Nuclear Control Systems

Seeking Obsolescence Tolerant Replacement C&I Solutions for the Nuclear Industry

Issue	1
Date	September 2007
Publication	6th International Conference on Control & Instrumentation: in nuclear installations

Ultra Electronics
NUCLEAR CONTROL SYSTEMS
Innovation House, Lancaster Road
Ferndown Industrial Estate, Wimborne,
Dorset, BH21 7SQ

+44 1202 850450
www.ultra-ncs.com
www.ultra-electronics.com

Contents

1. HISTORY 3

2. OPTION STUDIES 4

3. FINAL COMPONENT TECHNOLOGY CHOICE 5

4. CIVIL NUCLEAR APPLICATIONS 7

5. WAY FORWARD 9

1. History

The existing Reactor Control and Instrumentation (RC&I) equipment for the Vanguard and Astute Class platforms in the UK submarine fleet was designed in the early 1980s, using CMOS 4000 series logic, 16-bit processors and discrete analogue components. Of its time, the system was “leading edge” and the underlying component technologies proved to be stable and well supported during the systems lifetime until the late 1990’s when the CMOS 4000 series began to be phased out.

A cornerstone of the safety justification for the system was a lifetime justification for the electronic components, based upon theoretical predictions and accelerated life testing. With the justified component lifetime running out and the availability of components to re-manufacture the system rapidly diminishing there was real need to develop a replacement system.

During the mid1990’s the customer initiated a series of studies into new and innovative instrumentation architectures, component technologies and design processes. As part of this work, it was recognised that their existing subcontractor base had limited experience with the technologies and processes being identified in these studies. They therefore began looking for a new partner to support the detail design and implementation work. In autumn 2000, The customer approached Ultra Electronics, an established supplier of electronic systems in the defence and civil aviation market sectors, whom they had identified as having the required skill-set.

2. Option Studies

After an initial joint programme of work to develop the new innovative RC&I design concept and once the full development costs had been established, the decision to adopt a lower risk (and lower cost) option based on a more conventional architecture was taken.

At this point, COTS solutions were briefly considered but these were quickly ruled out for a number of reasons including:

a) The level of design disclosure from the COTS suppliers to support the required safety analysis

b) The availability of COTS products to support some of the legacy sensor interfaces

c) The ability of COTS solutions to provide the required level of accuracy

d) The ability of some COTS solutions to fit within the existing space envelope

e) The uncertain lifetimes for the COTS products

f) The ability to control and justify the manufacturing techniques used on COTS products – particularly with the move to lead free solders.

Having established that a bespoke design solution was the only viable option a number of architecture concepts were evaluated. It was eventually decided to implement a rack by rack technology refresh, preserving many of the features of the original architecture. The benefit of this approach was that it resulted in minimal disturbance to the form of the existing safety case. However, there remained a concern over the future stability of the underlying component technology.

3. Final Component Technology Choice

The component marketplace is now dominated by the telecommunications and personal computer industries that have short product lifecycles and are constantly striving for smaller and more high-performance products. This leads to shorter product lifetimes, migration to smaller packages and component die shrinks. In addition, although military equipment is technically exempt from the movement to lead-free solder under the RoHS and WEEE directives, the defence community is no longer a significant enough player in the marketplace to influence the component manufacturers who, at the time of the study, were moving away from tin-lead compatible package types in preparation for the implementation of these directives. This led to a concern that whatever technology choice was made it would not be supportable in the long term.

After much thought and discussion a decision was taken to insulate the design from the changes in the component marketplace by implementing two strategies:

1. Digital design would be implemented in FPGA technology programmed in VHDL using a rigorous development process originally developed by the customer. This was a means of separating the digital design from the technology, making it transportable to newer devices and technologies.

2. The majority of the analogue design, bus interface devices and memory devices would be implemented inside hybrid devices, with components stockpiled in die form under a controlled environment. Hybrids were chosen because they were a long established fabrication technique that would be continued to be used for the foreseeable future in niche applications (e.g. avionics). Even so, the design process was constrained to ensure that manufacture was possible by a number of companies. This approach provides a high degree of insulation from the rapidly changing component marketplace and assures the ability to manufacture the components well into the future. It also gave the added benefit that some parts of the legacy design could be leveraged and enhanced in a supportable technology.

An example of the cards and hybrids produced using the above approach is shown in Figure 1 and Figure 2 respectively.

Ultra Electronics are now working with the customer are to design and integrate over 25 card designs of this type. As part of the design process, the component types used are being minimised through the use of a common component database, thereby rationalising the component stockholding required. Reliability and lifetime justifications are being produced for each component, supported by in-service evidence, die inspection and, where necessary, accelerated life testing. This gives high levels of confidence that the availability targets for safety functions will be met and that the stockholdings are adequate.

