

The logo for SafetyInEngineering, featuring the text "SafetyInEngineering" in a sans-serif font, enclosed within a stylized rectangular border composed of multiple parallel lines that create a 3D effect.

SafetyInEngineering

Modern High Integrity C&I for Nuclear Applications

Jim Thomson

www.safetyinengineering.com

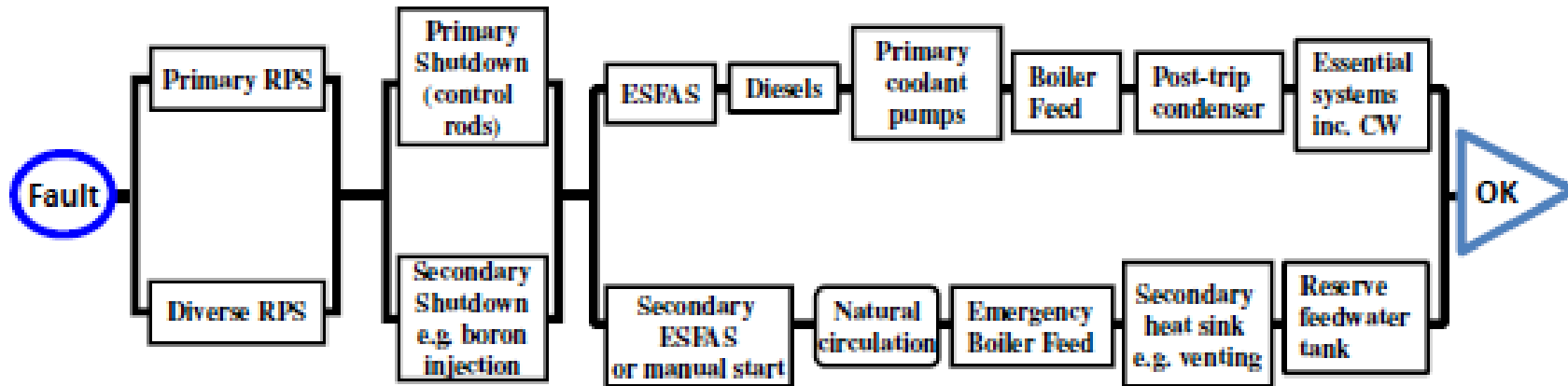
March 2014

Agenda

1. C&I architectures – O&G, aircraft, NPPs
2. Complex failure modes in complex systems:
Case study – Qantas A330, 2008
3. What are the problems with software systems?
4. The marketplace for high integrity systems
5. Conclusions

1. C&I architectures

Reactor protection systems – diverse routes to cold shutdown

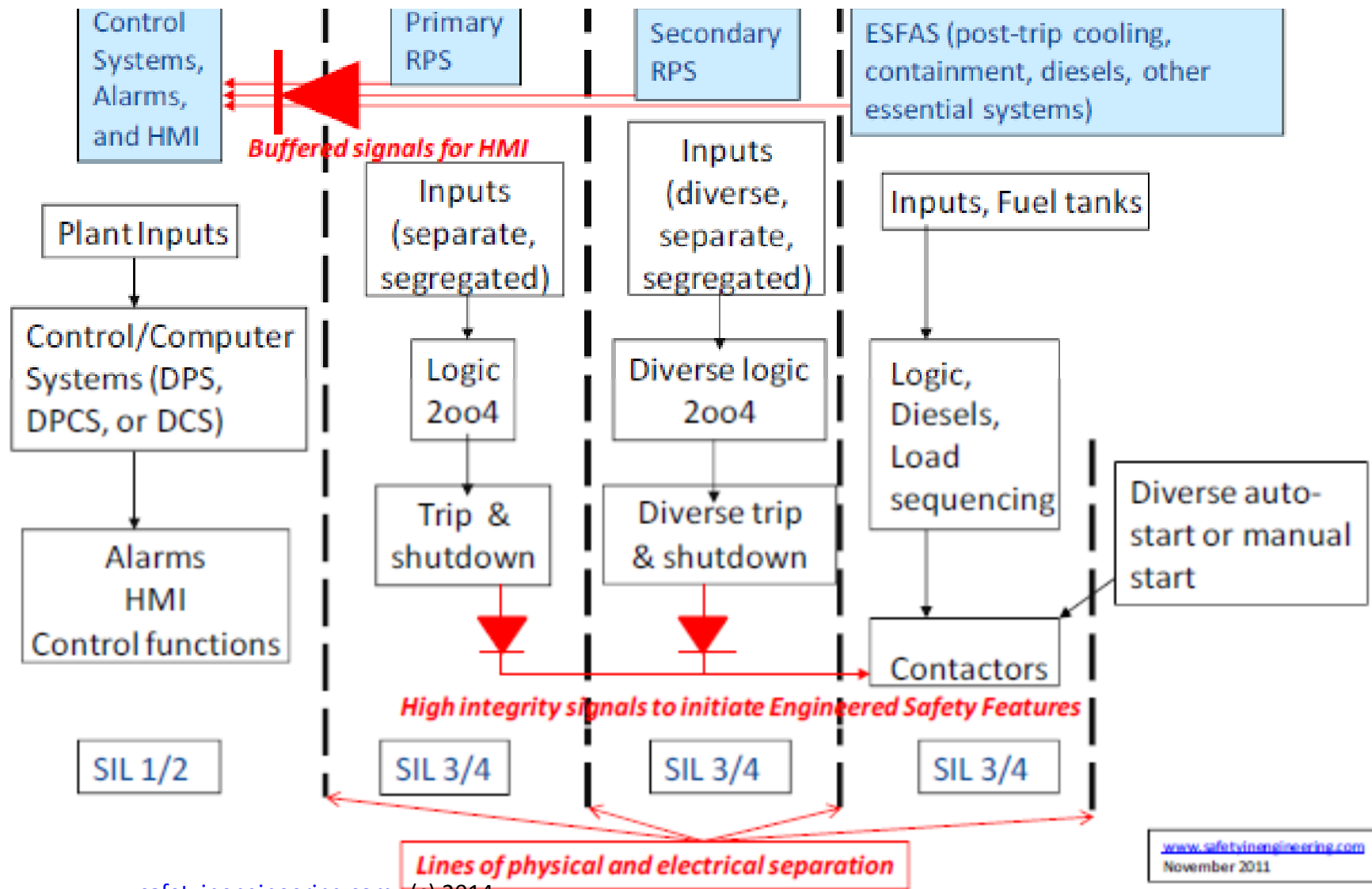


Fault detection and Reactor Trip initiation	Reactor Shutdown	Post-trip systems sequencing control	Primary Coolant	Secondary Coolant	Heat Sink
---	---------------------	--	--------------------	----------------------	--------------

Notes:

1. This is an attempt to make a generic representation of diversity within reactor protection systems for all reactor types, so some simplification has been necessary. Details will differ significantly according to the design of the power station, especially with respect to post-shutdown cooling systems.
2. The diagram does not show redundancy – most (or all) of the above systems will also incorporate redundancy.
3. RPS = Reactor Protection System
4. ESFAS = Essential Safety Features Actuation System
5. Any route from 'fault' to 'OK' must be viable and meet reliability criteria.

