[SP-SEC-DetRiskMatrix]

Europe's Rail System Pillar Cybersecurity Domain - Matrix of the Detailed Risk Assessment v1.1

Target Risk: low

Please read the Security Guideline which explains the usage of this tool. The guideline is available at https://ertms.be/activities/ertms-security-core-group

Threats				Risk Assessment - unmitigated Risk Assessment (with only prefulfilled measures) - G-6b					Risk Delta	System Requirements - G-6c		Compensation Measures - G-6e			Final Risk Assessment - G-6f							
Threat Catalogue	Relevance	Covered by / Reference to - G-6a	Reason for reference to other threat - G-6a	Exposure - G-6b	Vulnerability - G-6b	Likelihood - G-6b	Impact - G-6b	Actual Risk - G-6b	Risk Delta - G-6b	Measure (SR) from 62443-3-3	Explanations for SRs	Measures from 62443-3-3	Compensating measures and explanations	Measure IDs	Exposure - G-6f	Vulnerability - G-6f	Likelihood - G-6f	Impact - G-6f	Actual Risk - G-6f	Final Risk Delta G-6f	Risk acceptance Explanation G-6e	Explanation (e.g. for Exposure, Vulnerability, Impact)
G-0.13 Interception of Compromising Interference Signals	Yes			3	2	4	A	high	3			ORG 3.1; NET 1.6; NET 1.8; NET 2.1; COMP 1.1	SP-SEC-Comp.5.1-2 Use of standard security libraries and hardware (reduces risk of side-channel attacks) CR.11 + CR 11 RE 1: Physical tamper resistance and notification		1	1	1	A	Medium	1		
G-0.14 Interception of Information / Espionage	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 2.1; SR 2.1 RE 1; SR 3.9; SR 4.1; SR 4.1 RE 1; SR 4.1 RE 2; SR 4.3		ORG 1.2; ORG 2.2; ORG 3.1; NET 1.6; NET 1.7; NET 1.8; NET 2.2; NET 2.3; NET 3.2; COMP 1.1; DATA 1.7; USER 1.1; USER 1.11; USER 1.14; USER 1.15; USER 1.16; USER 1.17; USER 1.18; USER 2.1; USER 2.2			1	1	1	A	Medium	1		
G-0.15 Eavesdropping	Yes			3	3	5	A	very high	4	SR 3.9; SR 4.1; SR 4.1 RE 1; SR 4.1 RE 2; SR 4.3		ORG 1.2; ORG 2.2; ORG 3.1; NET 1.6; NET 1.7; NET 1.8; NET 2.1; NET 2.2; NET 2.3; NET 3.2; COMP 1.1; DATA 1.7			1	1	1	A	Medium	1		
G-0.16 Theft of Devices, Storage Media and Documents	Yes			3	3	5	A	very high	4	SR 1.5 RE 1; SR 1.9 RE 1; SR 4.2; SR 4.2 RE 1; SR 7.3		ORG 1.2; ORG 1.3; ORG 1.4; ORG 1.5; ORG 3.1; NET 1.4; NET 1.7; NET 1.8; DATA 1.1; DATA 1.2; DATA 1.6; AVAIL 1.1; AVAIL 2.3	CR.11 + CR 11 RE 1: Physical tamper resistance and notification		3	1	3	2	Medium	1		
G-0.17 Loss of Devices, Storage Media and Documents	Yes			3	3	5	A	very high	4	SR 1.5 RE 1; SR 1.9 RE 1; SR 4.2; SR 4.2 RE 1; SR 4.2; SR 7.8		ORG 1.3; ORG 1.4; ORG 1.5; ORG 3.1; NET 1.4; NET 1.7; NET 1.8; DATA 1.1; DATA 1.2; DATA 1.6; AVAIL 2.1; AVAIL 2.3	CR.11 + CR 11 RE 1: Physical tamper resistance and notification		3	1	3	2	Medium	1		
