Applying ISA 99 and ISA 88 Principles: An Often Overlooked Aspect of Manufacturing and Packaging Systems Integration

Garvan McFeeley
Chief Information Officer
UrmaSys
IDA Industrial Estate,
Collooney,
County Sligo
Ireland
Tel: +353 71 91 645 99
Fax: +353 71 91 348 33
garvan.mcfeeley@urmasys.com

Shane Loughlin
Manufacturing Technologies Director
UrmaSys
IDA Industrial Estate,
Collooney,
County Sligo
Ireland
Tel: +353 71 91 645 99
Fax: +353 71 91 348 33
shane.loughlin@urmasys.com

KEY WORDS
FDA, GAMP, OEM, ISA 88, OPW, ISA 99, OEE, PackML,

ABSTRACT

This paper demonstrates that leading Original Equipment Manufacturers (OEMs) of manufacturing and packaging equipment can utilize both the ISA 88.05 modular approach to automation and the security guidelines as outlined in ISA 99 to refine their product offering, towards the product offering of Information Technology OEMs, so that they can continue to earn continuous revenues over the life of the equipment by providing value add services, which increase the Availability of their equipment, to their customers. This demonstration is reinforced with real world examples and quantified with data gathered from a recent project consisting of a fully automated manufacturing and packaging line for a world class biomedical device manufacturer.
INTRODUCTION

The project, which this paper is based on, consists of the implementation of 4 fully automated manufacturing and packaging lines over a 3-year period for a world-class biomedical device manufacturer. The main measure for success on this project is that each line must achieve an (Overall Equipment Effectiveness) OEE in excess of 90%. Other characteristics which added to the complexity of the project included FDA 21 CFR Part 11 compliance, and the incorporation of Electronic Signatures.

In order to provide the highest chance of success, existing equipment was analyzed. The Performance and Quality of the process was under good control but the Availability of the equipment was the main source of variability. Sources of downtime, which affected Availability, were classified as either High Frequency Short Duration Stoppages or Low Frequency Long Duration Stoppages.

Over the following sections both of the above sources of downtime are explored, and the strategies, which were implemented in order to minimize their impacts, have been outlined in detail. The paper goes on to explore the business models utilized by manufacturing OEMs and the unique business opportunity that exists whereby manufacturing OEMs can assist the end users to dramatically increase equipment availability.

HIGH FREQUENCY, SHORT DURATION SToppages

If the concept of Availability is to be introduced in a comprehensive fashion into a manufacturing facility, it must be borne in mind that the system must be easy for all personnel in the manufacturing facility, the technology providers and the OEMs to understand and converse clearly and concisely with the minimum of confusion.

The PackML State Model [1] provides an ideal starting point, because it provides a common terminology, which all personnel in the organization ranging from Operators, Supervisors, Engineers and Managers can easily understand. This combined with the fact that it will be incorporated into the ISA 88.05 standard in the near future ensures that it is not a custom solution. By expanding the state model to include a few more states such as starved and blocked, an extremely deep insight as to the machine’s availability can be achieved.

With a machine centric software approach, applying the PackML State Model, as depicted by Figure 1, the state model is transposed to the controller. Using a high-level language or (human-machine-interface) HMI software at this point, enables the data to be retrieved across OPC and logged to a Database. The resulting data can then be made available to any computer on the network via Web Pages.
The Machine Centric Software Approach provides many advantages such as:

- The OEM has the most intimate knowledge of the machine and as such can create a State Model that facilitates root cause analysis on his particular equipment.
- The application has only to be created once thus the OEM can spread the cost spread over all subsequent machines.
- The machine is “Publishing” its data to industry standard interfaces. The cost of interfacing this data to other IT Systems by the End Users’ IT Department is drastically reduced.
- The machine data is available to be viewed by all personnel in the organization with the correct access rights without any licensing costs.

