Leveraging Standards for Manufacturing Digital Transformation

by Jacob Chapman, Grantek Systems Integration and TAG Member, IEC/TC 65

Introduction

Manufacturers today are in the grips of the Fourth Industrial Revolution, adopting technologies to improve real-time visibility and optimization of their business. Digital Transformation is a very challenging pursuit, and many organizations struggle not only with technology, but also how to affect change within the organization, justify the costs, and maintain momentum against a shared vision. Technical standards play a critical role in that effort.

The Challenge Manufacturers Face

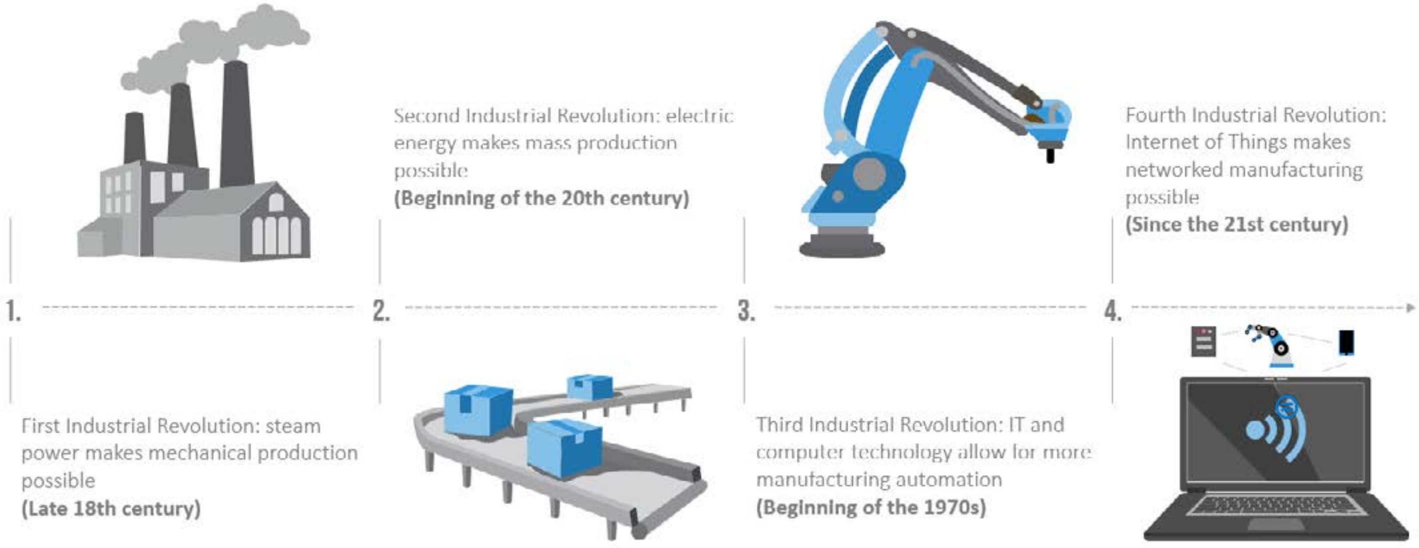
Industrial manufacturing today is not what it was 20 years ago, and systems at that time were very different from 40 years ago. For example, the 1970s marked the start of Third Industrial Revolution, when IT computer technology allowed for automating complex systems, and manufacturers raced to adopt the technology in order to speed up their manufacturing processes, increase their output, reduce their prices and maintain their competitive edge. But it only took a few decades to transition from the third Industrial Revolution to the fourth, which indicated a record-breaking pace for manufacturing innovations globally. As we've seen in many areas of our daily lives, the introduction of computer technology has changed the rules of the manufacturing game so rapidly, it's hard to keep track of what the rules are at any given time.

