TRANSNET BW

RESILIENZ KRITISCHER INFRASTRUKTUR

Perspektive der TransnetBW

DR. TOBIAS WEIßBACH

Stuttgart, 24.07.2025

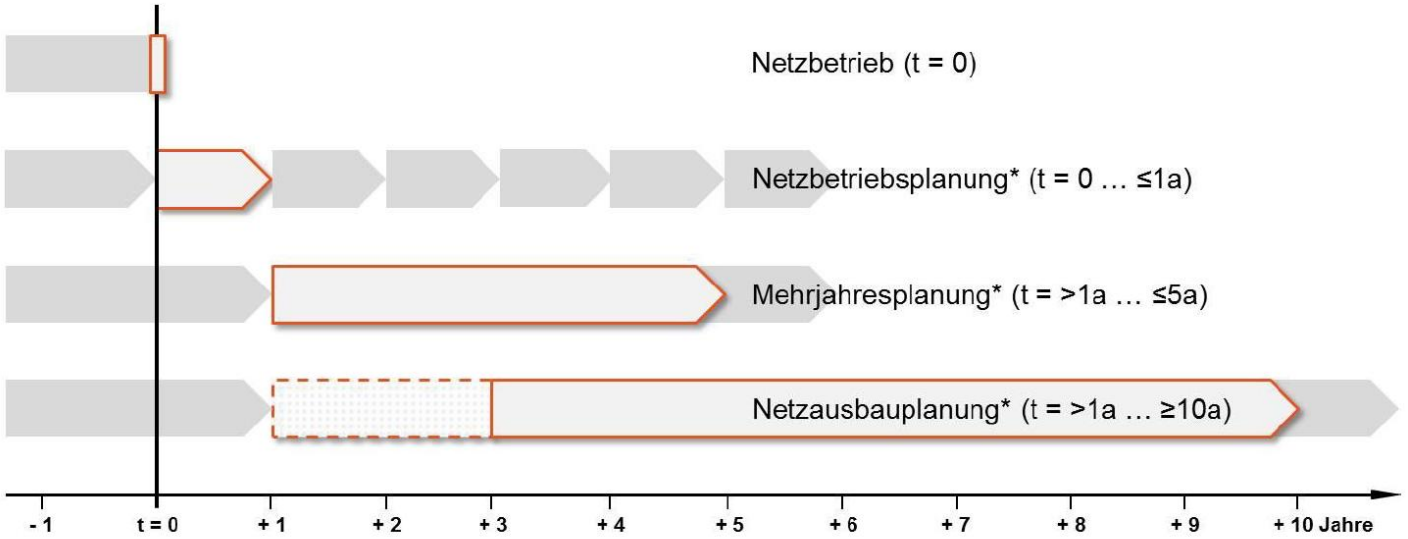
TRANSNET BW

01 EINORDNUNG: RESILIENZ AUS ÜNB-PERSPEKTIVE

EINE SICHERE ENERGIEVERSORGUNG SETZT RESILIENZ AUF MEHREREN EBENEN VORAUS

Resilienter Netzbetrieb

Resiliente Netzplanung



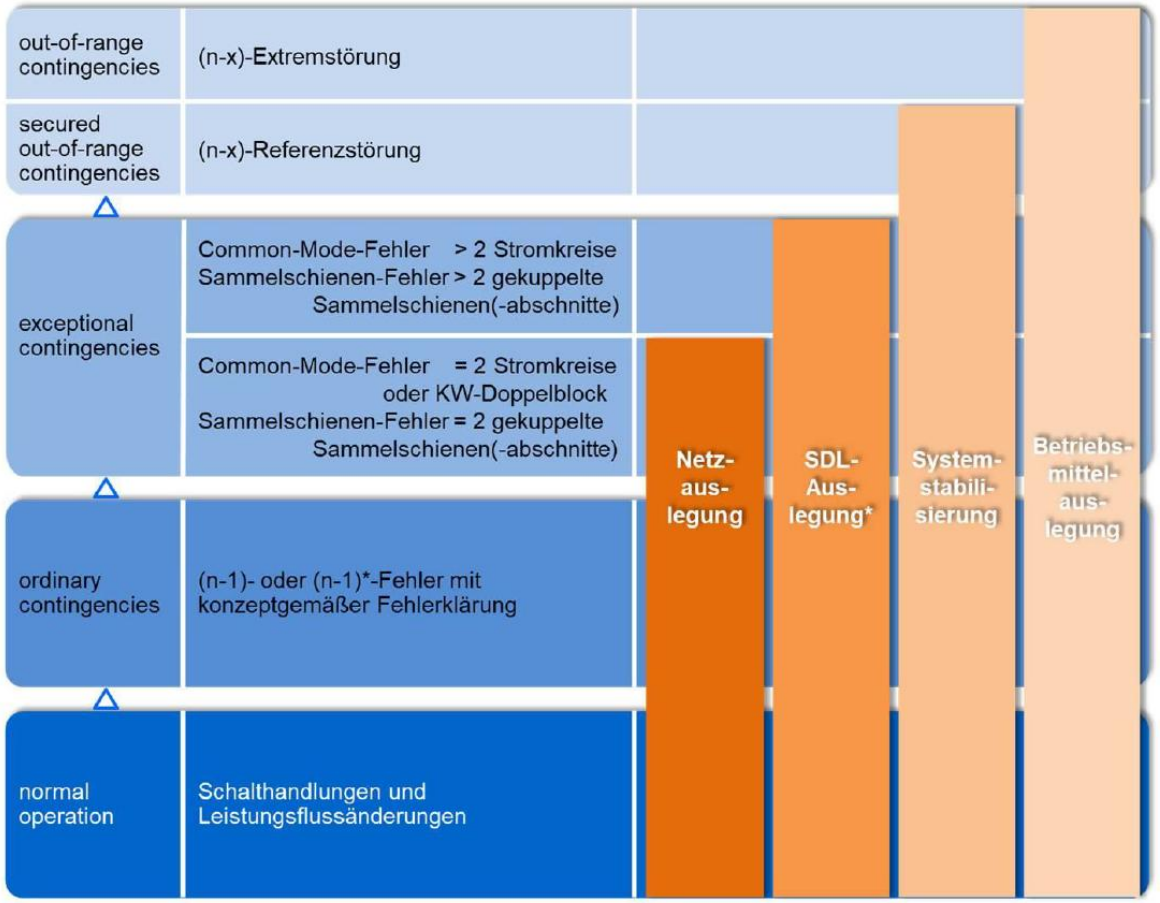
* Die Prozessdarstellung beginnt vereinfachend erst ab t = 0. Die dem Online-Netzbetrieb zeitlich vorgelagerten, rollierenden ÜNB-Prozesse, die hier nur schematisch dargestellt sind, erfolgen mit dem entsprechenden zeitlichen Vorlauf.