G-0.19 Disclosure of Sensitive Information	Yes			3	3	5	A	very high	4	SR 1.10; SR 4.1; SR 4.1 RE 1; SR 4.1 RE 2		ORG 1.3; ORG 1.4; ORG 1.5; ORG 2.2; NET 1.6; NET 1.7; NET 1.8; NET 2.1; NET 2.2; NET 2.3; NET 3.1; NET 3.2; NET 3.3; COMP 2.2; COMP 2.1; COMP 2.2; COMP 3.2; COMP 3.4; DATA 1.1; DATA 1.2; DATA 1.6; DATA 1.7; USER 1.6; USER 1.5; USER 1.6; USER 1.7; USER 1.8; USER 1.10; USER 1.11; USER 1.12; USER 1.14; USER 1.18; USER 2.1; USER 2.2; USER 2.4; EVENT 1.1; EVENT 1.3; EVENT 1.9; EVENT 3.4		3	1	1	1	A	Medium	1		
G-0.20 Information or Products from an Unreliable Source	Yes			3	3	5	A	very high	4	SR 3.4; SR 3.4 RE 1		ORG 1.1; ORG 1.4; ORG 1.5; ORG 1.6; ORG 3.1	CR 3.10 RE 1: Update authenticity and integrity		3	1	1	A	Medium	1		
G-0.21 Manipulation of Hardware or Software	Yes			3	3	5	A	very high	4	SR 3.4; SR 3.4 RE 1		ORG 2.2; ORG 3.1; CM 1.1; CM 1.3	CR 3.14: Integrity of the boot process		3	1	1	A	Medium	1		
G-0.22 Manipulation of Information	Yes			3	3	5	A	very high	4	SR 3.1; SR 3.1 RE 1		ORG 2.2; ORG 3.1; CM 1.3	CR 3.14: Integrity of the boot process		3	1	1	A	Medium	1		
G-0.23 Unauthorised Access to IT Systems	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.2; SR 1.2 RE 1; SR 1.2; SR 1.4; SR 1.5; SR 1.5 RE 1; SR 1.7; SR 1.7 RE 1; SR 1.8; SR 1.9; SR 1.10; SR 1.11; SR 1.13; SR 1.13 RE 1; SR 2.1; SR 2.1 RE 1; SR 2.1 RE 2; SR 3.9; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4		ORG 1.4; ORG 1.5; ORG 2.2; ORG 3.1			3	1	1	A	Medium	1		
G-0.24 Destruction of Devices or Storage Media	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.2; SR 1.2 RE 1; SR 1.5; SR 1.5 RE 1; SR 1.7; SR 1.7 RE 1; SR 1.8; SR 1.9; SR 1.9 RE 1; SR 7.1 RE 1; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4		ORG 1.4; ORG 1.5; ORG 3.1			3	1	3	2	Medium	1		
G-0.28 Software Vulnerabilities or Errors	Yes			3	3	5	A	very high	4	SR 3.7; SR 7.7		ORG 1.3; ORG 1.5; ORG 2.3	SP-SEC-Comp.5.1-1: M13 for IEC 62443-4-1 SP-SEC-Pgm 13.1-1: ML3 for IEC 62443-4-1		3	1	1	A	Medium	1		
G-0.30 Unauthorised Use or Administration of Devices and Systems	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.1 RE 2; SR 1.1 RE 3; SR 1.2; SR 1.2 RE 1; SR 1.3; SR 1.3 RE 1; SR 1.4; SR 1.5; SR 1.5 RE 1; SR 1.7; SR 1.7 RE 1; SR 1.8; SR 1.9; SR 1.9 RE 1; SR 1.10; SR 1.11; SR 2.1; SR 2.1 RE 1; SR 2.1 RE 2; SR 2.1 RE 4; SR 3.9; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4		ORG 2.2; ORG 3.1			1	1	1	A	Medium	1		
G-0.31 Incorrect Use or Administration of Devices and Systems	Yes			3	3	5	A	very high	4	SR 2.1; RE 3; SR 2.1 RE 4; SR 2.12; SR 2.12 RE 1		ORG 1.3; ORG 1.4; ORG 1.5; ORG 2.2			3	1	1	A	Medium	1		
G-0.32 Misuse of Authorisation	Yes			3	3	5	A	very high	4	SR 2.1; SR 2.12; SR 2.12 RE 1		ORG 1.3; ORG 1.4; ORG 1.5; ORG 2.2			3	1	1	A	Medium	1		
G-0.35 Coercion, Blackmail or Corruption	Yes			3	3	5	A	very high	4	SR 2.1; SR 2.1 RE 1; SR 2.12; SR 2.12 RE 1		ORG 1.2; ORG 1.4; ORG 1.5			3	1	1	A	Medium	1		
G-0.36 Identity Theft	Yes			3	3	5	A	very high	4	SR 2.1 RE 4; SR 2.12; SR 2.12 RE 1		ORG 1.5; ORG 3.1			3	1	1	A	Medium	1		
