ENERGIE NETZE STEIERMARK

Ein Unternehmen der ENERGIE STEIERMARK

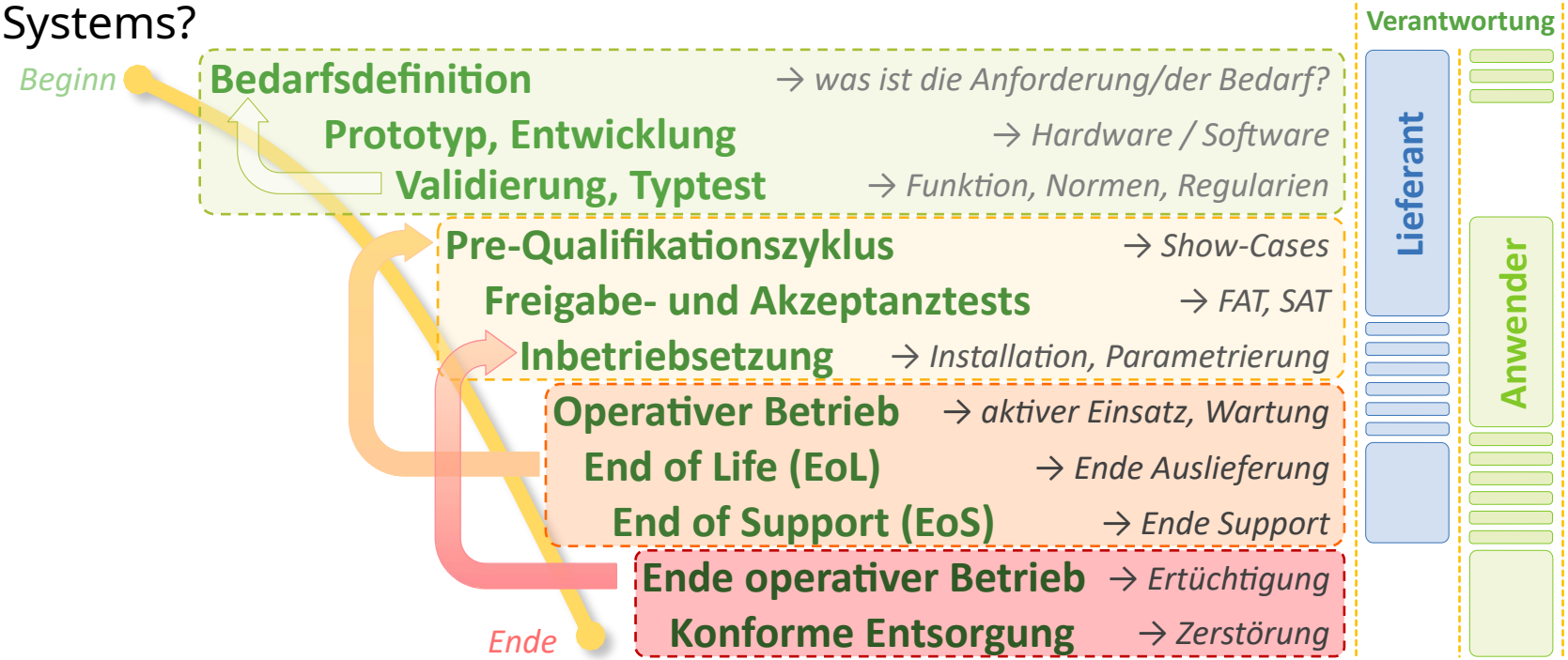
Herausforderungen im Lebenszyklus eines digitalen Schutzgeräts als Folge von Digitalisierung und NIS

Agenda

- Lebenszyklen eines digitalen Schutz- und Steuergerätes
- Herausforderungen innerhalb der unterschiedlichen Lebenszyklen
- Beispiel einer Wartungsstrategie für Sekundärtechniksysteme

Lebenszyklen eines digitalen Systems

- Wann beginnt und wann endet der Lebenszyklus eines digitalen Systems?