Quelle: https://www.netztransparenz.de/

Cyber-Resilienz

In einer Zeit rasant wachsender Digitalisierung, zunehmender Systemvernetzung und immer stärkerer Abhängigkeit von IT- und OT-Infrastrukturen wird **Cyber-Resilienz zur zentralen Voraussetzung für die sichere Energieversorgung** – insbesondere auch für Übertragungsnetzbetreiber als Teil der kritischen Infrastruktur.

NETZ, SYSTEMDIENSTLEISTUNGEN, BETRIEBSPROZESSE UND BETRIEBSMITTEL SIND AUF HOHE RESILIENZ AUSGELEGT



* Die Abdeckung von Exceptional Contingencies über die Auslegung der Systemdienstleistungen kann situationsbedingt variieren. So werden beispielsweise bei zu erwartenden Extremwettersituationen (Sturm, starker Schneefall, etc.) weiterreichende Vorkehrungen getroffen, da dann die Eintrittswahrscheinlichkeit von Störungsereignissen größer ist.

Quelle: https://www.netztransparenz.de/

1 Normal Operation (NO),
normale betriebliche Vorgänge (z. B. Schalthandlungen, marktbedingte Leistungsflussänderungen)

2 Ordinary Contingencies (OC)
Ausfall eines Betriebsmittels nach einer konzeptgemäßen selektiven Trennung vom Netz (z. B. Ausfall AC- oder DC-Stromkreis, Kraftwerksblock, HGÜ-Konverter, Blindleistungskompensationsanlage)

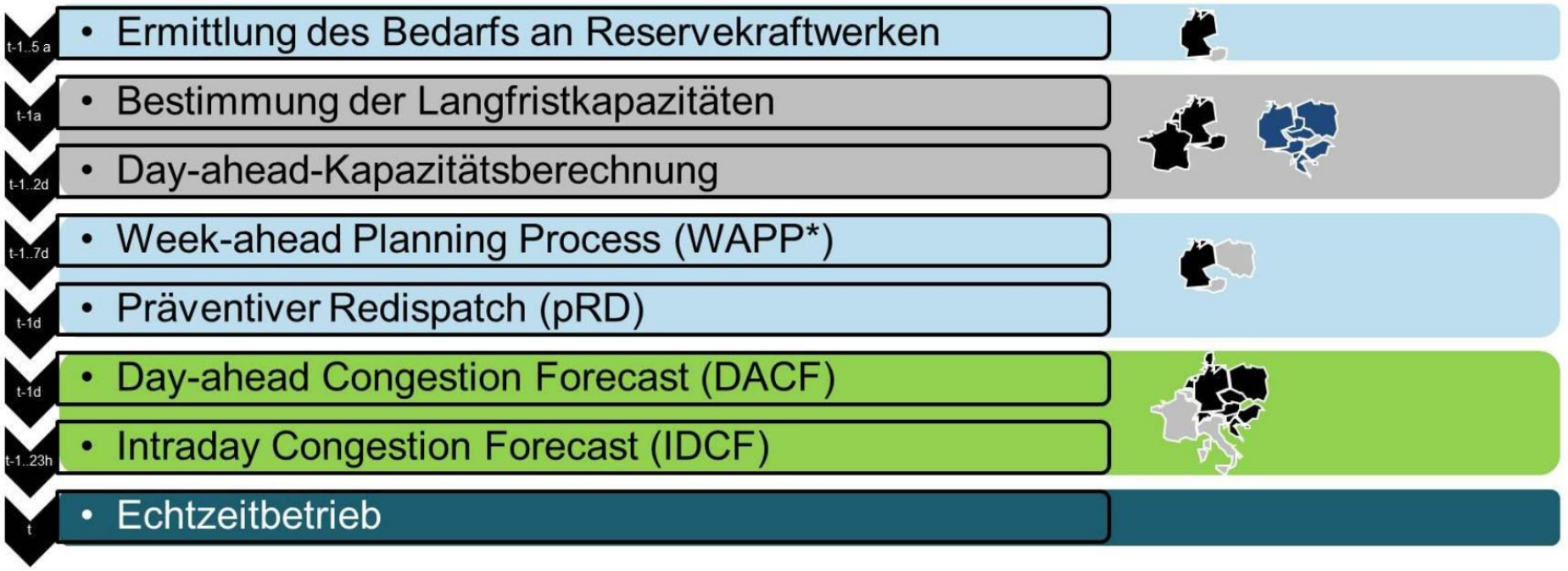
3 Exceptional Contingencies (EC)
Mehrfachfehler mit gemeinsamer Ursache (z.B. Ausfall gekuppelter Sammelschienen, Mastumbruch Doppelleitung, Ausfall KW-Doppelblock)