Figure 1: Machine Centric Software Approach
1.1 The PackML State Analysis

In order to ensure that a consistent approach was utilized to maximize the availability of the equipment in the manufacturing facility, the following guidelines were utilized:

- Keep the approach simple, and non domain specific
- Decide on a few Key Performance Indicators (KPIs)
  - Counters, PackML States (sub-divided into Machine Issues and Product Flow Issues) and Alarms were used
- Adopt a Pareto Analysis, Drill Down Approach
  - Analyze Counters
    - Look for periods of low production
  - Analyze PackML States for Root Cause Analysis
    - Determine Machine Issues – Faults, Stops & Restarts (see Figure 2)
    - Determine Product Flow Issues – Blocked and Starved (see Figure 3)
  - Analyze the Alarms if a lot of time is in the Aborted State
    - Reduce the high frequency short duration alarms
    - Reduce the low frequency long duration alarms

1.2 Time Domain Analysis

Utilizing Pivot Tables allowed the manufacturing facility to leverage all of its resources, on the one data set. The Pivot Table is a very commonly used tool in both the financial and managerial domain. It allows the user to see different trends and facilitates both the summarizing of data to determine totals, or expansion of data to find the detail. It was found that there was virtually no training requirement for the managerial and administration level to utilize this form of analysis.

Production personnel on the other hand quite quickly identified how well they were performing on an hourly basis against their “Competition” on other shifts, while engineering could focus on both the Product Flow issues and Machine Faults and restarts.

The elimination of Auto Scaling on the Y Axis as depicted in Figure 2, and Figure 3 portrayed that all users were operating to the same metrics and resources were not being misallocated.
Figure 2: Non-Producing States due to Equipment

Figure 3: Non-Producing States due to Product Flow
1.3 The Business Case

The cost of developing and installing the Machine Centric Software Approach was less than 5% of the cost of the overall machine. The resulting information allowed Manufacturing and Engineering personnel to increase the availability of the machine by 50%, over a 4-week period, with minimal equipment investment. This increase in availability can be translated into an increase in production in excess of €1,000,000 per annum, on this one machine.

The resulting optimization of the machine availability is depicted in Figure 4. It should be clear from Figure 4, that even though considerable advances have been made, enormous opportunity remains. Thus it should be borne in mind that this is a continuous improvement process.

![Figure 4: % of Time in PackML States Pre and Post PackML State Analysis](image)
LOW FREQUENCY, LONG DURATION STOPPAGES

The first step in analyzing the manufacturing facilities performance in responding to the low frequency, long duration stoppages was to evaluate typical response times as skills matrix as outlined in Figure 5 and Figure 6. Whereas the response times were reasonable, the complexity of the machines required detailed domain expertise for solving all but the simplest of problems. This is beyond the scope of engineers and technicians at an end user’s manufacturing facility.

The variance in the control platforms as supplied by the manufacturing OEMs to this production facility over the last 20 years has resulted in excess of 15 different PLC models, from 8 different PLC and controller manufacturers, together with 5 major servo motion control platforms, connected together using in excess of 12 different industrial networks.

Even in the unlikely event of the end user’s engineers having all of the required programming tools and software to connect to the above devices, the training overhead of ensuring that these engineers were competent on this enormous variety of platforms would be prohibitive.

The real potential for eliminating these stoppages on new machinery lies in ensuring the OEMs design their systems is such a way that the operator/technician can be connected virtually immediately with the Specialist in a manner outlined by Figure 7.

In order to ensure that providing the above connectivity between OEM and End User did not introduce any unnecessary risks to the end user’s manufacturing facility, the excellent work done by ISA 99 [102], [103] was leveraged on this project, and the resulting designs are contained over the following sections.

![Figure 5: Typical Response Times to Equipment Stoppages displayed in minutes.](image-url)

Copyright © 2006 WBF. All rights reserved.
Figure 6: Typical Skills Matrix expressed in % proficiency.

Figure 7: Ideal fault finding solution expressed as skill set and required proficiency.
ISA TO THE RESCUE

Convincing end user IT departments to allow remote access to their infrastructure is a mammoth task and should not be underestimated. Any connection to the Internet is extremely difficult to justify from an IT perspective. The ISA standards and associated papers provide an invaluable resource in order to ensure that a balanced, well informed approach leveraging on other End User’s previous experience is adopted.

