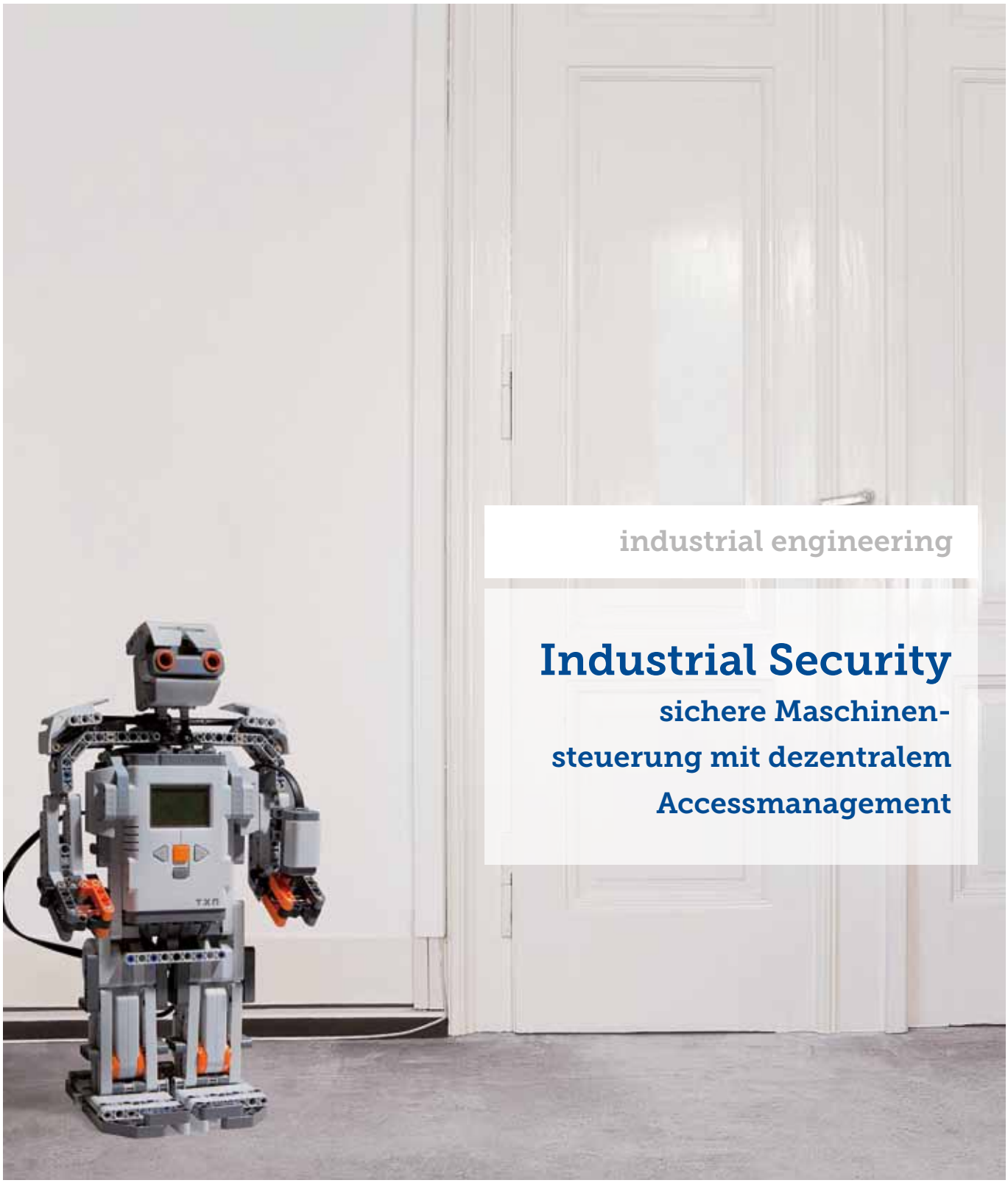
THINK SAFE THINK ICS



industrial engineering

Industrial Security

sichere Maschinen-steuerung mit dezentralem Accessmanagement

THINK SAFE THINK ICS

industrial security

Sichere Steuerung von Maschinen mit dezentralem Accessmanagement

Die ICS AG ist seit über 50 Jahren im Bereich Automatisierung, Logistik und Supply Chain Integration im Industriesektor tätig. Im Bereich Security bei IoT und Industrie 4.0 (z.B. Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit) haben wir im Rahmen der Entwicklungsarbeiten mit unseren Kunden festgestellt, dass es starke Sicherheitsbedenken seitens der Betreiber gibt, ihre Maschinen, Steuerungen und vergleichbaren Einrichtungen zu vernetzen.

