15th Triennial World Congress, Barcelona, Spain

TOWARDS AN OPEN DISTRIBUTED SYSTEM THAT ENCOMPASSES ACQUISITION, CONTROL AND SAFETY (ACS).

Professor George Turnbull
Managing Director / Open Automation and Control.

Abstract: Traditionally the three key areas of Acquisition Systems, Control Systems and Safety Systems have largely occupied three quite separate markets. Recently there have been developments that have created a move towards common solutions. A factor that has that has been a considerable influence in this has been the parallel move to Distribution. There are also strong moves towards Open-ness so that the Modern Integrated System is one that is Open, Distributed and encompasses Acquisition, Control and Safety. The paper elaborates on this and looks at the sort of host / target development system that is needed in the design of such systems in order for them to become widely accepted. The work in the PICSI project is then related to these needs.

1 INTRODUCTION.

This paper looks first at a brief history of what have been three different types of system – Acquisition, Control and Safety. It then looks at recent trends towards Distributed rather than Centralized Systems. Finally it examines the trend towards Open-ness which has to be accompanied by appropriate standards – either official or de-facto. These two trends could lead to a single system architecture that can encompass the three different types of system but this has to have a suitable integrated design environment that covers both host and targets in order to be successful. In fact it can be reasonably argued that the lack of such an environment has held back the moves to both Distribution and Open-ness.

The paper therefore moves on to discuss the fundamental requirements that such an environment should possess, a key factors being that people from different domains have to interact with the environment, both during development and also during use of the resulting system in different application environments. In that we are dealing with people with different backgrounds and skill levels, it is crucial that the during the development process skilled personnel with differing backgrounds can input in a way that is conducive with their training and once the system is deployed, people with lesser skills will find the system easy to install and use.

It is possible to look into each of the domains and find development packages and field equipment that fit the above criteria. The problem is that they are developed in isolation and are therefore not integrated. This integration must be achieved.

The integration of the various development packages and of the target environment is impossible unless appropriate interfaces are found. It is obviously desirable that these interfaces are standard – i.e. widely used. There are several developments in recent years that make this task possible and these are examined in the paper. Key components, each accompanied by varying degrees of standardization, are intelligent transducers, networking via the various field buses, graphical programming languages that allow sophisticated control algorithms to be fully encapsulated and the increasing use of the internet and related technology that can be successfully applied in a variety of industrially based applications.

Reference is then made to the PICSI project, which is described in detail in other papers in this session. This is aimed towards producing the sort of host / target environment that meets the criteria outlined here. In that this project is aimed at implementing a real commercial system, partners in the program include companies who can be regarded as “best of class” in their respective areas. There are three main focuses in the program, an easy-to-use method for choosing the optimal control strategy for a given plant, the development environment that integrates several packages that conform to relevant standards and a target environment based on RT Java.

Progress made so far, the planned field trials and the possible exploitation are all discussed here or in other papers. Finally consideration is made as to how to keep everything dynamic in order to cope with new technology that is relevant in the various areas.

2 THE HISTORY OF ACS SYSTEMS.

2.1 ACQUISITION SYSTEMS.

The need to gather data occurs in many different areas and has been traditionally been tackled in many different ways. This is because the needs have been sufficiently different such that a universal solution has not been possible. Let us just look at a few areas in order to understand why.

One of these areas has been in laboratories where the need is typically for high accuracy with speeds

dependent on the measured parameters. Distances are short, price pressures are not great and environmental and EMC conditions are quite benign.

Almost exact opposites occur in the so-called SCADA (Supervisory Control and Data Acquisition) Market. Here the data accuracy requirements are generally less, distances are very large (e.g. consider a gas pipeline) and both environment conditions and EMC can be severe. Data acquisition in the Factory and Process Markets cover situations between these two extremes.