4 Secured Out-of-Range Contingencies (SORC)
Fehler, die zu einer kaskadierenden Störungsausweitung führen können, aber durch Letztmaßnahmen ohne Schwarzfall (Blackout) zu beherrschen sind (z.B. Ausfall örtlich naher Freileitungen, Umspannwerke bzw. relevante Teil-netzbildungen)

5 Out-of-Range Contingencies (ORC)
Störungen, die zum Schwarzfall (Blackout) führen „dürfen“. Für diese Störungen werden Netzwiederaufbaupläne vorgehalten (z. B. kleine Teilnetze in Folge einer Teilnetzbildung).

Im Rahmen der Systemauslegung sind dabei die Ereigniskategorien 1 - 4 ohne Einschränkungen bzw. mit tolerierbaren Einschränkungen der Funktionsfähigkeit des Übertragungsnetzes zu beherrschen.

FRÜHZEITIG STARTENDE, ITERATIVE BETRIEBSPLANUNGSPROZESSE STELLEN AUSREICHENDE RESILIENZ IM NETZBETRIEB SICHER



Prozessführende Organisation(en)

- Deutsche ÜNB
- Regional Security Coordinator (RSC) mit Mitglieds-ÜNB
- RSC mit ÜNB der Kapazitätsberechnungsregion
- ÜNB der Regelzone

* Beim WAPP nimmt APG auch teil (DE+AT)

Quelle: https://www.netztransparenz.de/

CYBER-RESILIENZ – EINE SCHLÜSSELKOMPETENZ FÜR ÜBERTRAGUNGSNETZBETREIBER

Die technologische Landschaft entwickelt sich kontinuierlich weiter: klassische IT-Systeme verschmelzen mit betriebstechnischen OT-Komponenten, Netzleittechnik kommuniziert mit digitalen Plattformen, und neue Marktmechanismen erfordern Echtzeitdatenverfügbarkeit.

Diese zunehmende Komplexität schafft neue Angriffsflächen – sowohl technisch als auch organisatorisch.

Gleichzeitig beobachten wir weltweit eine Zunahme staatlich unterstützter oder kriminell motivierter Cyberakteure, die gezielt kritische Infrastrukturen ins Visier nehmen – sei es aus politischen, geopolitischen oder finanziellen Interessen. Die Ereignisse der letzten Jahre – etwa Angriffe auf Energieversorger, Pipeline-Betreiber oder Strommärkte – zeigen, wie real diese Bedrohung ist.

Cyber-Resilienz bedeutet daher weit mehr als klassische IT-Sicherheit.

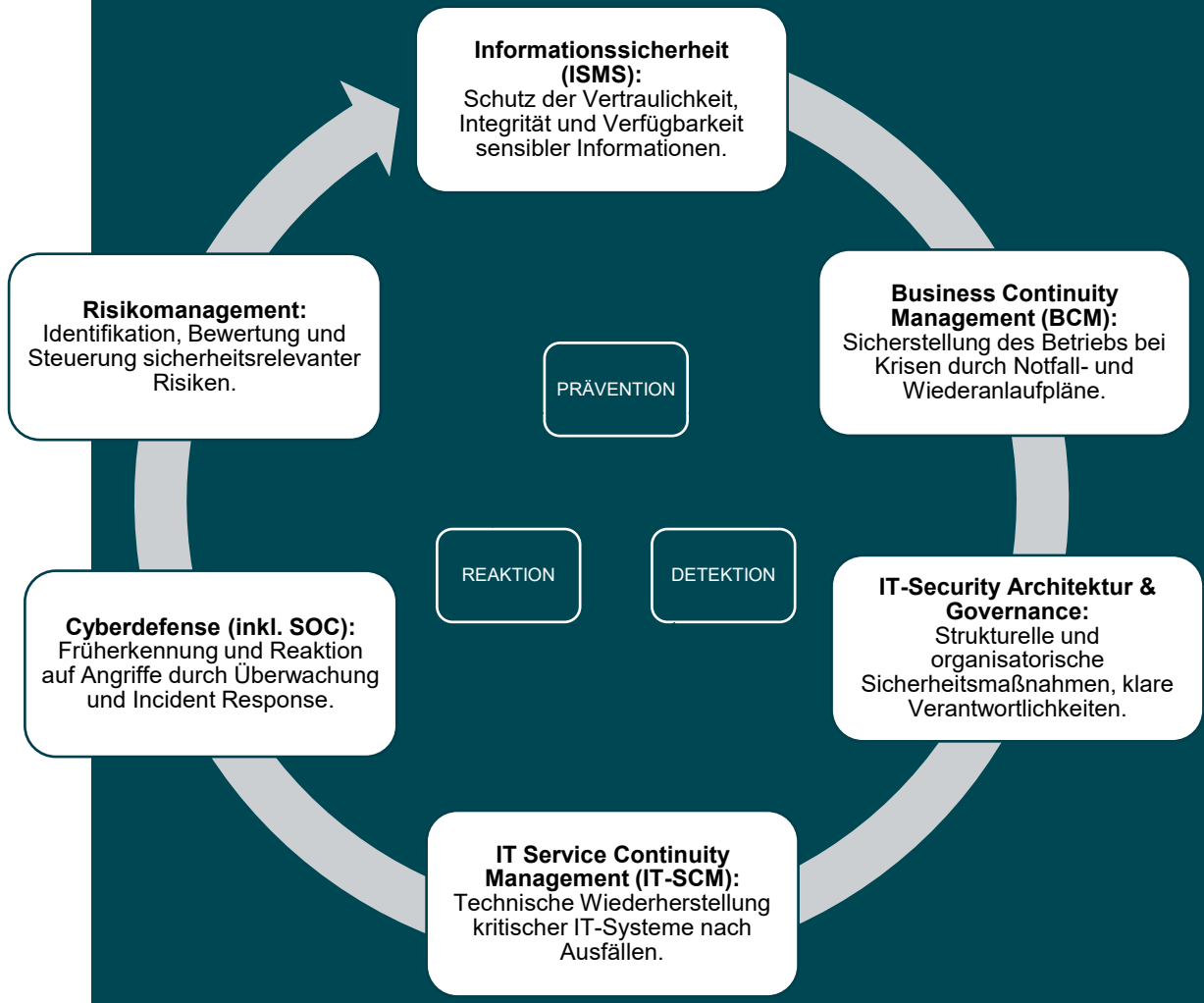
Cyber-Resilienz beschreibt die Fähigkeit eines Unternehmens, **Cyberbedrohungen frühzeitig zu erkennen**, **robust zu widerstehen**, **angemessen zu reagieren** und **sich schnell wieder zu erholen** – ohne den Betrieb nachhaltig zu gefährden.