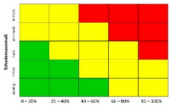
Herausforderungen und ihre Treiber

- Was sind „Treiber“ und welche Aktivitäten erfordern sie?

Netzbetrieb:	Energiewende, Netzausbau, Integration → neue Schutzkonzepte
OT-Security:	Verkabelungsgrade → Adaptierungen in z.B. Sternpunktbehandlung Regulatorische Vorgaben → Hard- und Softwareadaptierungen
Markt:	Elektronik-Verfügbarkeit → neue Hardware
Normung:	Neue Standards → Hard- und Softwareadaptierungen
Regulierung:	Vorschriften und Verordnungen → NIS, Network Code, …

Herausforderungen innerhalb des Lebenszyklus

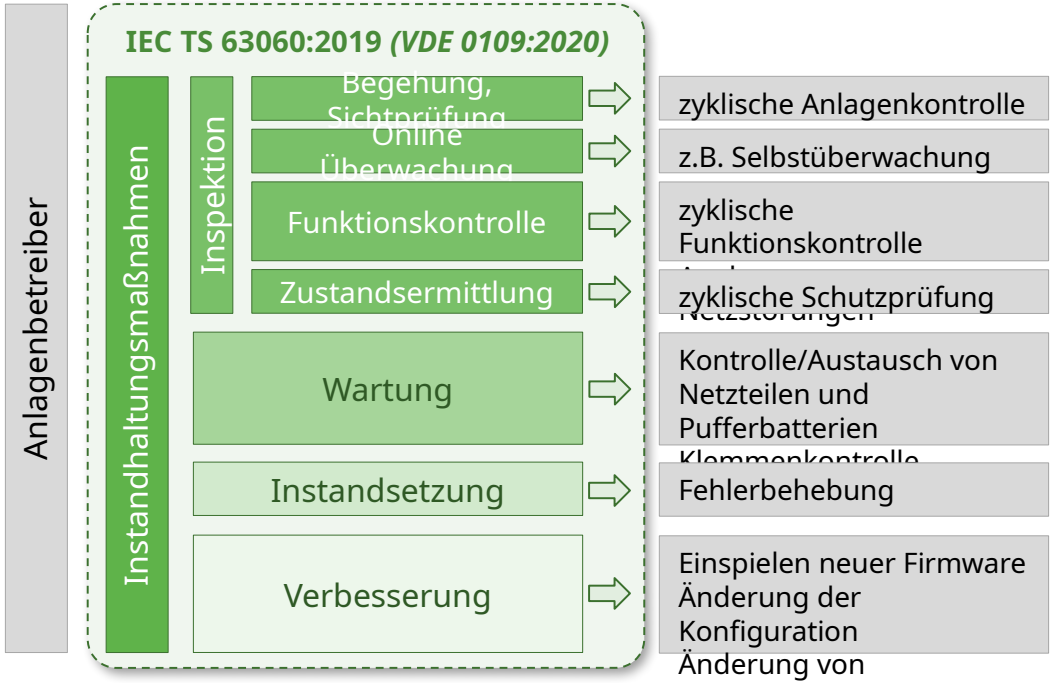
- Beispielhafte Wechselwirkungen/Herausforderungen aus Anwendersicht

	Netzbetrieb	OT Security	Anmerkung
Bedarfsdefinition	(neue) Funktionen	Regulative Vorgaben	
Prototyp, Entwicklung			
Validierung, Typtest			
Pre-Qualifikationszyklus	Reale Testumgebung	Reale Testumgebung	Virt. Device, Virt. Device, Virt. Device
Freigabe- und Akzeptanztests	Realistischen Umfang		Virtualisierungs-Layer
Inbetriebsetzung	*Teilsysteme in Betrieb*	*Security Konformität*	
Operativer Betrieb	*Stabilität (Z</I>, t_{AUS})*	*Update/Patch-Mgmt.*	
End of Life (EoL)	*Asset Strategie*		
End of Support (EoS)		*Security Konformität*	
Ende operativer Betrieb	*Verfügbarkeit (Umbau)*		
Konforme Entsorgung		*Security Konformität*	