The result of the above is that different companies with disparate approaches have covered these three markets. Factors that have lead towards common solutions include:

1. The development of A/D and D/A converters for the commercial market which are accurate, flexible and low cost.
2. Legislation for environment and EMC that is obligatory and although there are sometimes two levels, it really behoves any manufacturer to comply with the most severe.
3. The increasing use of the Intranet / Internet in order to allow remote viewing of data even when this is acquired in a compact area.
4. The advantages of distributed systems and the development of field buses – see later – in situations where traditionally individual wires have been taken to a central point and multiplexing schemes employed.

All of the above mean that it is possible for large companies like Siemens to produce equipment that can be used in all the above areas. The resulting volumes then make it hard for the small companies to compete beyond their specialties.

2.2 CONTROL SYSTEMS.

In process control an initial move away from centralized computer systems was reversed with the emergence of the DDC systems of the 1980's. It was the move to centralized displays which was part responsible for this apparent backwards step, but this was reversed in the 1990's with the emergence of the distributed control systems we see today.

In factory automation the move is more rapid, so-called Smart I/O is in some cases replacing traditional PLC's. This has been fuelled by field bus developments and moves to save wiring and numbers of terminals and enclosures.

One consequence of the above is that the DCS and PLC companies are now moving into each other's territories and also into the SCADA market Siemens have a common I/O for both markets.

2.3 SAFETY SYSTEMS.

The safety market is possibly the most diverse. A significant factor is that a this market has often been driven by disasters. In the process sector, the Alpha Piper accident lead to large TMR (Triple Modular Redundancy) Systems that provided a safety umbrella to the already installed DCS Systems. The need for quick action meant that this was the only viable route. In factories, the accent is largely on preventing accidents with high power, high- speed machinery. This has lead to developments like the Safety PLC. Note also the strong link between safety and high availability.

There are new sectors where safety standards are being re-examined, again largely as a result of disasters. These sectors include Transportation and Building Automation, both with recent disasters.

A generic standard, EN 61508, has emerged that is providing a new approach to safety and is leading to a generic approach plus derived standards that are tailored for the specific industry needs. One example is IEC 61511 for the process industries. This again strengthens the case for common solutions.

Again there is a move away from large centralized systems that are inherently complex to distributed solutions. For anyone who needs convincing of my hypothesis, go on a Siemens exhibition stand and see how common equipment is being used for Acquisition, Control and Safety in different sectors. However this is largely a single supplier solution – not open although often standards based.

3 DISTRIBUTED ACS SYSTEMS.

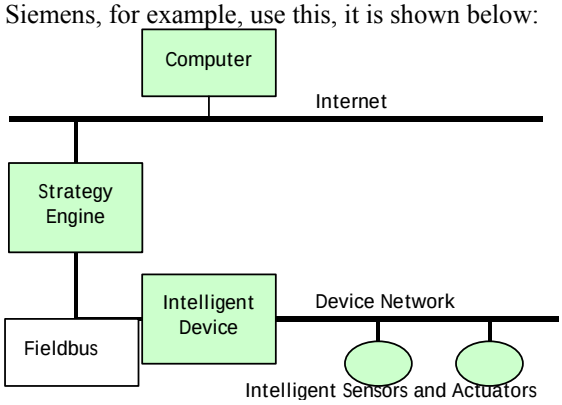
The advantages of distributed systems as far as Acquisition and Control can be summarized as:

- Significant cost savings in materials etc.
- Engineering costs significantly reduced.
- Better product through improved control.
- More effective maintenance procedures.
- Inherent reliability, safety and integrity.
- Better network technology has facilitated.

It can be seen that there are strong financial as well as technical advantages for a Distributed System. With regards to Safety most of the above criteria apply. In addition extra benefits can accrue such as:

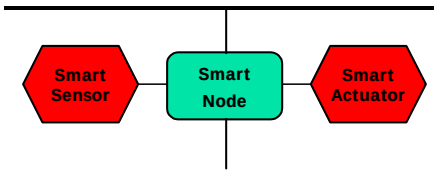
- All the arguments relative to economics.
- Principle of distributed vulnerability.
- Effect of the loss of one node contained.
- Effect of common mode failure less.
- Principle of Certified Component extended
- Nodes via "Best of Class" vendors – later.