Simplified, ideal C&I architecture for a nuclear power station

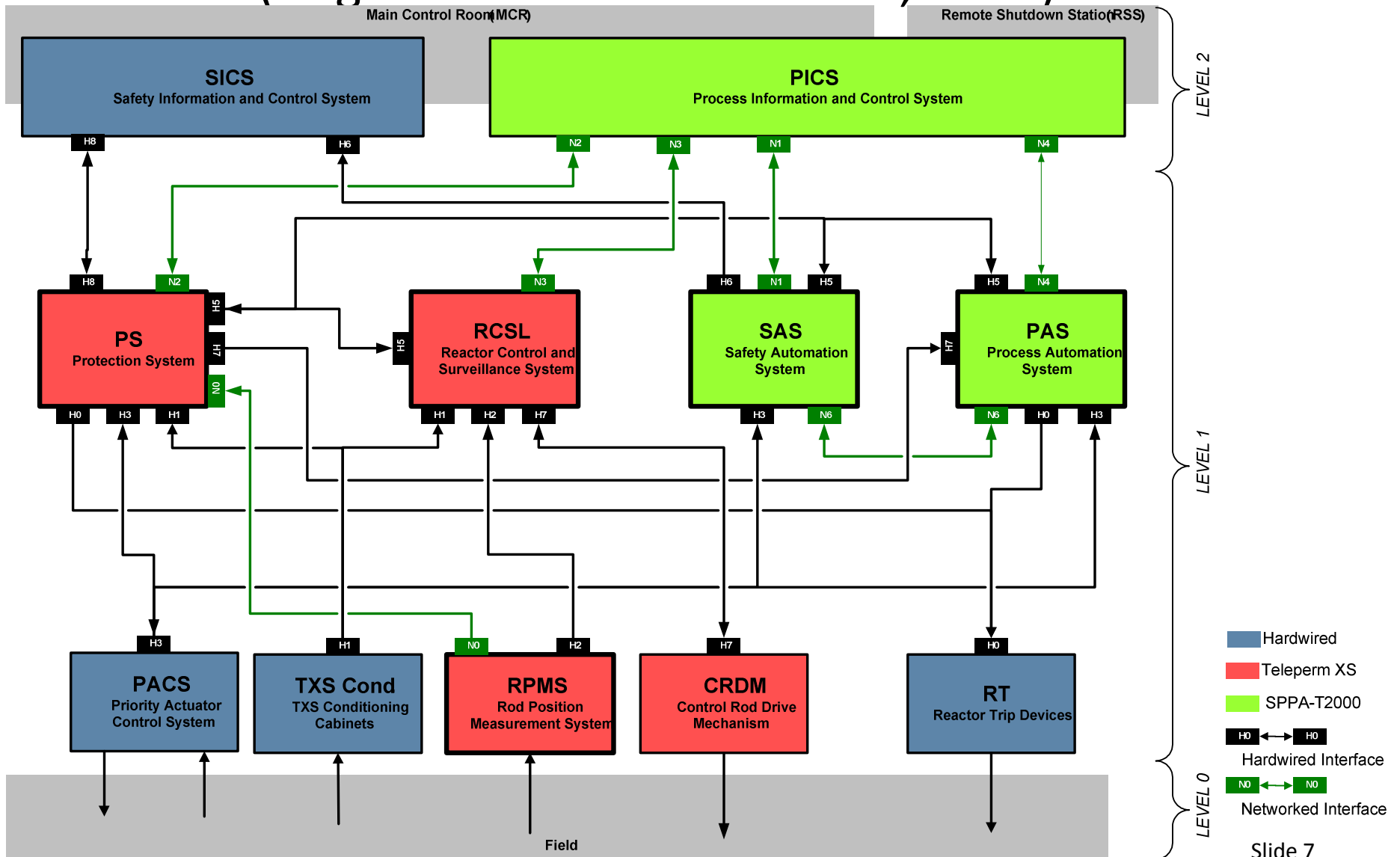


Why are the architectures of safety systems different in nuclear, oil and gas, and aviation?

1. The hazard magnitudes are significantly different .
2. There is a difference between voluntary and involuntary acceptance of risk, and between risks where there is also benefit (e.g. salary) and where there is none.
3. Aircraft inevitably have to mix up control systems and protection systems, at least to some extent, whereas in both NPPs and in O&G facilities it is possible (and desirable) to separate control and protection.

EPR C&I architecture

(original UK GDA submission, 2009)



ONR assessment of original EPR C&I proposals (2009)

- **ONR step 3 assessment:**
- **“The assessment revealed that the C&I architecture is overly complex with reliance on two computer based systems (originally developed by the same Company) and a high degree of connectivity between systems.”**
- **“.....lower safety class systems appear to have write access (permissives etc.) to higher safety class systems”**
- **“....substantiation of the reliability claims for the computer based SIS that use the Teleperm XS and SPPA-T2000 platforms (e.g. PS, Safety Automation System (SAS) and PAS)” etc**
- **In response to (*ONR comments*), EDF and AREVA provided further substantiation of the UK EPR C&I design and a commitment to undertake a number of modifications to the UK EPR C&I architectureto address the main areas of concern. The main commitments are summarised below:**
- One way communication will be implemented from the PS to the lower classified systems (should any exceptions be identified then they will be justified on a case-by-case basis).
- All signals transmitted between the Safety Information and Control System (SICS) and the PS will use a F1A (Class 1) path.
- A non-computerised backup system (10⁻³ pfd) will be implemented in order to provide protection and controls in case of total loss of C&I functions from the Teleperm XS and SPPA-T2000 platforms.
- Reduction of the reliability claims for the Teleperm XS (10⁻⁵ pfd to 10⁻⁴ pfd) and SPPA-T2000 (10⁻⁴ pfd to 10⁻² pfd) platforms.

EPR I&C (2014):

Taishan 1&2

Olkiluoto 3

Hinkley Point C (x2)

Flamanville 3

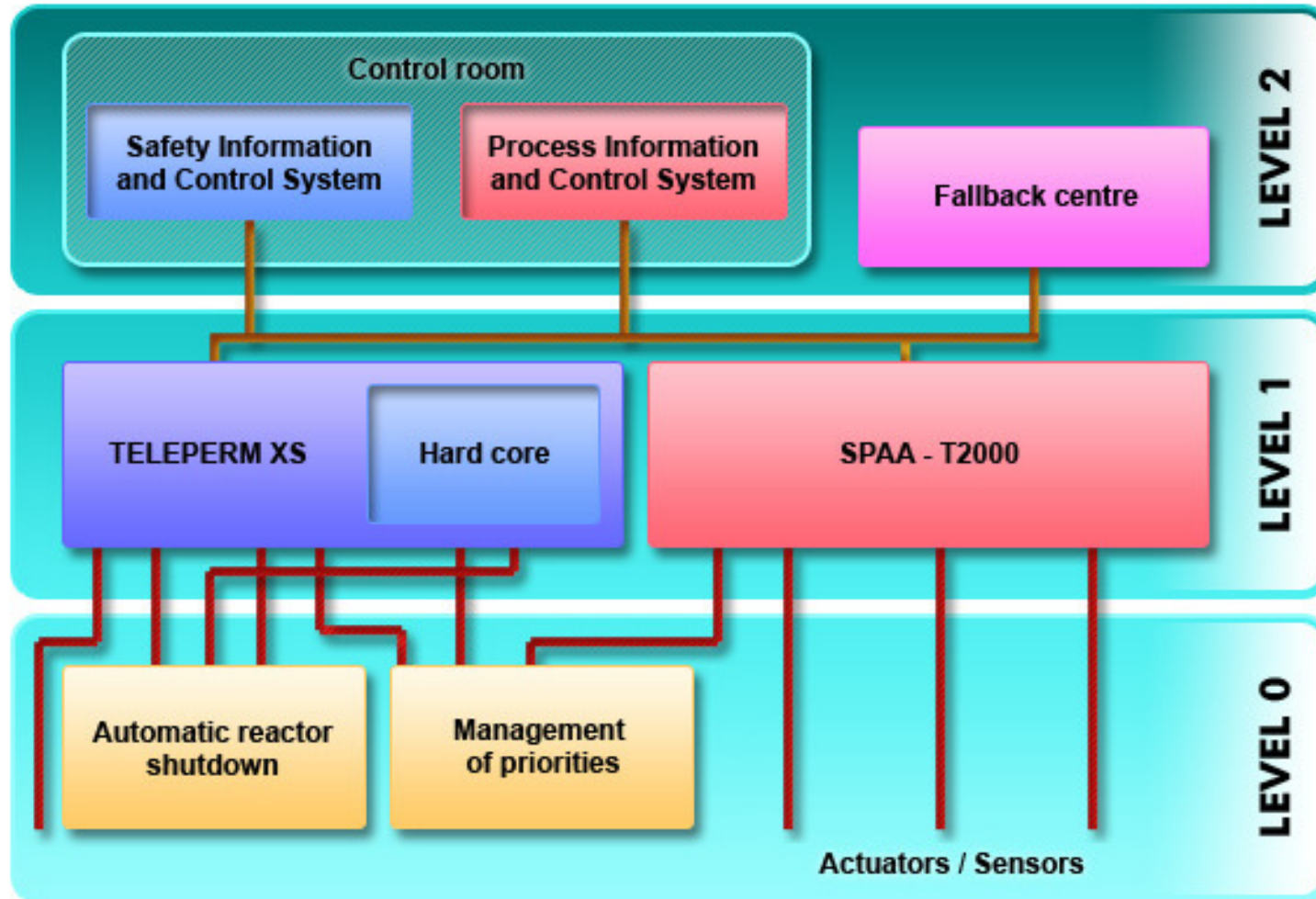
Six reactors, one design, three different C&I architectures?

1. Olkiluoto 3 had an additional **FPGA-based** diverse shutdown system designed in from the start as part of regulatory (STUK) requirements.
2. Hinkley Point C now has an additional **hard-wired** diverse shutdown system (the NCSS) installed at the request of ONR.
3. ASN (France – not a signatory of WENRA) has maintained its position that a diverse shutdown system is unnecessary, but some additional safety-related functions, originally only in SPPA-T2000, will now also be implemented in TXS (the ‘noyau duree’ or ‘hard core’). (*Announced April 2012*) Taishan will have the same design.

All three European Regulators – STUK, ONR and ASN - seem to agree that EPR I&C diversity as originally conceived was inadequate – they just don't agree what to do about it.

EPR C&I architecture

(Flamanville version, April 2012)



International standards

- These are a mess!! IEEE vs IEC; WENRA vs non-WENRA.
- We need a simple international ‘meta-standard’:
 - 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.