Gerade für Übertragungsnetzbetreiber, deren Systeme 24/7 zuverlässig funktionieren müssen, ist dies kein optionales Ziel, sondern eine betriebliche Notwendigkeit.

CYBER-RESILIENZ IST NUR SO GUT WIE DAS EFFEKTIVE ZUSAMMENSPIEL IHRER BAUSTEINE

Bausteine der Cyber-Resilienz:

- Strategische Informationssicherheit
- Notfall- und Krisenplanung (Business Continuity Management, IT Service Continuity Management)
- Durchdachte Sicherheitsarchitektur
- Klare Governance,
- Operative Cyberabwehr (Cyberdefense) und Response

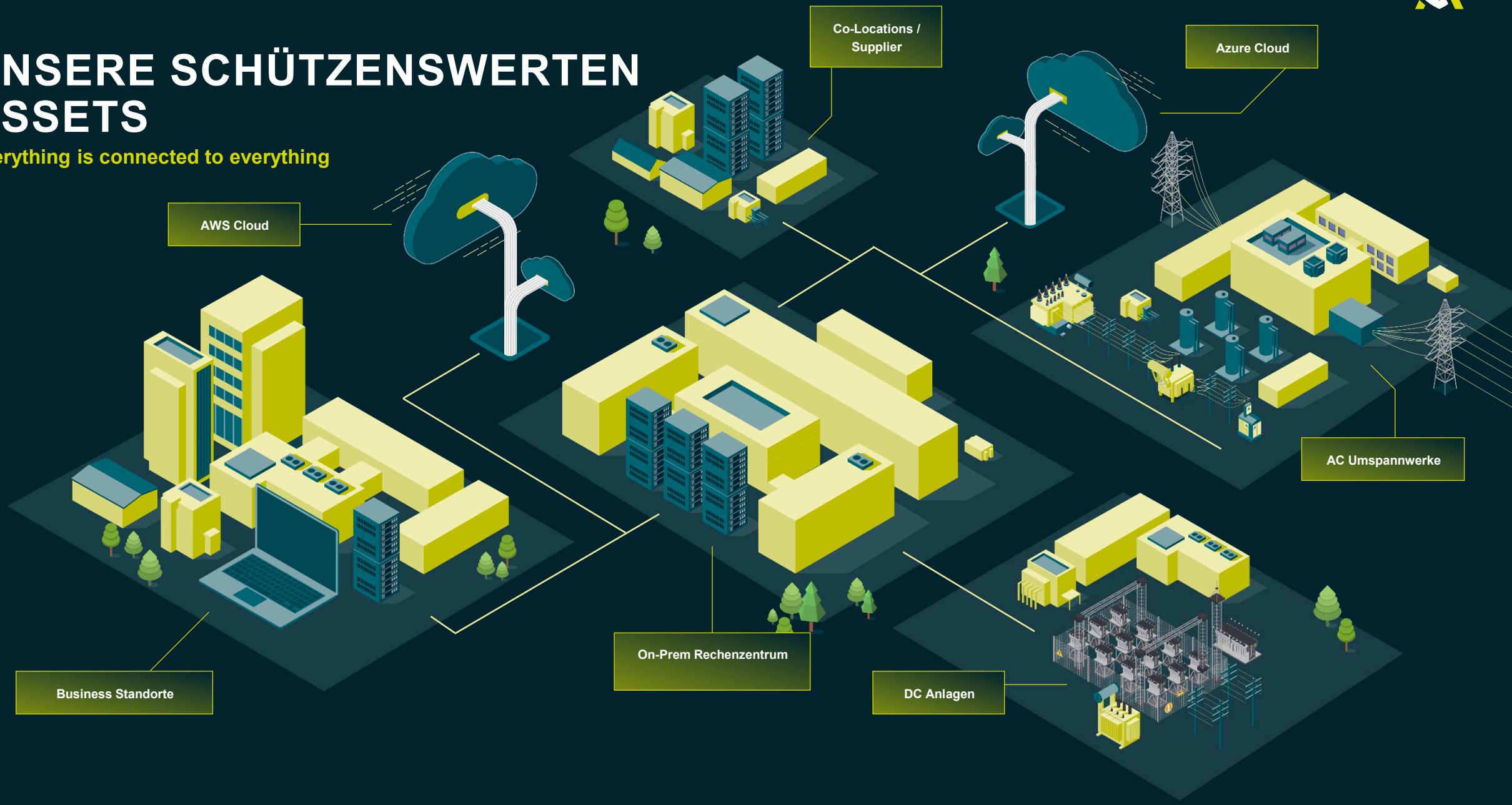


CYBER DEFENSE CENTER

02 CYBER DEFENSE CENTER DER TRANSNET BW

UNSERE SCHÜTZENSWERTEN ASSETS

Everything is connected to everything



DIE BEREICHE DER CYBERSICHERHEIT

PRÄVENTION, DETEKTION & REAKTION

PRÄVENTION