The approach that was taken on this project, and the relevant papers and the standards that were leveraged were as follows:

1. Perform general background research, and basic education
   a. The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems [100]

2. Evaluate the Risks to the Manufacturing Control Network (MCN)
   a. ISA TR99.00.02 - Integrating Electronic Security into the Manufacturing and Control System Environment [102]

3. Determine the Security Tools which can be utilized to minimize the Risks

4. Optimize the MCN design.
1.4 General Background Research

Byres and Hoffman [100], and Weiss [101] work provides a valuable insight to the vastly different approaches taken to security by IT and manufacturing personnel. The main findings from this background research were as follows:

- There is an accountability gap in many organizations
  - Awareness is still limited at the executive and operations levels. In addition, the CIO who has the responsibility for cyber security often has no accountability for control systems. Corporate culture has minimal accountability for cyber security of control systems. Very often, IT security or corporate operations is not aware of what networking and remote access has been implemented in the field [100].

- There is some statistical data on security incidents but where companies need to be more proactive in reporting attacks so that the overall bank of knowledge improves, and is kept current.
  - The British Columbia Institute of Technology Internet Engineering Lab (BCIT/IEL) maintains an industrial cyber security incident database that tracks incidents involving process control systems in all sectors of manufacturing. While most companies are reluctant to report cyber attacks or even internal accidents, there are now enough events to allow some basic statistical analysis of the data [101].

- It is very rare for attacks to come from the Internet
  - If attacks do occur from outside the plant floor, the infiltration rarely occurs directly from the Internet. Instead it typically is via backdoor connections such as desktop modems, wireless networks, laptop computers, trusted vendor connections [101]

- A company’s own employees represent the biggest threat
  - Employees caused over 50% of the recorded attacks [101]
  - A study by the FBI and the Computer Security Institute on Cybercrime, released in 2000 found that insiders carried out 71% of security breaches. This is supported by the realization that persons with high technical skill and process knowledge pose the greatest threat to an organization [104].
1.5 Evaluating the Risks

ISA 99.00.02 [102] provides an ideal framework for evaluating the risks associated with the MCN.

1.5.1 Applying ISA 99.00.02

A brief overview of the steps involved is as follows:

1. Define Risk Goals
2. Assess and Define Existing System
   a. Form Cross-Functional Team
   b. Pre-Risk Analysis Activities
      i. Perform Screening Inventory to Identify and Characterize Manufacturing and Control Assets
      ii. Develop Network Diagram
      iii. Update the Screening Inventory
      iv. Make Preliminary Assessment of Overall Vulnerability
3. Conduct Risk Assessment and Gap Analysis
4. Procure or Build Countermeasures
5. Define Component Test Plan
6. Test Countermeasures
7. Define Integration Test Plan
8. Perform Pre-Installation Integration Test
9. Define System Validation Test Plan
10. Perform Validation Test on Installed System
11. Finalize Operational Security Measures
12. Routine Security Reporting and Analysis
13. Periodic Audit and Compliance Measures
14. Reevaluate Security Countermeasures

1.5.2 Initial MCN Network Diagram

Figure 8 outlines the initial MCN network diagram that was created by analyzing the proposed architecture as supplied by each OEM. This MCN network diagram was expanded to include the technology providers. The role of the technology provider is one that is often overlooked, by many End Users. Many machines that are currently supplied by OEMs are extremely complex and very few OEMs have the in house resources to completely support a system, thus they rely on the technology providers to provide additional support. This represents a serious security breach due to the fact that the End Users may not be aware of who the OEMs are allowing to have access to the MCN.
From an IT perspective it may seem extremely wasteful to have 11 Modems on one line as outlined in Figure 8, but normally the OEMs install the Modems as part of their supply. Because each OEM may have a slightly different modem configuration, they are normally unwilling to consider other options. The cost of modems and the associated cost installation of an analogue telecoms line to the point of use were estimated at €1,500 per point or €16,500 per line as outlined in Figure 8.

