

ICS-Vorgehensmodell für die IT-Sicherheits-Risikoanalyse im Bahnumfeld: TÜV-geprüft und für gut befunden

Stuttgart, 10. Mai 2019: Ein ganzheitliches Vorgehensmodell für die Risikoanalyse im Bahnumfeld hat die Begutachtung durch den TÜV Süd mit Bravour bestanden. Patric Birr, RAMS Engineer und Head of Competence Center Security bei der ICS AG, entwickelte das ICS-Vorgehensmodell auf Basis der Normenreihe IEC 62443 bereits 2016.

Mit dem Begutachtungsergebnis durch den TÜV Süd hat das ICS-Vorgehensmodell jetzt offiziell alle Vorgaben erfüllt, die der Gesetzgeber an ein dem Stand der Technik entsprechendes Security Risk Assessment im Bahnumfeld stellt. Damit wird bestätigt, dass das Vorgehen den relevanten Standards und Vorgaben entspricht. Es kann ab jetzt als integraler Bestandteil von Sicherheitsbetrachtungen in der Domäne Bahn angewendet werden sowohl in der Systementwicklung als auch in späteren Lebenszyklus-Phasen.

„Wir sind stolz auf das positive Begutachtungsergebnis und profitieren jetzt davon, dass wir uns frühzeitig auf die wachsende Bedeutung der IT-Sicherheit im Bahnumfeld vorbereitet haben“, freut sich Birr. Der RAMS Ingenieur mit Schwerpunkt Security hatte Anfang 2017 in einem Vortrag vor Mitgliedern des Verbands der Bahnindustrie in Deutschland e.V. (VDB) sein Modell vorgestellt, das zu diesem Zeitpunkt bereits in einem Entwicklungsprojekt der Deutschen Bahn (DB) im Einsatz war. Dies erregte die Aufmerksamkeit des TÜV Süd, der schon kurz darauf mit der Begutachtung im Rahmen des Projektes DiB beauftragt wurde. Zum Abschluss dieser Begutachtung wurde im März dieses Jahres die IT-Sicherheits-Risikoanalyse für das im Projekt DiB entwickelte System durch den TÜV Süd erfolgreich zertifiziert.



Patric Birr entwickelte das ICS-Vorgehensmodell auf Basis der Normenreihe IEC 62443

Kontinuierliche und gesetzeskonforme Sicherheit für die Bahn

Die auf funktionale Sicherheit (Safety) ausgelegten, geschlossenen Systeme der Bahn werden durch die fortschreitende Digitalisierung geöffnet, womit sie anfällig werden für Cyber-Attacken. Das IT-Sicherheitsgesetz verpflichtet Betreiber Kritischer Infrastrukturen (KRITIS) dazu, ihre Informationssicherheit regelmäßig auf den Prüfstand zu stellen, dies betrifft auch die Bahnbranche.

Die einschlägigen Normen, Prozesse und Nachweisführungen stellen den Schutz der Verfügbarkeit sowie die Systemintegrität zur Wahrung der funktionalen Sicherheit in den Mittelpunkt. Um den gesetzlichen Anforderungen zur Konformität mit dem Stand der Technik nachzukommen, erweitert Birrs Modell, das in der Vornorm DIN VDE V 0831-104 beschriebene Vorgehen zur Anwendung der IEC 62443 im Bahnumfeld um eine mehrstufige, qualitative Risikobetrachtung. Dabei werden - unter Anwendung bewährter Ansätze über Bottom-Up und Top-Down Analysetechniken - schrittweise die vorhandenen Schutzmechanismen überprüft und bei Bedarf ergänzt.

(Autor: Julia Grewe)

Über die ICS AG

Die ICS AG ist seit mehr als 50 Jahren ein erfolgreiches, familiengeführtes IT-Beratungs- und Engineering-Unternehmen.

Die Spezialisierung liegt in den Geschäftsfeldern Industrial Engineering (Automation, Supply Chain, Logistic, Automotive), Transportation und den Bereichen Funktionale Sicherheit, Security & Safety sowie Informationssicherheit und DSGVO.

| Pressekontakt: | Fachlicher Kontakt |
|--|---|
| <p>ICS AG Marketing & PR Stefanie Henzler</p> <p>Tel.: +49 711 21037 – 40 E-Mail: presse@ics-ag.de</p> <p>Web: https://www.ics-ag.de/presse/</p> | <p>ICS AG Competence Center Security Patric Birr</p> <p>Tel.: +49 172 728 05 80 E-Mail: patric.birr@ics-ag.de</p> <p>https://www.ics-ag.de/kompetenzen/security-for-safety/</p> |