AEM
Association of Equipment Manufacturers

Cybersecurity for Machine Data for Non-Road Equipment

This document serves to provide a common language for the Association of Equipment Manufacturers (AEM) and its members to discuss cybersecurity in non-road equipment, educating and informing both internal and external stakeholders. **It is not intended to be all-inclusive or all-encompassing in nature, but instead should serve as a glimpse into the levels of cybersecurity for machine data in the non-road industry.**

Non-road equipment is designed to execute specific functions relative to its intended applications and tasks in non-road environments in agriculture and construction. Construction worksites, farm fields, dairies and feedlots, areas of animal husbandry, etc., are dynamic environments defined by fences or other boundaries with some level of restriction for access or entry. **These do not apply to on-road operation of non-road equipment.**

It is important to note that this does not apply to connections made outside of an OEM-supported interface.

About AEM

The Association of Equipment Manufacturers (AEM) is the North American-based international trade group representing non-road equipment manufacturers and suppliers, with more than 1,000 member companies and over 200 product types across five diverse industry sectors, including agriculture, construction, forestry, mining, and utility.

Cybersecurity for Machine Data for Non-Road Equipment

AEM
Association of Equipment Manufacturers

	ON-MACHINE	DATA TRANSFER LEVEL	OFF-MACHINE
Example Systems, Data, or Assets	Includes on-board machine data and verification of functional safety systems, including data from sensors, displays, third-party systems, and other connected systems.	Includes the handoff or transfer of machine data from on-board machine to off-board server or cloud based system.	Includes off-board machine data, including performance data and third-party data management systems.
Access Among Stakeholders	Equipment operator and owner have primary access to machine data, while OEM has primary access to functional safety systems; dealer and other stakeholders may have permissions-based access.	Any access provided is through a permissions-based authentication process that may involve one or more gateways or access points.	Equipment owner, project owner, team owner, and other stakeholders have primary access. OEM or system manufacturers, platform providers, etc., may have permission-based access.
Primary Responsibility for Securing Access Both Physical and Digital	OEM is responsible for securing access to the machine and connected systems (system of systems).	All parties are responsible for the security of the handoff or transfer of data, including connectivity and interoperability.	System manufacturer is responsible for determining accessibility and securing access to connected data.
Primary Responsibility for Detection of Threats to System	Each system manufacturer is responsible for detection of system threats and coordination of detection among other stakeholders. The non-road industry continues to discuss opportunities to better define detection with input from external stakeholders.		
Primary Responsibility for Protection of Individual Systems	OEM is responsible for making system fixes available, and it is the end users' responsibility to accept and utilize the available fix. OEM shall make these fixes available in conjunction with the system manufacturer.	Cybersecurity interface agreement is established between various OEMs and platforms. Through the agreement, responsibilities to the parties are established.	Platform provider is responsible for making system fixes available, and it is the end users' responsibility to accept and utilize the available fix. Platform provider shall make these fixes available in conjunction with the system manufacturer.
Primary Responsibility for Recovery Following an Incident	OEM maintains primary responsibility for recovery, with support from various other stakeholders, including the system manufacturer, system owner, etc.	All parties are responsible to maintain the integrity of the communication channel as part of the cybersecurity interface agreement.	Platform provider maintains primary responsibility from an inventory for recovery, with support from various parties such as the system manufacturer, system user, etc.
Existing Standards, Guidelines, and Best Practices	• ISO 24882 • ISO/SAE 21434 • ISO 15143 • MITRE Embed • Threat Model (Detection) and Automotive Threat Matrix • Other threat assessments and modeling exercises (for existing systems and safety)	• ISO 27001 Information Security Management System (ISMS) • Cybersecurity interface agreement example	• ISO 27001 Information Security Management System (ISMS) • FedRAMP • MITRE Attack Framework • Other threat assessments and modeling exercises (for existing systems and safety)
Example Scenarios or Situations	• Access to machine data • Access to machine operation or remote sensors (stationary or on machine) • Implement-to-machine communication • Attachment-to-machine communication • Machine-to-machine communication	• Telematics systems • Over-the-air updates • Live streams (in-bound/out-bound)	• Cloud-to-cloud communication • Site Management System (SMS) or Farm Management Information System (FMIS)
Corresponding Data Layer for Cybersecurity	**Layers 0, 1, & 2**	**Layers 1 & 2**	**Layers 2, 3, 4, & 5**