... Primäre Herausforderung

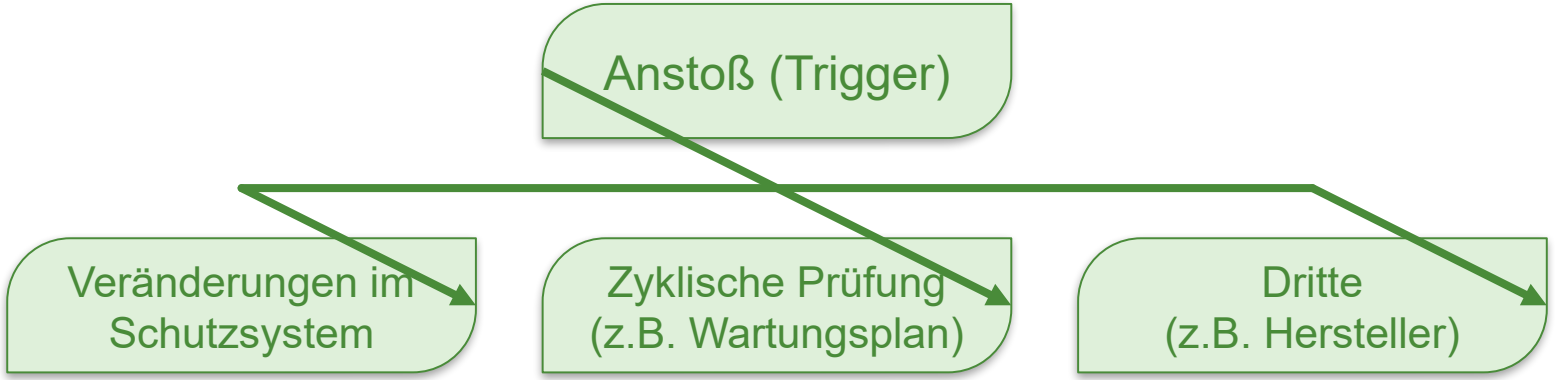
Beispiel: Wartungsstrategie (operativer Betrieb)

- IEC TS 63060:2019 - Allgemeine Aspekte und Methoden zur Wartung von Anlagen und Geräten *(VDE0109:2020)*



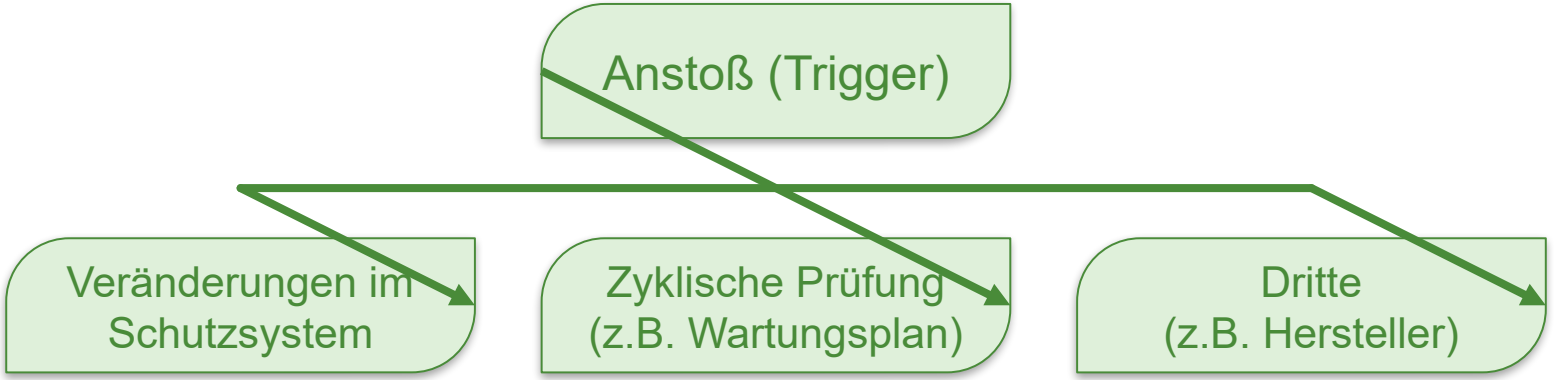
Beispiel: Wartungsstrategie (operativer Betrieb)

