IDENTIFYING PERFORMANCE ASSURANCE CHALLENGES FOR SMART MANUFACTURING

Moneer Helu*, Katherine Morris, Kiwook Jung, Kevin Lyons, Swee Leong

Engineering Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8260, Gaithersburg, MD 20899 U.S.A.

(*) Corresponding Author: moneer.helu@nist.gov / +1 3019753654

Abstract

Smart manufacturing has the potential to address many of the challenges faced by industry. However, the manufacturing community often needs assistance to leverage available technologies to improve their systems. To assure the performance of these technologies, this paper proposes a shared knowledge base that collects problem areas, solutions, and best practices for manufacturing technology. An Implementation Risk Assessment Framework (IRAF) is also described to identify the primary weaknesses of technologies in specific manufacturing contexts. Such approaches have the potential to stimulate new ideas and drive standardization activities critical to scale up and deploy smart manufacturing technologies successfully and quickly.

Keywords: Smart manufacturing; Performance assurance; Risk assessment; Standards

1. Smart manufacturing

Many concerns drive manufacturing innovation, including increased global competition; increased demand for a greater variety of products that are created faster, better, and greener; and increased scarcity of technical manufacturing talent [1-4]. Smart manufacturing addresses these concerns through the combination of advanced manufacturing capabilities and digital technologies introduced into every phase of the product life cycle [1,4,5]. Digital technologies have enabled the development of cyber-physical systems that promote interoperability between systems across the enterprise [1,5,6]. Such capability allows manufacturers to generate more and better intelligence through the efficient and effective use of data and information across many manufacturing systems [7]. This provides manufacturers with one of the primary benefits of smart manufacturing: decision-making support through improved monitoring, analytics, modeling, and simulation.

A growing challenge for smart manufacturing is that manufacturers often require technical insight to navigate the breadth and type of technologies now available to improve their systems [3]. Preliminary technology development and validation often occur in research environments, which can impede commercialization and use of technology because of implementation barriers that may be unknown to the developer [8]. To assure that smart manufacturing technologies work well together and with existing manufacturing systems, it is critical that manufacturers and solution providers collaborate to identify problem areas and pool solutions and best practices [3]. This shared understanding can enable successful deployment and more widespread adoption of smart manufacturing technologies to benefit the entire manufacturing community. Such a knowledge base can also help identify standardization opportunities and define the requirements for these standards.

2. Enabling technologies and implementation barriers for smart manufacturing

Developing a knowledge base of common problem areas and solutions for smart manufacturing requires that we first classify and understand the technologies and implementation barriers that currently exist in the manufacturing environment. We begin by focusing on a fundamental aspect of smart manufacturing: using operational data to make informed decisions. Enabling technologies that provide this capability may be considered using a general decision-making process, which involves scoping the

decision, identifying the data to collect, collecting data, transmitting and assessing the collected data, acting on the results of the assessment, and learning from this process to support future decisions. Figure 1 displays the cyclical nature of the decision-making process and maps examples of enabling technologies for sustainability assessment that support each step of the process.

Figure 1 also highlights the fact that each enabling technology may be hindered by a set of implementation barriers. For example, ISO 14000 may be very difficult to implement without expert guidance; networked devices may need to integrate with several interfaces and data protocols; wireless networks may experience interference from machines, structures, or other wireless networks; and cloud-manufacturing may incur the risk of loss of intellectual property. In general, many of the implementation barriers to smart manufacturing technologies can be clustered around resource and training requirements, cybersecurity risks, physical characteristics of the manufacturing environment, and limited standards and common interfaces and protocols.

