Birdf meeting- task 7

May 13 2022

Ron Insler – Rad Data Communication

RAD IOT GW

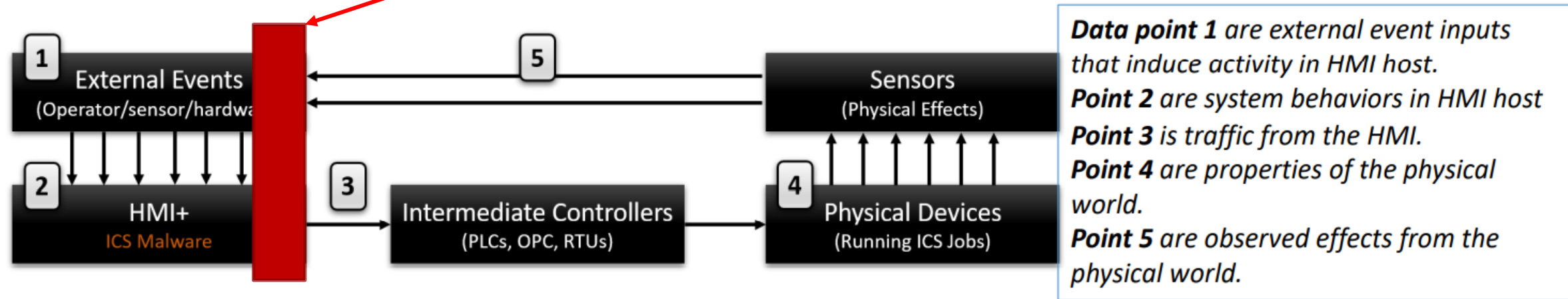**RAD**
Your Network's Edge®

Will monitor all data send or received by HMI

RAD GW
Secflow

Protocols like
Modbus
DNP3
IEC104

physical behaviors which are unique and essential to ICS malware attack operation.

1	**External Events** (Operator/sensor/hardwa...
2	**HMI+** ICS Malware
3	
5	**Sensors** (Physical Effects)
	Intermediate Controllers (PLCs, OPC, RTUs)
4	**Physical Devices** (Running ICS Jobs)

Data point 1 *are external event inputs that induce activity in HMI host.*
Point 2 *are system behaviors in HMI host*
Point 3 *is traffic from the HMI.*
Point 4 *are properties of the physical world.*
Point 5 *are observed effects from the physical world.*