A major technical restriction on Modems is their speed. Industrial Modems are typically limited to 56k. The production equipment installed on this project will have complex motion control and many will have vision systems. Also the typical project size for the PLCs on this line will be in the 1MB to 3MB range, thus it is not practical to provide support at these speeds via modem. In practical terms a minimum requirement for the support of this machinery is network access with 1MB bandwidth.
The use of engineering laptops as programming tools by the End Users’ employees represent an extremely vulnerable situation from the End Users’ perspective, when both Byres and Hoffman [100], and Weiss [101] work is considered.

1.5.3 Determine the Threat Probability Ratings

<table>
<thead>
<tr>
<th>Probability</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>A = Very Likely</td>
<td>1 = Severe Impact</td>
</tr>
<tr>
<td>B = Likely</td>
<td>2 = Major Impact</td>
</tr>
<tr>
<td>C = Not Likely</td>
<td>3 = Minor Impact</td>
</tr>
<tr>
<td>D = Remote Chance</td>
<td>4 = No impact</td>
</tr>
</tbody>
</table>

By applying the Threat Probability Rating as outlined in Figure 9 to the Initial MCN Network Diagram in Figure 8 the following Threat Probabilities were classified:

- Category A (Very Likely)
  - 5 x OEMs
  - 14 x technology providers
  - 3 x Programming Terminals
- Category C (Not Likely Chance)
  - 1 x Integrated MCN

Thus the use of the above modems introduces an enormous number of very likely Threat Probabilities to the MCN, while not delivering the required bandwidth and performance to allow the OEMs and technology providers to adequately support the supplied systems.

Programming terminals on the other hand create substantial exposure to attacks from insiders and must be eliminated.

The MCN should be isolated from the End Users LAN to prevent exposure from insiders also.
1.6 Determine Suitable Security Tools

Using ISA 99.00.01 [103] it was possible to identify suitable security tools to minimize the risks associated with access (both internal and remote) to the MCN.

- VPNs are the preferred solution from an IT perspective, because they are the industry norm, but they are not ideal from an MCN perspective because they allow unrestricted access to the LAN and do not offer any protection against the most frequent offenders which are insiders.
  - **VPNs do not protect the network and workstations against most data-driven attacks (i.e., viruses), some denial-of-service attacks, social engineering attacks, and malicious insiders [103].**

- SSH can be implemented in such a manner as to overcome the issues associated with VPNs by routing the insiders through the SSH servers
  - **In public key cryptography, a pair of different but related keys, usually known as a public-private key pair, replaces that single key. The private and public keys are mathematically related such that a public key can be used by others to encrypt messages to be sent to the holder of the corresponding private key, which then can be decrypted with that private key. A key holder usually circulates the public key to other users in the same community, but does not reveal the corresponding private key to the other users [103].**
  - **Secure Shell (SSH)—SSH is a command interface and protocol for securely gaining access to a remote computer. It is widely used by network administrators to remotely control Web and other types of servers. Typically, SSH is deployed as a secure alternative to the telnet application. However, SSH also has the ability to do port forwarding, which allows it to be used in all three deployments listed above. SSH is included in the majority of UNIX® distributions on the market, and is typically added to other platforms through a third-party package [103].**
  - **There are no known security weaknesses with the dominant public key/PKI encryption algorithms [103].**

- Use Firewalls to isolate the MCN, but augment them with an Intrusion Detection System (IDS), and route all access, both remote and insiders, through the SSH Servers.
  - **While the firewall is the lock on the door to the process network, it is not the burglar alarm. You need some method of monitoring traffic and identifying malicious activity on the network. The tool to achieve this is known as an intrusion detection system (IDS) and can range from a simple scan detector, to a heuristic engine that profiles user behavior, to a system that takes explicit action against the suspected intruder. In the process world, traffic patterns tend to be very consistent so even simple traffic matrices that show who is talking to who can be a big help [101].**
The layered security model is very strong if it is implemented without exceptions. Unfortunately, we all know there will be exceptions. For example, a control vendor may need to connect to a PLC via a modem to offer technical support. As tempting as it might sound, banning non-standard connections outright is not usually feasible since the primary goal is ease of production, not ease of security. What is needed is a system that can ensure that exceptions are logged and handled by means other than the standard firewall access. For example a configuration policy and tracking system of all modem connections might be a first step. A more advanced solution might be to set up a secured remote access server attached to the firewall as a common dial-in point for all vendors [101].

