CPS, ICS, OT – ojemine. Wie finde ich mich im OT-Begriffsdefinitionendschungel zurecht?

Presentation by **Anna Habenegg**
ITSecX, St.Pölten 02.10.2026

Anna Habenegg

Seit über 10 Jahren in der IT mit Fokus auf Cybersecurity und OT-Security tätig.

Fokusbereiche:

- IT-Security Architecture
- Secure Networking
- OT-Security

Kontaktdaten

PwC Cybersecurity & Privacy | Senior Associate
Mobile: +43 676 5872077
Email: anna.habenegg@pwc.com



TLP yellow (recipients only)

Warum ist OT Security wichtig?

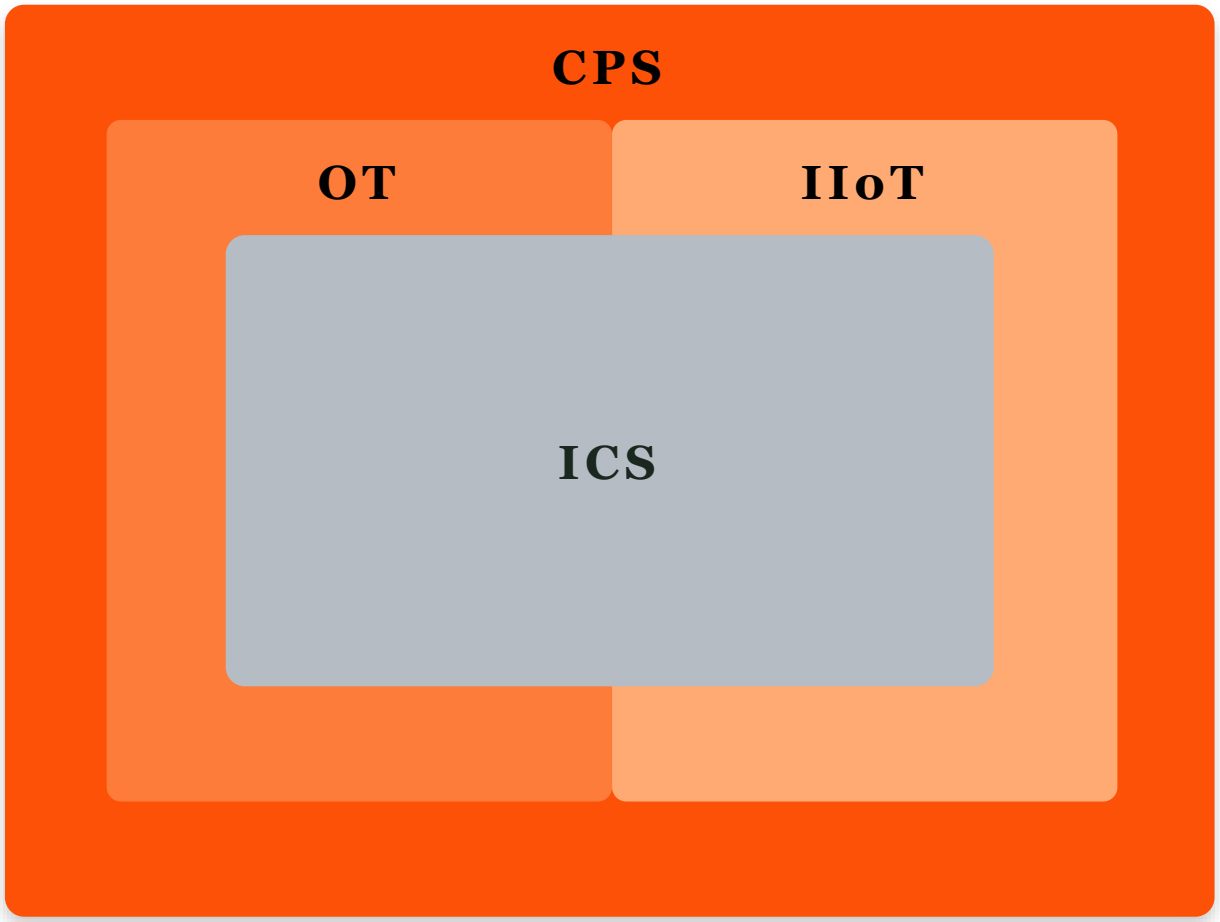
IT Priorities	OT Priorities
	Safety
Confidentiality	Availability
Integrity	Integrity
Availability	Confidentiality



In der OT ist die **Safety** am **wichtigsten**!
Ein Ausfall in der OT gefährdet Menschen, Umwelt, Produktion und Daten.