What is the architecture commonly used in implementing Distributed Systems? The most common structure is a three-tier architecture - Siemens, for example, use this, it is shown below:



In this model, the choice of fieldbus is industry specific and also geography can be an influence. The approach to Safety must follow this – e.g. ProfiSafe. The disadvantage, apart from technical considerations is that the combined solution is not universal across applications and across countries.

A World -wide / Industry-wide solution is possible if we collapse the architecture. Three-tier architecture can be collapsed into two-, or in the limit, one-tier. A single tier architecture based on (Industrial) Ethernet is technical feasible:



There are now solutions to all the problems that prevented the use of Ethernet as a control network see later. It is also feasible to use it in a safety application. The key elements of a Modern Distributed System are practical implementations of:

- The Smart Transducer- sensor/actuator.
- The Strategy Unit with embedded control, embedded web server and relevant services.
- Enhancements to the Intranet / Internet – to embrace Acquisition, Control and Safety
- Standards that will address the total problem.

The other significant move, referred to above, should be considered at this time. This is the move to Open Systems. This is becoming a very strong move and the two main reasons are summarized below:

- Do I want to avoid being totally dependent of a single source of supply?
- Do I want the ability to choose 'best of class components' for my process?

▪If the answer is positive for both questions, this is the reason to look at Open Systems. To implement a strategy requires careful choice of standards

What then is involved in this careful choice of standards? We need to look into each of the areas listed above – Smart Transducer, Strategy Unit, Safety Considerations and the Internet and Intranet Networks. The solutions are still not fully clear but let us look at some possibilities and see whether sensible choices can be made and if some extra research is applicable.

Firstly, considering the key elements outlined, let us look at a list of possible standards:

- Smart transducers: IEEE 1451, SEVA.
- Strategy engines:
  - Programming: EN 61131 well accepted
  - Target Code: Real Time JAVA.
  - Web/Enabled: OPC, Browser, XML.
- Safety Issues: EN 61508 acclaimed.
- Intranets/Internets Obvious base but many issues e.g. Messaging and Safety to solve.

Let us examine these items in turn. Firstly the IEEE 1451 standard for Smart Sensors that was initiated by NIST. The key features are summarized below:

- Network-independent standard.
- Two parts which can stand-alone.
- 1451.1 Network Connectivity.
- 1451.2 Smart Transducer Definition.
- It defines the STIM, its TEDS and the TII.
- Many forms of packaging are possible

Now consider the SEVA standard. This is based on work done at Oxford University that is sponsored by the Invensys Group. Sensible strategies are needed if sensor data is unreliable. The key features of the SEVA sensor (the actuator is similar) are:

- Performs fault detection using full expertise of senior designer of the device.
- Corrects each measurement as required.
- Assesses full validity of each measurement
- Described in device - independent terms.Sensor no longer just generates a measurement, but also assessment of quality

The focus of the work at Oxford is to keep the plant operating, possibly at reduced efficiency, if the quality of measurement is diminished. The analogy that is used is that of the "limp home car". Although safety is not at the moment being considered, the researchers recognize that the information available can be used for safety purposes. This could be a valuable extension to the work and is being discussed.

Now let us look at the programming language specification, EN 61131-3 for programming

strategies. The key features are:

- Supported by major DCS and PLC vendors.
- Central to the Open Control movement.
- Vendor independent courses - varied skills.
- Choice of languages - SFC, FBD and ST.
- Interest in JAVA/RT-JVM as 'back-end'.
- Complex Sequencing implemented via SFC's

Some key extensions to EN 61131-3 are proposed in the relatively new standard IEC 1499. These extend the function block model in two areas:

- Allows for multiple nodes, i.e. networking.
- Allows for event driven/triggered models.

