Supporting UNECE R155 With Embedded Software From Vector

Coverage of the Mitigations per Product

Ref	Mitigation according to UNECE R155 (Annex 5)	MICROSAR Classic	MICROSAR Adaptive	Flash Bootloader
M1–M5	(not relevant for embedded software)	N/A		
M6	Systems shall implement security by design to minimize risks	Crypto stack, SecOC, TLS, IPsec, Secure Diagnostics, IDS, Secure Software Update, veHsm	Crypto Stack, SecOC, TLS, Secure Diagnostics, Identity & Access Management, IDS, UCM (Secure Software Update)	Crypto Stack, Secure Diagnostics, Identity & Access Management, Secure Software Update
M7	Access control techniques and designs shall be applied to protect system data/code	Secure Diagnostics	Secure Diagnostics, Identity & Access Management	Secure Diagnostics
M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data	Secure Diagnostics	Secure Diagnostics, Identity & Access Management	Secure Diagnostics
M9	Measures to prevent and detect access shall be employed	IDS	Identity and Access Management, IDS	Secure Diagnostics
M10	The vehicle shall verify the authenticity and integrity of messages it receives	Crypto Stack, SecOC, TLS, IPsec	Crypto Stack, SecOC, TLS	Crypto Stack
M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)	Crypto Stack, veHsm	Crypto Stack (Hsm Crypto Providers)	Crypto Stack
M12	Confidential data transmitted to or from the vehicle shall be protected	Crypto Stack, TLS	Crypto Stack, TLS	Crypto Stack
M13	Measures to detect and recover from a denial of service attack shall be employed	IDS	IDS	*
M14	Measures to protect systems against embedded viruses/malware should be considered	IDS, veHsm (Secure Boot)	IDS	veHsm (Secure Boot)
M15	Measures to detect malicious internal messages or activity should be considered	SecOC, TLS, IDS, IPsec	SecOC, TLS, Identity & Access Management, IDS	*
M16	Secure software update procedures shall be employed	Crypto Stack, Secure SW Update	Crypto Stack, UCM (Secure Software Update)	Crypto Stack, Secure Software Update

Ref	Mitigation according to UNECE R155 (Annex 5)	MICROSAR Classic	MICROSAR Adaptive	Flash Bootloader
M17	(M17 is not defined in the standard)	N/A		
M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege	Secure Diagnostics	Secure Diagnostics, Identity & Access Management	Secure Diagnostics
M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions	Secure Diagnostics, IDS	Secure Diagnostics, Identity & Access Management, IDS	Secure Diagnostics
M20	Security controls shall be applied to systems that have remote access	Crypto Stack	Crypto Stack, Identity & Access Management	Crypto Stack
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	veHsm (Secure Boot)	Depends on the used operating system	veHsm (Secure Boot)
M22	Security controls shall be applied to external interfaces	Crypto Stack, SecOC, TLS, IPsec, Secure Diagnostics	Crypto Stack, SecOC, TLS, Secure Diagnostics	Crypto Stack, Secure Diagnostics
M23	Cybersecurity best practices for software and hardware development shall be followed	covered by the processes in Vector's CSMS		
M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data	Crypto Stack, Secure NvM	Crypto Stack, Identity & Access Management	Crypto Stack

*: This mitigation is not relevant for Flash Bootloader use cases.