Support of UNECE R.155 with Elektrobit products

Ref ID	Cybersecurity mitigation	Elektrobit product offering
M1	Security controls are applied to back-end systems to minimise the risk of insider attack.	*Out of scope for embedded software*
M2	Security controls are applied to back-end systems to minimise unauthorised access.	*Out of scope for embedded software*
M3	Security controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage.	*Out of scope for embedded software*
M4	Security Controls are applied to minimise risks associated with cloud computing.	*Out of scope for embedded software*
M5	Security Controls are applied to back-end systems to prevent data breaches.	*Out of scope for embedded software*
M6	Systems shall implement security by design to minimize risks.	EB cadian, EB tresos, EB corbos, EB zoneo, EB zentur
M7	Access control techniques and designs shall be applied to protect system data/code.	Secure diagnostics: EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader Identity and access management: EB corbos AdaptiveCore Access control and authorization: EB corbos Linux Secure boot: EB tresos Bootloader, EB zentur
M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data.	Secure diagnostics: EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader Identity and access management: EB corbos AdaptiveCore Access control and authorization: EB corbos Linux Protection and access control of cryptographic material: EB corbos AdaptiveCore, EB zentur Secure storage: EB tresos AutoCore
M9	Measures to prevent and detect unauthorized access shall be employed.	Intrusion detection: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo SwitchCore Shield Secure diagnostics: EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader Identity and access management: EB corbos AdaptiveCore Access control and authorization: EB corbos Linux Separation and isolation: EB corbos Hypervisor, EB corbos Linux
M10	The vehicle shall verify the authenticity and integrity of messages it receives.	Secure communication: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo Secure diagnostics: EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader Cryptography: EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur
M11	Security controls shall be implemented for storing cryptographic keys.	Protection and access control of cryptographic material: EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur
M12	Confidential data transmitted to or from the vehicle shall be protected.	Secure communication: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo Cryptography: EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur
M13	Measures to detect and recover from a denial of service attack shall be employed.	Intrusion detection: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo SwitchCore Shield Firewall: EB zoneo Recovery: EB corbos AdaptiveCore
M14	Measures to protect systems against embedded viruses/malware should be considered.	Intrusion detection: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo SwitchCore Shield Secure communication: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo Separation and isolation: EB corbos Hypervisor, EB corbos Linux Secure boot: EB tresos Bootloader, EB zentur
M15	Measures to detect malicious internal messages or activity should be considered.	Intrusion detection: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo SwitchCore Shield Secure communication: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo Identity and access management: EB corbos AdaptiveCore

Support of UNECE R.155 with Elektrobit products

Ref ID	Cybersecurity mitigation	Elektrobit product offering
M16	Secure software update procedures shall be employed.	Secure software updates: EB cadian, EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader Secure diagnostics: EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader Cryptography: EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur
M17	NOT DEFINED	
M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege.	Separation and isolation: EB corbos Hypervisor, EB corbos Linux Access control and authorization: EB corbos Linux Secure diagnostics: EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader Identity and access management: EB corbos AdaptiveCore
M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions.	Elektrobit CSMS ensures that security procedures are defined and followed for the development of Elektrobit products and projects.
M20	Security controls shall be applied to systems that have remote access.	Cryptography: EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur Secure communication: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo Identity and access management: EB corbos AdaptiveCore Secure diagnostics: EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader
M21	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle.	Secure boot: EB zentur, EB tresos Bootloader Secure software updates: EB cadian, EB tresos Bootloader, EB tresos AutoCore Cryptography: EB corbos AdaptiveCore, EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur
M22	Security controls shall be applied to external interfaces.	Secure diagnostics: EB corbos AdaptiveCore, EB tresos AutoCore, EB tresos Bootloader Secure communication: EB corbos AdaptiveCore, EB tresos AutoCore, EB zoneo Separation and isolation: EB corbos Linux, EB corbos Hypervisor, EB tresos Embedded Hypervisor Cryptography: EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur
M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity testing with adequate coverage. Cybersecurity best practices for system design and system integration shall be followed.	Cryptography: EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur Separation and isolation: EB corbos Linux, EB corbos Hypervisor, EB tresos Embedded Hypervisor Elektrobit CSMS ensures that cybersecurity best practices for software development are effectively followed.
M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data.	Secure boot: EB tresos Bootloader, EB zentur Access control and authorization: EB corbos Linux Cryptography: EB corbos AdaptiveCore, EB tresos AutoCore, EB zentur

The listed Elektrobit products can support the system in implementing the mitigations for the threats targeted by the UN R.155, but need to be integrated into a system cybersecurity concept. Get in contact with Elektrobit's cybersecurity experts for details and support.