# Vulnerabilities in SCADA Systems

What Are We Protecting Against?

Mark Benedict [1]*

[1]Ultra Electronics, 3eTI, 9713 Key West Avenue, Suite 500, Rockville, Maryland USA 20850
(*E-mail: Mark.Benedict@ultra-3eti.com and Phone: 301-529-6447)

## FORMAT

6-12 page paper plus 30-minute presentation

## KEYWORDS

Cybersecurity, Network Intrusion, Stuxnet, Risk Assessment, SCADA, Industrial Control System

## ABSTRACT

Cybersecurity relating to critical infrastructure is a growing concern to governments and large enterprises. The risks are increasing due to a rise in published vulnerabilities, wider connectivity, and adoption of open standards that can expose networks and critical edge devices to serious exploits. Yet the approaches taken to mitigate these risks often are ignored, or inadequate and inconsistent.

Over the last two decades, control system manufacturers, utilities and the federal government have been aware of security issues posed by legacy SCADA systems that monitor and control much of the U.S. infrastructure. As control systems have become increasingly interconnected with other control networks and with corporate data networks, the potential for intrusions has grown. Due to the wide range of industrial control implementations, architectures, and impacts, the industrial cybersecurity market is rightly advocating a risk-based management approach. However, technology and attackers often outpace the assumptions made in the risk assessment, leading to a "protect against the last attack" approach. Then, if the attack is so new, or is paradigm shifting (Stuxnet), it takes the industry a long time to even begin to address it. For example, Stuxnet overcame an “air-gapped” network, yet the majority of protection advice calls for better perimeter security. How does this security approach address network perimeter breaches or "insider-attacks?" Can these even be protected against, or identified? Good perimeter security and computer end-point protection are sound security recommendations, but are they enough and do they really protect against the threats going forward?

Cybersecurity often is presented as complicated. In reality, the concepts of cybersecurity are straightforward. It is the implementation that is difficult, and security should complement safety rather than oppose it. When the cyber risk cannot be adequately explained, any mitigation solution cannot be validated for effectiveness. Security is an inherent foundation for any industrial automation facility and must be integrated throughout the system lifecycle.

This paper will outline some of the emerging trends and vulnerabilities in the attack space, and what is means for the current approach to industrial cybersecurity. It will present fundamental questions every SCADA and other industrial control owner should ask of their security solution – including what is actually

being protected. An industrial control or automation system is not the same as an enterprise IT system because the impacts are different. Security solutions must fit within the operational constraints of the system and within the risk appetite of the client organization. Otherwise the fix can cause a greater impact overall than an attack.

## ABOUT THE AUTHOR

**Mark Benedict** *has nearly 20 years of experience in cutting edge network, data systems, information security, military research, technology acquisition, and operations, and is an expert in the field of Information Assurance, high availability data centers, and network security. Prior to joining 3eTI in January of 2014, Mr. Benedict has held numerous prestigious positions including consulting for top-tier technology companies and serving in active military theatres around the globe as well as helped design and implement technology solutions for US Department of Defense and the North Atlantic Treaty Organization (NATO). He has directed Department of Defense engineering and technology organizations and held a Department of Defense Top Secret /TK/SI/SCI security clearance, in addition to directing international airborne and ground based military command and control information systems. Most recently, Mr. Benedict was promoted to Colonel in 2010 and assigned to the Information Assurance Directorate, National Security Agency (NSA) at Fort George G. Meade, Maryland, where he was responsible for developing and supporting secure national security communications for space based reconnaissance and communication satellite platforms. Mr. Benedict has retired from active military service to lead 3eTI's Business Development efforts, including directing 3eTI's strategic Sales and Marketing activities.*