

Secure PHA Review for Managing ICS Risks

Jim Gilsinn¹

¹Jim Gilsinn, Kenexis, 3366 Riverside Drive, Suite 200, Columbus, OH 43221

(*Email: jim.gilsinn@kenexis.com and Phone: 614-323-2254)

SUBMISSION TYPE

30 minute presentation

6-12 page paper plus 30-minute presentation

3 foot wide x 4 foot high large format poster

KEYWORDS

Industrial control system, process hazards analysis, cyber, security, risk

ABSTRACT

Cyber security for industrial control systems (ICS) and other critical infrastructures has been through various stages of hype. At first, there were many that asked why it was even important. Then, we went through various phases of the sky is falling and ICS are all easily hackable. We've been through a large number of incidents that spread from the business environment and even a few that have truly been nation-state ICS targeted attacks.

Throughout it all, many have been trying to use the experience from the safety-related industries to develop a more quantitative way to determine the real risks from cyber security incidents. While this may never reach the level of quantitative rigor that the safety-related industries have developed in process hazards analysis (PHA), there are ways to join the two processes to come up with a more quantitative approach.

This presentation focuses on a Security PHA Review (SPR) that incorporates the safety PHA process with security-related aspects. It doesn't force the user to make wildly speculative guesses on percentage likelihood and the motivation of the attacker, like some risk models. It uses a more conservative and holistic approach that looks at the possibility of compromise based upon factors like the system design, the layers of protection applied to the system, and the capability to monitor and detect an incident.

Using SPR allows for a combination of countermeasures to be applied to the system to mitigate the potential consequences. Simple mechanical solutions may be much easier to implement and just as effective as hugely complex network redesigns at preventing potential consequences. These types of solutions can be explored more easily when a combined approach, like SPR, is used.

ABOUT THE AUTHORS

Jim Gilsinn Contact: jim.gilsinn@kenexis.com

Jim Gilsinn is a Principal Engineer at Kenexis responsible for leading a team of experts with developing, designing, implementing, and assessing secure and reliable ICS. Jim has more than 25 years of electrical engineering, networking, and programming experience with 15 years specializing in ICS performance, reliability, and cyber security. Jim is the co-chair of ISA99, developing the ISA/IEC 62443 series.