2. Complex failure modes in complex systems

Case Study:
Qantas A330 flight 72,
Singapore-Perth,
7th October 2008

“Complex systems almost always fail in complex ways.”
Columbia Accident Investigation Board Report, August 2003

Complex failure case study: QANTAS A330 'upset', 7 October 2008

Figure 48: Example of damage to the fittings above passenger seats (centre section)

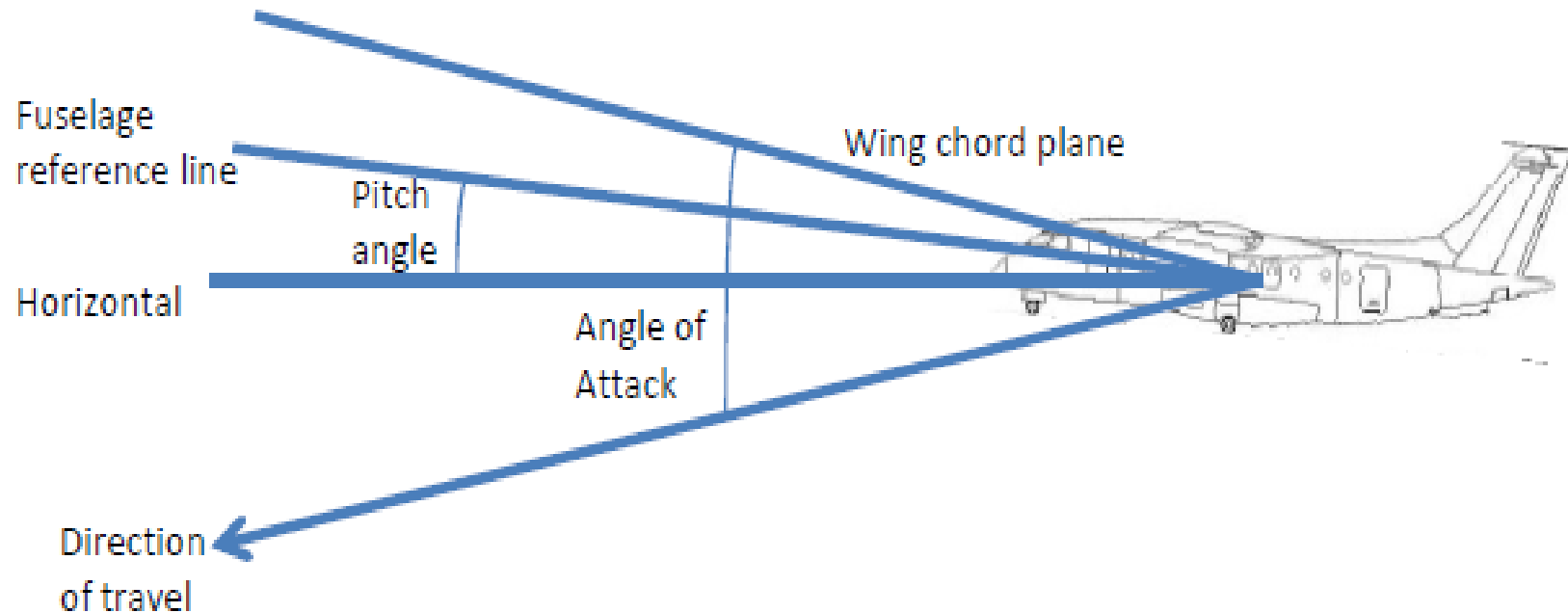


Figure 50: Example of damage to the ceiling panels in the aisle (rear section)



Injuries	Crew	Passengers	Total
Fatal	-	-	-
Serious	1	11	12
Minor	8	99	107
None / unknown	3	193	196
Total	12	303	315

Angle of Attack vs Pitch vs Direction of Travel



The pilot cannot readily sense the Angle of Attack – he relies on instruments.

ADIRUs: “ring-laser gyroscopes”

- Modern Inertial Reference Units, such as ADIRUs, use *ring laser gyroscopes*, together with accelerometers and GPS to provide raw data.
- A ring laser gyroscope consists of a ring laser having two counter-propagating modes over the same path in order to detect rotation.

Air Data Inertial Reference Units (ADIRUs)

Figure 7: ADIRU 1 (ADIRU 4167) from QPA



Angle Of Attack is a critical safety parameter for the EFCS, and the Flight Control Primary Computers use three independent AOA signals to check their consistency, signals AOA1, AOA2 and AOA3.

The AOA signals are created by Air Data Inertial Reference Units (ADIRUs).

The AOA value is then fed into the flight control system and used, in particular, to drive signals to the elevators in the tailplane which control aircraft pitch.

Key factors from the in-flight upset of Qantas Airbus 330-303, 7th October 2008

(adapted from Australian Transport Safety Bureau report AO-2008-70)

Aircraft was in level cruise at 37000 feet

Flight control systems require accurate Angle Of Attack (AOA) data, which are provided by 3 redundant Air Data Inertial Reference Units (ADIRUs).

The Electronic Flight Control System (EFCS) uses 3 Flight Control Primary Computers (FCPCs). One of these acts as 'Master'.

AOA is a critically important flight parameter. Three ADIRUs provide redundancy and fault tolerance. Three FCPCs use the 3 independent AOA values to check their consistency. Using Normal Law for control, the average of AOA1 and AOA2 is used. If either AOA1 or AOA2 deviates (e.g. a signal spike), the FCPCs use a memorised value for 1.2 seconds.

Key factors from the in-flight upset of Qantas Airbus 330-303, 7th October 2008

(adapted from Australian Transport Safety Bureau report AO-2008-70)

0440:26 ADIRU 1 started providing multiple intermittent spike signals. Crew received numerous warning messages (mostly spurious).

“The data-spike failure mode.....involved intermittent spikes on air data parameters being sent to other systems as valid data without a relevant fault message being displayed to the crew.”


0442:27 Aircraft suddenly pitched nose down. The command lasted <2 seconds. At least 110 passengers and 9 crew injured, 12 seriously. A second less severe pitch down occurred at 0445:08.

“There was a limitation in the algorithm used by the A330/A340 FCPCs for processing AOA data. This limitation meant that, in a very specific situation, multiple AOA spikes from only one of the three ADIRUs could result in a nose-down elevator command. (Significant safety issue)”

“The FCPC algorithm was very effective but it could not correctly manage a scenario where there were multiple spikes in either AOA1 or AOA2 that were 1.2 seconds apart.....it is very unlikely that (this) FCPC design imitation could have been associated with a more adverse outcome.....The occurrence fitted the classification of a ‘hazardous’ effect rather than a ‘catastrophic’ effect.....only known case of the design limitation affecting an aircraft’s flight-path in over 28 million flight hours.....limitation was within the acceptable probability range.....”

Key factors from the in-flight upset of Qantas Airbus 330-303, 7th October 2008

(adapted from Australian Transport Safety Bureau report AO-2008-70)



“.....the development of the A330/A340 flight control system during 1991 and 1992 had many elements to minimise the risk of design error.....None of these activities identified the design limitation in the FCPC’s AOA algorithm.....Overall, the design verification and validation processes used by the aircraft manufacturer did not fully consider the potential effects of frequent spikes in data from the ADIRU.”

There were two other known occurrences of the data-spike failure mode, on 12th Sept 2006 and 27th Dec 2008.

**Mayday declared, flight diverted
and landed successfully at 0532.**

3. What are the problems with software systems?

What are the problems with software systems?

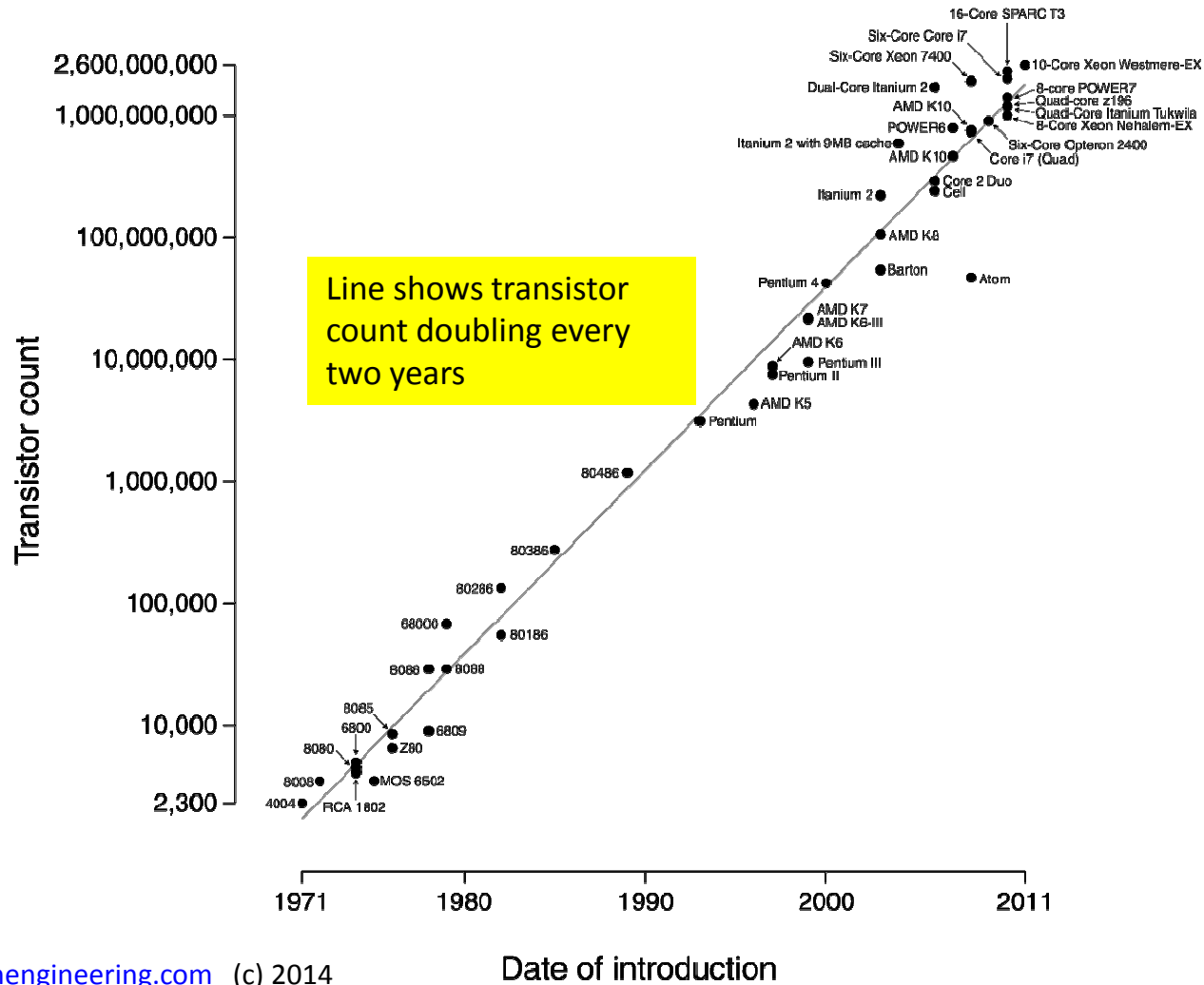
Overall: Software systems are not readily amenable to inspection and testing in the same way as older analogue equipment.

