CHAIRMAN Resource

From: Joe Weiss <joe.weiss@realtimeacs.com>
Sent: Tuesday, August 21, 2018 2:28 PM
To: CHAIRMAN Resource
Subject: [External_Sender] Status of your abstract submitted for the NPIC&HMIT 2019 meeting
Attachments: The Hole in Nuclear Plant Cyber Security – Process Sensors - ANS abstract 7-30-18.pdf

Attention: Patrick Castleman

NRC just issued the nuclear plant cyber security Reg Guide 5.71, proposed Revision 1. Yesterday, my abstract on the hole in nuclear plant cyber security was accepted for the American Nuclear Society (ANS) I&C Conference (abstract attached). Sensors, including analog sensors, are outside scope of the 2010 version and Revision 1 of the Reg Guide. Analog sensors are also susceptible to cyber attacks though NRC is only addressing "Digital Instrumentation and Control". I have mentioned before that NSIR is not adequately coordinating with the NRC's Electrical Engineering and I&C Branches which may explain why this safety problem is "falling through the cracks". What do you suggest should be done to address this gap in nuclear plant safety?
Respectfully,
Joe

Joe Weiss PE, CISM, CRISC, ISA Fellow, IEEE Senior Member, Managing Director ISA99
Applied Control Solutions, LLC
(408) 253-7934
(408) 253-7974 Fax
(408) 832-5396 Cell
joe.weiss@realtimeacs.com
www.realtimeacs.com
blog site: www.controlglobal.com/unfettered
Book URL: http://www.momentumpress.net/books/protecting-industrial-control-systems-electronic-threats

----- Forwarded Message -----
From: ANS EPSR <epsr@ans.org>
To: joe.weiss@realtimeacs.com
Sent: Monday, August 20, 2018 12:50 PM
Subject: Status of your abstract submitted for the NPIC&HMIT 2019 meeting

26973

The Hole in Nuclear Plant Cyber Security - Insecure Process Sensors

Dear Author:

Congratulations, your abstract has been accepted for presentation in the 11th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC & HMIT 2019), February 9-14, 2019, Orlando, FL. When completing your full paper for submission, the Review Committee recommends that you consider the following suggestions and comments:

==========

Please submit a full paper for a technical review. Please ensure that the paper includes a discussion of analog sensors, and what is meant by "hacking" an analog sensor and how you propose to address this. It is not clear from the abstract whether what is described can be defined as part of plant cyber-security.

==========

SESSION ASSIGNMENT: A Preview Program online will identify the day, time, and paper order of your session. Make sure there are no overlaps with any other obligations you may have. If you notice you are scheduled for multiple sessions at the same time, contact the proceedings office right away. Bring your presentation to the meeting with you on a USB drive.

PROCEEDINGS: ANS will be publishing the full papers for this meeting in flash drive format. Guidelines and template for full paper preparation can be found at http://www.ans.org/meetings/c_1 under the NPIC & HMIT 2018 meeting. The full paper deadline is September 14, 2018. You can start working on your full papers but the system for submitting your full paper will not be available until August 31, 2018. Full papers must be submitted electronically to http://epsr.ans.org/meeting/?m=294.

The Copyright form for your paper is provided at http://www.ans.org/meetings/c_2. Please complete this form as soon as possible and email it to:

NPIC & HMIT 2019
Ellen Leitschuh
American Nuclear Society
555 N. Kensington Ave.
La Grange Park, IL 60526
eleitschuh@ans.org

MEETING REGISTRATION: I encourage you and any coauthors to attend the NPIC & HMIT 2019 meeting. All speakers are expected to register for the meeting. Additionally, all speakers and session chairs should register at the registration desk and check-in at the speakers' desk to indicate their presence and provide information to allow for communication during the Conference. I look forward to receiving your full paper and thank you for making this conference a success.

