WG9 IIOT CYBERSECURITY

ISA99 F2F June 2018

Suzanne Lightman, Chair

- The group will analyze the specific characteristics of the IIoT in terms of threats, attack surface and vulnerabilities, and examine whether the approach developed by the ISA99 committee for securing IACS is appropriate and sufficient for IIoT. In particular, it will examine the content to be given to the concept of "secure by design" objects, as a prelude to a possible certification. It will examine the arrangements to be made to secure the architectures, either in a centralized or decentralized approach, classifying data transmitted from the perspective of inherent risk, and to detect any anomalies.

PURPOSE OF GROUP

APPROACH OF THE WG9

- The group has developed a table of contents for the report that contains:
  - Definitions
  - Overview of IIoT
  - Concerns with the cybersecurity of IIoT
  - Current known threats/attacks
  - What other SDOs are doing
  - What 62443 currently covers
  - Gaps in 62443
  - Existing tools and techniques
  - Needed tools and techniques
  - Recommendations

ASSUMPTIONS

- The discussion is limited to the use of IoT in industrial systems and does not consider other uses (even if they are the same technology)
- The report will present the range of existing definitions and will not select any single definition
- The report is not a standard and will not be written as one
- The report is considering 62443 primarily
  - The information presented will not be exhaustive

- The group has:
  - Heard presentations on threats and attacks currently existing
  - Identified SDOs that are active in the area
  - Looked at the range of definitions
  - Identified some preliminary concerns
- These discussions are documented in both minutes and in a draft table of contents on the website

CURRENT PROGRESS

- Proliferation of communications with IIoT
- Proliferation of applications at lower levels of the control system architecture
- New, and unanticipated, movement of data
- Lack of controls for new functions
  - Lack of application controls
  - Inadequate identity management
  - Lack of tools for management

CURRENT CONCERNS IDENTIFIED

- Lack of trustworthiness due to these concerns
- Loss of control and visibility over automated systems due to these concerns

CONCERNS CONTINUED

- Although it is early in the process, the group has identified some preliminary thoughts
  - The current definitions of target security levels is defined in terms of attacker expertise and is not particularly helpful for IIoT
  - 62443 is focused on network-level controls and IIoT may require more attention given to application level controls
  - 62443 discusses authentication but not authorization and that may need to be included to deal with IIoT concerns

PRELIMINARY THOUGHTS

NEXT STEPS

- The working group is still gathering information and developing thoughts.
- Activities underway include:
  - Presentations on work by other SDOs
  - Research on existing tools and techniques for managing IIoT cybersecurity
  - Development of the final report

WG9'S QUESTIONS

- What is the process for commenting on the draft of the report, if any?
- What is the process for issuing the report?

- October 2018
  - First draft completed
- January 2019
  - Draft issued for comment (if necessary)
- March 2019
  - Report issued
- This timeline is subject to change once the Working Group understands the issuance procedures and any required commenting period

VERY ROUGH TIMELINE

QUESTIONS?