



Identity und Access Governance für Ihre Operational Technology (OT)

www.tuv.com/informationssicherheit

 **TÜVRheinland[®]**
Genau. Richtig.

Identity und Access Governance in OT

VERSCHMELZUNG VON IT- UND OT-NETZWERKEN

Im Zuge der Globalisierung und der voranschreitenden Automatisierung erfolgt eine immer weiterreichende Digitalisierung von Herstellungs- und Produktbetreuungsprozessen. Es kommt dabei zu einer Verschmelzung von IT-Netzwerken mit den bisher isolierten OT-Netzwerken.

Damit sind OT-Netzwerke und alle darin vorhandenen Elemente wie ICS, SCADA, Sensoren, Aktoren sowie ganze Maschinenanlagen über die IT-Netze erreichbar und angreifbar. Hierzu existieren bereits auf OT-Netze und ICS-/SCADA-Steuerungen spezialisierte frei zugängliche Such- und Hack-Tools.

Weltweit bekanntgewordene Beispiele der letzten Jahre zeigen exemplarisch erfolgreiche Angriffe oder offene Schwachstellen in Atomkraftwerken, Wasserkraftwerken, Wasserversorgungen oder in Stahlwerken. Hier ergeben sich somit neue Angriffsszenarien, die in ihrer Auswirkung von punktueller Schädigung eines einzelnen Produktionsprozesses, über Stilllegung bzw. Beschädigung kompletter Fabrikationsstätten, bis hin zu globalen Auswirkungen auf die Umwelt und Gesellschaft z.B. in der Energieversorgung oder Wasserversorgung reichen können.

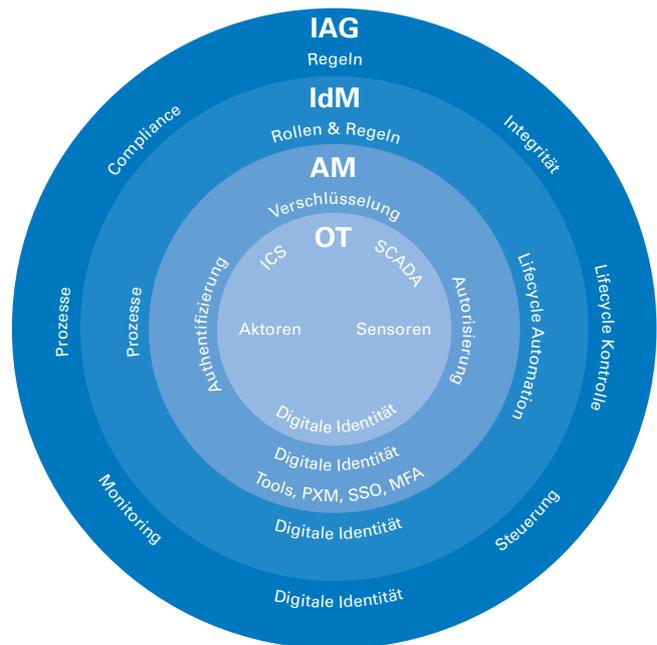
ALLE OT-ELEMENTE UND PERSONEN INTEGRIEREN

Um weiterhin die Sicherheit von OT-Netzwerken gewährleisten zu können, müssen die Prinzipien der Informationssicherheit aus den IT-Netzwerken in die Betrachtung und Verwaltung der OT-Netzwerke übertragen werden.

Hierbei sind sowohl die Identifizierung und Identitätsverwaltung als auch die Zugriffsverwaltung und Zugriffssteuerung von allen beteiligten Akteuren, Systemen, Steuerungseinheiten, Sensoren, Aktoren und Maschinenanlagen als Kernbausteine einer umfassenden und sicheren Digitalisierung unerlässlich. Damit bedarf es einer zielgerichteten Identity und Access Governance, die einerseits übergreifend IT-Netzwerke und OT-Netzwerke betrachtet und andererseits alle OT-Elemente ebenso wie handelnde Personen als eigenständige digitale Identitäten auffasst.

TÜV Rheinland
Digitale Transformation & Cybersecurity
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
cybersecurity@tuv.com
www.tuv.com/iam

IDENTITY ACCESS GOVERNANCE (IAG) SCHICHTENMODELL



Unsere Methodik geht bei der Übertragung der IAG-Prinzipien von IT- auf OT-Netze von einer schichtweisen Betrachtung aus:

- In der innersten Schicht ist das OT-Netz mit seinen Elementen zu sehen.
- Dies wird gekapselt durch Identity und Access Management Schichten (AM und IdM).
- Gesteuert wird alles durch die äußere Identity Access Governance Schicht.

Im Rahmen der Identity und Access Governance erfolgt die kontinuierliche Steuerung und Kontrolle aller Identity und Access Management Lösungen und damit verbundenen Technologien, Prozesse und Vorgaben.

Gerne unterstützen wir Sie rund um das Thema ganzheitliches Identity und Access Management und Identity und Access Governance im Bereich verknüpfter IT- und OT-Netzwerke. **Fragen Sie uns!**