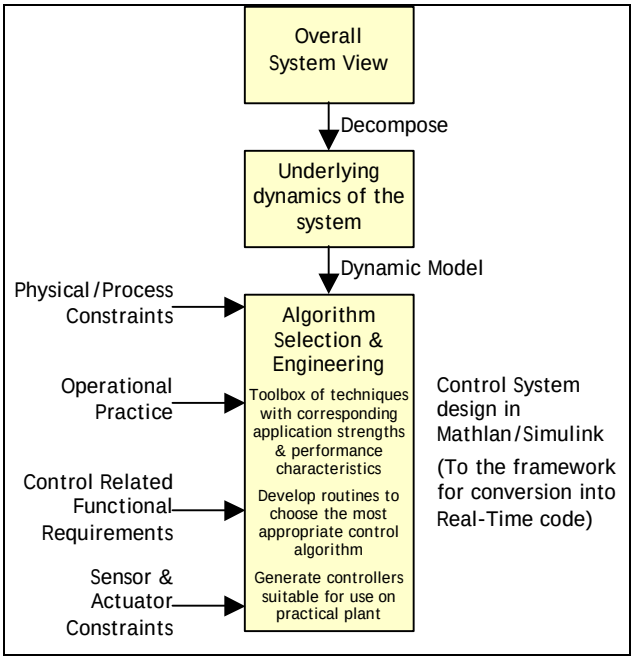
These are two very important extensions, although the workarounds can be devised for implementations do not include these extensions.

Another extension, that should be considered, is the use of Java rather ST or IL as the output. Some of the reasons for this choice are given below; the most powerful is the rapid increase in Java as a programming language and WORA (below).

- It is now extremely widely used.
- Therefore many trained Programmers.
- WORA – Write Once Run Anywhere.
- Structured with strong data typing.
- Object-Oriented with encapsulation.
- Problems that relate to real-time.

As far as Host / Target development, the usual model is to develop under, say, Windows NT or Linux, and for the target code to run on a JVM (Java Virtual Machine). The main problem to be solved for real-time applications is achieving the determinism and overall performance that is needed. There are two groups drawing-up specifications and moving towards Beta-Site testing – details are given below.

At this stage, we need to consider Control in more detail. EN 61131 obviously provides a good environment whereby a process engineer can put together strategies based on modern control algorithms. In order for the control engineer to develop these, however, requires an environment like the one shown below:



Also if the code is to be certified against SIL levels, it should be developed in a modern CASE environment. One based on UML has many advantages, such as:

- UML is extremely well accepted.
- Therefore many trained people.
- Rich set of notations and semantics.
- Applicable to a wide set of modeling.
- Used in a wide range of domains.
- The safety community favors it.
- The main problem is again Real-Time.

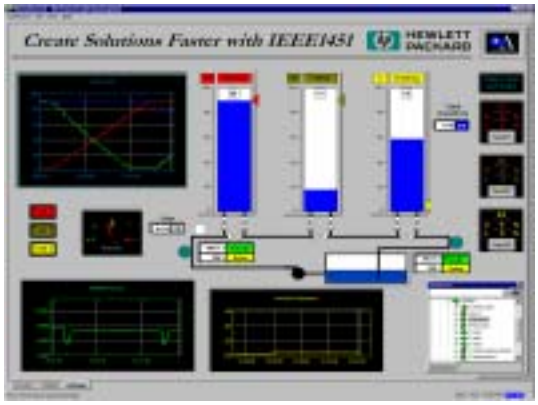
We have already outlined how IEC 1499 allows the use of IEC/EN 61131-3 in a distributed system. We have also shown how attractive a one-tier model is and suggested Ethernet as the network.

The standard commercial versions of Ethernet are generally unsuitable for real time / determinism. The factors, listed briefly above, that make this possible are:

- Industrial Ethernet receiving much interest
- It can be used at all levels in the hierarchy
- Inherent problems of determinism soluble.
- Redundancy exists–safety version possible.
- 10 and 100M versions - soon to be 1GByte.
- Riding on back of commercial technology.