Figure 1: Example Card

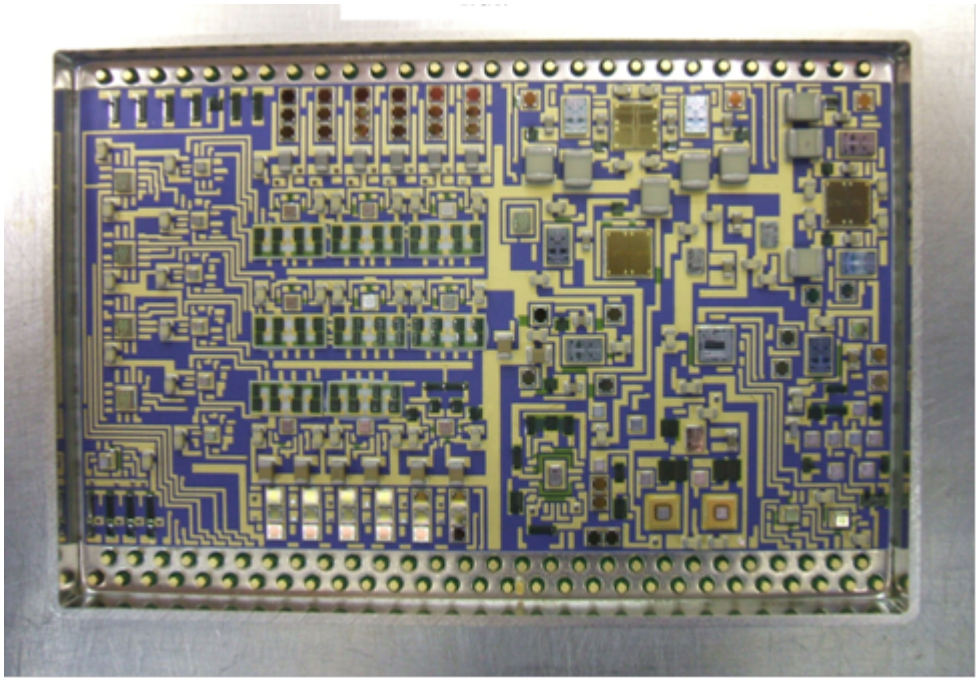

Figure 2: Example Hybrid implementation

4. Civil Nuclear Applications

More recently Ultra Electronics has become involved in looking at replacement solutions for Civil Nuclear operators in the UK. Although not subject to the same space constraints as the submarine applications many of the issues are similar. In particular:

a) A significant proportion of the components in use within current systems are now obsolete

b) While not subject to lifetime limits, component ageing is becoming a concern, particularly in the context of station lifetime extension programmes.

c) Design disclosure from COTS suppliers for replacement equipment is often inadequate to provide a robust safety justification.

d) COTS products are subject to peremptory change and have an uncertain lifetime

e) COTS products sometimes fail to provide the required accuracy and electrical isolation.

Moreover, with the drive for increased performance, modern processors are becoming more complex in their architectures, allowing concurrent and out of order execution of instructions. This makes the execution of software on modern processors difficult to justify and complicates the worst case timing analysis. In the future, processor architectures may also become re-configurable to cope with the decreasing reliability of the underlying silicon, further complicating any analysis.

Many COTS suppliers make claims of compliance with safety standards, but as standards vary between different industries (e.g. Rail – EN50129, Aviation - DO178B, Defence - Def Stan 00-56, Process - IEC 61508), this can create a confused compliance picture when trying to compare products, with little accepted wisdom or guidance. The UK nuclear industry has aligned with IEC61508 along with the process industry and nuclear specific interpretations - IEC61511 and IEC61513. The industry requires a high level of assurance that these functional safety standards have been complied with. However, these standards have only achieved widespread support in the Programmable Logic Controller (PLC) marketplace and some instrumentation applications.

Relative to other parts of the electronics industry, PLC manufacturers are geared to lower volumes and stable product families with long term support. Third party accreditation to IEC61508 has been achieved by a number of manufacturers, but it is generally only applicable to a sub-set of the functionality offered by their products. In addition, many of the current PLC products incorporate elements of legacy systems, that pre-date modern safety standards, hence, compliance arguments are often complex.

The UK Nuclear Industry is not a significant player in the PLC marketplace but is insistent on the provision of design documentation and qualification evidence rather than accepting third party accreditation. In many cases, the evidence provided by manufacturers has been deemed inadequate to the extent that some engineers are now down-grading the claimed SIL ratings by 1 or even 2 SIL levels for nuclear use. This approach has been perceived as a threat by some COTS suppliers to their mainstream business, both in terms of IPR and

reputation, and has made them more guarded about the information they are prepared to disclose. This leaves the UK Nuclear Industry struggling to assemble adequate justification evidence for COTS systems and in some instances has lead to complete project failure.

