodizes** festgeschrieben (“Security plan for critical infrastructure protection” requirement to all TSOs as already prescribed in the “System Operation Guideline” SysOp).
- Im Rahmen des **Winterpakets** wurde ein spezifischer Network Code für Cyber-Security im Stromsystem vorgeschlagen, um einen einheitlichen Rahmen für die Identifikation von Risiken und Bewertung von Gegenmaßnahmen zu gewährleisten.

CYBERSECURITY RÜCKT ZUNEHMEND IN DEN FOKUS DER REGULIERUNG

- Im September 2017 hat die EC ein neues Paket mit Vorschlägen zur Weiterentwicklung des aktuellen Rahmens und neuen Instrumenten veröffentlicht (https://ec.europa.eu/digital-single-market/en/policies/cybersecurity):
  - Stärkung von ENISA
  - Einführung eines europäischen Zertifizierungsmechanismuses
  - Erweitere Meldepflichten, insbesondere unverzügliche Meldung von Vorfällen an die EU
  - Netzwerkbildung und Wissensmanagement (Aufbau eines European Cybersecurity Research and Competence Centre)

- Viele Fragen bleiben aber offen:
  - Weiterentwicklung von NIS? Vorgabe von strengeren EU-Anforderungen?
  - Rolle der DSO-Entity bei Entwicklung der Netzkodizes? Umfang und Tiefe des NC Cyber-Security?
  - Rolle regionaler Kooperationsmechanismen? (REF, RSCs etc.)

ENTWICKLUNG DES EU-RAHMENS IM ZEITVERLAUF



PROJEKTÜBERSICHT

- Studie: **„Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector "**
- Zeitrahmen: Oktober 2017 bis Juli 2018
- Projektteam: Ecofys, Offis

- Übergeordnete Ziele
  - Entscheidungsgrundlage für Politik
  - Input für Entwicklung von NC Cyber-Security

- Inhaltliche Ziele
  - Methodik zur Identifikation von Cyber-Risiken im EU-Stromsystem
  - Analyse und Bewertung existierender Maßnahmen
  - Bewertung zusätzlicher Maßnahmen, Einordnung damit verbundener Kosten

ÜBERSICHT DER ARBEITSPAKETE

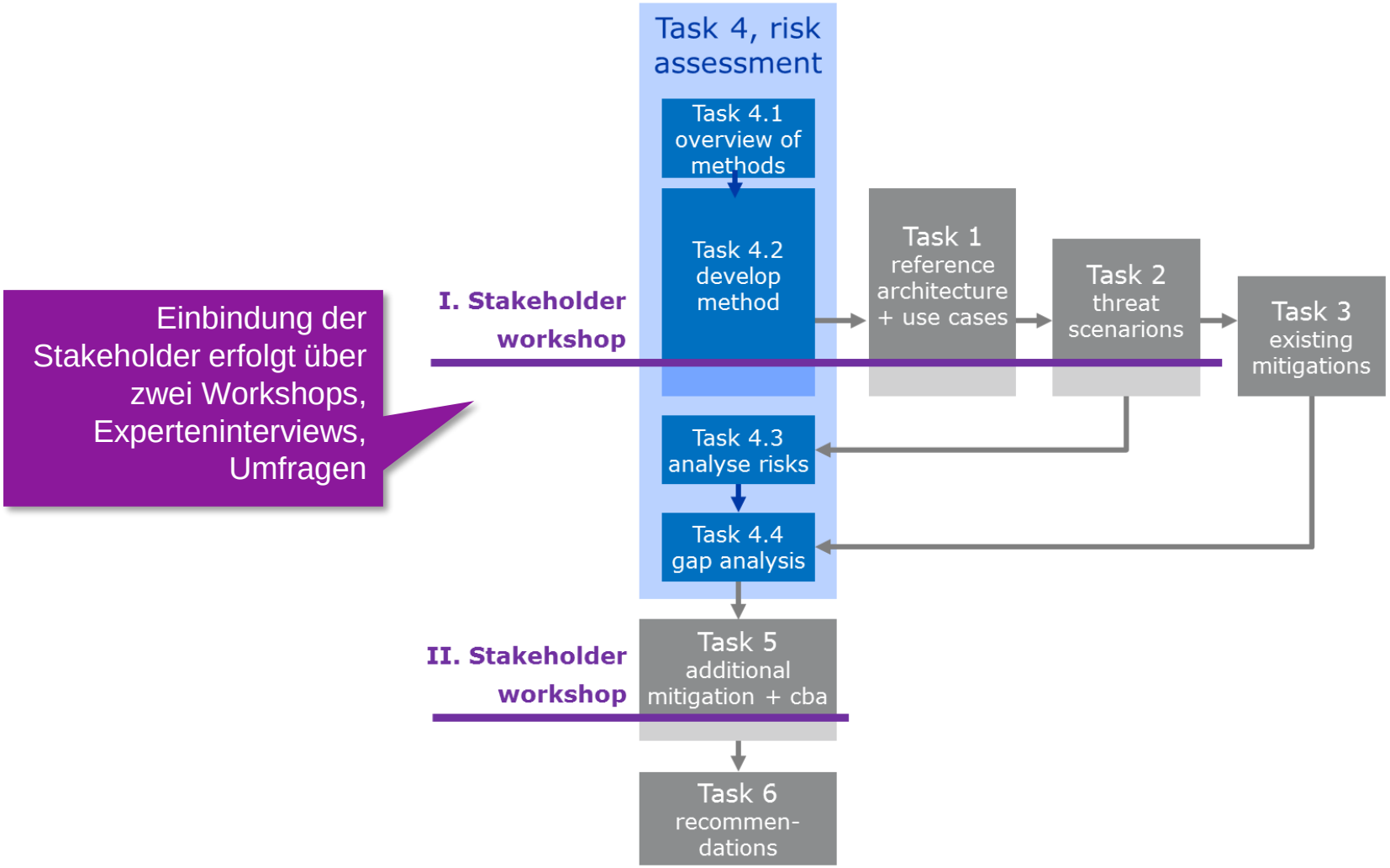
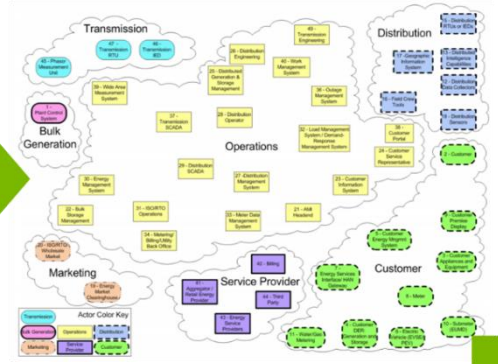
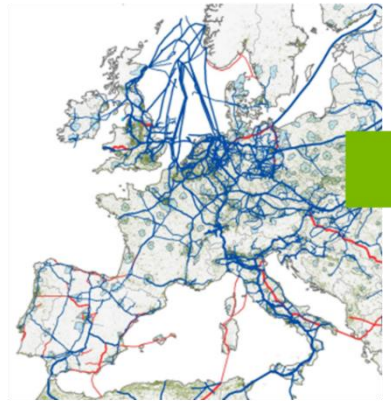
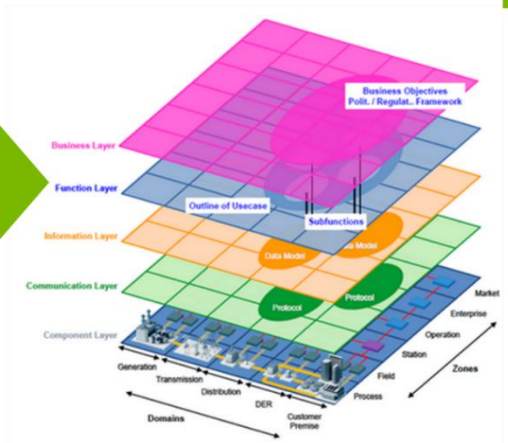


