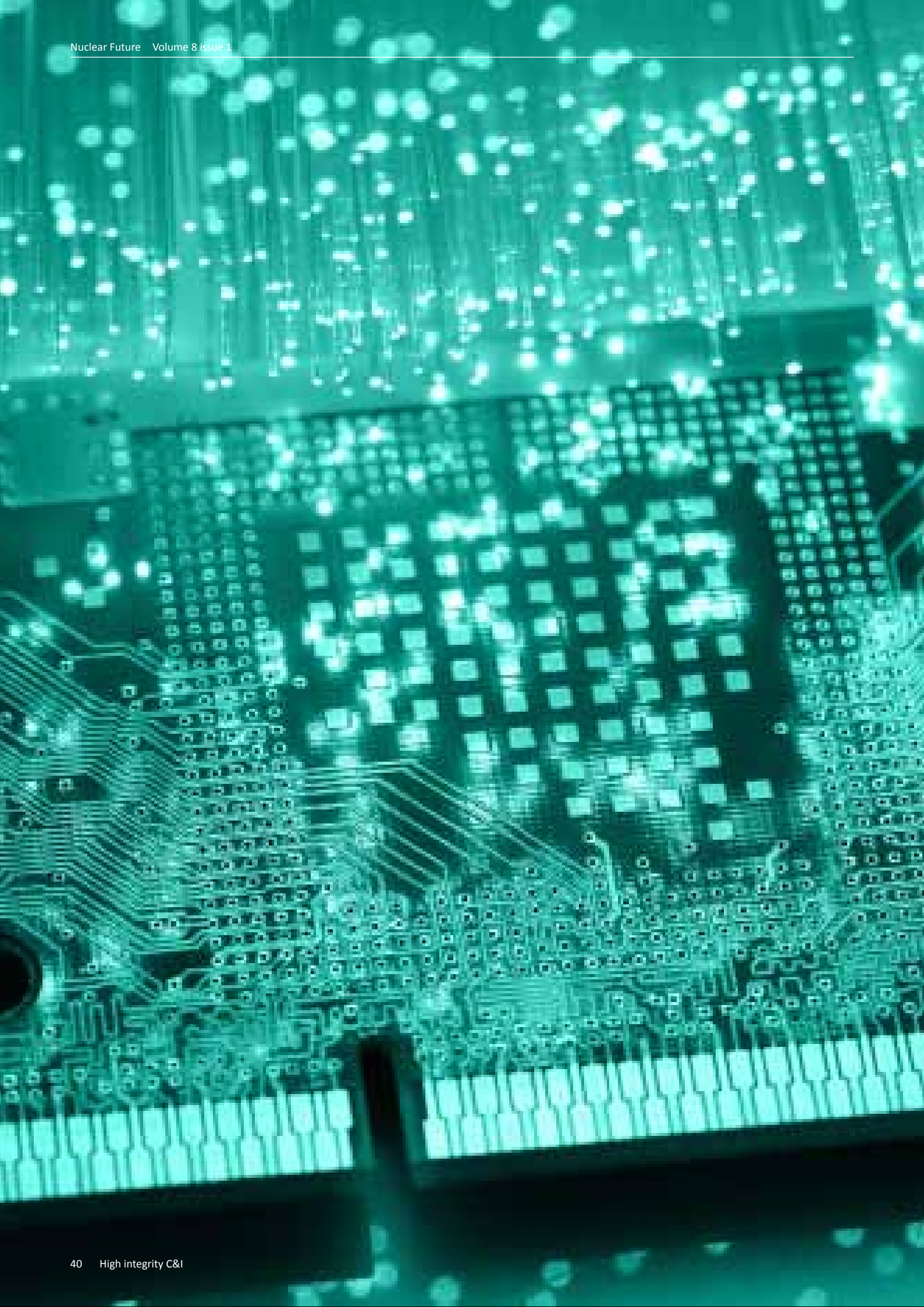

Key threats and issues for high-integrity C&I

Jim Thomson looks at the major issues facing operators, designers and regulators of high-integrity control and instrumentation

This paper presents an overview of some of the fundamental concerns that affect operators, designers and regulators of high-integrity control and instrumentation (C&I) at the present time. The selection of 'key threats and issues' is personal but, I hope, non-controversial. Several of these are not new, but are long-standing matters that just refuse to go away.