1. Ensuring accurate specification (**specification problem**)
2. Complexity of software (**verification problem**)
3. Complicated failure modes of smart components (**FMEA problem**)
4. Microprocessor 'physics of failure' (**ageing failure modes problem**)
5. Demonstrating claimable reliability (**reliability problem**)
6. Proof testing: There are far too many possible system states so full negative testing is impossible (**validation problem**)
7. Cyber attack (**security problem**)
8. The '**diverse software**' problem
9. The '**management of change**' problem

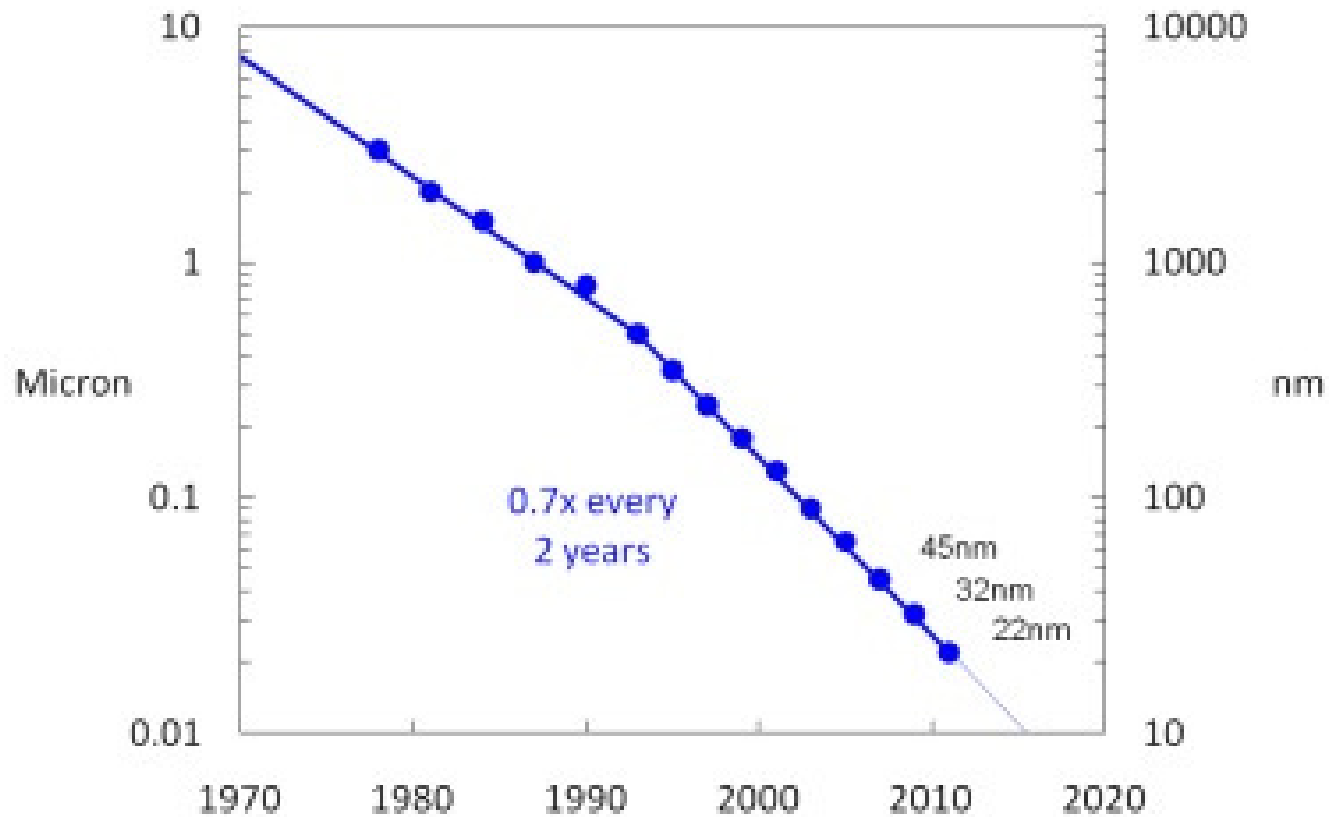
*Microprocessor 'physics of failure'
(ageing failure modes problem)*

Miniaturisation – new failure modes

Microprocessor Transistor Counts 1971-2011 & Moore's Law



Moore's Law – Feature size



Kashiwazaki– Kariwa, Japan



In 2001 a failure of control rod transponder circuit boards at Kashiwazaki-Kariwa Nuclear Power Station Unit 5 (Japan) rendered the control rods inoperable. Following detection of the defective cards, an analysis revealed that **the failure mechanism was aluminium conductor breakage in the ICs caused by electro migration** (the transport of metal atoms induced by high electric current). Aluminium grain size was too small which increased susceptibility to electro migration. The affected ICs had been manufactured between 1985 and 1990.

Failure analysis methods and manufacturing quality control and testing have been improved. This effect is potentially more significant in more modern ICs where the level of miniaturisation is much greater.

Demonstrating claimable reliability
(reliability problem)

QA vs Reliability

- IEC 61508 and related standards, in essence, assume a correlation between system graded QA and system reliability.
- The correlations implicit in IEC 61508 (etc) are the output of expert judgements.
- These correlations are not objectively verifiable (*but they are the best we have.....*)

Licensing limits and precedents for nuclear high-integrity software reliabilities

1. ONR has identified 10^{-5} as the maximum possible claim for non-diverse C&I systems.
2. The ONR (and also WENRA) have identified a 10^{-4} limit for software-based systems.
3. ONR have never yet licensed a software-based system on the basis of a 10^{-4} reliability claim. (*Sizewell B Primary protection System (PPS) was licensed (eventually) on the basis of a safety case sensitivity analysis assuming 10^{-3} PPS reliability. The Sizewell B Pre-Construction Safety Report (PCSR) had indicated a 10^{-4} claim would be made. This is relevant because the EPR GDA is more-or-less equivalent to a PCSR – see item 5 below.*)
4. The Generic Design Analysis (GDA) for EPR challenged 10^{-5} claims for the Teleperm XS-based primary protection system that were in the original GDA submissions. EdF-Areva revised this to a 10^{-4} claim. A hard-wired diverse system was also incorporated.
 - ONR have never yet been asked to license a high-integrity FPGA-based system. (*However, they have indicated privately that they see software reliability limits as being applicable also to FPGAs.*)
 - The GDA for Westinghouse AP-1000 has not been closed out. Open items include those relating to C&I reliability claims.

Proof testing
(validation problem)

Statistical Testing using Bayesian Inference

Claimable SIL levels, after a number of observed failures N ,
with a given number of operating demands or operating time M ,
at 50% and 80% confidence

No of demands (or operating time) No of observed failures	10		100		1000		10000		100000		
	Confidence	50%	80%	50%	80%	50%	80%	50%	80%	50%	80%
0		1.6 E-1	2.3E-1	1.6 E-2	2.3E-2	1.6 E-3	2.3E-3	1.6 E-4	2.3E-4	1.6 E-5	2.3 E-5
1		2.69 E-1	3.89 E-1	2.69 E-2	3.89 E-2	2.69 E-3	3.89 E-3	2.69 E-4	3.89 E-4	2.69 E-5	3.89 E-5
2		3.92 E-1	5.32 E-1	3.92 E-2	5.32 E-2	3.92 E-3	5.32 E-3	3.92 E-4	5.32 E-4	3.92 E-5	5.32 E-5
5		7.42 E-1	9.27 E-1	7.42 E-2	9.27 E-2	7.42 E-3	9.27 E-3	7.42 E-4	9.27 E-4	7.42 E-5	9.27 E-5
10		13.0 E-1	15.4 E-1	13.0 E-2	15.4 E-2	13.0 E-3	15.4 E-3	13.0 E-4	15.4 E-4	13.0 E-5	15.4 E-5
20		23.9 E-1	27.0 E-1	23.9 E-2	27.0 E-2	23.9 E-3	27.0 E-3	23.9 E-4	27.0 E-4	23.9 E-5	27.0 E-5
30		34.6 E-1	38.3 E-1	34.6 E-2	38.3 E-2	34.6 E-3	38.3 E-3	34.6 E-4	38.3 E-4	34.6 E-5	38.3 E-5