To win the game 20 years ago, a manufacturer needed to increase output and efficiency through automation. But now that's just a basic requirement to play. Since the 21st century the name of the game has become real-time optimization throughout the entire supply chain by having systems that report real-time logistics and production data to business-level systems in order for the business to make strategic and operational decisions based on real-time conditions. These systems come in the form of OEE, SPC, MES, Sensor-to-Cloud (IoT), and other systems, That is what the fourth Industrial Revolution is about, that is what Digital Transformation describes, and it's the biggest challenge that manufacturers face today.

Connectivity Limits Progress

Acatech—a working academy based in Germany which provides information and advice to politicians and the public on technical subjects—developed and published a study in 2017 titled Industrie 4.0 Maturity Index which received attention globally and has most recently been updated with a 2020 edition. That study described stages of Digital Transformation maturity, which started with a "Computerization" stage and ended in an "Adaptability" stage of maturity. A subsequent study of manufactures was then performed by the Industrie 4.0 Maturity Center and found that 80% of participants measured within the second "Connectivity" stage of maturity.

Figure 1 – Timeline for the 4th Industrial Revolution


Second Industrial Revolution: electric energy makes mass production possible
(Beginning of the 20th century)
Fourth Industrial Revolution: Internet of Things makes networked manufacturing possible
(Since the 21st century)
1.
2.
3.
4.
First Industrial Revolution: steam power makes mechanical production possible
(Late 18th century)
Third Industrial Revolution: IT and computer technology allow for more manufacturing automation
(Beginning of the 1970s)

The index and results demonstrate that connectivity is a requirement for Digital Transformation, manufacturers generally have achieved that at a fundamental level, but are struggling to advance beyond that.

Fundamentally, it is easy to understand that systems that facilitate Digital Transformation require deep and secure connectivity. But that concept becomes complicated when you dive into the details, and it becomes apparent why manufacturers struggle to advance further. I'd propose that the underlying Industrial IT Infrastructure upon which Smart Factory systems run is the primary limiter preventing more rapid progress.

The Role of Industrial IT Infrastructure

Industrial IT infrastructure—which is the networking, PCs and servers, and the cybersecurity systems for the industrial systems—is analogous to civil infrastructure like highways, which enable you to get where you want to go through the use of a car. Highways are incredibly costly to build and maintain and they are critically important but in spite of that, most drivers don't appreciate the highway itself; the car they drive and the good time they make on their commute is what they appreciate.

Within manufacturing, the Industrial IT infrastructure is the highway, and Smart Factory technologies are the car that get an organization towards Digital Transformation. Like highways, the Industrial IT infrastructure is costly to develop and maintain, and in spite of that businesses don't value the infrastructure as much as they do the Smart Factory technologies that give them real-time visibility and optimization.