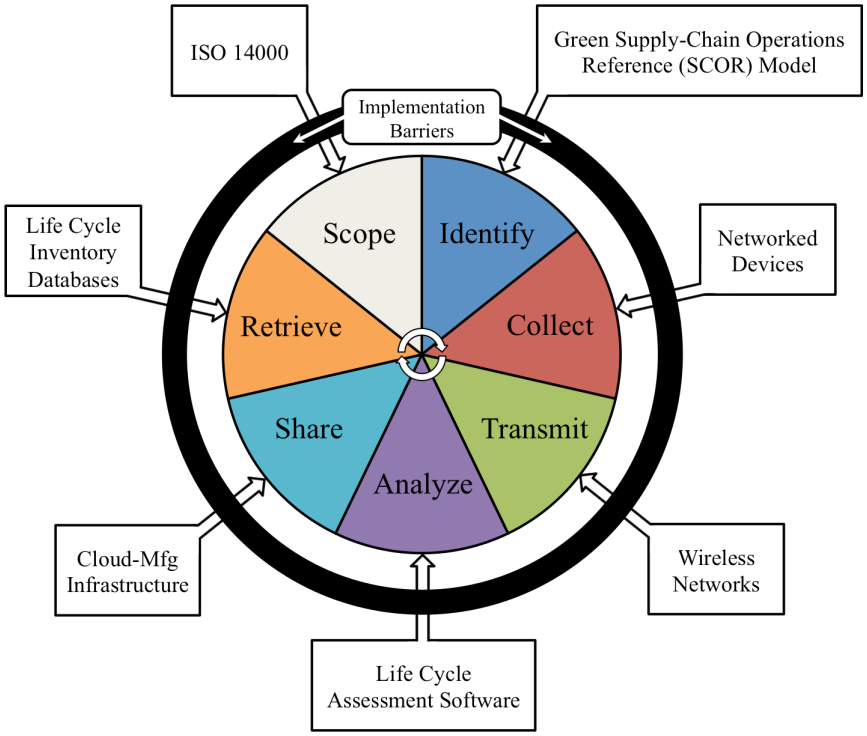

Figure 1. Examples of enabling technologies for sustainability assessment that support each step of the decision-making process; each technology may be limited by a number of implementation barriers.

Formally organizing implementation barriers for smart manufacturing into a knowledge base can enable a risk assessment framework that allows manufacturers and solution providers to identify the primary weaknesses of a technology within the context of a particular manufacturing system. This framework can help identify priority areas for deployment and testing objectives for individual organizations. It can also help identify areas of higher risk in terms of criticality and frequency, which can determine where the standardization of both interfaces and practices may be appropriate. To accomplish these goals, the framework should be community developed and comprehensive for all manufacturing domains. One of the major goals of the research introduced here is to generate an Implementation Risk Assessment Framework (IRAF) to ensure the viability and success of new manufacturing technologies.

3. Implementation Risk Assessment Framework

An exemplary approach upon which to model the IRAF is the Common Weaknesses Enumeration (CWE) organized by the MITRE Corporation [9]. The CWE is a formal classification of weaknesses and security flaws exhibited by software. It has been developed by the software community and contains over 800 weaknesses. The CWE has two companions: the Common Weakness Scoring System (CWSS) and the Common Weaknesses Risk Analysis Framework (CWRAF). The CWSS provides a standard score for software weaknesses that captures the likelihood and prevalence of the weakness [10]. It includes factors such as the inherent risk of the weakness, the strength of the controls against the weakness, the barriers that must be overcome to exploit the weakness, and the characteristics of the weakness unique to specific environments. The CWRAF prioritizes weaknesses based on the appropriate business context [11]. Its methodology is based on the observation that all software weaknesses lead to eight classes of technical impacts (e.g., modify data or execute unauthorized code) that may occur at one of the four layers of the system in which they operate (e.g., network or application). This observation allows one to rank each software weakness consistently by assessing the significance of the impacts of the weakness on each layer of the system and using this analysis to weight its CWSS score.

An analogous observation may be made in manufacturing since all of the types of implementation barriers may be clustered based on their impact on the manufacturing system. For example, these impacts may be to personnel (e.g., more training required to use technology); capital (e.g., more time or money required to set up technology); infrastructure (e.g., more equipment required to run technology); or intellectual property (e.g., technology requires more protection against cyberattacks). These impacts will also occur in one of the layers of the manufacturing hierarchy (i.e., process, machine, cell, line, factory, and enterprise). Thus, one may rank implementation barriers using the IRAF by assessing the significance of a barrier's impacts on each layer of the manufacturing system analogously to the CWRAF methodology for software weaknesses.

Figure 2 provides an overview of the IRAF methodology to rank implementation barriers for manufacturing technology. This methodology may be illustrated by considering an MTConnect-enabled networking solution for machine tools in a small-to-medium enterprise manufacturing regulated parts. First, the manufacturing system should be defined using technical archetypes, which are common definitions of the components of manufacturing systems. Such a definition allows one to incorporate domain-specific context into the IRAF using common terms for the types of implementation barriers and impacts that are relevant. The technical archetypes in the example could include machine tool controllers, network connections, software applications, computers, servers, and web clients.

The domain-specific context also informs the weighting of the potential impacts of an implementation barrier. This context for the example could include lacking resources for computers or servers, lacking staff experience in networking components, and exposing sensitive information about regulated parts. Therefore, barriers that impact capital, personnel training, or cybersecurity could lead to the highest weightings in the example. Using these weightings and the list of implementation barriers (i.e., the knowledge base described in Section 2), a list of relevant barriers may be identified. The weightings for the identified barriers may be coupled with the barriers' scores (analogous to the CWSS) to generate the final ranked list of implementation barriers for the specific technology and system of interest.