Alternative system options are available, particularly for more mainstream processing, primarily from flight critical applications the avionics sector. However, the products are expensive and the read across from the standard certification packages (e.g. for DO178B compliance) into the nuclear industry appears largely un-proven.

Bespoke solutions designed in accordance with the IEC61508 process are possible but are expensive when approached on a single system basis. They also lack the operation history of the COTS products, although it could be argued that, with frequent upgrades and the availability of software “patches” for download, the operational history claims on many COTS products are difficult to justify.

It should also be remembered that replacement systems are subject to the full rigour of modern standards, which were not in place when the original C&I infrastructure was put in place. In many cases the underlying architecture of the original system is not compatible with modern standards either in terms of redundancy, diversity or product integrity. This makes like-for-like replacements unsuitable and leads to significant difficulties in establishing the necessary architecture and safety requirements for replacement systems.

Faced with the increasing difficulty and cost of specifying, procuring and justifying new systems within the UK regulatory environment, though there have been some significant programmes, investment in replacement C&I equipment is limited and overspends are common. The C&I infrastructure within the UK therefore continues to age, with a proportion of investment directed towards stabilisation and refurbishment, targeted on areas where technology still exists or minimum change solutions can be determined. Operating risk in the majority of areas, therefore, continues to grow.

5. Way Forward

The majority of C&I equipment within the UK Nuclear Industry is not functionally challenging for modern electronics systems, but qualification and safety justification is causing significant difficulty. Clearly, this issue is not going to be solved on a single project basis. The nuclear industry needs to accept that its influence in the marketplace is limited and target its investment to obtain the maximum leverage and benefit. One way of doing this is to identify the key technologies required for future equipment replacement programmes and focus its investment on these. There are three approaches for achieving this, all of which may be valid dependent on the technology under consideration, which are to:

a) Work with key COTS suppliers to generate the justification evidence required for selected items from their existing product ranges, accepting that there may be limits to the evidence available and placing greater emphasis on the valid operational history of the product.

b) Commission customised “cut-down” versions of existing COTS products which are easier to justify, recognising that this largely invalidates any operational history.

c) Commission bespoke products which can be developed from the start with nuclear qualification and use in mind, using simpler architectures that are easier to justify. These products can also be designed with long-term support in mind.

In this environment, the customised and bespoke solutions become economic, as the cost of development and qualification can be spread across a number of programmes. However, whichever approach is adopted for a key technology, there must be a clear understanding of the level of evidence required to support its generic use at a specified integrity level across the UK nuclear industry.

For such a “key technology” focussed approach to be a success will require partnerships between operators and suppliers, as well as close liaison with the regulator. This focus of investment on a small number of common equipment items should provide sufficient influence to obtain greater co-operation from key COTS suppliers. Moreover, the widespread use of common equipment in the nuclear industry will provide the user-base to maintain stable product baselines, gather credible operational statistics, retain supplier support and implement controlled obsolescence management programmes.

The safety justification of modern electronics is currently a difficult process and is still the subject of academic debate. Some research work has been funded in this area by the nuclear industry (e.g. through the CINIF programme) but it is very limited and has so far failed to provide practical guidance that is widely available to industry. In view of the limited adoption of IEC 61508 by COTS manufacturers, there appears to be a need to review the current heavy reliance on placed on design process evidence against the more test orientated approaches used in other market sectors e.g. avionics. Indeed, more flexibility to justify products from other market sectors, particularly at the lower SIL levels, would yield significant benefits in terms of the range of products available.

Where specific design methodologies are preferred for the nuclear industry that are not in widespread use, there may be a need to invest in tool development and training to establish

these preferred methodologies in the supplier base. There may also be a need to invest in the generic capability of key suppliers to grow their ability to produce designs of the required integrity and design assurance.

Unless a more pragmatic approach can be found for C&I equipment qualification and justification, the infrastructure in the UK will continue to age and the C&I design capability to atrophy. If investment continues to be directed towards refurbishment and stabilisation programmes rather than to developing replacement solutions, many of the benefits offered by modern technology will be lost to the industry and, without new equipment, ALARP arguments will not be advanced. Moreover, this piecemeal approach will not reduce the operating risk significantly; and, the lack of investment will deprive the nuclear industry of suppliers that are capable of developing and justifying safety related C&I solutions.

Ultimately, with the advent of new build plants, new C&I equipment will need to be introduced into the UK. If there is no proven UK supplier base for such equipment, it is likely that it will be sourced outside the UK as part of a complete reactor “package”. The justification of such equipment may place significant emphasis on its operational history in other countries and may be subject to significant political pressure. The remaining UK supplier base will find difficulty in establishing significant participation in the new C&I infrastructure, further diminishing the skills base available in the UK to support nuclear operations and leaving longer term system support in the hands of overseas organisations.