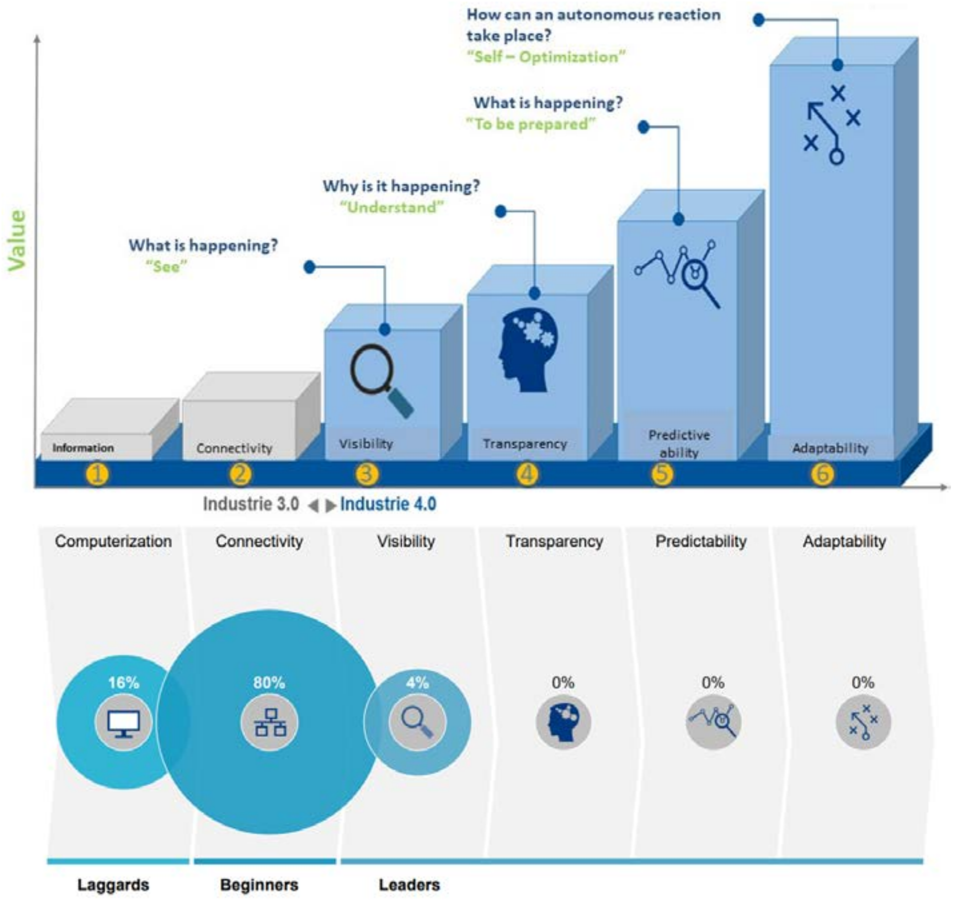


Figure 2 – Acatech Industrie 4.0 Maturity Index and Study Results

The Industrial IT Problem

The problem that most manufacturers find themselves in is that the industrial IT infrastructure was not built to support Smart Factory technologies. Usually, the Industrial IT infrastructure is built and deployed to support individual control systems. There is a very significant difference between the two.

For example, for a small control system to run, a low-cost unmanaged switch that simply passes network traffic through is sufficient, and an independent physical server located in an IT closet can host the application. But as these systems and servers add up and are interconnected—as they have been to perform plant-wide data collection and remote access—the low-cost switches can't handle the increasing traffic load, there are too many independent physical servers to maintain properly, and even worse, the entire infrastructure is extremely insecure.

In many cases the only way to properly correct the infrastructure is to design and deploy a new plant-wide infrastructure which some organizations do, but most find too difficult. Infrastructure is notoriously difficult to demonstrate an ROI through traditional methods, it is disruptive to the organization, it is laborious and complex, and the long-term value is not understood broadly.

Tie Infrastructure Investment to Digital Transformation and Security

The solution to the Industrial IT problem will never be solved at the facility-level, because operational teams' priorities focus on efficiency and productivity. Project ROI requirements are a strong example of this: including the (expensive) costs of a proper infrastructure within a typical engineering project bloats the costs of the project, throws off the ROI, and ultimately does not get approved. The costs of re-architecting a network, consolidating servers, or deploying security management tools must be justified against the value they provide, which is the strategic value that digital transformation brings and the risk reduction that security brings to the organization.

Strategy and business risk is managed at the corporate and executive level, which is where the costs of solving the Industrial IT problem can be justified against the strategic and business risk reduction value it brings. That business justification step itself is a challenging one, but it's dwarfed by the subsequent labor needed to effectively implement change throughout the organization and actually solve the problem.