G-0.37 Repudiation of Actions	Yes			3	3	5	B	high	3	SR 2.12; SR 2.12 RE 1		ORG 1.3; ORG 1.4; ORG 1.5; ORG 2.2			3	1	1	B	Low	0		
G-0.38 Misuse of Personal Information	Yes			3	3	5	C	high	3	SR 2.12; SR 2.12 RE 1		ORG 1.3; ORG 1.4; ORG 1.5; ORG 3.1			3	3	2	C	Low	0		
G-0.39 Malware	Yes			3	3	5	A	very high	4	SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 3.3; SR 3.3 RE 1; SR 3.3 RE 2; SR 3.4; SR 3.4 RE 1		ORG 1.3; ORG 1.5; ORG 2.2	CR 3.14: Integrity of the boot process		3	1	1	A	Medium	1		
G-0.40 Denial of Service	Yes			3	3	5	A	very high	4	SR 3.6; SR 7.1; SR 7.1 RE 1; SR 7.1 RE 2; SR 7.2					3	1	2	C	Low	0		
G-0.42 Social Engineering	Yes			3	3	5	A	very high	4	SR 2.1 RE 4; SR 2.8 RE 1; SR 2.12; SR 2.12 RE 1		ORG 1.2; ORG 1.4; ORG 1.5; ORG 3.1			3	1	1	A	Medium	1		
G-0.43 Attack with Specially Crafted Messages	Yes			3	3	5	A	very high	4	SR 3.5; SR 3.7		ORG 2.2; ORG 3.1			3	1	1	A	Medium	1		
G-0.44 Unauthorised Entry to Premises	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.1 RE 2; SR 1.1 RE 3; SR 1.6; SR 1.6 RE 1		ORG 1.2; ORG 1.3; ORG 1.4; ORG 1.5; ORG 2.2; ORG 3.1			3	1	1	A	Medium	1		
G-0.45 Data Loss	Yes			3	3	5	A	very high	4	SR 7.1; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4; SR 7.5					3	1	1	A	Medium	1		
G-0.46 Loss of Integrity of Sensitive Information	Yes			3	3	5	A	very high	4	SR 1.5 RE 1; SR 1.9 RE 1; SR 3.4; SR 3.4 RE 1; SR 7.1; SR 7.5		CM 1.3			3	1	1	A	Medium	1		
G-0.47 Harmful Side Effects of IT-Supported Attacks	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.2; SR 1.2 RE 1; SR 3.9; SR 3.12; SR 7.7					3	1	1	A	Medium	1		
IND.1.2 Insufficient integration of OT into the security organisation	Yes			3	3	5	A	very high	4	SR 2.3 RE 1		ORG 1.1; ORG 1.2; ORG 2.1; ORG 2.4			3	1	1	A	Medium	1		
IND.1.3 Insufficient integration of OT into operational processes	Yes			3	3	5	A	very high	4			ORG 1.1; ORG 1.2; ORG 1.4; ORG 2.4			3	1	1	A	Medium	1		
IND.1.4 Insufficient access protection	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.1 RE 2; SR 1.1 RE 3; SR 1.2; SR 1.2 RE 1; SR 1.4; SR 1.5; SR 1.5 RE 1; SR 1.7; SR 1.7 RE 1; SR 1.8; SR 1.9; SR 1.9 RE 1; SR 1.10; SR 1.11; SR 1.12; SR 1.13 RE 1; SR 2.1; SR 2.1 RE 1; SR 2.1 RE 2; SR 2.1 RE 4; SR 7.1; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4; SR 7.5		ORG 2.2; ORG 3.1			3	1	1	A	Medium	1		
IND.1.5 Insecure project planning process/application development process	Yes			3	3	5	A	very high	4	SR 1.6; SR 1.6 RE 1; SR 2.3 RE 1; SR 6.2; SR 7.6		ORG 1.1; ORG 1.3; ORG 1.5; ORG 2.1; ORG 2.3	SP-SEC-Comp.5.1-1: M13 for IEC 62443-4-1 SP-SEC-Pgm 13.1-1: ML3 for IEC 62443-4-1		3	1	1	A	Medium	1		
IND.1.6 Insecure administration concept and remote administration	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.1 RE 2; SR 1.1 RE 3; SR 2.1; SR 2.1 RE 1; SR 5.1; SR 5.1 RE 1; SR 5.1 RE 2; SR 5.1; SR 5.1 RE 3; SR 7.4		ORG 1.1; ORG 1.3; ORG 1.5	SP-SEC-Comp.6.1-2 Secure Configuration SP-SEC-Comp.5.6.1-1 Secure Update		3	1	1	A	Medium	1		