The issues have been separated into three categories, as follows:

- Standards, regulations and licensing
- Equipment life and C&I upgrade projects
- Illegal activity

The views expressed are strictly personal and do not reflect any of my current or previous affiliations.

Standards, regulations and licensing

Lack of clarity and consistency in national and international standards

There are two parallel, broadly consistent sets of international standards – the IAEA/IEC standards (notably IAEA 1095 and 1116, and IEC 61508, 61513, 60880, 62138 and 12207) and the NRC/EPRI/IEEE standards (notably IEEE 1012, 1074 and 7-4.3.2), see Figure 1.

IAEA standards try to reflect a wide range of national practices, sometimes without making unambiguous recommendations. IEC standards set out to be clear and unambiguous and global in scope; however, in the USA, the Nuclear Regulatory Commission (NRC) uses IEEE standards and EPRI guidelines for reactor protection software. Both sets are broadly comparable in scope, but there are some significant differences, e.g. IEEE requirements for high-integrity software are less onerous than IEC 60880, especially for pre-developed software.

The existence of these two sets of standards causes difficulties for vendors, and the world marketplace is split for some vendors into 'USA/China' and 'everywhere else'. This is inefficient and anti-competitive.

Further ambiguity arises from, for example, the UK's nuclear regulator which imposes more restrictive SIL band definitions than IEC 61508, i.e. this represents a 'UK only' overlay. Also, there is WENRA (the Western European Nuclear Regulators' Association), which has its own guidance on reactor software, but the French regulator ASN is not a signatory.

This confusion has manifested itself recently in the submission by EDF Energy/Areva of a C&I architecture for the UK EPR which was unacceptable to the UK regulator.

The worldwide nuclear industry would benefit greatly from international standards that are accepted and unambiguously applied in all countries. One approach would be a short, simple 'meta-standard' for reactor protection, e.g. just to say that:

- control and protection shall be separated;
- diverse reactor protection shall be fitted, one of the diverse systems shall be hard-wired; and
- control and protection systems reliabilities shall be commensurate with ensuring that risk criteria are satisfied.

Restriction of Hazardous Substances (RoHS) regulations

UK RoHS regulations came into force in July 2006, and are enforced by the National Measurement Office *www.bis.gov.uk/nmo/enforcement/rohs-home*. These regulations are, among others things, seeking to stop the use of lead-based solders, which will affect the safety justification of electronic equipment in at least three ways, namely:

- affect the manufacturing processes;
- non-lead-based solders can be more brittle than lead-based solders, which may affect shock resistance and seismic withstand capability; and
- tin-based solders (the favoured substitute) can lead to the generation of tin whiskers that may cause short circuits and unpredictable failure modes. See for example *http://nepp.nasa.gov/whisker/* and *www.calce.umd.edu/tin-whiskers/whiskermovies.htm* (see Figure 2).

Many consumer products such as Apple iPod, Nintendo Wii, some mobile phones and some laptops are already RoHS-compliant, so these issues are clearly not insuperable, at least for equipment with relatively short life spans.

In the nuclear industry, safety justification for the replacement of old (lead-based) components with new (RoHS-compliant) components will require careful consideration, because licensees will have to adhere strictly to their configuration management and management of change procedures.

Licensees will be dependent upon suppliers to provide clear notification when components are changed to RoHS-compliant versions, and the suppliers may also be asked to provide safety case evidence of fitness-for-purpose. It is possible to test components from suppliers for RoHS-compliant solder using X-ray fluorescence, e.g. *www.niton.com/RoHS-Compliance-Hi-Rel.aspx?sflang=en*.