Indicative SIL levels

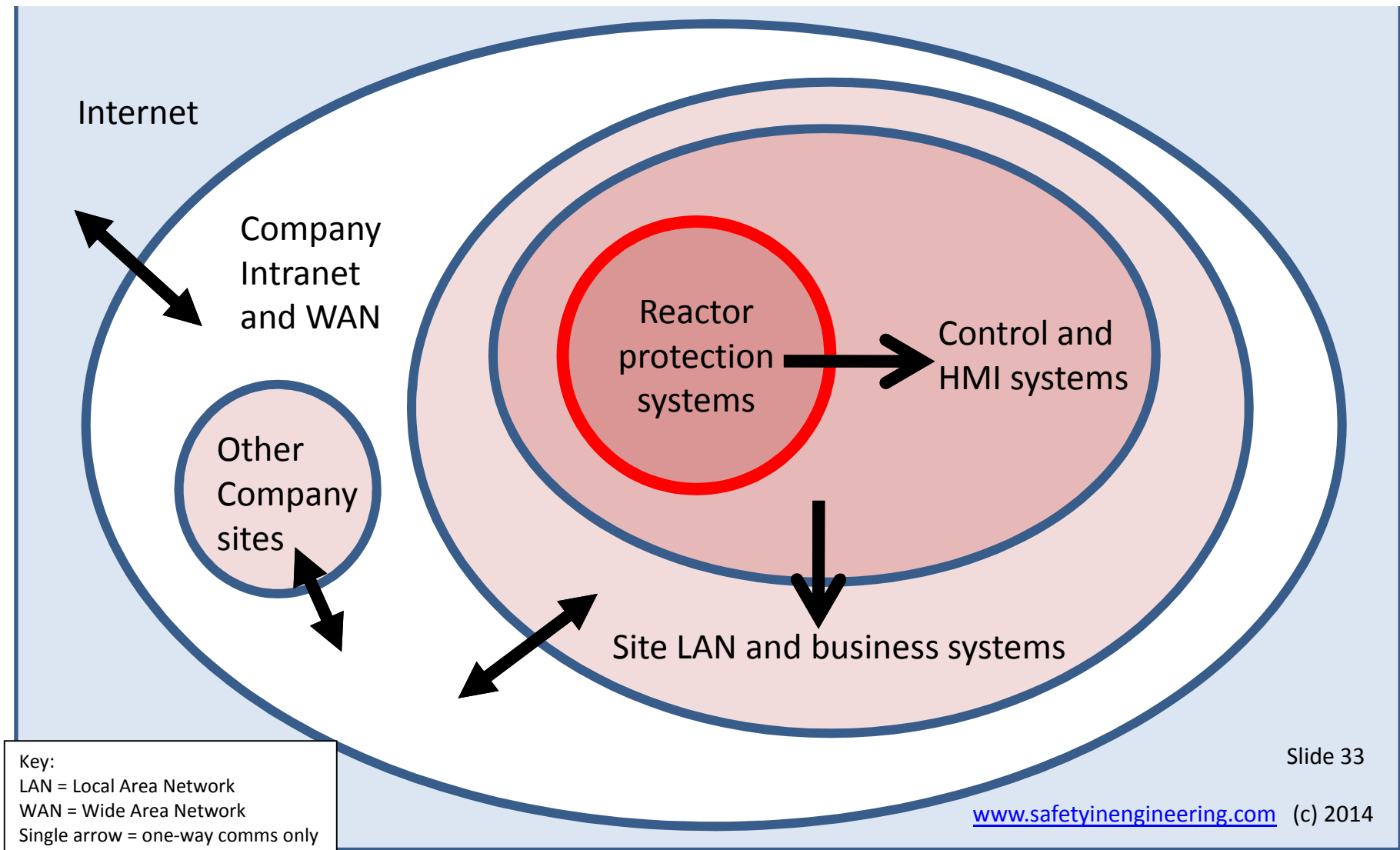


Cyber attack
(security problem)

Cybersecurity

- APT1 (Advanced Persistent Threat): Run from a Chinese Army office in Shanghai. Responsible for multiple major cyber-attacks on western organisations (including Areva). Spear-phishing emails with .exe files attached (which are disguised as .pfd files). See www.mandiant.com
- Stuxnet/Duqu/Flame: extremely clever cyber-weapons which are designed to paralyse industry, developed by US NSA/CIA, using 'zero-day' weaknesses in Windows.
- Software developers and operators must understand *threat vectors* throughout software development lifecycle.

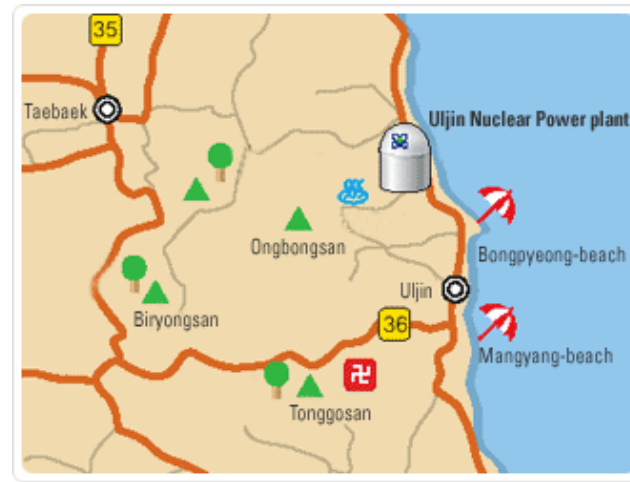
Cybersecurity barriers in nuclear power stations



The diverse software problem

1. There have been philosophical challenges (in the UK especially) about the credibility of 'diverse' software.
2. ONR were unhappy about diversity between Teleperm XS and SPPA-T2000 (formerly known as Teleperm XP).
3. Hence UK-EPR has a hard-wired Diverse Reactor Protection System.

Software change management: Uljin 3, South Korea



In 1999 an incident at Uljin Nuclear Power Station Unit 3 in Korea corrupted data on the performance net of the plant control computer. The incident was caused by the failure of an Application-Specific Integrated Circuit (ASIC) chip on part of a network interface module. Several non-operational pumps started without any demand, some closed valves opened and other open valves closed, and some circuit breakers switched on or off. There was also some relay chattering. Due to the response of the operators and because of diverse systems, the incident was mitigated without adverse consequences. **A review of the systems found that a common-cause software error was the likely cause. It was found that there was no provision to protect against foreign writes in the global memories within the communication network.** As a result, software modifications were implemented that included a change of data format, mirror testing, status testing, and hardware foreign write protection. Extensive modifications, including hard-wired backups, were subsequently carried out.

4. The marketplace for high-integrity C&I systems

The marketplace for high integrity systems

Potential products for short-listing include the following (alphabetical order). All are generally claimed to be SIL3-capable or better, and will generally offer 2004 logic:

- ABB System 800
- **Areva Teleperm XS**
- Emerson DeltaV SIS
- Honeywell Safety Manager
- **Invensys Tricon**
- **RADIY (FPGAs)**
- Rockwell/ICS Triplex
- **Rolls-Royce Spinline**
- **Westinghouse Common Q** and CSI (*CSI is FPGAs*)
- Yokogawa ProSafe RS and SLS (*SLS is magnetic logic*)
- *Others: **Mitsubishi MELTAC, Doosan-HFC, CTEC-HolliSys, etc***

Areva Teleperm XS design features

- Strictly cyclic operation, no process-controlled interrupts
- Standardized, simple software structure
- Automatic code generation from function diagrams
- Client base – 74 sites (all nuclear)
- Originally designed to IEC standards

Invensys Tricon design features

- Triple modular redundant (TMR)
- Fault tolerance
- No interrupts
- Extensive self-test and diagnostics
- Client base – >1000 sites (nuclear, O&G, refineries, etc)
- Originally designed to IEEE/NRC standards

Westinghouse Common Q design features

- Uses ABB AC160 modular controller
- Self test and diagnostics
- Watchdogs
- Client base – 22 nuclear sites
- Originally designed to IEEE/NRC standards

Rolls-Royce Spline design features

- Developed using Esterel SCADE
- Self test and diagnostics
- Fail-safe, fault-tolerant
- Client base – 85 nuclear sites
- Originally designed to IEC standards

Each company guards its IP carefully – it is not easy to identify clear differentiators through a fog of jargon and knowledge-protection