4. Summary

Successful smart manufacturing technologies require standards that enable developers and users to understand potential problems in the technologies and identify solutions for specific manufacturing contexts. The IRAF formally organizes barriers to the implementation of manufacturing technology and enables users to rank these barriers for a manufacturing system and technology of interest through the use of community-developed standards and tools. Developing standards and tools for the IRAF requires consensus from the manufacturing community around a consistent set of technical archetypes of manufacturing systems, implementation barriers, and scores for each barrier based on factors such as its

likelihood and prevalence. The National Institute of Standards and Technology (NIST) is conducting preliminary research to generate an initial list of implementation barriers and define a format for the entries in this list to support such efforts. Perhaps the biggest challenge is to bring together communities of experts to ensure the comprehensiveness and accuracy of the IRAF methodology. The IRAF has the potential to stimulate new ideas and drive standardization and the requirements for standards by identifying major implementation barriers. It may also help close the innovation "valley of death" by addressing scale-up and deployment issues at lower TRLs to enable more reliable and quickly developed technologies.

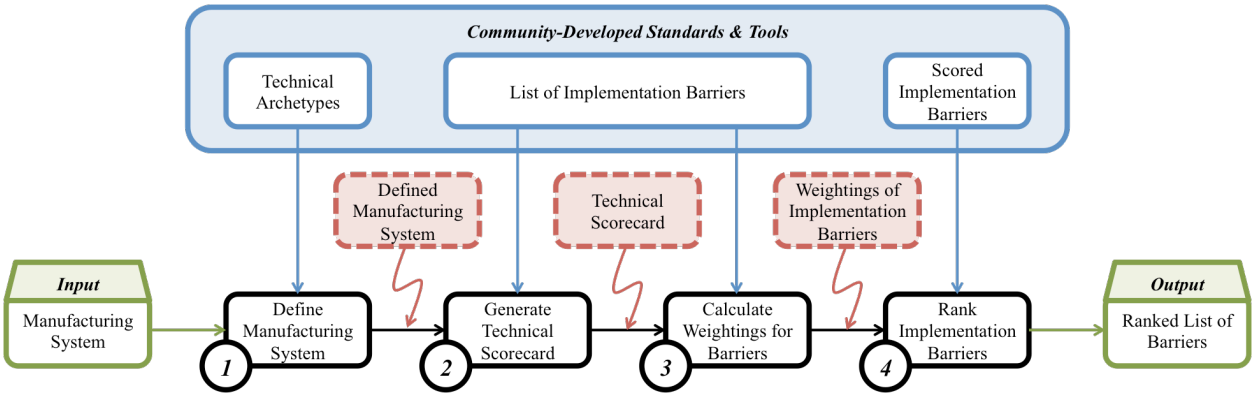

Figure 2. The use of community-developed standards and tools (blue) during each step of the Implementation Risk Assessment Framework (black) to rank implementation barriers for manufacturing technology including the intermediate outcomes of the analysis (red).

Acknowledgements and Disclaimer

The authors would like to acknowledge Don Libes for his helpful feedback. Certain commercial systems are identified in this paper. Such identification does not imply recommendation or endorsement by NIST. Nor does it imply that the products identified are necessarily the best available for the purpose.

References

[1] Evans PC, Annunziata M. Industrial Internet: Pushing the Boundaries of Minds and Machines. General Electric Technical Report; 2012.
[2] Jovane F, Koren Y, Boër CR. Present and future of flexible automation: towards new paradigms. CIRP Annals – Mfg Technology 2003;52(2):543-60.
[3] President's Council of Advisors on Science and Technology, Steering Committee of the Advanced Manufacturing Partnership 2.0 (AMP2.0). Report to the President: Accelerating U.S. Advanced Manufacturing; Oct 2014.
[4] Smart Manufacturing Leadership Coalition. Implementing 21st Century Smart Manufacturing: Workshop Summary Report; June 2011.
[5] Helu M, Hedberg T. Enabling smart manufacturing research and development using a product lifecycle test bed. Procedia Mfg 2015; to appear.
[6] Wright P. Cyber-physical product manufacturing. Mfg Letters 2014;2:49-53.
[7] Jung K, Morris K, Lyons KW, Leong S, Cho H. Mapping strategic goals and operational performance metrics for smart manufacturing systems. Procedia Comput Sci 2015;44:184-93.
[8] U.S. Department of Defense. Technology Readiness Assessment (TRA) Guidance; May 2011.
[9] The MITRE Corporation. Common Weakness Enumeration: A Community-Developed Dictionary of Software Weakness Types, v. 2.8; 31 July 2014. Accessed 21 April 2015. <https://cwe.mitre.org/>
[10] The MITRE Corporation. Common Weakness Scoring System (CWSS), v. 1.0.1; 5 Sept 2014. Accessed 21 April 2015. <https://cwe.mitre.org/cwss/>
[11] The MITRE Corporation. Common Weakness Risk Analysis Framework (CWRAF), v. 0.8.3; 3 April 2013. Accessed 21 April 2015. <https://cwe.mitre.org/cwraf/>