Sincerely,

Pradeep Ramuhalli
Michael Doster (I&C)
James Turso (I&C)
Ron Boring (HFE)
Carol Smidts (HFE)
Technical Program Cochairs

The Hole in Nuclear Plant Cyber Security – Insecure Process Sensors

Joe Weiss, PE, CISM, CRISC
Managing Partner, Applied Control Solutions

Nuclear plant control system cyber security is to prevent impacts on nuclear safety, reliability, and/or regulatory compliance. Cyber events are defined as electronic communications between devices that affect confidentiality, integrity, or availability. There is no mention of the cyber event having to be malicious nor is it easy to identify a cyber event as being malicious. Monitoring of control system Operational Technology (OT) networks is necessary, but NOT sufficient, to maintain safety and protect control systems and processes. Control system network monitoring is addressed in Regulatory Guide 5.71 and NEI-0809. Control system network monitoring assumes the anomaly/vulnerability correlates to actual system impacts because the control system network does not have the capability to directly monitor the process. Currently, the major I&C suppliers do not provide secure, authenticated process sensors for safety or non-safety applications. As ICS cyber security is effectively the network, cyber security of process sensors has effectively been ignored in Regulatory Guide 5.71 and NEI-0809 (no mention of the word "sensors") as well as multiple other industry cyber security standards. Both Regulatory Guide 5.71 and NEI-0809 mention DIGITAL Instrumentation and control systems. However, analog sensors can also be cyber vulnerable. It is possible to hack analog and digital process sensors before they become Ethernet packets and the control system network anomaly detection systems would not be aware nor would the PLCs or HMIs which effectively defeats situational awareness as required by Regulatory Guide 5.71 and NEI-0809. Process sensor cyber-related issues can, and have, caused catastrophic damage and injuries/deaths yet were not identified as being cyber-related. The Three Mile Island core melt was an example where sensor-related cyber issues contributed to the catastrophic failure.

Cyber security of process sensors and sensor networks is where cyber security and nuclear safety are directly related. The sensor process noise is indicative of sensor health and process health. Flow-induced vibration, loose parts monitoring, sensing line clogging, etc. are monitored using process noise. However, much of the higher frequency process noise has been filtered by the serial-to-Ethernet convertors (gateways) before the sensor signal becomes an Ethernet packet. Consequently, monitoring Ethernet networks cannot provide the necessary information as to the health of the sensor or the process. This is a potential safety problem that has not been addressed. There have been many cases of sensor-related cyber incidents, including some that were catastrophic, and at least one malicious hack of a process sensor. Moreover, there has recently been a demonstration of hacking an ANALOG sensor where neither the PLC nor HMI are aware that the sensor has already been compromised.

Stuxnet made it abundantly clear that sensor monitoring must be done before the sensor becomes an Ethernet packet as the HMI can be compromised. One way to perform sensor monitoring that is not susceptible to hacking is to monitor the electrical characteristics of the sensor before it becomes an Ethernet packet. This approach can address the hole that currently exists with the lack of cyber security and authentication of process sensors and sensor networks. The paradigm shift would be to monitor the electrical characteristics of the process sensors which provide a direct view of the process. Correlating the process sensor electrical characteristics to network anomaly detection can help determine if the actual system impacts are cyber-related. The electrical characteristics of the process sensors are independent of the type of process being monitored and cannot be hacked. This improves cyber security, reliability, productivity, and nuclear safety. Monitoring electrical characteristics provides confidence in the data input to network anomaly detection, process historians, predictive maintenance programs, Security Information Event and Management (SIEM) systems, and first principles models. As sensor electrical characteristics monitoring is independent of the network, zero days and other advanced cyber threats including supply chain compromises become a secondary concern for operations. Actual plant implementations in a water facility, combustion turbine power plant, and chemical plant have demonstrated the validity of the approach by monitoring pressure, differential pressure, temperature, pH, and other sensor measurements and identifying process issues not identifiable from the HMI.