Key Attributes of Different Types of Logic Element for High-Integrity Applications

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	Mainten-ance aspects	Configuration management and change control	Obsoles-cence risk for operator	Cost	Other comments
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 arrange-ments 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.	OS V&V required in addition to application s/ware. Watchdog function requires particular attention.
FPGA or PLD	Cannot handle complex functions unless embedded processors are used *(in which case other advantages are lost….)*	Full negative testing could 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. *(See note about SRAM. Some sort of attack on design software, leading to latent failure modes, could be postulated.)*	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	Types of FPGA 1. SRAM (Altera, Atmel, Xylinx) – potentially susceptible to cyber attack. Rewritable. 2. Flash (Microsemi) – rewritable. 3. Antifuse (Microsemi) – non-rewritable so most secure and best suited for RPS-type applications
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 require-ments	Uses coils and magnetic cores to construct logic gates, e.g. Yokogawa Prosafe SLS.
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 unrevealed failure modes.	Straight-forward	Fixed at installation	Low	As above + bigger space require-ments	
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 failure modes such as contact welding.	Straight-forward but maintenance burden can be high	Fixed at installation	Low	As above + large space require-ments	