1.7 Minimizing the Risks

By applying the Security Tools that were identified to the MCN an optimized MCN as outlined in Figure 10 was created.

The following high-risk items are eliminated from the MCN:

- Modems
- Programming Laptops
- Engineering Workstations
- Raw connections to the Web

Every access point has a firewall and IDS as standard. This includes:

- The Corporate Firewall for Web Access
- The SSH Servers Firewalls
- The MCN Server Firewall

The SSH Servers provides the following advantages:

- 2 Servers are provided for redundancy
- All access to the MCN with programming applications are through the SSH Server(s). This includes:
  - End User Engineers
  - OEM Engineers
  - Technology provider Engineers
- The SSH Servers have Intrusion Detection System (IDS) together with network monitoring applications, so that the overall health and status of the network can be monitored at all times.
The SSH Servers only forward the ports on the IP addresses which have been assigned to the User. This ensures that:

- The User only has access to the port on the IP address of the device(s) that they must support.
- One User cannot get access to another Users data or applications, even if they exist on the same IP address.

**Figure 10: Optimized MCN Network Diagram**

It is important to note that the MCN Network Diagram outlined in Figure 10 achieves a significant lower Threat Probability on all of the Risks that have been identified.

From a bandwidth perspective, the MCN can support 100MB and can easily be upgraded to 1GB as required. The only potential bottleneck in the MCN Network Diagram outlined in Figure 10 is the OEMs and End Users internet access speeds, but 10MB connections are now commonplace, and are more than fit for purpose.
1.8 The Business Case

The cost of developing and installing the MCN which facilitates Remote Access as outlined in Figure 10 was actually less than the cost of implementing modems on the 4 lines, thus it is justified from a hardware perspective alone, but the true benefit of the MCN in Figure 10 can be evaluated when the cost to production of solving technical issues is evaluated. Over the following sections 2 separate incidents, one without remote support from the technology provider, and one with, are compared and contrasted.

1.8.1 Incident 1

In May during the commissioning of the integral print inspection system, a serious issue was discovered by the system engineer, which meant the system could not operate at the required frequency. Given access to the system, enabled the domain expert identified almost immediately, once the expert was given access to the system. Unfortunately enormous delays as outlined in Figure 11 were experienced during this process.

![Figure 11: Fault finding process without Remote Connectivity](image)

Even though it would be safe to assume that the fault-finding process would be expedited if the equipment were in production as opposed to commissioning, some very stark issues became apparent. They were as follows:

- An extremely long time was spent evaluating the issues and providing support. Even though both of the engineers in question were very experienced, the fact that they did not have an escalation structure in place meant that they had nowhere to turn when they could not debug the issue.
- Support engineer had to attempt to emulate the problem in their laboratory, but they did not have all of the necessary equipment available, and this caused unnecessary delays.
• The expert simply was not available when the problem was finally escalated.
• When the expert was finally available and traveled to site it only took him 4 hours to actually fix the problem.

If the above issues occurred in a production environment, the cost of the issue is multiplied by a factor of 3 for each working day that passed without a resolution, due to the fact that the plant operates on a 24-hour basis. Thus the above actual problem which took in excess of 11 working days to resolve would cost 11 Days x 24 Hours x €2,100 Line Revenues / Hour which results in excess of €550,000.
1.9 Incident 2

In July there was another serious issue with the integral print inspection manifesting as an intermittent system crash. At this stage the MCN was installed as per Figure 10 it facilitated immediate remote connectivity to the technology providers with no latency involved due to traveling or trying to emulate the problem. Also it allowed the local engineer to ensure that only a small amount of time elapsed during the evaluation phase, before he requested support. The support engineer escalated the issue very quickly to the expert and on this occasion the expert had to actually escalate the issue to the system designer.

