Preferential Subject N° PS2

Real Evidence for Security Conformance

M. SEEWALD **CISCO** **Germany** **maseewal@cisco.com**	**D. HOLSTEIN** **OPUS Consulting Group** **United States** **holsteindk@ocg2u.com**	**T.W. CEASE** **Consultant** **United States** **twcease@ieee.org**

In the past several years there have been several attempts to develop a security conformance program that provides real evidence that Solution Providers have built security protection into their product and services that conforms to a specified standard. The most notable attempt was developed by Wurldtech Technologies of Vancouver, Canada. In 2012, working with The International Instrumentation User's Association (WIB) in the Netherlands, Wurldtech developed Report M2784 X10 "Process Control Domain - Security Requirements for Vendors." Based on these requirements Wurldtech developed a conformance program that required "real evidence" to achieve a requested level of security certification for their product and services. A vendor could apply for one of three levels of certification: BRONZE for conformance to the basic requirements, SILVER for conformance to an intermediate set of security enhancement requirements, and GOLD for conformance to a full set of applicable security enhancement requirements. In effect the graduated levels of conformance were designed to indicate an improve level of security protection and degree of maturity required to perform the tasks; albeit a subjective scale.

This paper describes the conformance program, how it was implemented, and the challenges experienced when performing a conformance audit of the real evidence offered by Solution Providers. The program was performed in three stages described in more detail: 1) Scoping the applicable requirements for a defined product (system, subsystem, component) and supporting services, 2) establishing a baseline of the real evidence needed to satisfy and audit of conformance, and 3) assessing the evidence to establish an appropriate level confidence for the certificate of satisfaction. Performing all three stages of the program proved difficult for the Solution Providers. These difficulties are described in the paper as well as the accommodation provided by the auditor to reach a compromised solution for certification.

The use case examples in this paper included large, medium and small industrial automation Solution Providers, and a EPU Solution Provider for Smart Meter deployment. The EPU Solution Provider is the most interesting because the success of the conformance audit was closely linked to the rate adjustment sought by the EPU. Other U.S. Public Utility Commissions (PUCs), or equivalent rate oversight agencies, closely followed the progress of this program to determine its effectiveness.

Based on these experiences, the requirements specification developed by the WIB was turned over to IEC TC 65 WG10 to be a standard. The approved standard is IEC 62443-2-4 "Industrial Communication Networks – Network and System Security – Part 2-4: Security Program Requirements for IACS Service Providers." This paper concludes with a subjective assessment of the quality the program specified by IEC 62443-2-4 compared to the original objective of the WIB/Wurldtech program.