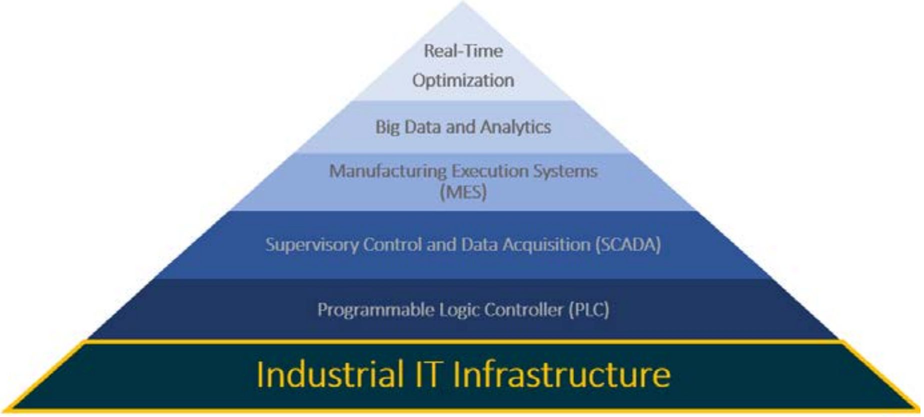
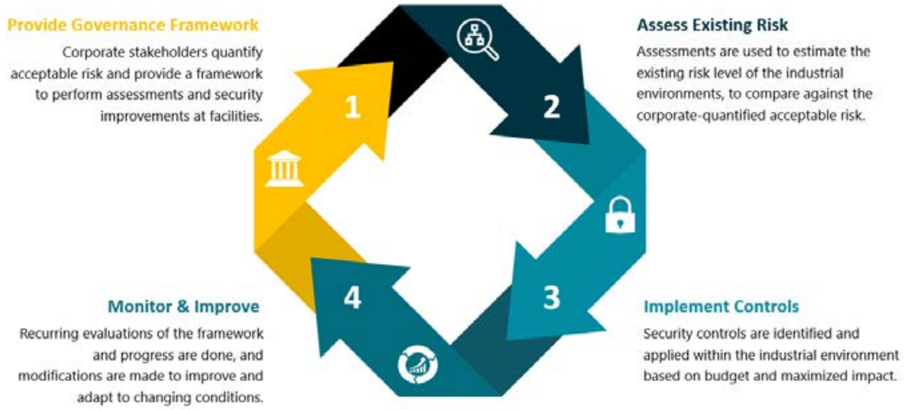

Real-Time Optimization
Big Data and Analytics
Manufacturing Execution Systems (MES)
Supervisory Control and Data Acquisition (SCADA)
Programmable Logic Controller (PLC)
Industrial IT Infrastructure

Figure 3 – Industrial IT Infrastructure Foundation

Use IEC-62443 to Achieve Digital Transformation

I put forward that the IEC-62443 is the best framework for manufacturers to lean on in order to solve the Industrial IT problem, develop an operational environment that is able to adopt Smart Technology platforms, and thus achieve digital transformation. That may sound like a reach considering that IEC-62443 is an ICS cybersecurity standard, but there are more reasons than not that it is the tool to solve the problem.

Figure 4 –Simplified ICS Cybersecurity Risk Management Cycle



Provide Governance Framework
Corporate stakeholders quantify acceptable risk and provide a framework to perform assessments and security improvements at facilities.

Assess Existing Risk
Assessments are used to estimate the existing risk level of the industrial environments, to compare against the corporate-quantified acceptable risk.

Implement Controls
Security controls are identified and applied within the industrial environment based on budget and maximized impact.

Monitor & Improve
Recurring evaluations of the framework and progress are done, and modifications are made to improve and adapt to changing conditions.

First, we have learned through recent decades of innovation that for a device or system to be secure, it must be built from the ground up with the appropriate security requirements and controls in mind. Developing any device or system first and then securing it later simply does not work; there are too many layers within the system for it to be secured later. **This is why IEC-62443 security approaches should be incorporated even before organizations begin designing and deploying new Industrial IT components during Digital Transformation.**

Second, the depth of connectivity and security the organization needs varies throughout the industrial environment. One particular facility may be of strategic importance to the business, and thus deserves enhanced connectivity, monitoring and optimization to improve the business' position in the market. Another system in a separate facility may pose the greatest operational risk to the business should a security incident occur. A challenge that the organization will face while solving the Industrial IT problem and pursuing digital transformation is to identify the varying requirements and distribute investments where they are

