

Things to consider when selecting a safety system

By Paul Gruhn, PE, CFSE
ICS Triplex
Houston, TX

KEYWORDS

Safety Instrumented System, SIS, Safety PLC, Safety

ABSTRACT

This paper offers a scoring/selection criteria for safety instrumented system programmable logic solvers based on three dozen different criteria. Company, hardware and software issues are considered. Each factor is initially scaled from -2 and +2. However, different criteria should have different weighting factors based on different application requirements. Criteria that are not important (e.g., size may not matter for a land based installation, fault tolerance may not be important for a batch operation, etc.) should be rated as 0 so as not to falsely skew the overall rating based on something that doesn't matter. Criteria that may be very important (e.g., fault tolerance when uptime is critical, small size for an offshore application, very high speed for turbomachinery, etc.) should have a multiplication or weighting factor applied. Such criteria would then have a rating scale of -4 to +4, or -6 to +6, to show their greater significance. Numbers can then be totaled for an overall score, as well as viewed in a table providing an easy visual ranking (i.e., system X has more positive scores than system Y).

INTRODUCTION

Just as each project is different, what is the most appropriate safety system may differ for each project as well.

Vendors will often promote what they believe to be their unique differentiators and why they believe their system to be the best. Unfortunately, what a vendor perceives as an important feature may not always have an associated real benefit in the mind of the user. Every system can't be "best". Ford, Chevy and Chrysler don't all tell people they make the "best" car. Besides, you don't need what's "best" (e.g., are you driving a Rolls Royce, or do you even consider that to be the "best" car?) All you really need is *what's suitable* for your application at *a price you're willing to pay, from someone you trust* (e.g., a used Ford sedan from a dealer where a friend of yours is a salesman).

Most requests for quotations (RFQs) for safety logic solvers in the process industry call for SIL 3 certification. While there are very few SIL 3 requirements for safety instrumented functions (including

field devices, not just the logic solver), if you have just one SIL 3 loop, that may be reason enough to specify a SIL 3 rated logic solver (as the logic solver is common to all the loops). Specifying a SIL 3 rated logic solver is often viewed as a conservative and safe choice, even if you don't have any SIL 3 requirements. However, over specifying may mean over spending, so perhaps it may make sense to consider potentially lower cost hardware that only meets SIL 2 requirements.

Like most things in life, when there are few choices available, selecting between them is relatively simple. However, when the number of available selections is large, and they all differ from each other in a myriad of ways, choosing between them can seem overwhelming. Rather than decide in such cases, some fall back on the old saying "nobody got fired for buying IBM". In the process industry, this is often referred to as "the herd mentality" (you can't be faulted for doing what the rest of the herd is doing). But what if in reality a group of cavemen are purposely driving the herd over a cliff? What if it's really the lemming mentality? If your peers wear purple spiked hair, are you going to also?

If a SIL 3 logic solver is desired, there are approximately a dozen different manufacturers to choose from, and five basic configurations (i.e., simplex, hot back-up, 1oo2D, triplicated and quad). How can you choose between them all?

This paper offers a scoring system based on evaluating three dozen different criteria. Each factor is initially scaled from -2 and +2. However, different criteria should have different weighting factors based on different application requirements. Criteria that are not important (e.g., size may not matter for a land based installation, fault tolerance may not be important for a batch operation, etc.) should be rated as 0 so as not to falsely skew the overall rating based on something that doesn't matter. Criteria that may be very important (e.g., fault tolerance when uptime is critical, small size for an offshore application, very high speed for turbomachinery, etc.) should have a multiplication or weighting factor applied. Such criteria would then have a rating scale of -4 to +4, or -6 to +6, to show their greater significance. Numbers can then be totaled for an overall score, as well as viewed in a table providing an easy visual ranking (i.e., system X has more positive scores than system Y).

COMPANY ISSUES

Knowledgeable Staff

Companies don't deal with companies; people deal with people. Many users have downsized to the point where they must rely on outside expertise and support. Two types of knowledge should be considered; the vendors knowledge of their products, as well as their knowledge and understanding of your industry, applications and best practices. For example, can they help you develop your specifications, provide the best practices for implementing overrides, etc.? Are their people involved in standards development? Do their people have safety certificates or certifications?