- Wartungsanforderung



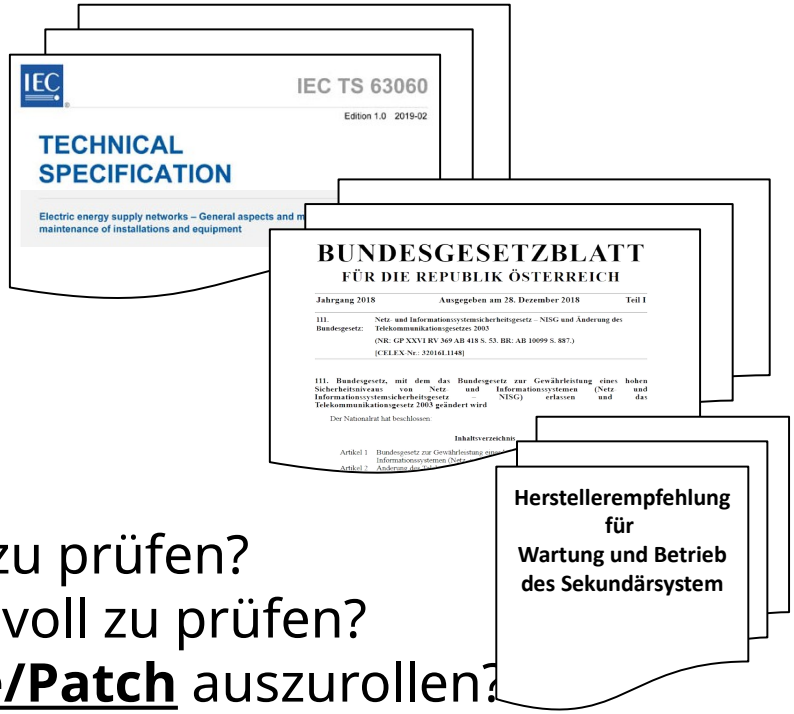
Beispiel: Wartungsstrategie (operativer Betrieb)

- Wartungsanforderung



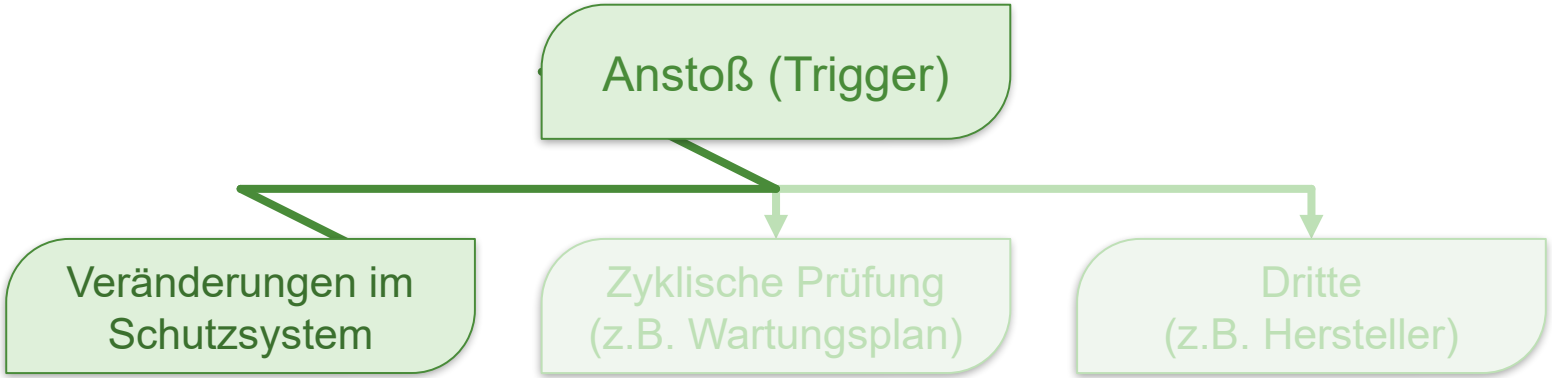
Wann ist es sinnvoll zu prüfen?
Was (Prüfumfang) ist sinnvoll zu prüfen?
Wann ist ein **Firmware-Update/Patch** auszurollen?

