Make a safe decision.
Questions to ask a Safety/Critical Controls Supplier.

An easy to use guideline for selecting a safety/critical control system.

Containing 25 of the most frequently asked questions concerning industrial safety systems and their manufacturers.

Intention.

Various acknowledged experts of safety related automation technology have collected some of the most relevant questions to be asked to Safety/Critical Controls Suppliers.

These questions can be used as a guideline for selecting a safety system. As that decision should be a safe one, the intention of this document is to reveal hidden costs and any safety related problems. The complete life cycle from purchase to maintenance of a safety system is covered.

The questions are primarily based on international accepted standards such as IEC, CE, CSA, NFPA, OSHA, DIN etc and are a result of years of experience in the process industry.

This concentration of information as contained in the following 25 questions will provide an invaluable easy to understand and use tool.

A. Basics.

1. Quality.

➢ **Quality control of manufacturing and inspection procedures are of prime concern in safety/critical controls. High quality should mean less failures which in turn will give more availability with associated safety and less downtimes.**
Can the vendor's latest (i.e. within the last 24 months) released company quality procedures and compliance documents be inspected?

2. Manufacturing.

➢ **Specialist suppliers of safety/critical controls systems should develop and manufacture high quality, leading edge technology certified to accepted international standards.**
Can the vendor provide for inspection and demonstrate their product test procedures for all safety related components as manufactured in their own facilities?

3. TÜV-Certification.

➢ **TÜV is recognised as a world leader in safety certification of critical systems and their applications. Only approved components offer the safe use of all components.**
Can the vendor supply proof of TÜV auditing with the compliant certificates for their safety/critical equipment revalidated to include any recent component modifications? Does the vendor supply the complete TÜV approval reports to review the relevant restrictions therein?

4. CE-Compliance.

➢ **In many parts of the world compliance to the CE standards are necessary. 'Good engineering practice' coupled to the legal requirements should ensure reliable safety/critical systems.**
Can the vendor show complete safety/critical system CE compliance without the use of additional 3rd party supplied auxiliary equipment?

5. Compatibility.

➢ **Once purchased an end-user will operate their safety/critical systems for many years. Investments in personnel training and spare parts have been made on a long term basis.**
Can the vendor warrant that future system developments will have downwards compatibility to existing configurations?

6. Programming tool.

➢ **Most vendors offer different safety systems for different applications. To reduce costs for personnel training the same programming tool should be used to operate the various systems.**
Can the vendor show that their systems can be operated using a single programming tool?

7. Product Development.

➢ **Continual product evolution ensures that all companies should be constantly updating their product ranges yet using alternative market proven technologies. This is especially so where substitution of obsolete components are required.**
Can the vendor confirm that obsolete components are not included within their current product range?

8. R&D-Budget.

➢ **Only the usage of leading edge technology fulfils the customers growing demand for maximum cost effective safety/availability. It is a fact that innovative companies spent at least a minimum of 10% of their income for R&D purposes.**
How much investment does the vendor commit for development of their safety solutions?

9. Experience.

➢ **Safety related automation tasks are a very specialised field of the complete automation process with each application having its own needs. Experience is the irreplaceable basis to provide safe, reliable and cost-efficient solutions.**
How many years of experience in safety-related automation tasks has the vendor and how is this reflected in numbers of installations?

10. Long time partners.

➢ **The realisation of safety related applications requires a trustful and intensive co-operation. The end-user must be sure, that the vendor will be his reliable and independent partner not only today but also tomorrow.**
Can the safety system vendor show a continual, stable trading position for the previous 5-10 years?

11. Field proven new technologies.

➢ **As the classical safety systems such as 1oo2D or 2oo3/TMR are coming to the end of their abilities, new technologies are evolving. New technologies must also be proven on their reliability. To give the customer the surety of a field proven system, a significant number of installed leading edge systems must be shown.**
How many installed systems of their current products can the vendor show?

B. Technical Details.

12. Safety Time.

➢ **To achieve the safe operation of the plant many industrial plants specify a Safety Time (ST) and require a responsive output time from a critical input signal being measured in milliseconds. Typically this response time should be a guaranteed worst case scenario of a minimum two complete program scan times plus all reaction periods.**
Can the vendor confirm in milliseconds their Total Response Time (TRT) and being defined as the totalisation of input, program and output scans with complete system diagnostics (i.e. all relevant circuitry) including verification times?