TLP yellow (recipients only)

Wie die Begriffe zusammenhängen



CPS – Cyber Physical System
Breitestes Konzept, umfasst auch IIoT, Medizintechnik und Smart Grid.

OT – Operational Technolgy
Der industrielle Betriebskern innerhalb der cyberphysischen Welt.

IIoT – Industrial Internet of Things
Der Teil der industrielle Internet of Things Komponenten beinhaltet.

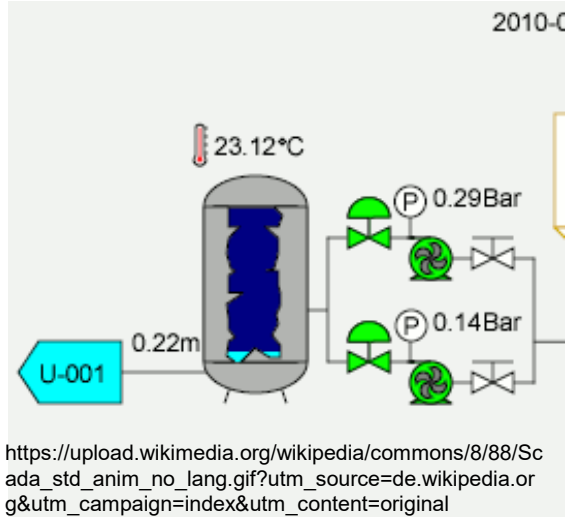
ICS – Industrial Control System
Die Steuerungssysteme, die den Betrieb tatsächlich regeln.

TLP yellow (recipients only)

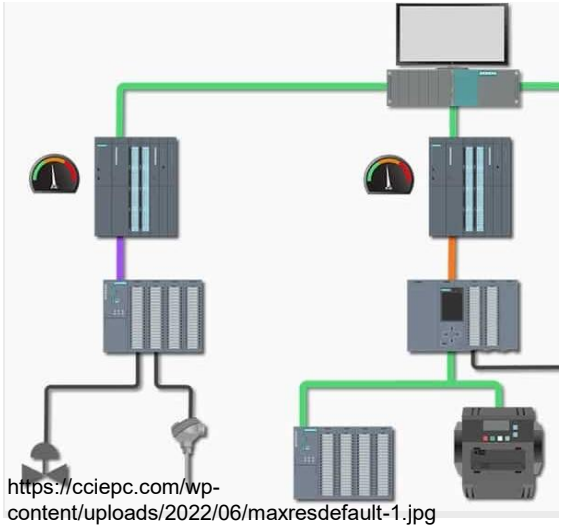
ICS – Industrial Control System



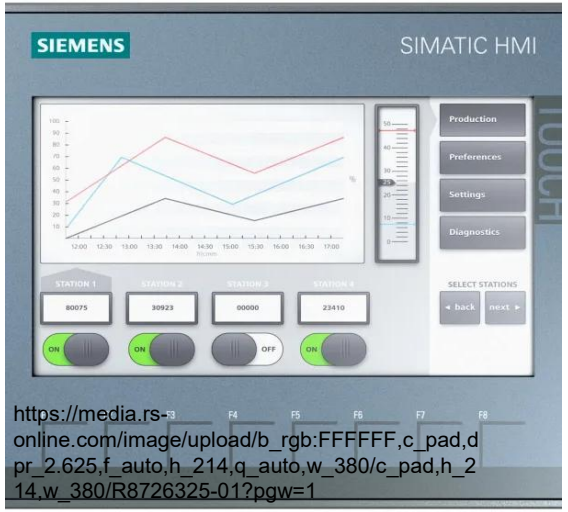
https://de.wikipedia.org/wiki/Logo_%28SPS%29



https://upload.wikimedia.org/wikipedia/commons/8/88/Scada_std_anim_no_lang.gif?utm_source=de.wikipedia.org&utm_campaign=index&utm_content=original



https://cciepc.com/wp-content/uploads/2022/06/maxresdefault-1.jpg



https://media.rs-online.com/image/upload/b_rgb:FFFFFF,c_pad,dpr_2.625,f_auto,h_214,q_auto,w_380/c_pad,h_214,w_380/R8726325-01?pgw=1

PLC

Programmable Logic Controller

Deutsch: SPS (Speicherprogrammsteuerung)

Programmierbare Steuerung, die Sensoren auswertet und Motoren oder Ventile ansteuert.