Beispiel: Wartungsstrategie (operativer Betrieb)



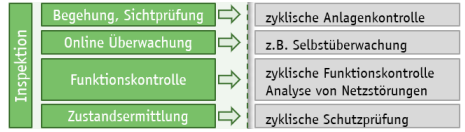
Wann ist es sinnvoll zu prüfen?
Was (Prüfumfang) ist sinnvoll zu prüfen?
Wann ist ein **Firmware-Update/Patch** auszurollen?

Beispiel: Wartungsstrategie (operativer Betrieb)



- Geringfügige Anpassungen (Einzelparameter), z.B. Zonenreichweite für Tagesprovisorium
  → *Leitfaden: „Umstellung von Einzelparameter“ grundsätzlich unkritisch*
  - Via Fernwartung oder Vorort, sorgfältiges Vorgehen
  - Aktuelles und aktives Reserveschutzkonzept
- Alles andere bedingt eine vollständige Überprüfung wie bei einer zyklischen Prüfung

Beispiel: Wartungsstrategie (operativer Betrieb)

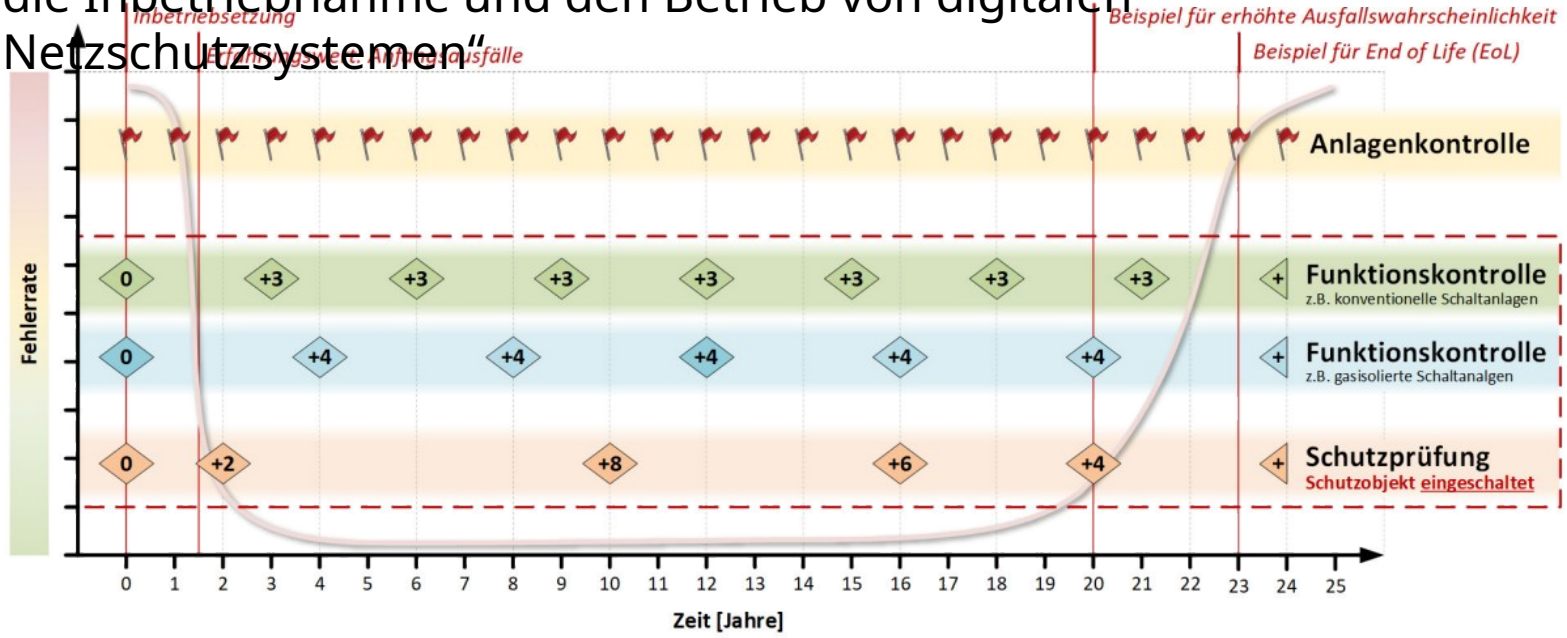


Mapping „Inspektion" auf IEC TS 63060:2019

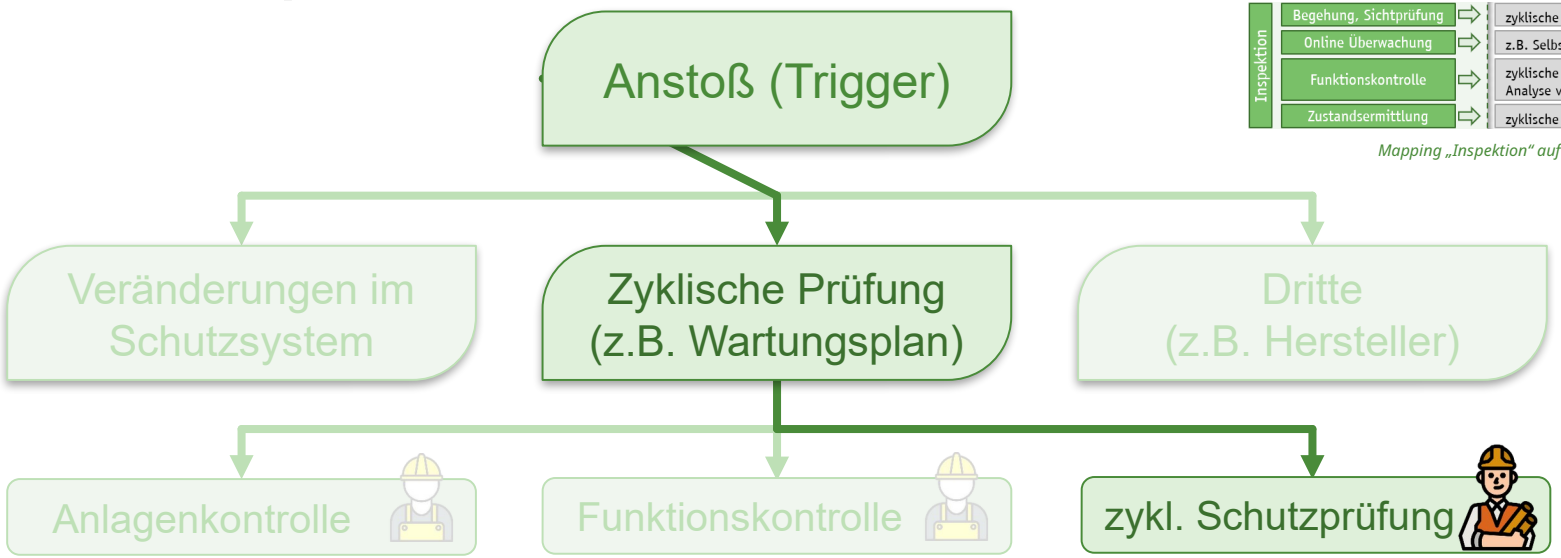
* *Aufbauend auf dem „Leitfaden für die Inbetriebnahme und den Betrieb von digitalen Netzschutzsystemen" in enger Zusammenarbeit mit dem Netzbetrieb*

Beispiel: Wartungsstrategie (operativer Betrieb)