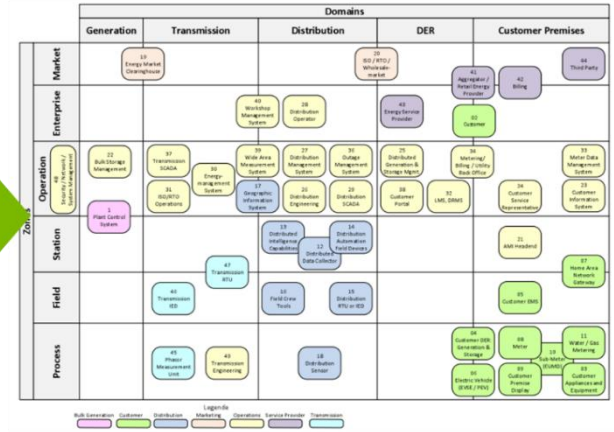
ILLUSTRATION VORGEHEN ARBEITSPAKET 1

Überführung der physischen Systeme in Reference-Architektur und Beschreibung / Auswahl von relevanten use cases (auf Grundlage von M/490 SGAM)









OFFENE FRAGEN, USE CASES UND ANGRIFFSSZENARIEN

- Welche dürfen nicht fehlen?
  - Sektorkopplung/Gas
  - TSO/DSO Interaktion
  - TSC
  - Anlagenzugriff/Softwareupdate durch Hersteller
  - Etc.?

OFFENE FRAGEN, GEGENMAßNAHMEN / INSTRUMENTE

- Inventarisierung existierender Maßnahmen mittels Literaturrecherche und Umfrage. Welche Akteure dürfen in der Umfrage nicht fehlen?
- Brauchen wir zukünftig zusätzliche Anforderungen / Maßnahmen?
- These: Existierende Maßnahmen sind ausreichend, aber die Implementierung ist der kritische Faktor. Sind somit primär zusätzliche prozessuale Maßnahmen gefragt?
- Könnte mehr Open Source-Protokolle etc. die Identifikation von Risiken verbessern?
- Ist die Einführung von Zertifikaten sinnvoll / kosteneffektiv? Oder sollte der Schwerpunkt auf regelmäßigen Konformitätsprüfungen / Audits liegen?
- Sollten Anlagen bei Netzanschluss zukünftig IT-technischen Sicherheitsanforderungen entsprechen? (Mindest-Sicherheitsniveau vergleichbar zum iMSys, welches Sicherheitsniveau ist geeignet?)
- Sollten die erweiterten Anforderungen auf EU-Ebene (Stärkung der NIS) oder nationaler Ebene eingeführt werden?

OFFENE FRAGEN, KOSTENABSCHÄTZUNG

- Welche Methoden zur Kostenabschätzung sind anerkannt / robust?
- Welche Akteure dürfen in der Umfrage zur Kostenmethodik nicht fehlen?
- Was stellt eine geeignete Metrik dar? (Anteil an Asset-Kosten)
- Welche Einflussfaktoren sind die wesentlichen Kostentreiber?
- Sollten Netzbetreiber IT-Sicherheit als Kostenblock im Rahmen der Anreizregulierung zukünftig separat ausweisen, um ein besseres Monitoring zu ermöglichen?

BEI OFFENEN FRAGEN KÖNNEN SIE UNS GERNE KONTAKTIEREN.

Michael Döring
m.doering@ecofys.com
+49 (0)30 29773579-13

ECOFYS
A Navigant Company