Schwerpunkte:

- Industrial Security
- Secure System Control – IEC 62443
- Identity Access Management
- Security by Design

industrial security

Secure System Control

Wichtigste Grundlage: Standards einhalten

Secure system control - Dieses Szenario greifen wir auf, um auf Basis des hier vorgestellten Demonstrators Lösungsmöglichkeiten unter Nutzung von Standardkomponenten aufzuzeigen.

Grundvoraussetzung für ein solches „sicheres“ System, ist die Einhaltung von IT-Security-Mindeststandards. Diese sind in der **Normenreihe IEC 62443** für Hersteller, Betreiber und Integratoren gleichermaßen beschrieben und bieten eine gute Basis für ein ganzheitliches Schutzkonzept.

Bestandteil der IEC 62443: VDI/VDE 2182 und ISO 27000

Technischer Aufbau des Steuerungsmodells

Im Folgenden wird der **technische Aufbau** aus Sicht von **IoT und Security** im Detail erläutert:

Über die **Leitzentrale** werden die Steuerbefehle für den Verladekran vorgegeben. Dazu muss sich ein Benutzer **per NFC** an der Leitzentrale **authentifizieren**.

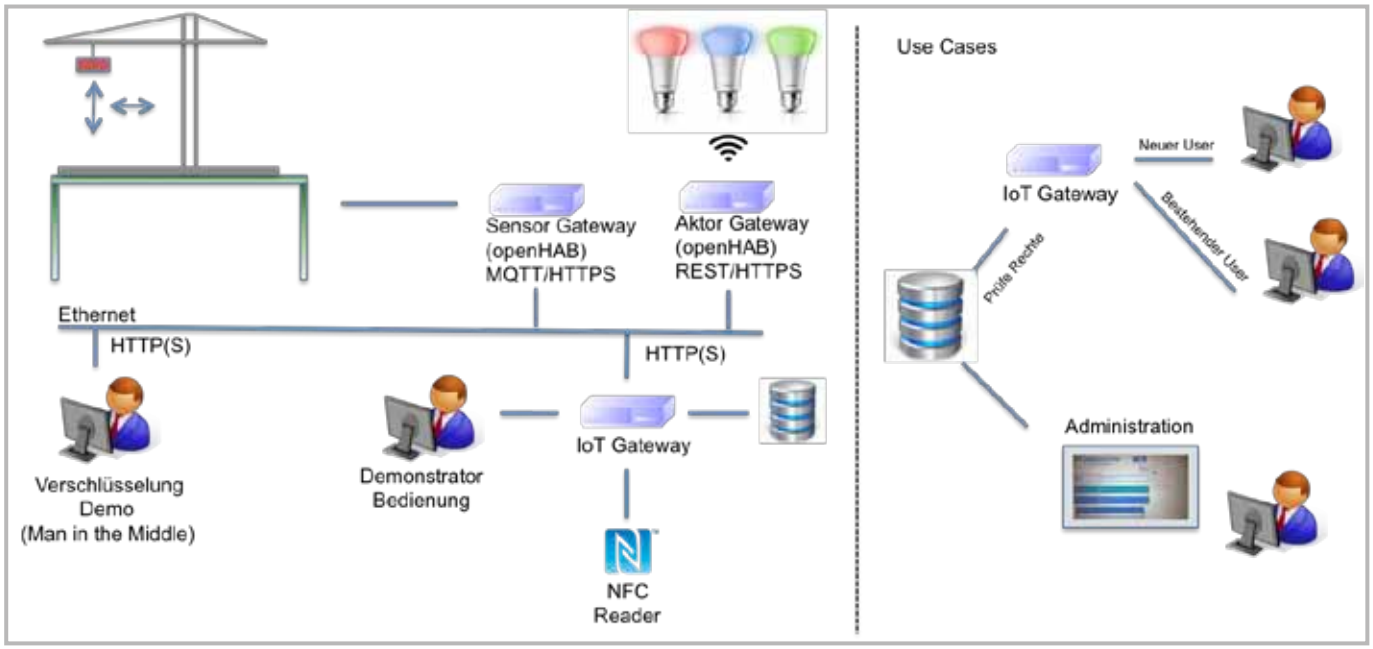
Die Befehle werden anschließend **verschlüsselt** über das Netzwerk an das **Aktor-Gateway übertragen**, wo sie nach erfolgreicher Prüfung der Authentifizierung ausgeführt (ansonsten verworfen) werden.