Let us look at those in more detail.

Since Industrial Ethernet is receiving a lot of interest, various companies like Hirschmann are providing solutions based on today's technology. These involve the use of smart switches and routers that can give guaranteed timed of delivery. One fundamental principle is to segregate IT related and real time traffic. The only downside is that these solutions tend to be complex and costly, eating away at the obvious benefits. However the achievement of a one-tier solution is still present. However there is an extension to the standard that addresses the problem of determinism – IEEE 802.1p. This allows system designers to prioritize messages, guaranteeing the delivery of time critical data and thus giving deterministic response times and repeatable results. Also some suppliers have developed solutions using proprietary code residing above the standard TCP/IP stack – see below. The problem of redundancy is being tackled in the same way. The extension to the standard is IEEE 802.12. This provides the ability to add redundant links to the network to facilitate automatic recovery of network connectivity when there is a link or repeater failure anywhere in the network path. In the mean time there are proprietary solutions from companies like Hirschmann. The move to 1 GByte also helps tremendously in achieving high speed so again we are benefiting from advances in commercial technology.
The use of Ethernet allows us to Web-enable the various strategy nodes and the sort of thing that is possible was shown at the ISA show where IEEE 1451 was first launched. The key feature of the demonstration was self-declaration. A browser screen is shown below:



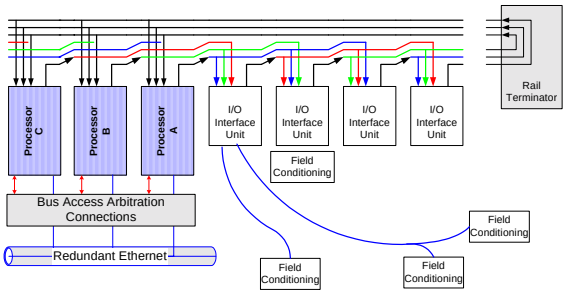
It was at this show that Hewlett Packard showed their implementation of deterministic Ethernet. This allowed synchronization across nodes to around 200 ns. Details can be found on their web site www.hpie.

Thus there are no technical reasons why Ethernet cannot be used for real time applications – proprietary solutions exist today and extensions to the standard are well underway.

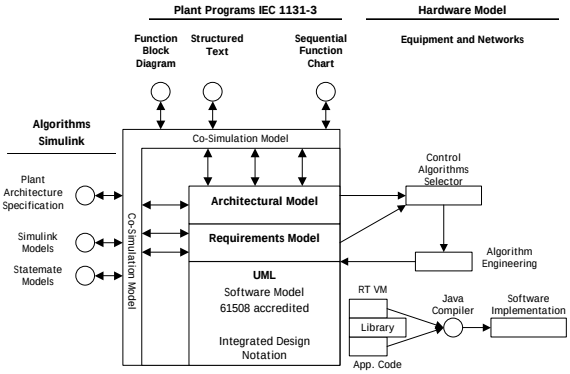
The strategy engine can take many forms, DCS node, PLC or more recently intelligent I/O. The picture below shows a recent example of such a node that

can be used in IS applications:

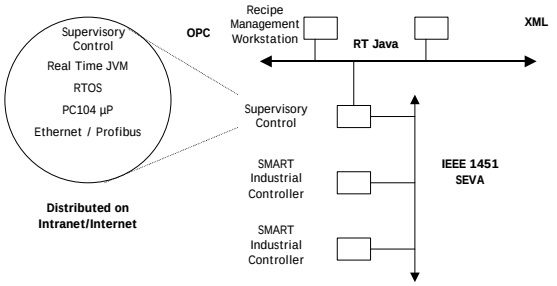
Work is underway to allow this node to be enhanced so that both dual and triple redundancy can be added to the node with virtually no extra cost in the simplex node. It can thus embrace Acquisition, Control and Safety. The scheme is shown below:



Now to the PICSI project described elsewhere in this session. The Environment Architecture is shown below.