- Beispiel für dynamische Prüfintervalle, entsprechend dem „Leitfaden für
die Inbetriebnahme und den Betrieb von digitalen Netzschutzsystemen“



Beispiel: Wartungsstrategie (operativer Betrieb)



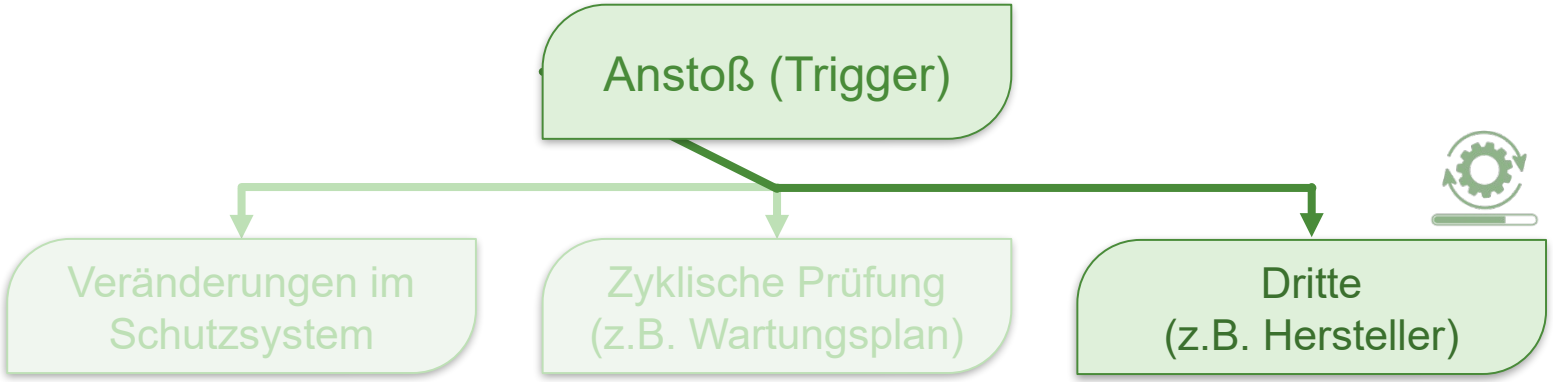
Inspektion		
	Begehung, Sichtprüfung	zyklische Anlagenkontrolle
	Online Überwachung	z.B. Selbstüberwachung
	Funktionskontrolle	zyklische Funktionskontrolle Analyse von Netzstörungen
	Zustandsermittlung	zyklische Schutzprüfung

Mapping „Inspektion“ auf IEC TS 63060:2019

- *Aktualität der Schutzeinstellung*
- *Schutzprüfung in allen Fehlerschleifen (Anregung, Zonenwerte, Überlast, …)*

** Aufbauend auf dem „Leitfaden für die Inbetriebnahme und den Betrieb von digitalen Netzschutzsystemen“ in enger Zusammenarbeit mit dem Netzbetrieb*

Beispiel: Wartungsstrategie (operativer Betrieb)

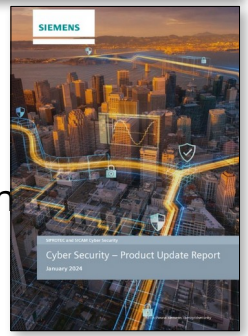


- Prozess zur Bewertung von Relevanz, Risiko und Auswirkung etablieren (Audit!)
  1. Risikoidentifikation und -analyse (**Betroffenheit**)
  2. Risiko**bewertung** und Dokumentation
  3. Risiko**steuerung**: vermeiden, vermindern, verlagern, tragen
  4. Risikokommunikation (**Awareness**)

Beispiel: Wartungsstrategie (operativer Betrieb)