Parallel sammelt das **Sensor-Gateway** die Daten der Sensoren (Abstand, Stromverbrauch) und überträgt sie an die Leitzentrale.

Für die Demonstration wurde bei einem Teil der Sensordaten auf eine Verschlüsselung bewusst verzichtet, um einen „Man-in-the-Middle-Angriff“ demonstrieren zu können.

Eine **visuelle Rückmeldung** über den Status der Authentifizierung und der Sensoren wird über Signallampen realisiert.

Aufbau Steuerungsmodell anhand eines Krans:



Industrial Security

Hohe Anforderungen werden gestellt

Die industriellen Sicherheitsansprüche stellen hohe Anforderungen an die effiziente Angriffserkennung und somit die Absicherung von Produktionsanlagen gegen Cyberangriffe. Interne Manipulationen oder fehlerhafte Konfigurationen stellen in diesem Kontext ebenfalls zunehmende Herausforderungen dar. Daher setzen wir die **IT-Sicherheitslösung IRMA©** ein.

IRMA – Industrie Risiko Management Automatisierung
(Achtwerk GmbH & Co. KG)

Vorzüge einer solchen Lösung auf einen Blick:

- Überwachung der Visualisierung des aktuellen Sicherheitsstatus des IT-Netzes
- Benennung und Bewertung relevanter IT-Risiken
- Kontinuierliches Monitoring der Produktionsanlagenkommunikation
- Entdeckung von Cyberangriffen und Manipulationen in Echtzeit
- Zuverlässige Alarmmeldungen

„Durch Web-Applikationen, welche nicht die unternehmenskonformen Anmeldeverfahren verwenden, entstehen vielfach Sicherheitslücken."

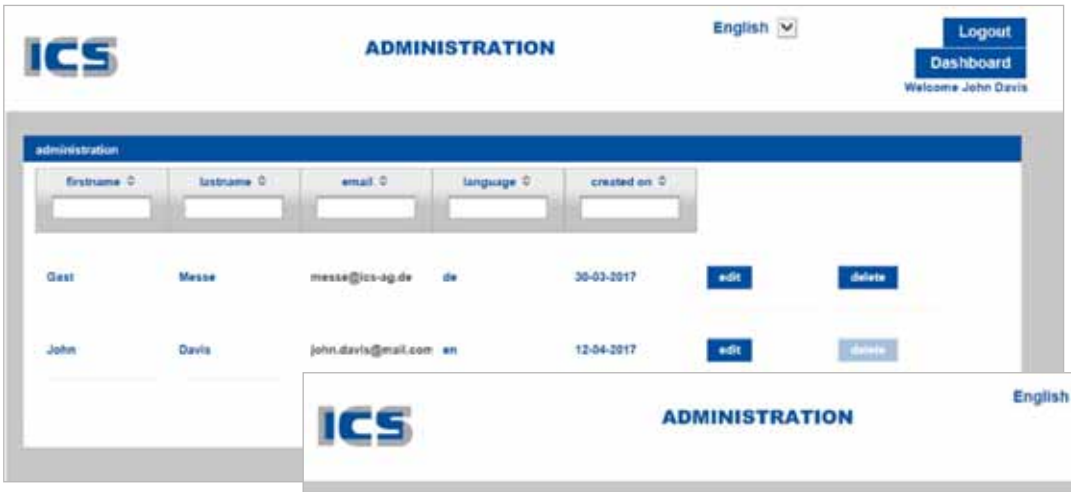
Martin Zappe, BU Manager Industrial Engineering