IND.1.7 Insufficient monitoring and detection procedures	Yes			3	3	5	A	very high	4	SR 6.1; SR 6.1 RE 1; SR 6.2; SR 7.8		ORG 1.1; ORG 1.3; ORG 1.5; ORG 2.2; CM 1.1			3	1	1	A	Medium	1		
IND.1.8 Insufficient test concept	Yes			2	2	3	A	high	3	SR 3.2; SR 3.3 RE 1; SR 3.3 RE 2; SR 3.7		ORG 1.1; ORG 1.3; ORG 1.5; ORG 2.3	SP-SEC-Comp.5.1-1: M13 for IEC 62443-4-1 SP-SEC-Pgm 13.1-1: ML3 for IEC 62443-4-1		3	1	1	A	Medium	1		
IND.1.9 Insufficient life-cycle concepts	Yes			3	3	5	A	very high	4	SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 7.6 RE 1; SR 7.8		ORG 1.1; ORG 1.3; ORG 1.5; ORG 1.6; ORG 2.3; CM 1.1			3	1	1	A	Medium	1		
IND.1.10 Insufficient security requirements for procurement	Yes			3	3	5	A	very high	4	SR 7.6 RE 1; SR 7.8		ORG 1.1; ORG 1.6; ORG 2.1; ORG 2.3			3	1	1	A	Medium	1		
IND.1.11 Use of insecure protocols	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.2; SR 1.2 RE 1; SR 1.8; SR 1.9; SR 1.11; SR 2.1; SR 2.1 RE 1; SR 2.6; SR 2.6 RE 1; SR 2.5; SR 2.7; SR 3.1; SR 3.1 RE 1; SR 3.5; SR 3.6; SR 3.8 RE 1; SR 3.8 RE 2; SR 3.8 RE 3; SR 4.3		ORG 1.4			3	1	1	A	Medium	1		
IND.1.12 Insecure configurations of components	Yes			3	3	5	A	very high	4	SR 6.1; SR 6.1 RE 1; SR 6.2; SR 7.6; SR 7.6 RE 1		ORG 1.3; ORG 2.2; ORG 2.3; CM 1.1; CM 1.3	SP-SEC-Comp.5.3.6-1 Hardening / Least functionality		3	1	1	A	Medium	1		
IND.1.13 Dependencies of OT on IT networks	Yes			3	3	5	A	very high	4	SR 5.1; SR 5.1 RE 1; SR 5.1 RE 2; SR 5.1 RE 3; SR 5.2; SR 5.2 RE 1; SR 5.2 RE 2; SR 5.2 RE 3; SR 5.3; SR 5.3 RE 1; SR 5.4; SR 5.4 RE 1; SR 5.4		CM 1.2			3	1	1	A	Medium	1		
IND.2.1.2 Insufficient user and authorisation management	Yes			3	3	5	A	very high	4	SR 2.8 RE 1		ORG 1.1; ORG 1.3; ORG 2.3			3	1	1	A	Medium	1		
IND.2.1.3 Insufficient logging	Yes			3	3	5	A	very high	4	SR 2.8; SR 2.9; SR 2.9 RE 1; SR 2.10; SR 2.11; SR 2.11 RE 1; SR 2.11 RE 2; SR 6.1; SR 6.1 RE 1		ORG 2.3			3	1	1	A	Medium	1		
IND.2.1.9 Manipulated firmware	Yes			3	3	5	A	very high	4	SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 3.4; SR 3.4 RE 1		ORG 1.6; ORG 2.2; ORG 2.3; ORG 3.1; CM 1.3	CR 3.10 RE 1: Update authenticity and integrity		3	1	1	A	Medium	1		
IND.2.2.1 Incomplete documentation	Yes			3	3	5	A	very high	4	SR 6.1; SR 6.1 RE 1		ORG 1.1; ORG 1.3; ORG 1.4; ORG 2.3; CM 1.2; CM 1.3	SP-SEC-Pgrm-5-1 SP-SEC-Pgrm-13.4 SP-SEC-Comp.6.3-1		3	1	1	A	Medium	1		
IND.2.2.1 Incompletely documented remote maintenance access in the OT	Yes			3	3	5	A	very high	4			ORG 1.6; ORG 2.3; CM 1.3	SP-SEC-Pgrm-5-1 SP-SEC-Pgrm-13.4 SP-SEC-Comp.6.3-1		3	1	1	A	Medium	1		
IND.2.2.2 Insufficient availability due to dependencies on office and building IT	Yes			3	3	5	A	very high	4	SR 2.3 RE 1; SR 5.1; SR 5.1 RE 1; SR 5.1 RE 2; SR 5.1 RE 3; SR 5.2; SR 5.2 RE 1; SR 5.2 RE 2; SR 5.2 RE 3; SR 5.3; SR 5.3 RE 1		CM 1.2	SP-SEC-Sev-3-1		3	1	1	A	Medium	1		