SCADA

Supervisory Control and Data Acquisition

System zur Überwachung von technischen Anlagen (z.B.: Stromnetze, Wasserwerke)

DCS

Distributed Control System

System zur Überwachung und Steuerung einer industriellen Anlage (z.B.: Produktionsanlagen, ´Chemieanlage).

HMI

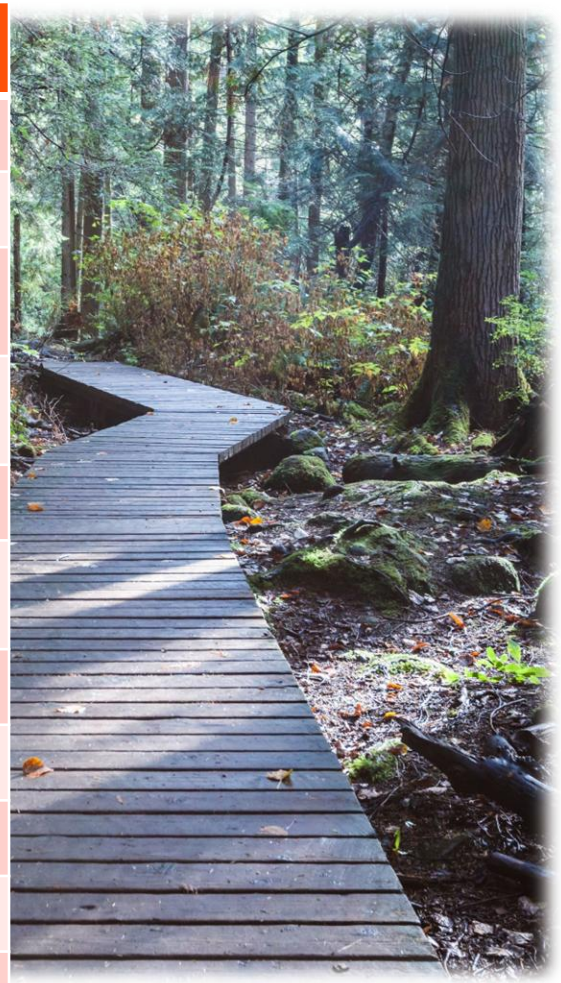
Human Machine Interface

Benutzeroberfläche zur menschlichen Überwachung einer Maschine oder Anlage.

TLP yellow (recipients only)

Landkarte durch den Dschungel

Asset	OT	ICS	CPS	IIoT	IoT	Kritikalität
PLC an einer Produktionslinie	Ja	Ja	Ja	Nein	Nein	Hoch
HMI an einer Maschine	Ja	Ja	Ja	Nein	Nein	Hoch
Vibrationssensor an einem Motor	Ja, wenn im Prozess integriert	Nein	Ja	Ja	Nein	Mittel
Office Laptop	Nein	Nein	Nein	Nein	Nein	Kommt drauf an ☺
SCADA Server	Ja	Ja	Ja	Nein	Nein	Sehr hoch
Smartwatch vom Produktionsleiter	Nein	Nein	Nein	Nein	Ja	Sehr niedrig
Fernwartungs-Gateway	Nein	Nein	Ja	Nein	Nein	Hoch
Safety Controller	Ja	Ja	Ja	Nein	Nein	Sehr hoch
Klimaanlage	Nein	Nein	Ja	Ja	Nein	Mittel/Hoch
Elektroauto Ladestation	Nein	Nein	Ja	Ja	Nein	Niedrig
Barcode Scanner mit Android OS	Nein	Nein	Ja	Ja	Ja	Mittel/Hoch



TLP yellow (recipients only)

IEC62443

Internationale Normenreihe für die Cybersicherheit industrieller Automatisierungs- und Leitsysteme (IACS).

Von ISA und IEC gemeinsam entwickelt, ursprünglich als ISA-99 gestartet.

Risikobasiert statt reiner Checkliste: der Schutz richtet sich nach der tatsächlichen Bedrohung.

1	62443-1-x	**Allgemein** Konzepte, Terminologie und Modelle als Fundament der ganzen Reihe.
2	62443-2-x	**Richtlinien und Prozesse** Sicherheitsprogramm für Betreiber und Anforderungen an Dienstleister.
3	62443-3-x	**System** Zonen und Conduits, Systemanforderungen und Security Level.
4	62443-4-x	**Komponente** Sicherer Entwicklungsprozess und technische Anforderungen an Produkte.