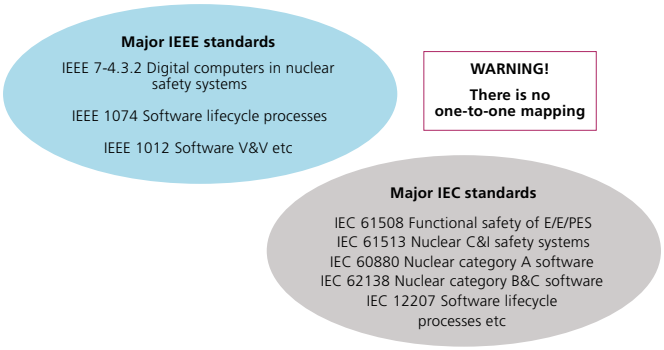

Figure 1: *IEEE and IEC standards*

Figure 2: *Human Hair vs. Metal Whisker: Metal Whiskers are commonly 1/10 < 1/100 times thinner than a human hair!*

Intellectual property rights (IPR) vs. independent safety assessment (ISA)

ISA is an essential part of the process of safety assessment and licensing for high-integrity nuclear systems. IPR requires there to be clear, binding confidentiality agreements between the supplier and the assessor. Notwithstanding this, however, some suppliers continue to be apprehensive and restrictive in the way they will deal with companies performing Independent Safety Assessment (ISA) – particularly if the ISA is being done in another country. Suppliers need to approach ISA in a positive way, provide adequate information, and deal with the people doing ISA in a positive way.

Operators and regulators have a role to play here, since they can bring pressure to bear on the suppliers, via their contractual arrangements, to encourage openness with the ISA contractor.

Equipment life and C&I upgrade projects

IC feature size

Feature sizes of 30nm or so are now being achieved, and 10nm feature size is predicted by 2015. It is likely that these ICs may suffer diffusion-induced failures, which may be highly unpredictable in their failure modes, within a few years of manufacture. Hence they will be unsuitable for high-integrity applications in the nuclear industry.

Manufacturers and licensees will have to consider mitigating strategies to cope with this problem. Such strategies could include:

- Bulk storage of spare components – so-called 'die-banking'. In order for die banking to work effectively three things need to happen: the customer needs to be informed with up-to-date product obsolescence information; the die banker needs to make the necessary 'last time buys' required to stock enough product to service the lifetime of the project; and, lastly, the product needs to be managed and stored appropriately in order to guarantee yield and maintain quality. See for example *www.ue.com.hk*.
- A specialist supply chain may yet evolve for long-life ICs using larger feature sizes of the order of 100nm or more in order to achieve lifetimes of say 20 years or more. This option may be expensive!

Through-life support vs. product life-cycle and power station lifetimes

Older stations are having their lives extended to 50 or more years, and new stations are being designed with lives of 60 years. However, power station control equipment (DCS, DPS, SCADA) may require complete replacement after only 15 to 25 years, and such replacements have been shown to be difficult – budgets and timescales are rarely met. Either (a) suppliers should try to keep older products available for a much longer timescale so that like-for-like replacement of components is achievable indefinitely, or (b) new power stations should be designed to facilitate changeover of DCS equipment, or both.

This issue is clearly related to the IC feature size issue above. The most realistic option is (b) since the nuclear industry is unlikely to have full control of the supply chain. New power stations and other plants should be designed to facilitate changeover of major C&I equipment, e.g. by having dual terminations for major components installed during initial construction, with suitable spare space available, so that mid-life C&I refits can be carried out in a much more simple and structured way.

Backfit project risks

Around the world, the record of major C&I backfit/digital upgrade projects (to replace power station DCS/DPCS/HMI systems) has been poor. Projects run late and significantly over-budget. The reasons for this are varied but can include some or all of the following:

- insufficient recognition by senior management (of both the utility and vendor) of the project risks – especially licensing risks – leading to insufficient vigilance at all stages of the project;
- inadequate safety functional specification (including control loop functionalities and Safety Integrity Levels) by the utility before the prime contract is let;
- inadequate assessment of available technologies before selection of the main candidate technology;
- insufficient recognition of the significance of the evolution of C&I/software standards since the power station was first commissioned;
- inadequate recognition by vendors of the extent to which their equipment SIL claims will be tested by licensees and regulators; and
- the complexity of backfit projects:
  - compliance with gated project management arrangements (such as PRINCE2 or FELGATE);
  - compliance with IEC 61508-type C&I lifecycle arrangements;
  - full understanding of the design basis for all the C&I equipment to be replaced (thousands of I/O and full HMI replacement);
  - compliance with the necessary design, manufacture,