IND.2.2.3 Insufficient regulations for the use of OT remote maintenance access	Yes			3	3	5	A	very high	4			ORG 1.1	SP-SEC-Pgrm-10		3	1	1	A	Medium	1		
IND.2.2.4 Insufficient human oversight over OT remote maintenance sessions	Yes			3	3	5	A	very high	4	SR 2.1 RE 4		ORG 1.3	SP-SEC-Pgrm-13.1-7		3	1	1	A	Medium	1		
IND.2.5 Direct IP-based access to systems from insecure zones	Yes			3	3	5	A	very high	4	SR 5.1; SR 5.1 RE 1; SR 5.1 RE 2; SR 5.1 RE 3; SR 5.2; SR 5.2 RE 1; SR 5.2 RE 2; SR 5.2 RE 3; SR 5.4		ORG 2.2; CM 1.2			3	1	1	A	Medium	1		
IND.2.6 Insecure alternative OT remote maintenance access to the cause of faults	Yes			3	3	5	A	very high	4	SR 2.6; SR 3.1; SR 3.1 RE 1; SR 3.4; SR 3.4 RE 1					3	1	1	A	Medium	1		
IND.2.7 Insecure design of OT remote maintenance accesses	Yes			3	3	5	A	very high	4	SR 2.6; SR 3.1; SR 3.1 RE 1; SR 3.4; SR 3.4 RE 1		ORG 1.4; ORG 1.5			3	1	1	A	Medium	1		
IND.2.8 Outdated technical concepts for OT remote maintenance access	Yes			3	3	5	A	very high	4	SR 2.6; SR 3.1; SR 3.1 RE 1; SR 3.4; SR 3.4 RE 1		ORG 1.1; ORG 1.4; ORG 1.5; ORG 2.4; CM 1.3			3	1	1	A	Medium	1		
CON.1.1 Insufficient key management for encryption	Yes			3	3	5	A	very high	4	SR 1.8; SR 1.9; SR 1.9 RE 1		ORG 1.5			3	1	1	A	Medium	1		
CON.1.8 Compromise of cryptographic keys	Yes			3	3	5	A	very high	4	SR 1.5; SR 1.5 RE 1; SR 1.8; SR 1.9; SR 4.3 RE 1		ORG 1.3; ORG 1.4; ORG 1.5; ORG 1.6; ORG 2.1	SP-SEC-Comp.5.5.2-2 SP-SEC-Comp.5.5.2-3		3	1	1	A	Medium	1		
CON.1.9 Expired certificates	Yes			3	3	5	A	very high	4	SR 1.8; SR 1.9; SR 1.9 RE 1		ORG 1.3; ORG 1.4; ORG 1.5			3	1	1	A	Medium	1		
CON.2.1 Missing data backup	Yes			3	3	5	A	very high	4	SR 7.1; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4; SR 7.4		ORG 1.3; ORG 1.4; ORG 1.5; CM 1.3	SP-SEC-Pgrm-12.3-1		3	1	1	A	Medium	1		
CON.2.2 Missing recovery tests	Yes			3	3	5	A	very high	4	SR 7.4		ORG 1.3; ORG 1.4; ORG 1.5; CM 1.3	SP-SEC-Pgrm-12.3-2		3	1	1	A	Medium	1		
OPS.1.1.5 Problems with the automated distribution of patches and changes	Yes			3	3	5	A	very high	4	SR 7.3; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4		ORG 1.5; ORG 2.2; ORG 2.3			3	1	1	A	Medium	1		
OPS.1.1.6 Insufficient recovery options for patch and change management	Yes			3	3	5	A	very high	4	SR 7.3; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4					3	1	1	A	Medium	1		
OPS.1.1.8 Manipulation of data and tools during patch and change management	Yes			3	3	5	A	very high	4	SR 1.1; SR 1.1 RE 1; SR 1.1 RE 2; SR 1.1 RE 3; SR 1.2; SR 1.2 RE 1; SR 1.3; SR 1.3 RE 1; SR 1.4; SR 1.5; SR 1.5 RE 1; SR 1.7; SR 1.7 RE 1; SR 1.8; SR 1.9; SR 1.9 RE 1; SR 3.1; SR 3.1 RE 1; SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 3.4; SR 3.4 RE 1		ORG 2.2; ORG 2.3; CM 1.3			3	1	1	A	Medium	1		