Maßnahmen und Strategien, die darauf abzielen, Sicherheitsvorfälle zu verhindern, bevor sie auftreten. Dazu gehören z.B. Informationssicherheit, Sicherheitsrichtlinien, IT/OT-Security Architektur, Security Awareness, Risikomanagement, Cyber Threat Intelligence,…

DETEKTION
Prozesse und Technologien, die darauf abzielen, Sicherheitsvorfälle zu erkennen, sobald sie auftreten. Dies umfasst die kontinuierliche Auswertung von Angriffserkennungssystemen.

REAKTION
Maßnahmen, die ergriffen werden, um auf erkannte Sicherheitsvorfälle zu reagieren und deren Auswirkungen zu minimieren. Dazu gehören Incident Response, Koordination und Notfallmaßnahmen.

PROAKTIVE & REAKTIVE CYBERSICHERHEIT

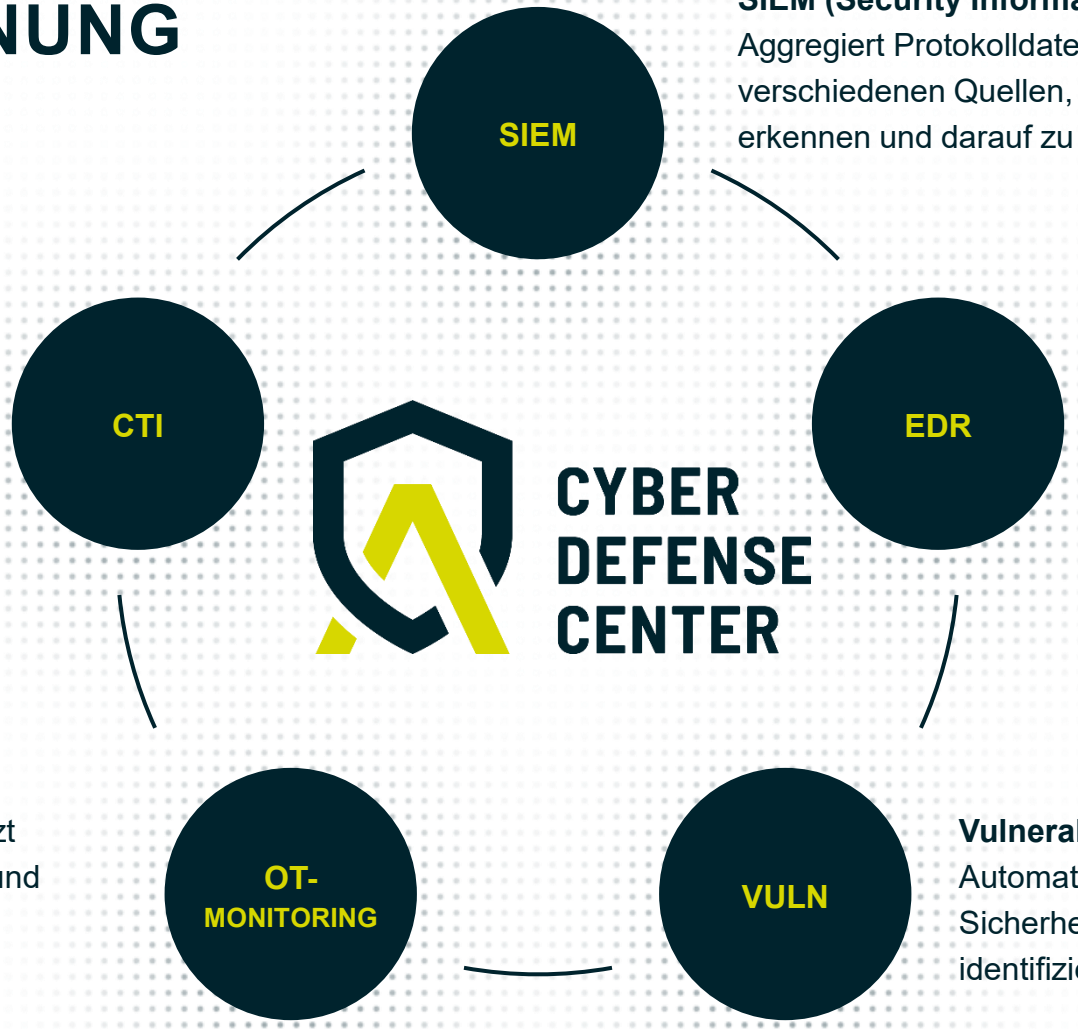
Diese Definitionen sind Teil eines umfassenden Ansatzes zur Cybersicherheit, der sicherstellen soll, dass TransnetBW sowohl proaktiv als auch reaktiv auf Bedrohungen vorbereitet ist.