Outline comparison of four NRC- approved microprocessor safety systems

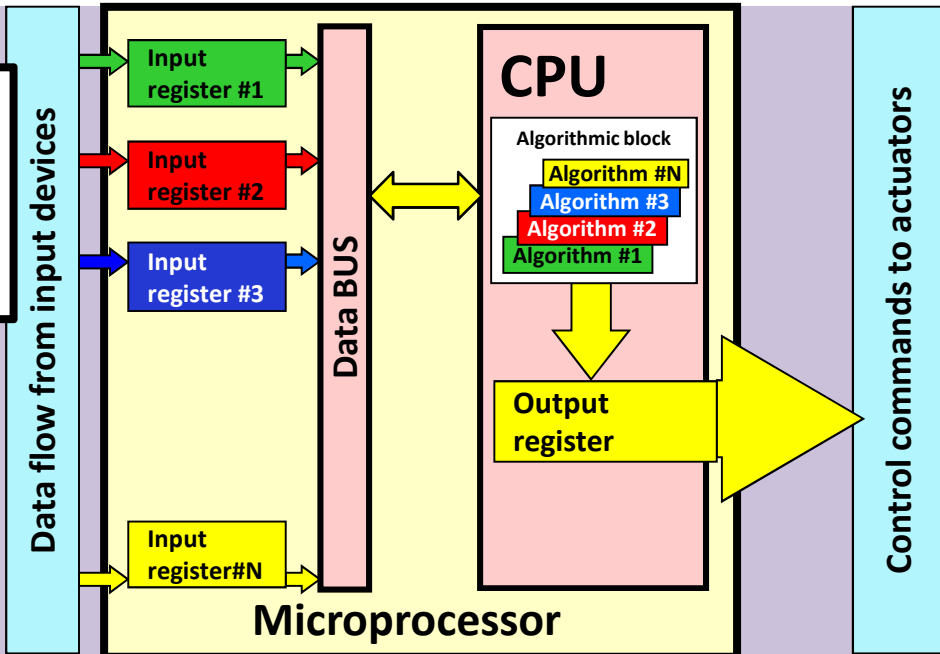
US digital upgrade marketplace

(Nuclear Engineering International, Nov 2012)

Table 1: Market for digital upgrade systems in the US (excludes new build)						
Item	Candidate system for upgrade	Probability of upgrade in 10 years	Cost of first upgrade (\$m)	Cost of additional upgrades (\$m)	Plants still left (out of 104)	Total (\$m)
1	RPS/SSPS	50%	100	40	80	1630
2	NSSS controls	80%	20	15	75	900
3	BOP controls	90%	15	5	60	275
4	NIS processing	80%	10	5	70	280
5	Turbine controls	90%	40	20	40	740
6	Radiation monitoring	70%	10	5	40	150
7	Annunciator	70%	10	5	50	180
8	DG sequencer	50%	10	5	70	180
9	Plant computer	95%	25	15	50	720
10	PAMS/LTOP	80%	10	3	70	175
11	Digital rod control	70%	10	5	40	150
Total digital upgrade market						5355

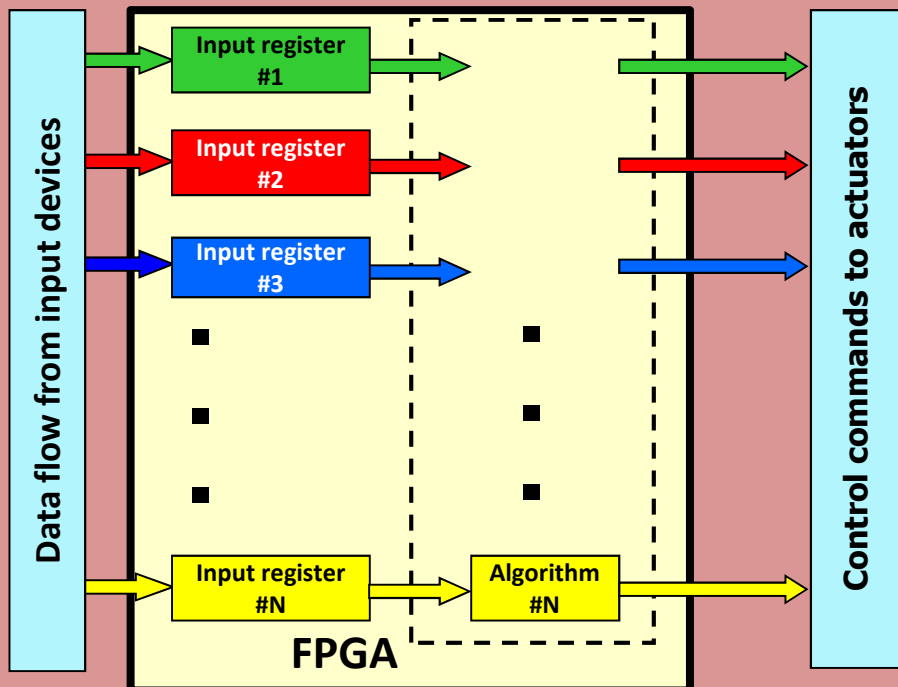
FPGAs compared to microprocessors

Microprocessors have serial data processing....



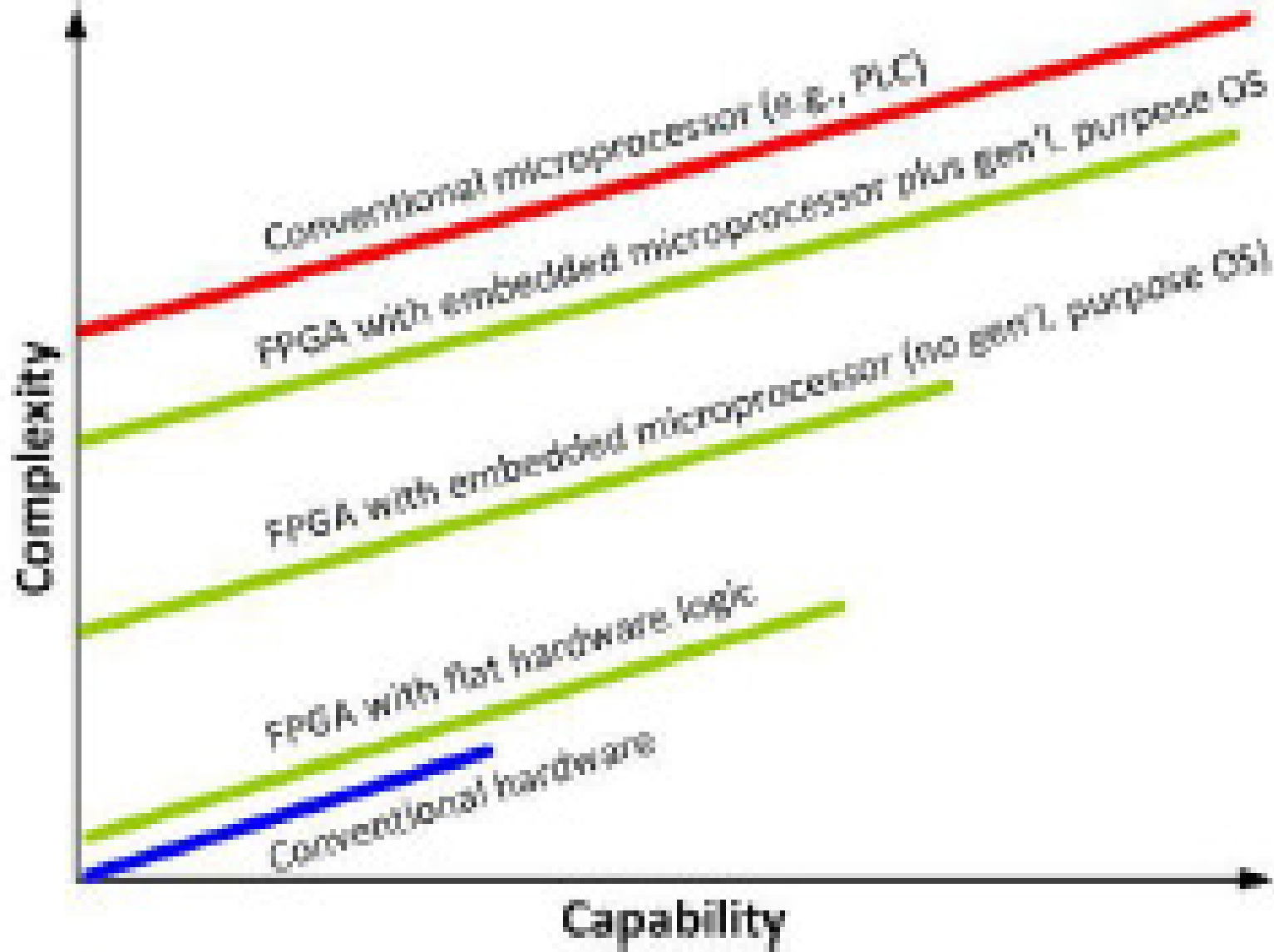
....but simple FPGAs can be just logic solvers with parallel data processing and no software.....

(although complex FPGAs can have embedded microprocessors.....)



