

2019-2020 Progress Report

2019-2020 Accomplishments

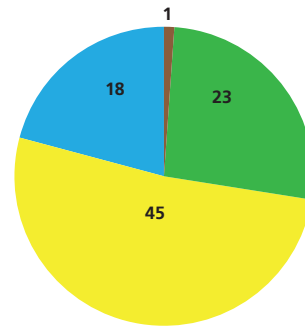
- Project 12 Safety Instrumentation: completed
- Drilling: started to define cybersecurity requirements
- IIoT: Architectures/Use-cases defined
- Micro-Certification: Selected vendor and courses
- CVSS: Researching alternatives to improve CVSS

2021 Planned Activities

- Drilling: Publish cybersecurity requirements
- IIoT: Complete risk assessments
- Micro-Cert: Complete training, summarize results
- CVSS: Pilot new tools & identify future improvements
- Identify and plan for Project 13

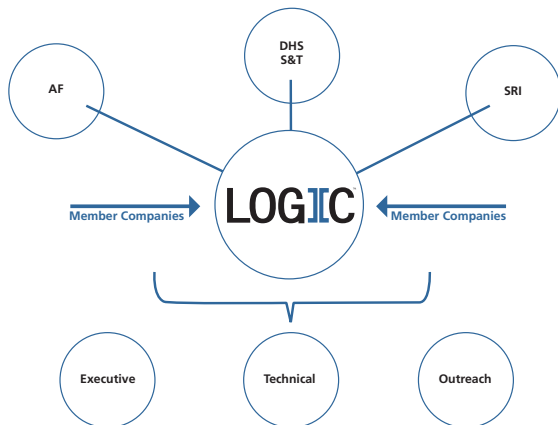
Vendors Resolved Many Risks Found in the Past 3 Projects

- 48% of gaps/risks found in the lab test were resolved or were low risk finding requiring no future action
- 52% of gaps/risks found in the lab test required action by the vendor after the test
- Average resolution time so far was 1.6 years per gap
- We are obtaining more results and will update statistics



P9 to P11 Summary of Findings

- Sum of Fixed onsite during assessment
- Sum of Plan for fixing post-assessment
- Sum of Other findings without an action plan
- Sum of Low risk, advisory or non-actionable findings



LOGIIC Outreach and Awareness Efforts

- LOGIIC Organization Capabilities Workshop resulted in work with NSCC, NIST NICE, and others
- LOGIIC-NCSC Joint London Workshop defined 2 studies
- LOGIIC-ACIC-GTI joint meeting with DHS identified valuable info
- LOGIIC-API joint meeting resulted in partnership opportunity
- API Presentation was given to share LOGIIC Project 11 SIS results
- Partnered with DOE to work with INL and other national labs

LOGIIC learning from each other and various parties

- Security Operation Center (SOC) visits, presentations, and sharing
- Open Process Automation Standards presentation was valuable
- ICS Cybersecurity Common Requirements were defined
- System and Network Monitoring Best Practice Sharing addressed processes, technologies, and various support issues
- Members shared Pen and Vulnerability Testing processes, info, etc.
- Consequence Driven, Cyber-Informed Engineering presentations

