PROGRAM SUMMARY

Program Title: Trustworthy Systems, Components, and Data for Smart Manufacturing

Program Leader: Fred Proctor

Associate Program Leader: Josh Lubell

Lead Division: 735

ABSTRACT:

Advances in computing and communication technology present great opportunities to improve manufacturing productivity. However, applying this technology without considering the unique needs of manufacturing can adversely affect safety, performance, quality, and cost. This program will research methods to measure the impact of new computing and communication technologies on manufacturing, and to establish a basis of trust in their application, delivering guidelines, best practices, and standards that enable manufacturers to confidently select and apply new technology.

OBJECTIVE:

To develop and deploy advances in measurement science, standards, and test methods that enable key dimensions of trust, including performance, reliability, and security, for smart manufacturing systems, components, and data.

WHAT IS THE PROBLEM?

Manufacturing continually evolves as advances in computing and communication technology becomes available. Often, the intended markets for new technologies have different requirements than manufacturing. Advances may be directed toward consumer markets where good performance on average is important, rather than toward manufacturing environments where high reliability and time-critical performance is essential. While it is tempting for manufacturers to leverage the rapid introduction of new features and lower costs that arise from economies of scale in the broader market, naively adopting new technology can result in unforeseen problems. Safety can be improved through more ubiquitous sensing, but may also be compromised due to unreliability. Performance can be increased through higher levels of information connectivity throughout the enterprise, but it may be compromised if systems optimized for consumer or other business use cases interfere with the rigid timing and low latency needs of industrial control systems. Quality improvements can be achieved through more automated sensing, but it may be affected if transient events otherwise invisible during interactive use appear as product defects. Costs can be reduced through increased automation, but initial cost savings may be eroded over time due to longer-term increases in costs for troubleshooting, repair, and ad hoc workarounds. Higher confidence between partners in the network of suppliers can be gained through better traceability and visibility, but may be lost if proven manufacturing relationships are disrupted by new technology. Aware of these consequences, manufacturers are seeking new methods that enable them to benefit from the rapid evolution of technology, while not putting their businesses at risk.

WHAT IS THE TECHNICAL IDEA?

The technical idea is to assess and ensure the adequate and predictable performance of new infrastructural or cross-cutting technology as applied in the manufacturing environment. This technology includes the rapidly evolving market in computing and communications, and the advent of the Industrial Internet of Things (IIoT). Through participation with industry groups, pilot projects at manufacturing sites, and testbed activities at NIST, the projects will research and develop measurement techniques that can determine the impact of new technology on manufacturing processes. The results of this research will inform guidelines, best practices, and standards that help manufacturers determine which technologies will best fit their needs, how to design systems that incorporate new technology, how to predict their effects on reliability, performance, and security, how to continually monitor their operations to ensure that they achieve the desired benefits, and how to maintain the level of confidence they have built with their supplier partners in a dynamic business environment.

WHAT IS THE RESEARCH PLAN?

The program is organized into projects determined from stakeholder needs in the areas of cybersecurity; wireless communication; monitoring, diagnostics, and prognostics; and supply-chain traceability.

The Cybersecurity for Smart Manufacturing Systems project is developing the measurement science basis for understanding the impact of cybersecurity technology on reliability and performance in a manufacturing environment. The results of this research will inform guidelines, best practices, and standards that help manufacturers determine which cybersecurity technologies will best fit their needs, how to design systems that incorporate new cybersecurity technology, how to predict their effects, and how to continually monitor their operations to ensure that they achieve the desired benefits.

The Reliable, High Performance Wireless Systems for Factory Automation project is developing robust requirements, system models, recommended architectures, and guidelines for the integration of reliable, low-latency wireless systems within factory work-cells to enable manufacturers to reduce costs, and increase mobility, efficiency, and flexibility in smart manufacturing systems.

The Prognostics and Health Management for Reliable Operations in Smart Manufacturing project is developing and deploying test methods to promote the implementation, verification, and validation of advanced monitoring, diagnostic, and prognostic technologies to increase reliability and decrease downtime in smart manufacturing systems.

The Supply Chain Traceability for Agri-Food Manufacturing project will develop common models for key data entities for security profiles, checklists, and traceability, work with industry and SDOs to enhance standards to support these entities, and provide links across platforms to exchange and merge data needed for traceability and security assurance. The goal is traceability of manufactured agri-food products through the sharing and merging of diverse data across supply chains, while ensuring that cybersecurity controls are effectively deployed.