Title: Liaison response to "Request for an Official IEEE 802 Position on Security for Layer-2 Peer-to-Peer Protocols in the IEC/IEEE 60802 Configuration Domain"

From: IEEE 802.1 Working Group[1]

For: Information

Contacts: Glenn Parsons, Chair, IEEE 802.1, glenn.parsons@ericsson.com
Jessy Rouyer, Vice-Chair, IEEE 802.1, jessy.rouyer@nokia.com
Mick Seaman, Chair, IEEE 802.1 Security Task Group, mickseaman@gmail.com
János Farkas, Chair, IEEE 802.1 TSN Task Group, janos.farkas@ericsson.com
Dieter Pröll, Chair IEC/IEEE 60802 Joint Project, dieter.proell@siemens.com
David McCall, Vice-Chair, IEEE 802.1 TSN Task Group, david.mccall@intel.com
James P. K. Gilb, Chair, IEEE 802, gilb_ieee@tuta.com
Karen Randall, Liaison Secretary, IEEE 802.1, karen@randall-consulting.com
Jodi Haasz, Senior Manager, IEEE SA Operational Program Management, j.haasz@ieee.org
Alpesh Shah, Secretary, IEEE SA Standards Board and Board of Governors, sasecretary@ieee.org

To: PROFIBUS and PROFINET International (PI)
Xaver Schmidt, Chairman of the Board, PI, xaver.schmidt@siemens.com
Dietmar Bohn, Managing Director, PI, dietmar.bohn@profibus.com
Günter Steindl, Head of Committee B PROFINET, PI, guenter.steindl@siemens.com

Date: Jul 16, 2026

Dear Colleagues,

The IEEE 802.1 Working Group would like to thank PROFIBUS and PROFINET International for reaching out in liaison statement https://www.ieee802.org/1/files/public/docs2026/liaison-PI-Layer2Securityin60802-0726.pdf about security for Layer 2 peer-to-peer protocols such as LLDP, gPTP, FRER and RSTP/MSTP.

The IEEE 802.1 common security approach is to secure all the Layer 2 peer-to-peer control protocols in a protocol agnostic manner using IEEE Std 802.1AE MAC Security (MACsec) to provide a zero trust architecture. We envision that any future Layer 2 peer-to-peer control protocol would be also secured this way.

Each of the protocols has a concept of controls that apply to the boundary if the protocol is not secured using MACsec, the setting of the control would enforce the boundary. If MACsec protects communication from an authenticated authorized device, the boundary configuration can be extended beyond the boundary either by specific management variables on the device for that purpose, or via IEEE Std 802.1X RADIUS-based communication to that device.

In general, there is no limitation on MACsec security in an IEC/IEEE 60802 configuration domain for fully operating systems. For security reasons modern cipher suite implementations require defense against what is known as side-channel attacks. This means that the implementations operate with fixed bounded delays; therefore, are compatible with time-sensitive protocols and systems. A certain amount of communication not protected by MACsec may be needed for initial power up and getting MACsec keys. Note that authentication protocols and MACsec key agreement itself are not dependent on MACsec and are secure on their own.

[1] This document solely represents the views of the IEEE 802.1 Working Group, and does not necessarily represent a position of IEEE, or the IEEE Standards Association, or IEEE 802.

Note that the IEEE 802 work is open and contribution driven. Participation is on an individual basis and technical discussion can be conducted based on individual contributions. The IEEE 802.1 Security and TSN Task Groups meet at Plenary and Interim sessions and hold electronic meetings in-between sessions as listed in the WG calendar: https://1.ieee802.org/wg-calendar.

Respectfully submitted,
Glenn Parsons
Chair, IEEE 802.1 Working Group