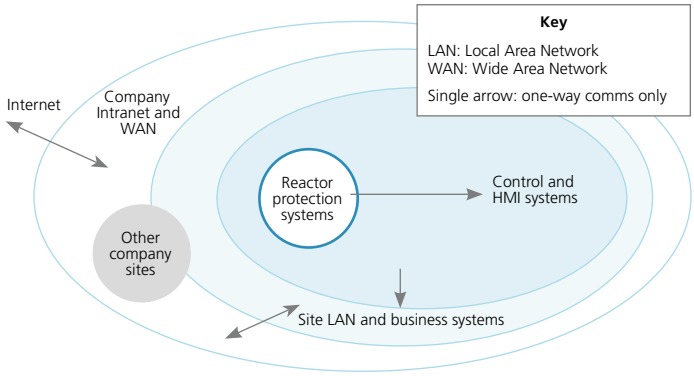

Figure 3: *Nuclear control and protection equipment must be designed and operated to avoid exploitation of any weaknesses in the software being exploited*

> "The worldwide nuclear industry would benefit greatly from international standards that are accepted and unambiguously applied in all countries"

installation and testing standards consistent with the required Safety Integrity Levels; and
– limited plant access to operational plant during station outages.

The way ahead seems to lie with some or all of the following:

- designing power stations to facilitate mid-life backfits (e.g. by installing dual terminations);
- the preparation and agreement of a high-level best-practice 'roadmap' for C&I upgrade projects in cooperation with the regulator;
- adequate resourcing of the project preparatory stages by the licensee; and
- adequate recognition of project risks by both the vendor and the licensee.

Illegal activity

Stuxnet worm

The Stuxnet worm is a 'game-changer' – weaknesses in the software of industrial control equipment have been exploited in a way that should cause all operators, designers and regulators to be worried.

Stuxnet used 'zero-day' weaknesses in Windows to attack Siemens Simatic controllers at an Iranian uranium enrichment plant. The Siemens units controlled centrifuge motors. The affected controllers caused the motors to run at the wrong speed while simultaneously sending signals to the SCADA systems to say they were operating at the right speed. Stuxnet was probably developed by a team of software engineers working for the Israeli government, possibly with US assistance.

Prior to Stuxnet's discovery, operators and equipment suppliers might reasonably claim that cyber-security was 'merely' a matter of ensuring adequate protection against solitary hackers, each working in complete isolation.

After Stuxnet, that viewpoint no longer has validity; nuclear control and protection equipment has to be designed and operated from the perspective that teams of highly organised software experts may be trying to exploit any weaknesses. In particular:

- firewalls must be maintained and be absolutely robust; and
- use of Windows-based equipment of any sort, in any nuclear safety-related applications, will require careful consideration and justification.

See Figure 3.

Counterfeit components

A circuit breaker where there is no switch, just a short between input and output, is a typical instance of a counterfeit component. Other examples include 'copper' cables where the copper content is much diluted. The author has even heard of complete fake sub-systems being supplied, from apparently reputable suppliers, with apparently kosher QA paperwork.

This problem is unlikely to go away, and indeed it will probably get worse. The lesson here is *caveat emptor*, especially when buying on the Internet: if you buy cheap you will get nasty. Be sure to use reputable suppliers, even if they are not the cheapest, and try to get as close to the source of the supply chain as possible.

Jim Thomson PhD, FIET, FIMechE, FNucI

Jim Thomson's background includes nuclear plant operations, R&D, design engineering, safety management, business improvement and safety consultancy.

After completing his PhD studies in process engineering at Aberdeen University, Jim started his career in 1979 at the Prototype Fast Reactor power station, Dounreay, before joining NNC (now Amec Nuclear) in Knutsford to develop safety cases for Heysham 2/Torness nuclear power stations. In 1989 he moved to SSEB/Scottish Nuclear doing design/project management and safety case management, before becoming Nuclear Safety Manager and then Protection and Electrical Systems Manager at British Energy.

In 2004 he left BE to become Technical Director/MD of Risktec (Glasgow). In 2007 he became Head of Technical Services in ESR Technology's Aberdeen office and later became Chief Operating Officer of ESR Technology, based in Warrington. He left ESR in 2011.

Jim specialises in consultancy in both safety management and high-integrity C&I. He has done international consultancy work (either nuclear or oil and gas), including third-party audits of high-integrity protection systems and independent assessment on C&I licensing for nuclear new-build. He sat on the IET degree accreditation panel from 2001 to 2004.

www.safetyinengineering.com