Trends, Issues, and New Standards for ICS Security

David Mattes[1]*

[1]Asguard Networks, Inc., 6312 30th Ave NW, Seattle, Washington, 98107, USA
(*correspondence: mattes@asguardnetworks.com, Tel: 425-213-4691)

FORMAT

6-12 page paper plus 30-minute presentation

KEYWORDS

Security, GSM, cellular, connectivity, networking, segmentation, VLAN, isolation, M2M, SCADA

ABSTRACT

This talk will be divided into three broad sections. First we will present an overview of Industrial Control Systems (ICS) security issues and trends and how these affect Water / Wastewater environments. This introductory session will provide examples of ICS networks and illustrate design vulnerabilities.

Second we will discuss standards from ISA (ISA 100.15), TCG (Metadata for ICS Security), and IETF (HIP and PKI) that focus on a specific issue related to ICS security: how to efficiently and scalably enable private, secure communications for ICS devices over untrusted shared networks. We will discuss how these standards relate to one another and their importance in providing a basis for interoperable product solutions.

In the third section we will present our efforts to implement these standards in a simple, easy to use product. We will outline the key requirements we believe such a product should have in order to integrate into real-world environments. We will present scaling, stress-testing, and operational data for our implementation. Finally, we will present a case study outlining the realized benefit from solutions based on these standards and technology.

About the Author:

David Mattes founded Asguard Networks to create products that address the challenge of managing connectivity and information security for Industrial Control Systems (ICS). Prior to Asguard Networks, David spent 13 years in Boeing's R&D organization. At Boeing, David focused on ICS security issues, particularly on the challenge of segmenting connectivity for ICS devices into private networks and securely connecting them to and through Boeing's Enterprise networks. David was the co-creator and technical and implementation lead on an architecture that not only satisfied Boeing's InfoSec governance and security requirements, but also met the needs of the end users.