Zuerst die eigene Rolle bestimmen

Betreiber *Asset Owner*

Startet bei 2-1 und 2-4: Sicherheitsprogramm und Dienstleister.

Integrator *System Integrator*

Nutzt 3-2 und 3-3: Risiko, Zonen und Systemanforderungen.

Hersteller *Product Supplier*

Arbeitet mit 4-1 und 4-2: sichere Entwicklung und Komponenten.

TLP yellow (recipients only)

IEC62443 3-3 Functional Requirements und Security Levels

Die sieben **Foundational Requirements** (FR) **strukturieren die Schutzmaßnahmen**. Die vier **Security Levels** definieren wie **stark** die FR geschützt werden.



FR 1 · IAC Identification and Authentication Control
Geräte und Menschen müssen sich ausweisen.



FR 2 · UC Use Control
Rechte vergeben, begrenzen und protokollieren.



FR 3 · SI System Integrity
Sicherstellung der Integrität von Software, Firmware und Prozessdaten.



FR 4 · DC Data Confidentiality
Sicherstellung, dass vertrauliche Daten von unberechtigten Dritten nicht mitgelesen werden können.



FR 5 · RDF Restricted Data Flow
Datenflüsse mittels Netzwerksegmentierung nach Zonen und Conduits begrenzen.



FR 6 · TRE Timely Response to Events
Vorfälle erkennen, melden und rechtzeitig darauf reagieren.



FR 7 · RA Resource Availability
Der Prozess läuft weiter, auch bei Störung oder Überlast.

Security Level (SL 0 bis 4)

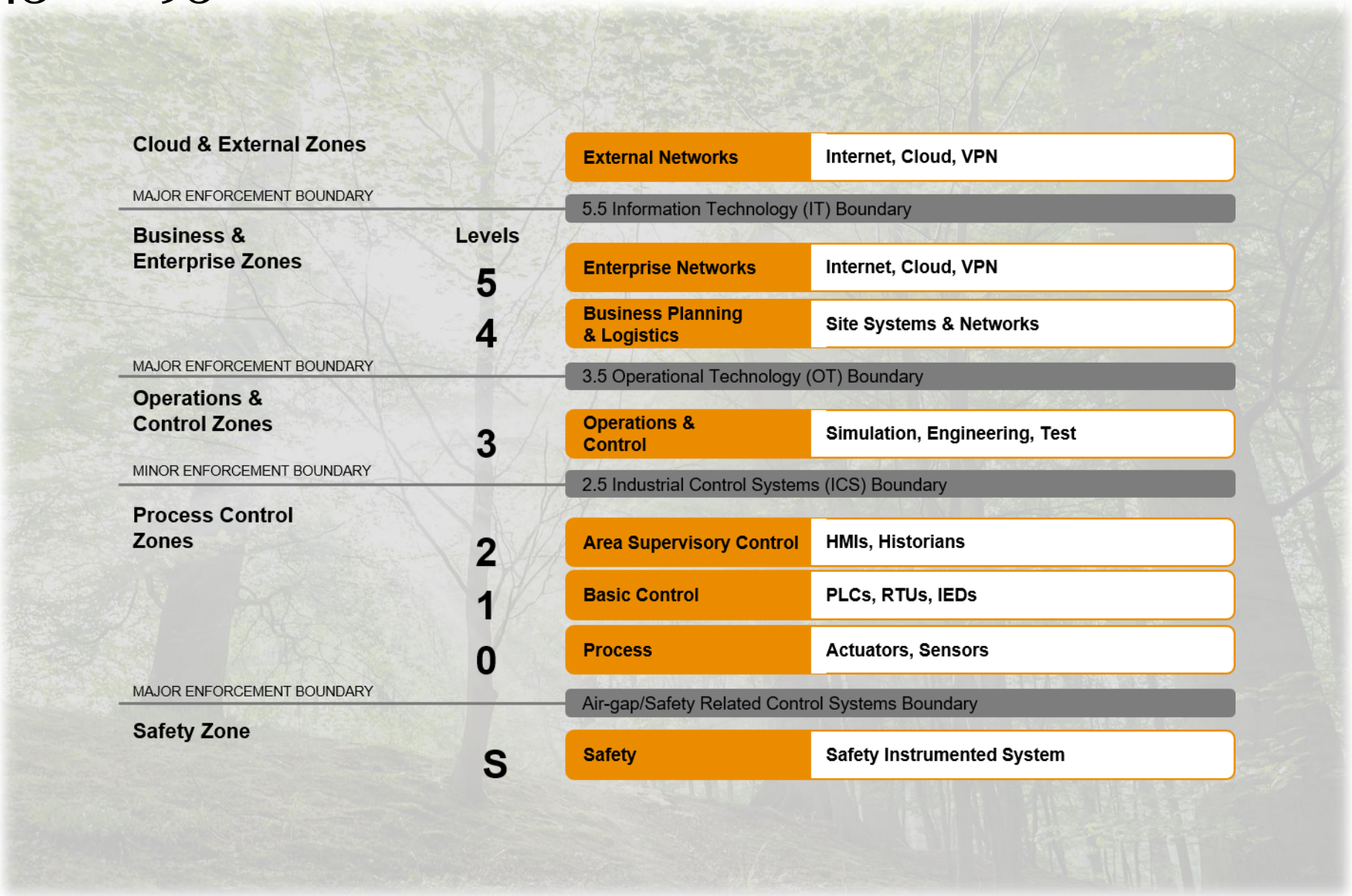
SL 0	keine besonderen Anforderungen
SL 1	Schutz vor zufälligem Fehlverhalten
SL 2	Schutz vor einfachen, absichtlichen Angriffen
SL 3	Schutz vor gezielten Angriffen mit Fachwissen
SL 4	Schutz vor Angriffen mit hohem Aufwand