The target architecture follows the collapsed model and is shown below:

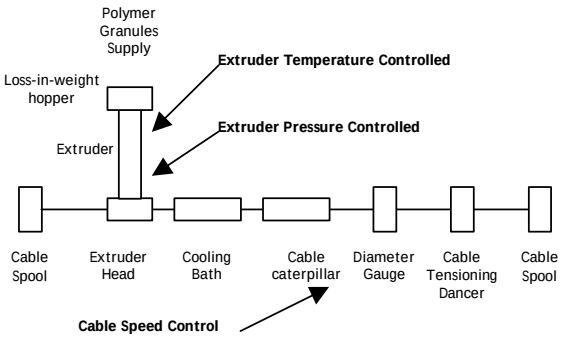


Now a few words about RT Java – this is covered in detail in another PiCSI paper. Once again, as with Ethernet there are proprietary solutions today and two standards initiatives that will hopefully converge.

The proprietary solution that has been investigated in the project with some success, provided that care is taken in choosing the right software architecture, is a clean room implementation from NewMonics. This overcomes problems like garbage collection in novel ways.

The two standards bodies are the Real-Time For Java Experts Group (RTJEG) and the J-Consortium. The development of the RTJEG specification initially laid down a number of guiding principles in order to delimit the scope of work and to introduce compatibility requirements. The standard is now in draft form and reference implementations are available. The J consortium has taken a similar approach and moves are underway to bring the two together.

The intended field trial, a representative production line, is shown below:



Does the project have relevance to safety? Although there is no work at present, it is clear that extension is sensible; the environment that is being produced will give highly reliable products embracing both hardware and software. It lends itself to expansion to be compatible with that needed to achieve SIL certified products. In fact this is core to the concept of developing Open Distributed Systems embracing Acquisition, Control and Safety

4 CONCLUSIONS/FUTUREWORK.

This paper has argued the case that the sensible way forward in Integrated Systems is Open Distributed Systems that encompass Acquisition, Control and Safety. This is evidenced by moves in the industry giants like Siemens to achieve this in a way that is not fully open. However, as with DCS, this would be a one-step forward, two-step backward since it reverses the trend to Open-ness. This is imperative for worldwide acceptance in a range of applications.

Open-ness allows for contribution from many experts in various fields/domains – this has similarities to the Open-source movement.

The work within the PICSI project points the way forward and is supported by companies who are both best of class and who are interested in promoting Open-ness. The key feature is that it provides an integrated environment for people from different domains to operate in and it is in touch with other key research in the various areas. Also through the Industrial Partners there is a good chance of Commercialization.

REFERENCES

IEEE 1451. Key web site www.ic.ornl.gov/p1451/: various specifications and articles.

SEVA. IEE Colloquium – Intelligent and Self-validating Sensors. June 21 1999. Also published standard BS 7986.

EN 61131-3. Book by Lewis, R.W. – "Programming industrial control systems using IEC 1131-3". IEE Publications 1995.

IEC 1499. Book by Lewis, R.W. - "Modeling control systems using IEC 61499". IEE Publications 2001.

JAVA. Good web site www.ddj.com/articles/2000/0002/ Information in RT Specification for JAVA.

Simulink. Company web site www.mathworks.com also contribution to UK Conference/ Nottingham by PICSI team.

UML Moore, A. Real-Time UML, Embedded System Journal, December / January, pp. 48-49.

INDUSTRIAL ETHERNET. Web site. www.iaona-eu.com/ Industrial Automation Open Networking Alliance.

EN 61508. Special Feature on Software Safety. IEE Computing and Control Engineering Journal. Feb. 1998.

INTERNET. "Monitoring and Control by Internet 2". Conference Proceedings. ERA Report 00-2000-0494.