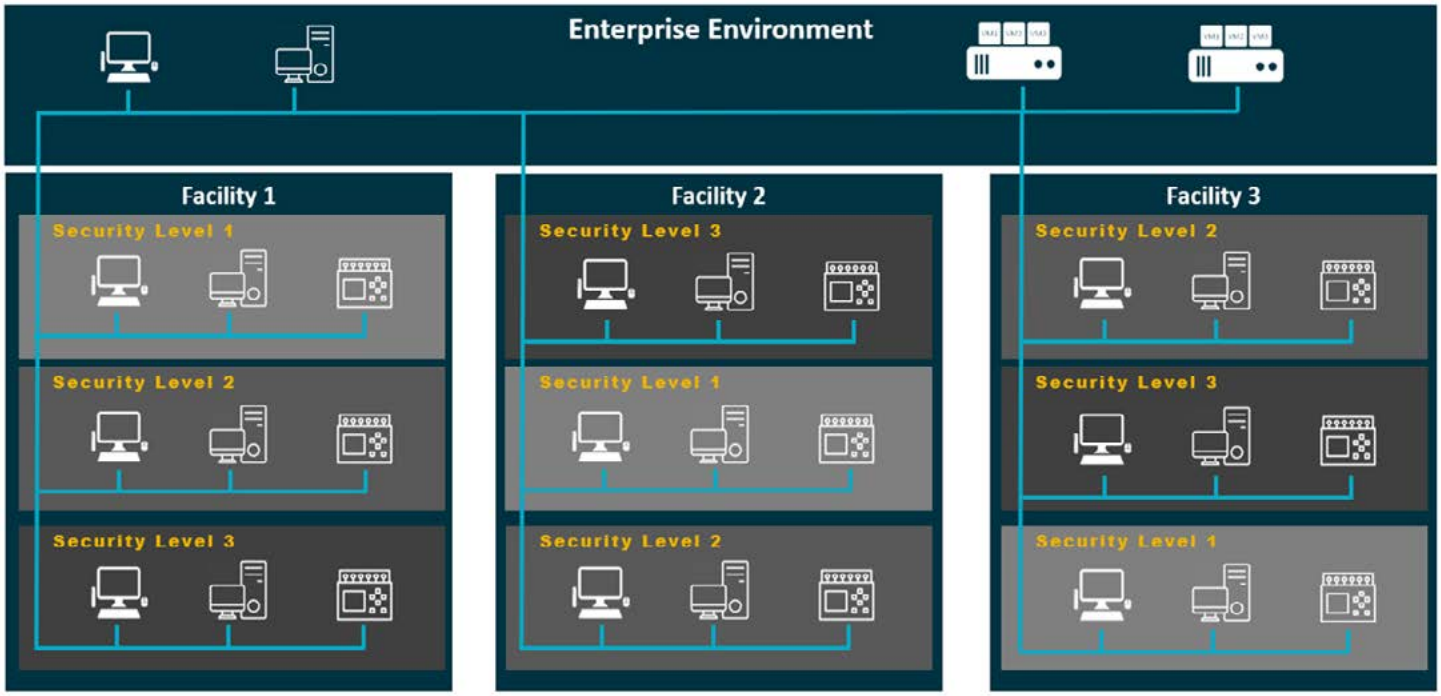


Figure 5 –Graphical Depiction of Security and Connectivity Investment Distribution

needed throughout the organization. This, too, is a consideration that is built into the IEC-62443 series of standards and achieved by first quantifying the amount of security risk reduction required for a system before identifying the security controls which should be implemented on that system. This approach can be leveraged and harmonized with the strategic value of digital transformation to appropriately distribute and justify investment.

Finally, a critical component for success in any multi-year, multi-facility initiative is to be able to monitor, re-evaluate and adjust on a continuous basis to adjust to changing conditions. A function for doing this is built into the IEC-62443 series of standards and that process can be leveraged to not only monitor and adapt the organization's security program in response to changing security risks, but also harmonize course corrections with changing strategic priorities and goals around digital transformation the Smart Factory technologies that the organization is prioritizing.