Past methods: Categorized into host and network anomaly detection techniques

Rad Meptagon cooperation
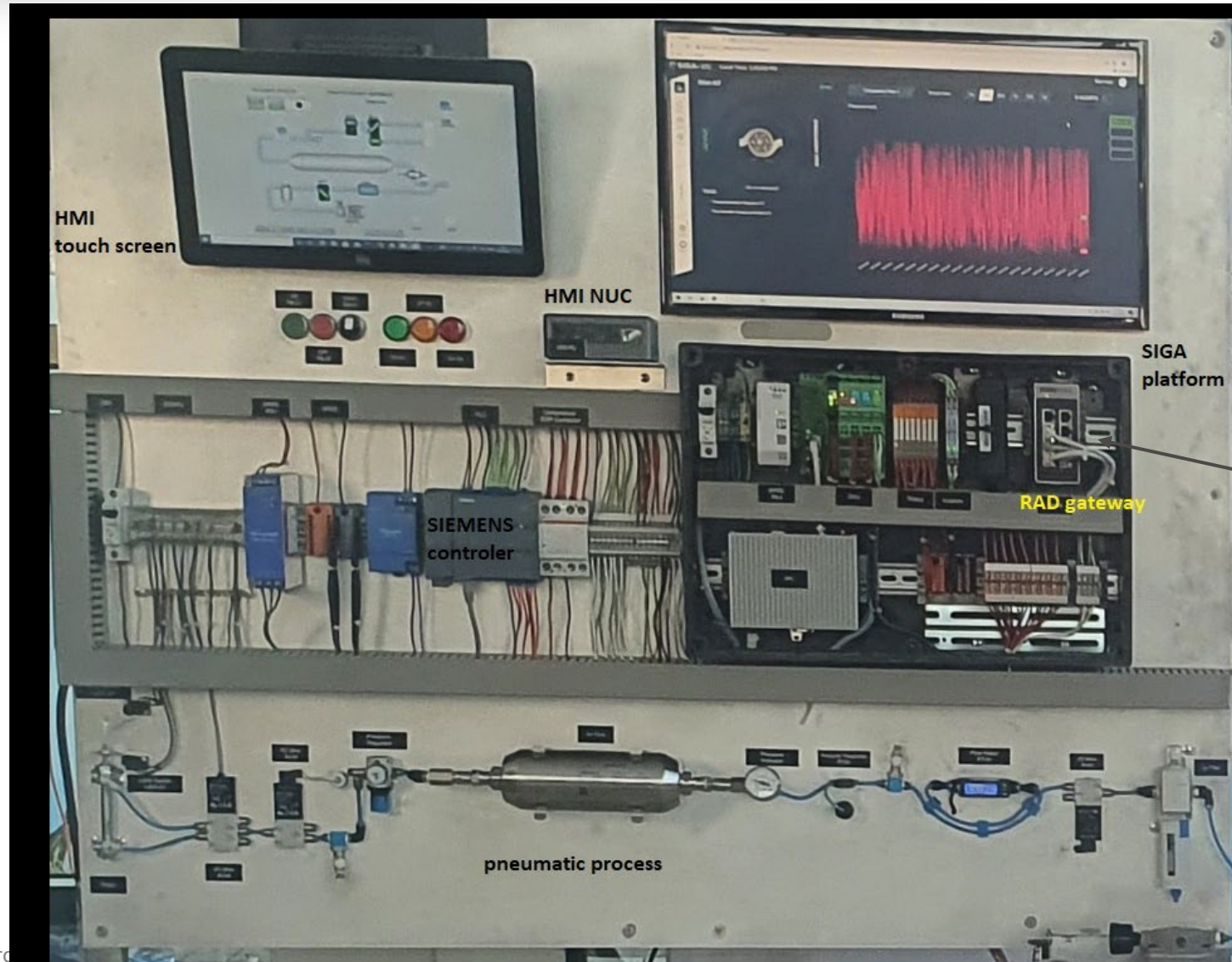
Task 7 current activities in progress until end of 2022

- Definition of the information to be collected by RAD's GW
  - Scada related information – protocol information such as Modbus , DNP3 , IEC104 , data packets paring and sequencing (time stamp) in progress
  - Network related Information : Jitter , delay , loss , rate (time serious) – completed
  - Synchronization related information – in progress
    - PTP packet related information [rate and timestamp, sequence, content]
    - GPS related information [SNR , Elevation and altitude and more]
- Research of what info needs to be locally process and what needs to be send for further analysis in the central analytic process. – still under study together with BGU
- Definition of API's to send the info to GIT system and BGU system – in progress
- Implementation of SW on RAD's GW. - Design completed implementation will start in end of may.
- Integration to Meptagon simulation system will start at end of may.
- Integration with Resource Innovations' HMI (Grid360) under collaboration

Task 7 Commercialization and Collaboration

- Commercialization
  - RAD is deployed with it's IOT GW at utilities like Exelon EVN CPC and much more. We are going to add Task 7 features to enhance the security of the overall solution by SW upgrade.
- Collaboration
  - We are going to collaborate with Delek US , GIT and possible ARAVA power both for testing the overall solution and real deployment as well as selling overall solution RAD GW/ GIT malware detection system.
  - We started collaboration with Meptagon to integrate Rad's GW with Meptagon's simulation kit to be able to simulate attacks.
  - We are planning integration with Resource Innovations' to provide readings of additional sensors via a different network (not the OT) for sensor data verification

Thank you
For your attention