Zusammenhang

Für jede Zone wird ein Ziel Level (SL-T) festgelegt. Daraus folgen je FR die konkreten System Requirements (SR). Höherer SL heißt mehr Anforderungen, nicht automatisch mehr Sicherheit.

TLP yellow (recipients only)

IEC 62443 ISA95 Model



TLP yellow (recipients only)

Gefahren im Dschungel



Flache Netze ohne Segmentierung: ein Einbruch erreicht sofort die Steuerung.



Unkontrollierter Fernzugriff von Herstellern und Dienstleistern.



IT Sicherheitswerkzeuge blind auf OT anwenden und so den Betrieb stören.



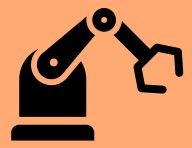
OT-Security als einmaliges Projekt statt als dauerhaften Prozess begreifen.



USB Sticks, Smartphone Ladekabel und externe Festplatten, die wild an OT-Systeme ansteckt werden.

TLP yellow (recipients only)

Der kleine Guide um nicht gefressen zu werden



Prozesse verstehen
Wenn Prozesse ganzheitlich verstanden werden, können sinnvoll erarbeitet werden.



Risiken bewerten
Die regelmäßige Bewertung von Risiken verbessert ermöglicht eine langfristige Planung.



Sichtbarkeit schaffen
Ein vollständiges Inventar aller Anlagen aufbauen. Was man nicht kennt, kann man nicht schützen.



Kontinuierlich überwachen
Passive, für OT geeignete Anomalieerkennung statt störender aktiver Scans.



Netzwerk segmentieren
Zonen und Conduits umsetzen und IT von OT über eine DMZ (Demilitarize Zone) sauber trennen.



Zugriffe kontrollieren
Least Privilege, Multi Faktor Authentifizierung und abgesicherter Fernzugriff über dedizierte Jumphosts.

TLP yellow (recipients only)

Bereit für den Weg durch den Dschungel!



Erst einordnen

CPS ist der Rahmen, **OT** der Betrieb, **ICS** die Steuerung, **IIoT** die vernetzten Geräte. Die Frage ist nie die Abkürzung, sondern der Prozess dahinter.



Rolle klären

IEC 62443 ist eine Reihe, kein Buch.
Betreiber starten bei 2-x,
Integratoren bei 3-x,
Hersteller bei 4-x.
FR sagt was, **SL** sagt wie stark.



Dranbleiben

Inventar, **Zonen** und **Conduits**, kontrollierte Zugriffe, passives Monitoring. **SAFETY** und **Security** gehören zusammen,
Sicherheit bleibt ein Prozess.

Der kleine Guide für große Taten

OT Betriebstechnik
ICS Steuerungssysteme
CPS cyberphysische Systeme
IIoT vernetzte Industriegeräte

PLC / SPS speicherprogrammierbare Steuerung
HMI Bedienoberfläche
SCADA Überwachung verteilter Anlagen
DCS Steuerung einer Anlage

IACS Automatisierungs und Leitsysteme
FR Grundanforderung, sieben Stück
SL Schutzstärke 0 bis 4
SR System Requirement je FR

TLP yellow (recipients only)

Welcome to the OT jungle!



© 2026 PwC Austria. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.