UNSERE WERKZEUGE ZUR ANGRIFFSERKENNUNG

TOOL-CHAIN CDC

SIEM (Security Information and Event Management):
Aggregiert Protokolldaten und analysiert Sicherheitsdaten aus verschiedenen Quellen, um Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren.

Cyber Threat Intelligence:
Bietet detaillierte Bedrohungsinformationen und Analysen, um Organisationen bei der Erkennung und Abwehr von Cyberangriffen zu unterstützen.



EDR (Endpoint Detection and Response):
Überwacht dedizierte Endgeräte kontinuierlich, erkennt verdächtige Aktivitäten und ermöglicht eine schnelle Reaktion auf Bedrohungen.

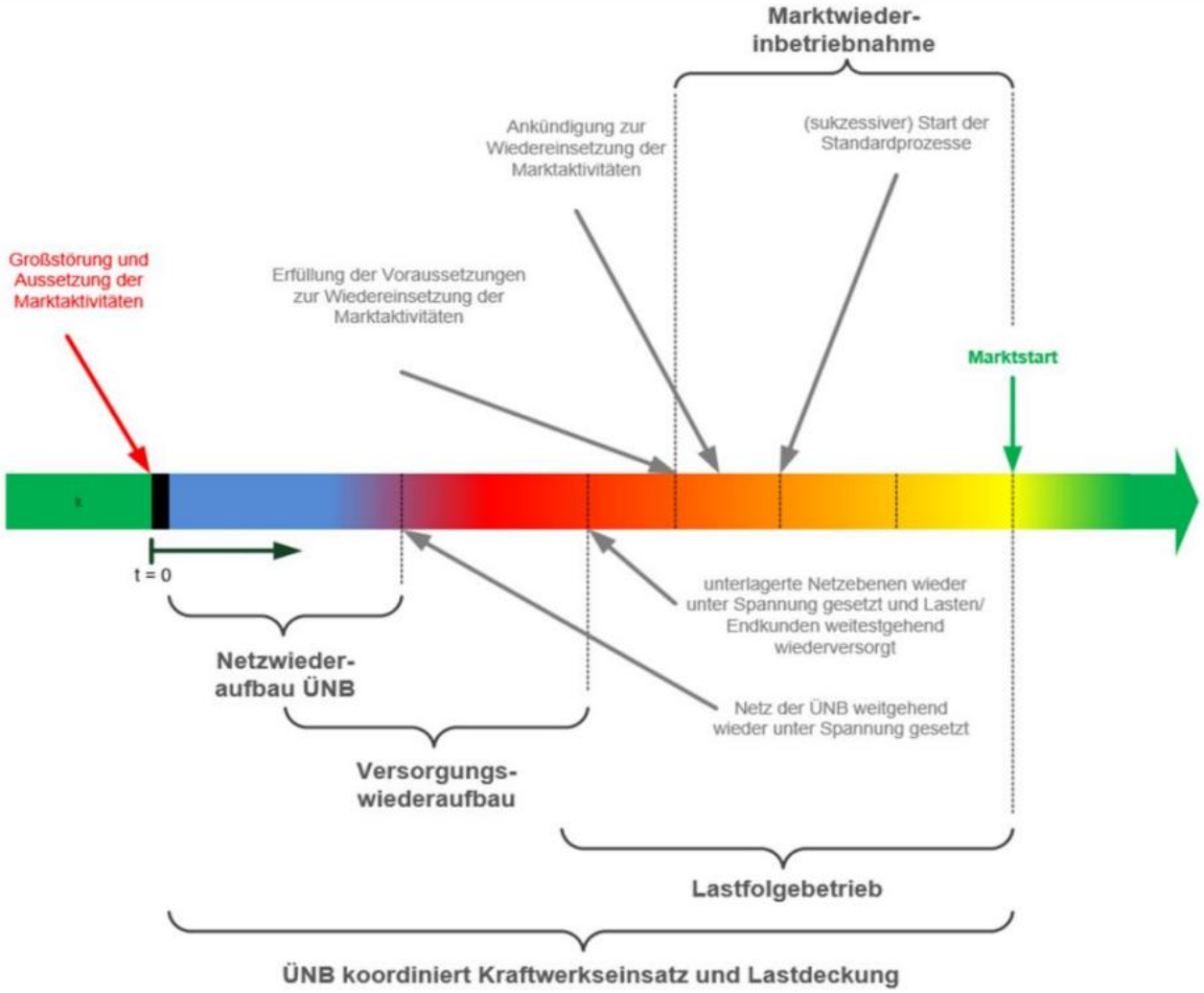
OT-Monitoring: Überwacht und schützt industrielle Steuerungssysteme (ICS) und Operational Technology (OT). Erkennt verhaltensbasierte Anomalien.