Diagrams adapted from RADIY

Courtesy EPRI



Types of high-integrity logic solvers and their attributes

Types of logic solver	Desirable attributes
<ul style="list-style-type: none">• Microprocessor• FPGA or other PLD• Magnetic logic• Analogue electronic logic• Relay logic	<ul style="list-style-type: none">• Can handle complex algorithms• Pre-service testability• Verifiable• Validatable• Licensable• Cyber-attack immune• Resistant to age-related failure modes• Ease of maintenance• Ease of configuration management• Low obsolescence risk• Low cost

Attributes of various high-integrity logic solvers

Type of logic elements	Can handle complex functions and algorithms?	Pre-service testability?	V&V	Licensing and safety?	Cyber-attack?	Single Event Upset (SEU) and other age-related failure modes such as electro-migration	Maintenance aspects	Configuration management and change control	Obsolescence risk for operator	Cost
Micro-processor	Can handle complex functions e.g. DNBR	Full negative testing cannot be achieved because of large number of inputs going into a common logic-solving element.	V-model approach well-defined but regulators can always ask for more, e.g. dynamic and statistical testing.	Ultimately depends on robust QA, comprehensive documentation, and full traceability from functional requirements, via implementation, to testing.	Potentially susceptible	Susceptible (especially for smaller feature size < 100nm)	On-line monitoring and test arrangements can reduce workload.	Configuration management and change control need to be extremely thorough.	High (short lifecycle)	Cost dominated by Engineering costs, i.e. hardware costs are less important.
FPGA or PLD	Cannot handle complex functions unless embedded processors are used (in which case other advantages are lost....)	Full negative testing <u>could</u> be achieved if (i) logic functions are simple and (ii) functions are segregated on FPGA chip and (iii) it could be proven by inspection that functions are segregated	V-model approach with full traceability. No OS but VHDL and place-and-route software need full V&V.	VHDL (and other) software used in design is complex and safety-critical. Current standards treat FPGAs like microprocessors but, if full negative testing could be carried out, then regulators would be more relaxed.	Probably immune.	Susceptible (especially for smaller feature size <100nm)	Straight-forward (like hard-wired logic)	May require configuration management and change control similar to microprocessor systems (although in principle it is fixed at installation)	Said to be low (Report by VTT, Finland)	As above
Magnetic logic	Cannot handle complex functions or algorithms	Full negative testing can be achieved	V-model approach well-defined. Full traceability required.	Some types of magnetic logic have been licensed in UK for RPS applications	Immune	No	Straight-forward	Fixed at installation	Low	As above + bigger space requirements
Analogue electronic logic	Cannot handle complex functions or algorithms	Full negative testing can be achieved	V-model approach well-defined. Full traceability required.	Licensable (because unreliability of individual elements is known.)	Immune	No but other potential unrevealed failure modes	Straight-forward	Fixed at installation	Low	As above + bigger space requirements
Relays	Cannot handle complex functions or algorithms	Full negative testing can be achieved	V-model approach well-defined. Full traceability required.	Licensable (because unreliability of individual elements is known.)	Immune	No but other potential unrevealed failure modes	Straight-forward but maintenance burden can be high	Fixed at installation	Low	As above + large space requirements

5. Conclusions

1. The future remains digital – we must keep finding ways of making it safe and licensable.
2. Complexity is bad for safety and licensability.
3. Simple ‘flat logic’ FPGAs look very promising.
4. The nuclear industry must avoid making exaggerated, unsupportable reliability claims.
5. Push back against fault analysts who want to make excessive C&I claims. Make them work harder at reducing their consequences assessments.

Thank you!

Additional information

Principles of laser gyroscope

In the 1980s, laser gyroscopes began to take over the work of their mechanical, and later, electronic, forebears, without the slightest resemblance in principle or operation to the earlier devices. The idea behind the ring laser gyroscope actually dates back to 1913, when a French physicist, Georges Sagnac, experimented with rays of light moving in opposite directions around a circular cavity on a turntable. Sagnac showed that when he rotated the turntable, the light traveling with the rotation arrived at a target slightly after the light traveling against the rotation. He believed he had proven the existence of ether in space. In fact, he was demonstrating a property of light that came to be understood much better with the invention of the laser in the 1950s.

A laser (light amplification by stimulated emission of radiation) operates by exciting atoms in a plasma to release electromagnetic energy, or photons, in a cavity. Each end of the cavity reflects the energy back and forth, and it forms a standing wave pattern. The wave frequency—its pattern of peaks and troughs—is determined in part by the length of the cavity.

“If you had a linear laser and the light bounced back and forth between two mirrors at either end, and if you [increased] the spacing between those two mirrors slightly, you would actually stretch the wavelength of the light in the cavity,” explains James Koper, the manager of ring laser gyro components for Kearfott Navigation and Guidance Systems, which manufactures the laser gyroscopes used in the B-2 bomber, the Global Hawk reconnaissance craft, and the Joint Stand-off Weapon, a glide bomb

“What causes the light to stretch? The fact that it had to go farther. Because when it comes back, it has to come back exactly the same way it left,” says Koper. “It has to resonate.”

Sagnac’s counter-rotating beams of light are analogous to beams in a linear cavity. If the turntable rotates clockwise, the beam traveling clockwise has farther to go to catch its starting point; the path of the counterclockwise beam is shorter.

In a given medium, “light travels at a constant velocity,” Koper says. “Einstein says you can’t change that. We definitely know that the beam going clockwise takes longer to get there than the beam going counterclockwise.”

In a ring laser gyroscope, the two counter-rotating beams are channeled to a photo detector. If the vehicle is not rotating, the beams remain in phase. If rotation is occurring, one beam continuously changes phase with respect to the other. A diode translates that moving interference pattern into digital pulses, each pulse representing an angle of rotation (typically .0005 degree per pulse, according to Koper). The rate at which the pulses are produced is also a measure of the rate of rotation.

In the JSOW glide bomb guidance package, Koper’s company also includes GPS receivers to update the ring laser gyros, which are arranged to measure yaw, pitch, and roll. Though the gyros are necessary for the constant feedback required for flight controls, the GPS system corrects any errors that inevitably build up in inertial systems.

<http://www.youtube.com/watch?v=eu4ZrzG-7ik>

www.safetyinengineering.com (c) 2014

Slide 48

Figure 4: Overview of a fly-by-wire flight control system

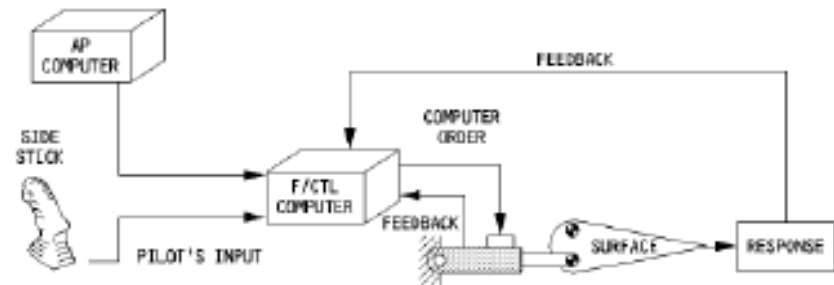
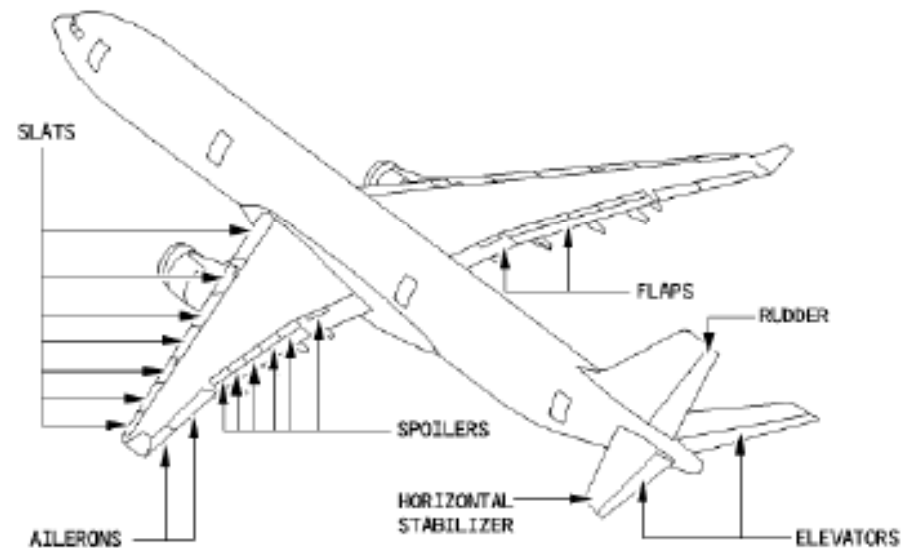