Identity Access Management

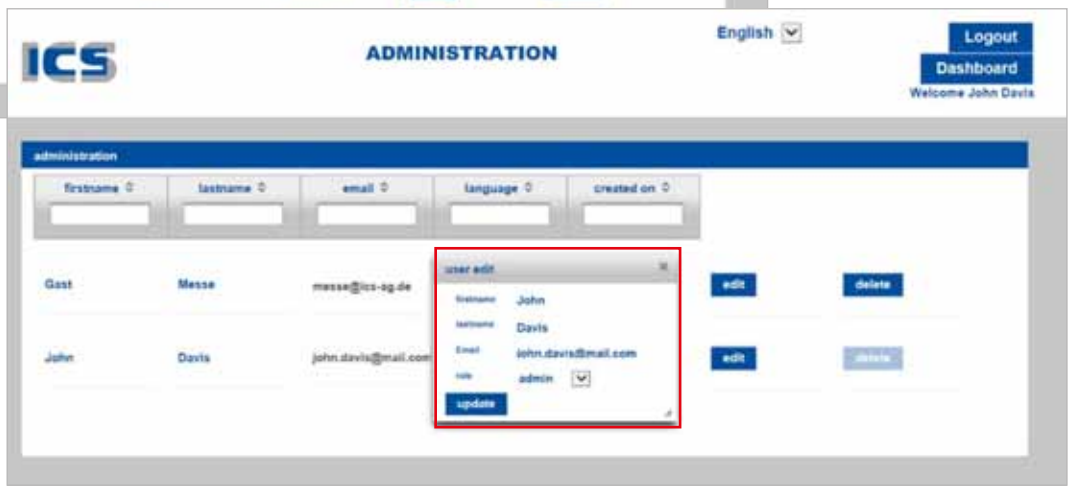
Die Administration der Benutzer wird über das ICS-ADMIN Tool abgewickelt. Wir haben es entsprechend industrieller Anforderungen basierend auf dem OAuth-Protokoll entwickelt. Die Rechtevergabe wird hiermit benutzerspezifisch vorgenommen (Identity Access Management – IAM). Entsprechend lässt sich der Kran ausschließlich nach den verfügbaren Benutzerrechten steuern.

Der Vorteil dieser individuellen IAM Lösung ist die vollständige Kontrolle über die zu integrierenden Prozesse (u.a. ohne Nutzung eines Cloud-Services) die mit der Rechteverwaltung einhergehen. Berechtigungen lassen sich zentral verwalten. Infolgedessen ist eine redundante Benutzerpflege in mehreren Systemen nicht notwendig, was den Aufwand und die Fehleranfälligkeit - und damit mögliche Securityschwächen - erheblich minimiert.

Gleichzeitig wird die Gesamtübersicht der vergebenen Benutzerrechte optimiert. Darüber hinaus können durch die offene Architektur auch standardisierte IAM Lösungen namhafter Hersteller angebunden werden.



Administration der Benutzer



Rollenzuweisung

industrial engineering

Lücken schließen Erfahrung nutzen

Wir arbeiten als **Safety- und Security-Manager** und begleiten unsere Kunden bei der Erstellung von sichereren Systemen sowie bei der Sicherung ihrer Daten und Unternehmenswerte im Sinne der IT-Security.

In **Workshops**, die auf jeden Kunden individuell zugeschnitten sind, identifizieren wir die relevanten Assets und Anforderungen. Wir erstellen **Risikoanalysen**, leiten daraus die wesentlichen Sicherheitsziele ab und entwickeln auf dieser **Grundlage Sicherheitskonzepte** für sichere Systeme und Anforderungen zum Schutz gegen Cyber-Angriffe.

Bei Bedarf übernehmen wir ebenfalls die Analyse der bestehenden Prozesse, um diese anschließend normgerecht und praxisnah zu optimieren bzw. zu gestalten. Unsere **zertifizierten Sicherheitsexperten** sind Ihnen ein verlässlicher Partner, sowohl bei der Dokumentation individueller Sicherheitsrichtlinien als auch bei der Integration in die jeweilige Prozesswelt – von der Personalschulung bis hin zum Support.

Selbstverständlich begleiten wir Sie auch bei der Vorbereitung und Durchführung von **IT-Security-Audits** entsprechend der ISO 27001ff wie diese z. B. mittlerweile regelmäßig in der Automobilindustrie üblich sind. Dabei greifen wir auf eigene Audit-Erfahrung zurück – die ICS AG ist entsprechend erfolgreich durch OEMs auditiert worden.

Über die ICS AG

Wir sind ein mittelständisches, familiengeführtes IT-Beratungs- und –Engineering-unternehmen. Seit 1966 entwickeln wir intelligente Lösungen für sicherheitskritische IT-Umgebungen. Unsere Leistung umfasst den gesamten Produktlebenszyklus von der Konzeption bis zur Zulassung eines Systems.

Mit 50 Jahren Erfahrung in der IT-Branche gehört die ICS AG zu den renommierten Softwaredienstleistern im Raum Stuttgart und weit darüber hinaus.

Sie sind verantwortlich für ein Bauteil mit besonderen sicherheitsrelevanten Merkmalen? Sie wollen oder müssen eine dokumentationspflichtige Sicherheits-Zertifizierung Ihres zu entwickelnden Systems erreichen?

In allen Punkten sind Sie gut aufgehoben bei unseren Experten der Business Unit Industrial Engineering.

Kontakt

ICS AG
Sonnenbergstr. 13
70184 Stuttgart

T +49 711 2 10 37 00
industry@ics-ag.de
www.ics-ag.de