Vulnerability Management / Schwachstellen-Scanning:
Automatisiertes Tool, das IT-Systeme auf Sicherheitslücken untersucht und diese zur Behebung identifiziert.

03 … UND WENN DENNOCH EINE GROßSTÖRUNG AUFTRITT?

TRANSNET BW

NETZWIEDERAUFBAU NACH EINER GROßSTÖRUNG

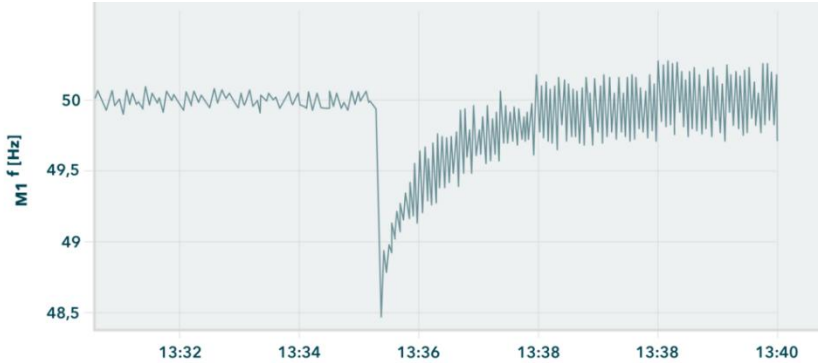


- Europäische und nationale Aufgabe
- Network Code Emergency & Restoration
- Vorbereitung: Primärenergievorhaltung, Betriebsversuche
- Basis: Vertragliche Ausgestaltung, seit 2025 Ausschreibung von Schwarzstartleistung nach EU-Vorgaben

TRANSNET BW

AUCH WENN DER ERNSTFALL ÄUßERST SELTEN EINTRITT – DAS HOCHFAHREN EINES NETZES MUSS REGELMÄßIG GEÜBT WERDEN

- Betriebsversuch 2024 der TransnetBW, EnBW AG sowie Illwerke vkw AG
  - Freischaltung eines Stromkreises vom schwarzstartfähigen Pumpspeicherwerk zur Versuchslast
  - Monatelange Vorbereitung in unternehmensübergreifenden Teams



Lastzuschaltung mit Frequenzsprung

  - Fazit: Das Notfallkonzept funktioniert, so dass das Netz im Ernstfall durch alle Akteure gemeinsam wieder hochgefahren werden kann.

- Regelmäßige Trainings und Schulungen halten den Wissensstand aufrecht.

- Betriebsversuche sind in regelmäßigen Abständen zu wiederholen.

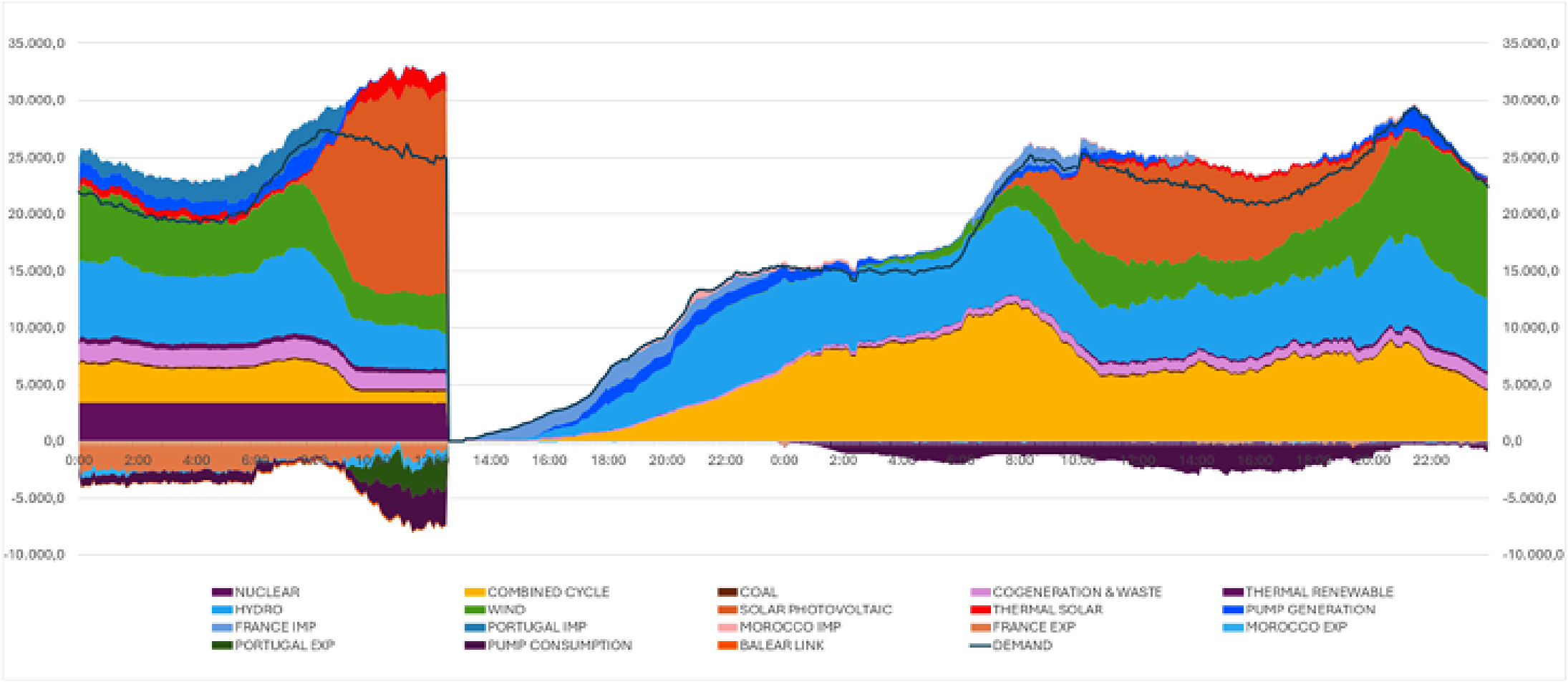
VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Dr. Tobias Weißbach
Leiter Innovative Marktlösungen und Produkte
Netzwirtschaft und Digitalisierung
TransnetBW GmbH
Osloer Str. 15-17
70173 Stuttgart
+49 151 62804027
t.weissbach@transnetbw.de