13. Time restriction.

➢ **Safety/critical control systems must operate at the highest level of availability or their effectiveness is dramatically reduced.**
Can the vendor confirm that TÜV and other certification authorities impose no time restriction whatsoever in the event of an initial single component failure?

14. Scaleable fault tolerance.

➢ **To avoid oversized solutions and to guarantee safe and economic operation of a plant, the redundancy of a safety/critical control systems must be scalable to the applications needs. Cost efficient solutions should achieve maximum safety without redundancy.**
Can the vendor provide solutions offering maximum safety combined with scalable redundancy at the I/O and/or CPU level, e.g. mono systems to be used up to SIL3?

15. Multiple faults occurring.

➢ **The ability of tolerating a fault is an important feature for the economic operation of a safety system. Today most safety systems are able to tolerate a single fault, some with or without time restrictions. Modern redundant safety systems are designed to tolerate multiple diverse failures at the same time.**
Can the vendor show that shutdowns or time restrictions of his system are not the consequences of diverse faults during the operational period?

16. 3-step-controllers.

➢ **Safety specialists agree that 3-step-controllers give superior safety coverage. Certain system configurations can operate even in single fault condition for unlimited periods.**
Can the safety supplier offer a 3-step-configurated system ("3-2-0" or "4-2-0") operating without time restriction in the event of a single fault?

17. Diagnostics.

➢ **To prevent false trips, that will cause costly shutdowns, safety systems are based on diagnostics to detect and locate faults. The more intensive the diagnostics are the lower is the risk of a undetected/false trip.**
Can the vendor show that their system carries out a full diagnostic evaluation during each system scan?

18. False trips.

➢ **To achieve safety coverage some systems use a voting principle. This means that at least 3 processors and associated I/O cards are required to meet SIL3. According to TÜV the loss of one component mandates a shutdown after a time period because the basic safety principle having been destroyed.**
Does the vendor supply safety systems that use a voting principle?

19. Hot repair.

➢ **One time or another in every system a fault on a module will occur. This is not a problem if the replacement of the faulty component is possible on-line without causing an interruption of the plant operation. Hot repair with automatic (non-manual) start-up should be possible without the need for additional hardware or cabling.**
Can the safety system vendor show that faulty components (e.g. a CPU) can be replaced whilst the complete system is still operating?

20. On-line modification.

➢ **When a program has been modified a software download might be necessary. This download operation should be possible whilst the system is on-line. To enable the safe functioning of the system the execution of the logic programme should not be stopped (i.e. suspended or frozen) even momentarily.**
Can the vendor show that on-line changes will not require a suspension of the operating programme?

21. Communication.

➢ **Connectivity between systems has today become a major point of interest. Communications from differing manufacturer's equipment can determine overall reliability and offer flexibility of choice for the end-user.**
Can the safety system vendor demonstrate their compliance and commitment to open networking standards (i.e. OPC, Ethernet etc) whilst still offering SIL3 approved communications between devices?

22. Input/output modules.

➢ **To achieve the safe operation of the plant TÜV approved field interfaces, including relays, both to and from the safety critical controller are necessary. Documented and currently valid approval must contain a description of use (i.e. "Approved for Safety"). Non-safety approved devices (i.e. "Non-interacting") should never be used in safety related applications.**
Can the vendor supply certification documents listing their complete and current range of TÜV approved equipment?

23. Cost-efficient SIL3 solutions.

➢ **In accordance with the requirements of IEC 61508 outputs in an SIL3 application must have two independent ways of de-energising a module in the event of a faulty relay/output. To fulfil this requirement some safety system suppliers achieve this either by the use of a second external relay on each output or the addition of another output card. The consequences of such solutions are additional costs for engineering, wiring and hardware supply. Leading technologies have now solved this dilemma by integrating diverse independent circuitry into their products.**
How does the safety system vendor fulfil the IEC 61508 requirements for SIL3 applications?

24. Maintenance costs.

➢ **Once installed a safety system should operate in a problem free mode for many years. Maintenance activities should be reduced to a minimum. The TÜV report for some safety systems states that regular (i.e. every 6 months) routines of costly maintenance must be carried out when used in SIL3 applications.**
Can the safety system vendor confirm that within SIL3 applications no routine maintenance is required?

25. Support.

➢ **Vendor support for critical controllers employed in high integrity applications is paramount to reliable, efficient and safe plants.**
Can the safety system vendor confirm and demonstrate their timely response with specialist (i.e. fully trained) assistance in a 24 hour, 365 day per year, globally co-ordinated environment?