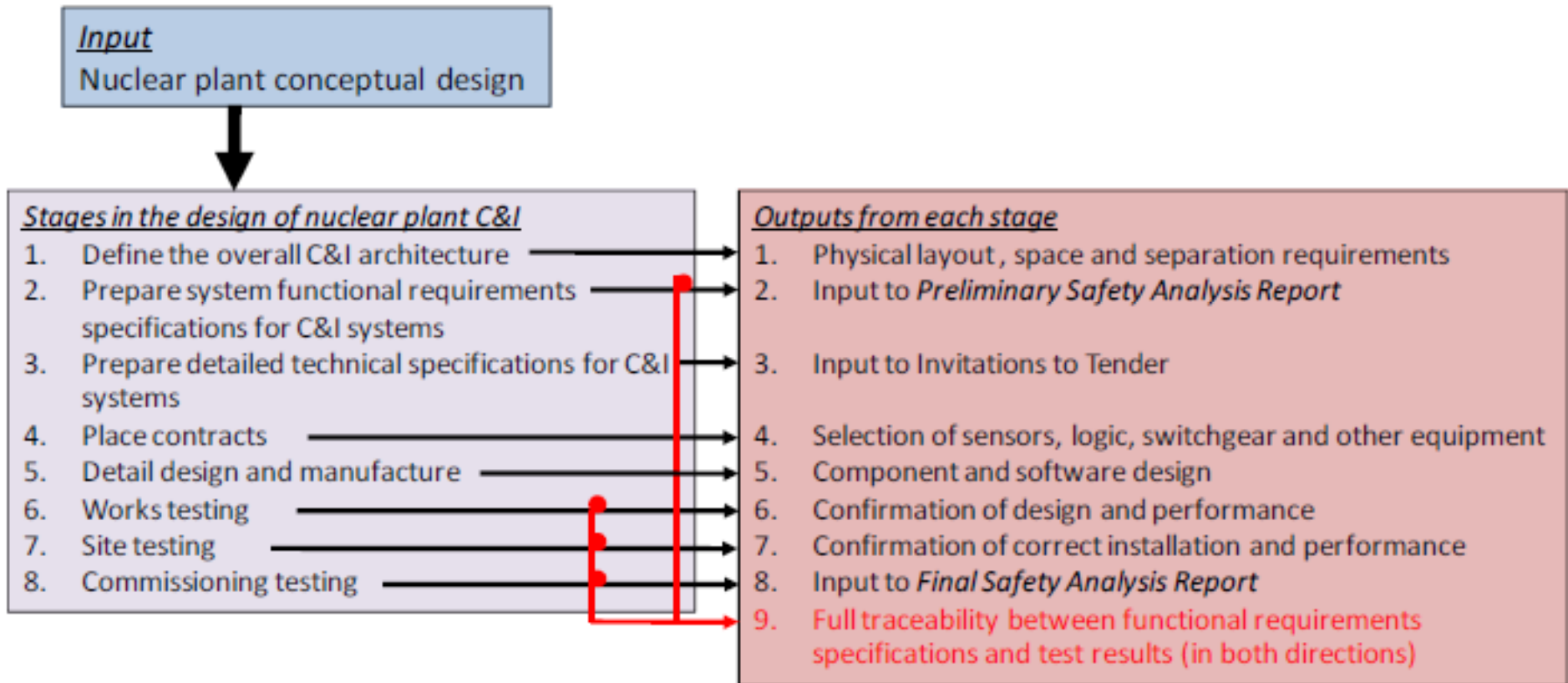
Figure 5: A330 flight control surfaces



The A330 EFCS had three flight control primary computers (FCPCs, commonly known as PRIMs) and two flight control secondary computers (FCSCs, commonly known as SECs). One of the FCPCs (normally FCPC 1) acted as the 'master' FCPC. It computed the appropriate control orders, and sent these orders to the other computers to action. More detailed information regarding the functioning of the FCPCs is provided in section 2.1.

Overall, the A330's EFCS provided many advantages relative to a conventional flight control system, including stability augmentation, reduced crew workload, and flight-envelope protection.

Idealised design process for nuclear plant C&I



The following is a very high-level, brief checklist from IEC 61508 part 3, Annex A. IEC 61508 is a very complex standard, and reference should be made to the standard for the necessary detail.

The degree to which each technique or measure has to be implemented depends on the SIL level required for the equipment. Not all techniques and measures are required for all SILs. All techniques and measures are important: some of the most important elements are in **bold**. Definitions of terms are given in IEC 61508 part 7.

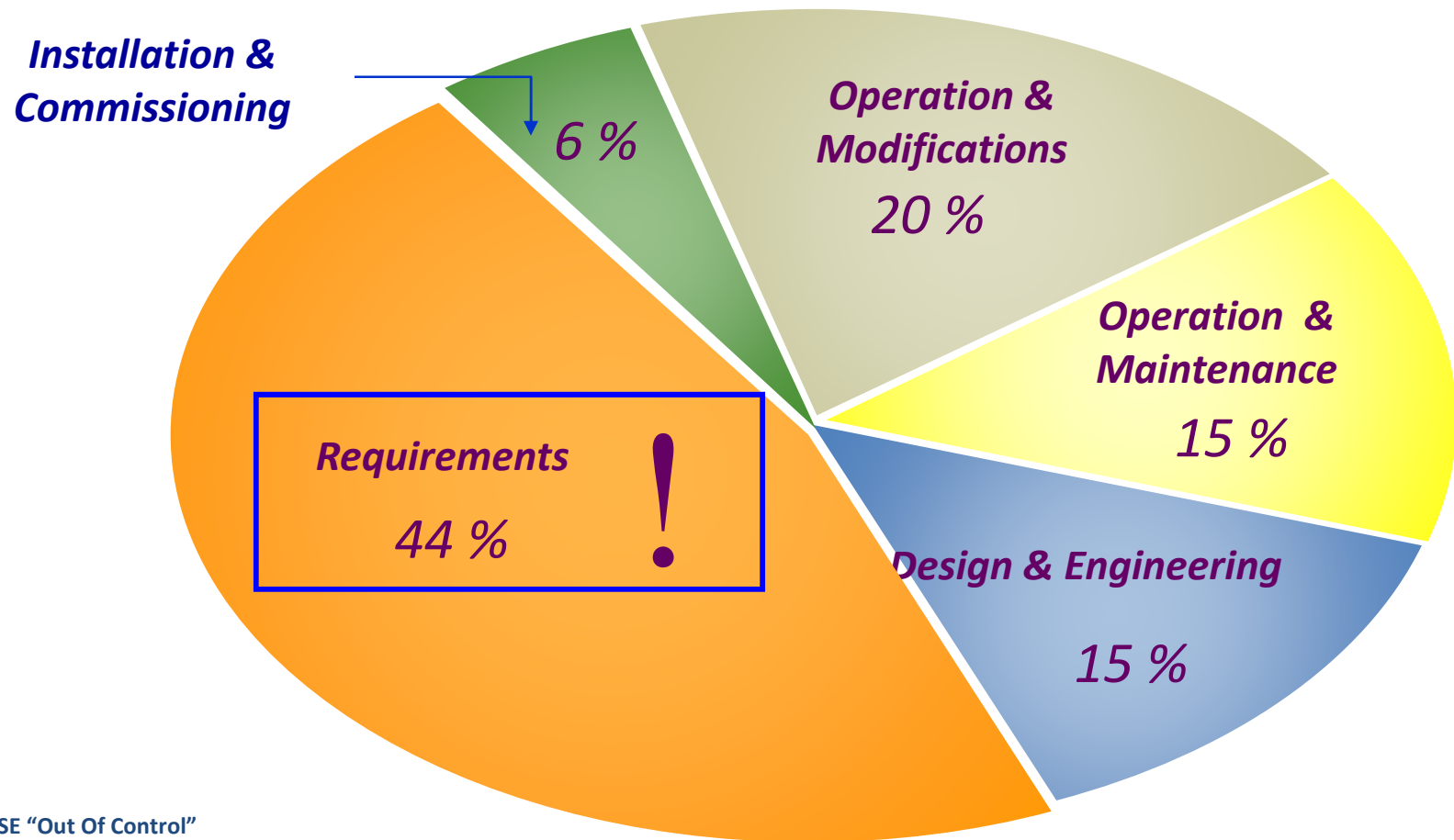
1. **Functional safety assessment**: checklists, truth tables, failure analysis, CCF analysis, reliability block diagrams
2. **Software requirements specification** – formal or semi-formal methods, traceability, software tools
3. Fault detection, error detecting codes
4. Diverse monitoring techniques
5. Recovery mechanisms or graceful degradation
6. Modular design
7. Trusted/verified software elements
8. **Forwards/backwards traceability at all stages**
9. Structured or semi-formal or formal methods, auto-code generation
10. Software tools
11. Guaranteed maximum cycle time, time-triggered architecture, maximum response time
12. Static resource allocation, synchronisation
13. Language selection, suitable tools
14. Defensive programming, modular approach, coding standards, structured programming
15. **Testing**: dynamic, functional, black box, performance, model-based, interface, probabilistic
16. Process simulation, modelling
17. **Modification/change control**: impact analysis, re-verification, revalidation, regression testing, configuration management, data recording and analysis
17. **Verification**: Formal proof, static analysis, dynamic analysis, numerical analysis

Digital I&C equipment examples

Product and supplier	NPP applications	Installed base
Teleperm by AREVA	<ul style="list-style-type: none"> ■ Reactor protection system ■ Engineered safety feature actuation system ■ Turbine control system ■ Rod control system ■ Condensate polishing system 	<ul style="list-style-type: none"> ■ USA: Callaway, Comanche Peak, Oconee ■ Europe: Bznau, Forsmark, Ringhals, Oskarshamn, Neckarwestheim, Biblis, Philippsburg [NEI June 2010, pp20-2], Paks, Santa Maria de Garofa, ■ China: Qinshan, Tianwan, Ling Ao
Common Q by Westinghouse	<ul style="list-style-type: none"> ■ Plant protection system ■ Engineered safety feature actuation system ■ Post-accident monitoring system ■ Core protection calculator system 	<ul style="list-style-type: none"> ■ USA: Calvert Cliffs, Watts Bar, Palo Verde ■ Korea: Uchin, Kori, Wolsong
Tricon by Invensys	<ul style="list-style-type: none"> ■ Reactor protection system ■ Engineered safety feature actuation system ■ Turbine control ■ Feedwater control ■ Rod position indication 	<ul style="list-style-type: none"> ■ USA: Oconee, D.C. Cook, Columbia ■ Europe: Kozloduy and Rovno
Eagle 21 by Westinghouse	<ul style="list-style-type: none"> ■ Digital reactor protection system 	<ul style="list-style-type: none"> ■ USA: Watts Bar, Sequoyah, Diablo Canyon, and Turkey Point ■ UK: Sizewell B ■ Czech Republic: Temelin

Other plants using digital I&C equipment include Chooz B (France) and Kashiwazaki-Karwa (Japan).

A useful reminder



Source - HSE "Out Of Control"

Causes of Systematic and Human failures

Slide 53