Backup

TRANSNET BW

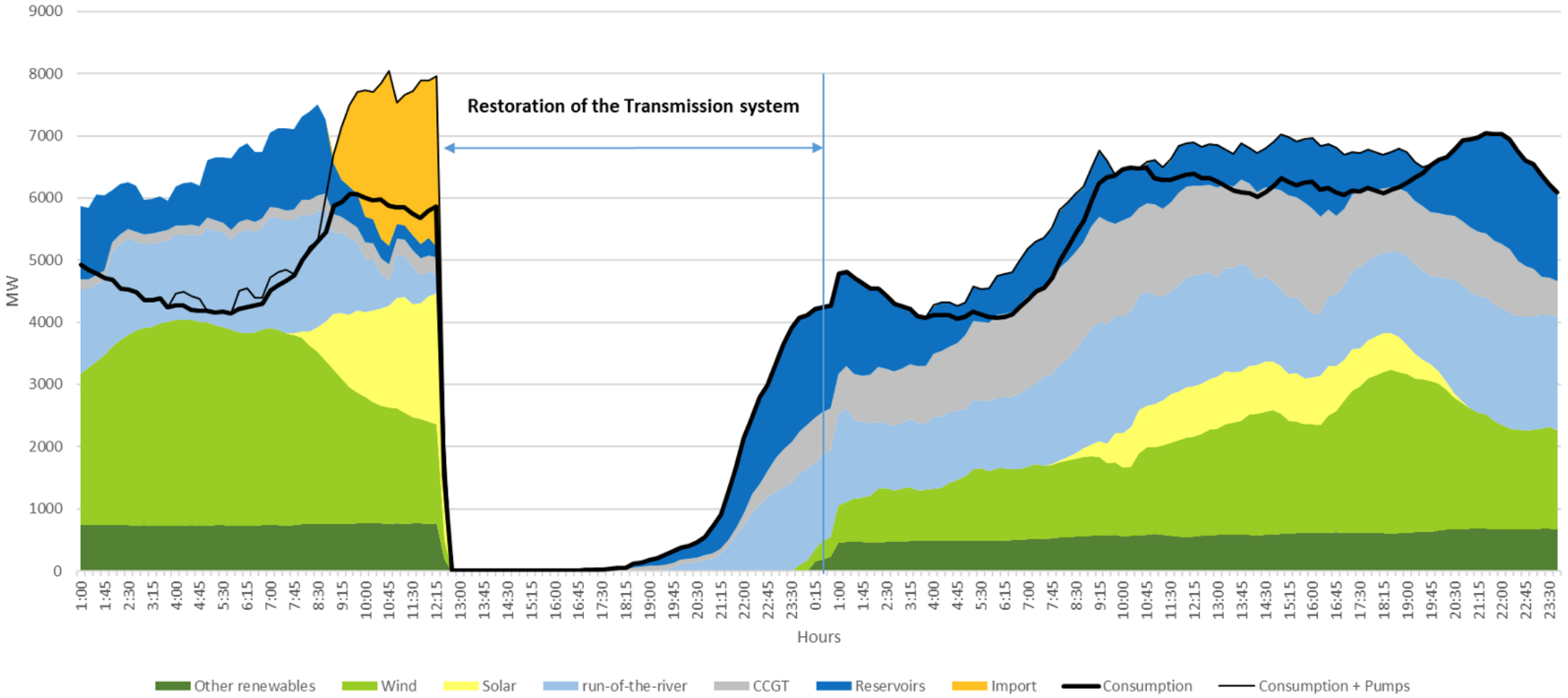
VERLAUF VON ERZEUGUNG UND LAST WÄHREND DES BLACK-OUTS AUF DER IBERISCHEN HALBINSEL AM 28. UND 29. APRIL – SPANIEN



Quelle: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/#Restoration_Process

TRANSNET BW

VERLAUF VON ERZEUGUNG UND LAST WÄHREND DES BLACK-OUTS AUF DER IBERISCHEN HALBINSEL AM 28. UND 29. APRIL – PORTUGAL



Quelle: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/#Restoration_Process

TRANSNET BW

Hinweis zur Nutzung von Präsentationen

Urheberrechte

- Diese Unterlage ist urheberrechtlich geschützt.
- TransnetBW GmbH muss vor Vervielfältigung, Weitergabe oder anderweitiger Nutzung der Unterlage ihre ausdrückliche Zustimmung erteilen.

Haftung

- Diese Unterlage wurde mit großer Sorgfalt erstellt.
- TransnetBW GmbH übernimmt keine Haftung für Aktualität, Richtigkeit und Vollständigkeit der Unterlage.