- Beispiel für risikobasierten Patch-Management-Prozess (**STEP 1**):
  - Vertraglich gesicherte Bereitstellung von zeitnahen Security- und Schwachstellen-Reports aller eingesetzten Komponenten
    - z.B. im Zuge von Rahmenverträgen (Ausschreibung)
    - Security-Report ist eine Bringschuld des Lieferanten/Herstellers
    - Übermittlung ¼ jährlich oder in kritischen Fällen spontan
  - Lückenlose Auflistung aller bekannten Schwachstellen in eigenen und in implementierten Drittprodukten
    - Nachvollziehbar beschrieben, damit Anwender die Betroffenheit einschätzen
    - Schweregrad durch Hersteller eingeschätzt und klassifiziert
    - Mögliche Gegenmaßnahmen um Risiko zu vermeiden oder zu minimieren
  - Dezidierte Empfängeradresse mit Zugriff aus allen betroffenen Domänen (Audit)

Dritte (z.B. Hersteller)



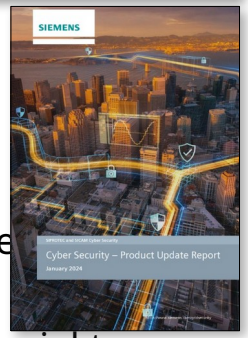
Beispiel: Wartungsstrategie (operativer Betrieb)

- Beispiel für risikobasierten Patch-Management-Prozess (**STEP 2**):
  - Bewertung der Schwachstellen durch interne Experten-Gruppe
    - OT-Security Verantwortlicher oder Stellvertreter
    - Verantwortlicher Schutztechniker
    - Verantwortlicher Leittechniker
    - Verantwortlicher Fernwirktechniker
    - Verantwortlicher Netzwerkstechniker

    Multi-Domain Evaluation

  - Entscheidung hinsichtlich Relevanz, Risiko und Maßnahme
    - Risiko ist unwesentlich/geringfügig: Verantwortlicher Fachbereich
    - Risiko ist mittel: Verantwortlicher für OT-Security in Verbindung mit Fachbere
    - Risiko ist hoch: Verantwortliche Abteilungsleitung für kritische Infrastruktur
    - Risiko ist kritisch/katastrophal: Bericht an Geschäftsführung → dezidiertes Projekt

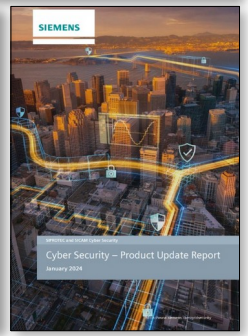
Dritte (z.B. Hersteller)



Beispiel: Wartungsstrategie (operativer Betrieb)

- Beispiel für risikobasierten Patch-Management-Prozess (**STEP 3**):
  - Bewertung der Change-Logs neuer Firmware
    - Funktionale Änderungen/Neuerungen: Fachbereich
    - Funktionsrelevante Fehlerbereinigungen: Fachbereich
    - Security relevante Fehlerbereinigungen: OT-Security Bereich
  - Roll-Out Prozess
    - 1. Teststufe der neuen Firmware in Laborumge
    - 2. Teststufe der neuen Firmware in einem abgeschalteten Abzweig an der Anlage
    - Roll-Out Freigabe für alle Abzweige gleicher Ty

Dritte (z.B. Hersteller)



Resümee

- IT- als auch OT-Security ist heute ein integraler Bestandteil unseres Alltags
- IT- als auch OT-Security lebt und bringt täglich neue Herausforderungen
- Schutz-, Leit- und Fernwirktechnik ist neben der OT-Security sowie der Netzwerk- und Übertragungstechnik eine Multi-Domain-Disziplin, die nur gemeinsam bewältigt werden kann
- Miteinander reden und voneinander lernen nimmt Ängste, schafft Vertrauen und bringt **alle** einen Schritt weiter

ENERGIE NETZE STEIERMARK

Ein Unternehmen der
ENERGIE STEIERMARK

Herausforderungen im Lebenszyklus eines digitalen Schutzgeräts als Folge von Digitalisierung und NIS

Oliver SKRBINJEK
Energienetze Steiermark GmbH
Tel. +43 664 6163805
Email: oliver.skrbinjek@e-netze.at

Horst PAAR
Energienetze Steiermark GmbH
Tel. +43 664 6167256
Email: horst.paar@e-netze.at