Challenges ahead for DB InfraGO as a railway infrastructure manager and KRITIS operator

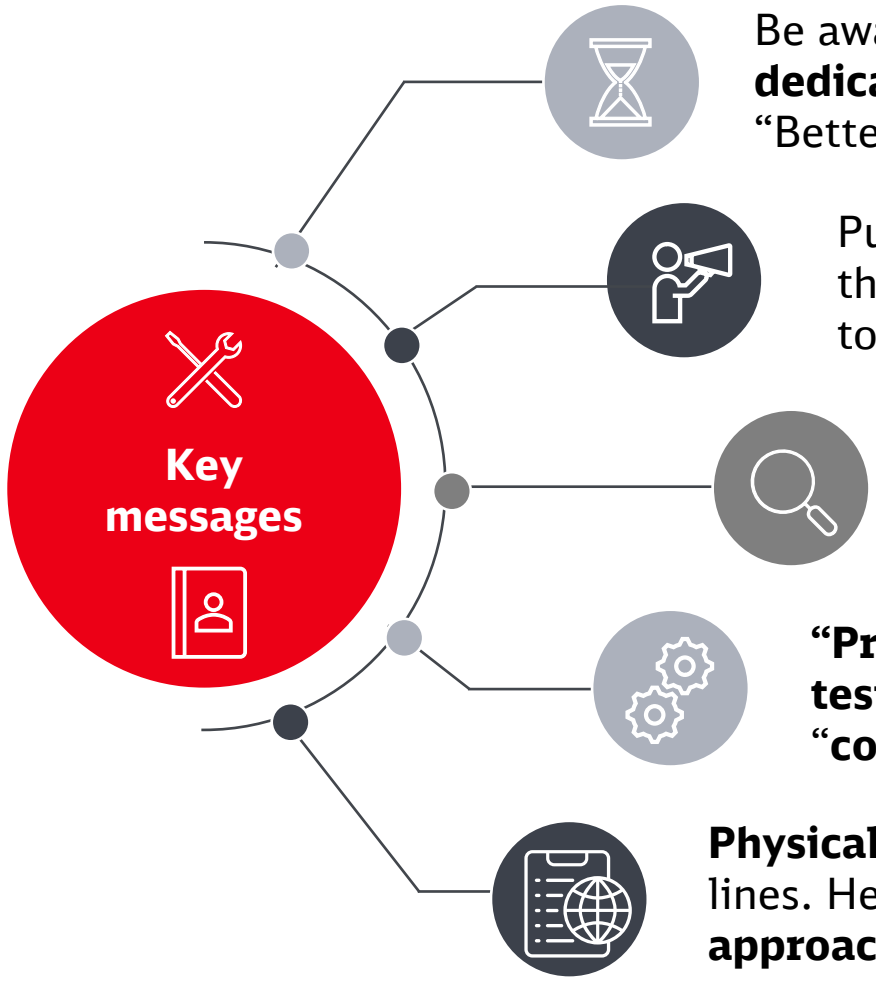
German-Finnish Business Forum 2025

5th November.2025 | Lübeck | Ulrich Zackor | OT-Security (I.ITS) | DB InfraGO AG

Management Summary: Challenges ahead for DB InfraGO as a railway infrastructure manager and KRITIS operator

- DB InfraGO as major business unit of DB Group is the largest, highest-capacity railway infrastructure manager and the largest station operator in Europe with revenues of €8.1bn and about 68.200 employees in 2024. As KRITIS operator DB InfraGO is subject to special requirements by the German Federal Agency for Information Security (BSI), i.e. it must take appropriate organisational and technical precautions for its information technology systems/components/ processes to ensure the security targets of availability, integrity, authenticity, and confidentiality.
- Today's geopolitical situation underpins public critical infrastructures being demonstrably in focus of government attackers, and especially railway companies became increasingly victims of cyberattacks in the recent years.
- As KRITIS operator DB InfraGO puts a special focus on the TEN-T core network as backbone of its critical transport service. An extensive E2E risk management and implementation of defined measures at DB InfraGO ensures compliance with KRITIS regulation. In the recent years DB InfraGO has implemented hundreds of technical, organisational and physical measures to improve security and resilience – nonetheless a lot is yet to be done. Security Operations Management ensures a 24/7 monitoring of railway-related IT/OT infrastructure at DB InfraGO. Besides cybersecurity, DB InfraGO strengthens and expands its Business Continuity Management and physical security actions
- Within the next couple of months two important laws regarding security and resilience of critical infrastructures will be passed by the German Bundestag to finally enforce EU-NIS 2 and CER directives.

Key take-aways based on the experience of DB InfraGO as KRITIS operator



Be aware that given today's threat landscape **resources dedicated to cybersecurity and resilience are well invested**. "Better safe (and secure) than sorry"

Put **cybersecurity and resilience and on your CEO agenda**, spread the message and carry out **awareness** activities. **Networking** helps to protect your networks and operations.

Identify your most important and most valuable processes, systems and assets. Conduct **risk-based prioritisation.**

"Practice makes perfect." Focus on practical/desktop **exercises to train, test and improve emergency and recovery procedures.** In many cases "**common sense**" may already help a lot. Don't be too academic.

Physical and cyberspace grow together in a digitised world with blurred lines. Hence security has to be implemented with an **integrated, holistic approach**.

Ulrich Zackor
Head of OT Security at DB InfraGO AG

Contact: ulrich.zackor@deutschebahn.com