The end result was that the issue was solved in the same working day. In this instance the Expert was located in London, while the System Designer was located in Austin, Texas. If both of these individuals had to travel to site in a sequential manner it would undoubtedly result in the loss of at least 1 week’s production. Taking the initial Line Revenues / Hour of €2,100, this would result in a net loss of €382,500, without taking into account the direct engineering cost. The actual time lost of 10 hours as opposed to 168 hours represents a saving in excess of €330,000 with this one incident alone.

Other interesting observations worth noting from this issue were:

- The fact that the System Designer is located to the west of the expert means that the working day can be easily extended without any work having to be carried out outside working hours by either person.
- The MCN in Figure 10 allows multiple connections to the system being diagnosed. At numerous times during this issue all of the engineers involved were on line to the problem at the one time. The knowledge transfer and training process that this presents is not to be underestimated.
• This method of connectivity facilitates a concurrent fault finding process as opposed to the traditional sequential model.
OEM BUSINESS MODEL

During the course of this project it became very apparent that even within this single end user’s manufacturing facility; completely different OEM strategies had been adopted by the various OEMs. The product offering which was available from the IT OEMs is much more refined than the product offering which is available for manufacturing OEMs and as such provides much better equipment availability. Enormous opportunities exist for premium manufacturing OEMs to move the product offerings up the value stream by adopting similar business models to their IT counterparts.

1.10 IT Systems OEM Business Model

In this facility the IT department has engaged on a long-term, strategic, mutually beneficial, partnership style arrangement with premium, world class, IT OEMs. This has resulted in an initial procurement price with a major support component that virtually guarantees very high availability. This commitment by the end user allows the IT OEMs to invest in substantial support infrastructure which at a minimum provides a 24 hour 7 day helpline with expert support on hand, remote connectivity and diagnostics, and next day hardware replacement.

1.11 Manufacturing OEM Business Model

The engineering and manufacturing departments on the other hand had historically adopted an approach whereby the final selection of the OEM is decided by the procurement department, with the engineering and manufacturing department providing recommendations. In the absence of any other robust, quantifiable selection criteria, the default criterion that is used for the selection of manufacturing and packaging OEM equipment is price. It is not uncommon for the vendor to be selected on price alone by the end user’s procurement department, irrespective of the engineering or manufacturing department’s requests, because they cannot make a clearly defined argument for that particular vendor.

None of the OEMs on this project offered a support component as standard, but even if it were offered, it would be extremely unlikely to be procured, because this equipment is categorized as a capital item and not a service. This approach means that OEMs, have no support component in their revenue streams and can never be certain of getting the repeat business, thus investment in structured modular coding techniques as being currently defined by ISA 88.05, support services, 24 hour 7 day helpline, improved documentation, etc. are simply not financially justified at present.

The current end user / manufacturing OEM relationship can be explained by Figure 12. It can be summarized whereby the OEM has no visibility to senior management except when it is escalated by production and engineering. Their services are not seen as being critical to the end user’s business and they are simply viewed as an engineering service provider, who can be replaced or substituted at will.
Manufacturing OEMs have a unique opportunity to develop and refine their product offering so that they can re-position themselves in the market place over a very short time period. By leveraging the PackML State Model (soon to be adopted by ISA 88.05), together with a Machine Centric Software Approach utilizing ISA 99 compliant remote connectivity, and Web Based technologies, the Manufacturing OEMs can drive enormous benefits in both their own organizations and in the manufacturing environments of their End Users. This will allow them to move to the top of the value stream as depicted by Figure 13, whereby senior management can immediately see the value add service that they can offer. The business question for manufacturing OEMs is simply:

“Do you want to be selling to a person who has a budget or the people who decide budgets?”

Figure 12: Current Customer / Manufacturing OEM Relationship
Figure 13: Potential Customer / Manufacturing OEM Relationship
REFERENCES


