*CID #55*

*[Comment]*

*I am surprised that there is no consideration of security in this document. Adversaries can be expected to attack factories that use wireless standards in the future, if only as part of attempts at extortion or stock market manipulation.*

*[Proposed Change]*

*At a minimum note the need for a security analysis and the need to use existing security standards, including 802.1AE and 802.11 wireless security. In updating the document also have in mind that that security guarantees of data integrity and data origin authenticity (received packets have been received as sent, and were sent by the authenticated system identified by the source MAC address) require the delivery of the original frame as sent, even if additional unsecured control information is added to or removed from the frame in transit.*

*[Discussion notes]*

*K.M. will produce a text on security requirements in FF.*

*M. S. need to cover data integrity and data security.*

*Short paragraph the security have to have authenticity of the packets.*

*1AE covers encryption as well.*

*Packets how they are sent and sent by authenticated device without being interfered by subsequently.*

*[Proposed text] Insert the following paragraph after line 53, page 4.*

*Security consideration is important for factory networks to protect confidentiality, integrity and availability of data. Security guarantees of data integrity and data origin authenticity (received packets have been received as sent, and were sent by the authenticated system identified by the source MAC address) require the delivery of the original frame as sent, even if additional unsecured control information is added to, or removed from the frame during transition. To satisfy the requirement, security standards are provided, which include IEEE Std 802.1X for Port-Based Network Access Control, IEEE Std 802.1AE for Media Access Control (MAC) Security, IEEE Std 802.11i for wireless security, IEC 62443 [N1] for industrial network and system security, and many others. Security guidelines may also enhance security level for operation and maintenance of the networks. Some of them cover networks for IoT Safety/Security Development [N2] and Flexile Factory [N3].*

*[N1] IEC 62443 Series, Industrial communication networks - Network and system security*

*[N2] Guidance for Practice Regarding "IoT Safety/Security Development Guidelines,"*

*Information-technology Promotion Agency (IPA), https://www.ipa.go.jp/files/000063228.pdf*

*[N3] Flexible Factory Security Guidelines, Flexible Factory Partner Alliance,   
https://www.ffp-a.org/document/files/190920\_FFSG\_p.pdf*