



**SECURITY**  
Klaus Lussnig, Industrial Automation  
[www.scada.online](http://www.scada.online)

Ei-Ei-OT!

## Sicherheit + Sicherheit gibt Sicherheit!

Wer stottert denn da? Schnelle Auflösung hier – FAT / SAT:

- Sicherheit für Betreiber zum Prozess der Wartung und Instandhaltung
- Sicherheit für Maschinen- und Anlagelieferanten
- Sicherheit gegen schädliche Manipulation und Angriffe

Die Uhr lässt sich nur schwer zurückdrehen. Die rasante Zunahme von Remote Access, bzw. Fernwartung auf die Anlagen, ebenso die vielen Datenverbindungen des IIoT für Predictive Services in der Cloud und Dienstleistungen, sind zwingend notwendig in der Gewährleistung, da bekanntermaßen Produktionsanlagen mit dem Internet verbunden sind. Fakt: Die Folgen der Zunahme von Cyberangriffen sind nur ein klarer Beweis.

Die Betreiber versuchen den Air-Gap wieder zu erlangen. Unterstützung vor Ort mit geprüften Engineering Workstations ist beim Kräftermangel sehr teuer gewor-

den. Neue Programmierungen und Softwareupdates lassen sich nicht in alle Ewigkeit aufschieben. Für die Betreiber eine schwierige Situation ohne Fernwartung, die Kosten für das benötigte Equipment und schnelle Vor-Ort-Verfügbarkeit von Fachleuten zu minimieren. Aus betrieblicher Sicht ist eine UNABHÄNGIGE Aufnahme und Anzeige im Leitstand, wann was auf der Anlage gemacht hat, gefordert. Vertrauen gut, Kontrolle besser.

Für die Lieferanten sind die Abnahmen bei Lieferung, die Dienstleistungen zur Unterstützung, aber auch die adhoc Tätigkeiten in der Gewährleistung bei Problemen, mit Personal vor Ort, kaum mehr zu erfüllen. Eine detaillierte Darstellung der Geräte und Systeme, inklusive der Kommunikationen und genutzten Protokolle, vereinfachen diese Tätigkeiten sehr. Änderungen von Dritten und Fehler werden unmittelbar angezeigt. Innerhalb kürzester Zeit stehen Asset-Dokumentation und ein logischer Netzstrukturplan zur Verfügung.

Nicht zuletzt kommen die Anforderungen zur Cyberresilienz und Security vom Gesetzgeber, den Eigentümern und Kunden hinzu. Die vermehrten, sehr erfolgreichen Angriffe zeigen, dass die aktuellen Risikobetrachtungen schnell zu überdenken sind. Systeme zur Angriffserkennung und im Schadensfall zur Forensic sind mehr als nur notwendig.

Die kontinuierliche Security-Betrachtung und Risikominimierung ergeben Einsparpotentiale für Lieferanten und Betreiber. Sämtlich aktuelle Informationen für die mehrmals jährliche, notwendige Risikoanalyse müssen mit wenig Aufwand zur Verfügung stehen. So sind die Anforderungen für ALLE Parteien mit den verschiedenen Anforderungen einfach umsetzbar.

Also: keine faulen Eier in der Ei-Ei-OT, sondern 3x Sicherheit auf einen Streich!

In Kooperation mit Acht-Werk  
[www.acht-werk.de](http://www.acht-werk.de)  
[www.irma-box.de](http://www.irma-box.de)

### ERWEITERUNG DER CYBERSICHERHEIT

## Neue Features von IRMA®

#### SYSLOG EVENT MANAGER: DER BESONDERE ...

Durch die Korrelation der Syslog-Meldungen mit der Anomalieerkennung im IRMA® System erhalten Betreiber zentral Systemmeldungen der Geräte und zeitgleich mögliche Änderungen im Verhalten innerhalb der Produktionsanlagen. So sehen sie auf einen Blick ob kritische Manipulationen erfolgt sind. Damit werden Protokollierung und Detektion an einem Punkt verbunden. IRMA® unterstützt damit die schnelle Reaktion, um Ausfälle und Schäden zu verhindern. Systemweit oder per Gerätegruppe/Geräte lässt sich die Severity (Schweregrad) für den Empfang der Meldungen auswählen. Der IRMA® Syslog Event Manager enthält eine Vielzahl integrierter

Aktionen, um im Falle eines Vorfalls automatisiert zu alarmieren.

#### MEHR SYSTEM-INTEGRATIONEN

Schnittstellen wie OPC UA DA oder MQTT erweitern die Anbindung an SCADA, Security Information und Event Management (SIEM), Security Operation Center (SOC). Zusätzlich sorgt ein verbesserter RestAPI für verlässlichen Zugriff auf Bedrohungsdaten, Assets und Verbindungen sowie die Alarmierung. Damit ist eine schnelle und direkte Integration von IRMA® in Management-, Leitstand-, SIEM- oder SOC-Systeme möglich.



#### IRMA GUARD - ALS APPLIANCE ODER VM BIETET EINZIGARTIGE VORTEILE

IRMA® Guard bietet einen konsolidierten Zugriff auf den Bedrohungslevel einer Anlage und Assets der

IRMA® Systeme, die im Feld oder in den Produktionsstandorten eingesetzt werden. So erfolgt die einfache Verwaltung der Cybersicherheit für Hunderte von verteilten Industrieanlagen. Dies ermöglicht jederzeit die zentrale Übersicht und Informationen für die Betriebsführung, um den ordnungsgemäßen Zustand der IRMA® Systeme zu managen. □

Industrial Automation GmbH  
Techniker Straße 1-3, A-6020 Innsbruck  
+43 512 272271 0  
[office@automation.team](mailto:office@automation.team), [www.scada.online](http://www.scada.online)