

From:

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

To:

Glenn Parsons, Chair, IEEE 802.1 Working Group

glenn.parsons@ericsson.com

Cc: Jessy Rouyer, Vice Chair, IEEE 802.1 Working Group

jessy.rouyer@nokia.com

Cc: Karen Randall, Liaison Secretary, IEEE 802.1

karen@randall-consulting.com

Cc: Jodi Haasz, IEEE SA Operational Program Management / IEEE SA Program Manager

j.haasz@ieee.org

Cc: Janos Farkas, Chair, IEEE 802.1 TSN Task Group

janos.farkas@ericsson.com

Cc: Dieter Proell, IEC/IEEE 60802 Joint Project Chair

dieter.proell@siemens.com

Liaison Letter

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

Dear Colleagues,

on behalf of the *PROFIBUS and PROFINET International (PI)*, we would like to raise an important topic regarding security in the context of IEC/IEEE 60802 and, more broadly, in Layer-2 domains used for industrial automation.

As the work around IEC/IEEE 60802 continues to mature, a key open question remains how IEEE 802 intends to address the security of essential peer-to-peer and control-plane protocols that are required for operation within the configuration domain. In particular, we are referring to protocols such as **LLDP**, **gPTP**, **FRER** and **RSTP/MSTP**.

From the PI perspective, this topic is highly relevant for practical deployment scenarios. These protocols are fundamental to engineering, commissioning, synchronization, topology discovery, and network operation. At the same time, they may introduce a

potential attack surface if their use within the configuration domain, or more generally within a Layer-2 domain, is not accompanied by a clear and consistent security concept.

We would therefore kindly, but explicitly, ask IEEE 802 to provide an **official statement** on how this topic is intended to be handled. In particular, we would appreciate clarification on the following points:

1. How does IEEE 802 envision the protection of Layer-2 peer-to-peer and control-plane protocols such as LLDP, gPTP, FRER, and RSTP/MSTP within the IEC/IEEE 60802 configuration domain?
2. Is there an intended common security approach for these protocols within a Layer-2 domain, and if so, what is the expected architectural model?
3. What role do IEEE 802.1AE and IEEE 802.1X play in this context, especially with regard to the protection of the configuration domain and its boundaries?
4. Are there limitations, assumptions, or exclusions that should be understood by users of IEC/IEEE 60802-based systems when applying these protocols in security-relevant industrial environments?

An official IEEE 802 position on this matter would be highly valuable for alignment between our organizations and would help provide implementers, device vendors, and end users with clear guidance for secure and interoperable system design.

We very much appreciate the constructive cooperation between PI and IEEE 802 and are confident that a clarified and coordinated position on this topic will be beneficial for the broader industrial ecosystem.

We would be grateful for your written response at your earliest convenience.

Sincerely,

Xaver Schmidt

Xaver Schmidt, Chairman of the Board, PI

Dietmar Bohn

Managing Director, PI

Günter Steindl

Head of Committee B PROFINET, PI