-2	-1	0	+1	+2
----	----	---	----	----

Relationship with Vendor

If you currently have equipment from one vendor, how well have they been supporting you? If you're installing a new system in another part of your plant, do you really want a completely different system than the one you may already have, be used to and have spare parts for? If you buy a second system from another vendor, you'll have to send people to more training classes, stock more spare parts, etc. The devil you know may be better than the devil you don't. You don't change spouses just because a prettier version walks by (no matter how much you may want to); the cost of "change" may be too great. Or, might you be replacing all your systems plant-wide? Is your current system aging and becoming difficult to support? Does your current vendor have a migration path to a newer system? Sometimes, the cost of *not* changing may be too great.

-2	-1	0	+1	+2
----	----	---	----	----

Support

No matter how superior a product may be, there will always be at least one problem at some point. Downtime costs a lot of money in some industries. Can the vendor provide the timely support you need? This may be remote via the phone and/or internet. Do they have service people that can travel to your location? Do they have people — their own or partners — that are local and can provide service even quicker? Do they offer support agreements or contracts?

-2	-1	0	+1	+2
----	----	---	----	----

Integration by Third Parties

Some vendors will not allow others to integrate their hardware. This could be due to their wishing to limit their liability, their product may be too difficult for others to integrate, or they may simply wish to keep their staff of specialists employed. If that vendor has no presence in your geographical area, you may not be comfortable with the remote relationship, or it may not meet contractual requirements for local content (e.g., for political or funding reasons). Other vendors do allow other companies to integrate their hardware. This allows you to work with your preferred local integration companies that offer you local support and service. However, dealing with a local company is no guarantee of success. The local company may not know the system nearly as well as they may say, and they may let the project people (and their knowledge) go once the job is over. The local company may not be able to help you in the future when you have a problem. Successful, long term relationships are often forged by having local representatives working with the vendor during project execution, system testing and installation.

-2	-1	0	+1	+2
----	----	---	----	----

HARDWARE ISSUES

Fault Tolerance Requirements

Everything fails; it's just a matter of when. Is the ability of continuing to operate in the presence of faults important to you or not? What is the cost, as well as the safety impact, of an unnecessary and unplanned shutdown?

When Simplex is Good Enough

If process uptime is not critical, and a shutdown caused by a non-redundant module failing is not a major problem in terms of lost production downtime and/or safety, then a simplex (1oo1) solution will be an acceptable and lowest cost solution.

When Redundancy is Called For

If process uptime is critical (e.g., an unnecessary and unplanned shutdown in a refinery has a significant financial as well as safety impact), then a redundant logic solver will be worth the extra expense. However, not all redundant systems offer the same level of fault tolerance.

1oo2D

The concept of 1oo2D is relatively simple. The system is dual redundant with both sides active and operating with their outputs in parallel (assuming energized outputs). Both sides must de-energize in order to cause a shutdown. If one side fails dangerously (i.e., stuck), diagnostics will detect the failure and open a secondary output, thereby changing the configuration of the system to running on the remaining healthy side. This system offers a fault tolerance of 1. (A fault tolerance of X means if there are X+1 dangerous failures, the safety function will not work.)

The limitation of any such design is that *no* system has 100% diagnostics. If the two channels in a dual redundant system don't agree, which one is correct? (If you have two watches and they don't agree, which one is correct?) Any undiagnosed discrepancy in such a system causes a shutdown (i.e., nuisance trip). This *does* happen in the real world. Operators of such system have been known to disable this discrepancy diagnostic feature in order to avoid nuisance trips. This naturally violates the system's safety manual.

Another limitation of some 1oo2D designs is that if *any* of the modules on one side fail, the entire system switches to run on the remaining side. If *any* of the modules then fail on the single remaining side, the system will shut down.

2oo3

Tripllicated systems offer the highest level of fault tolerance. If one slice disagrees from the other two, it is easily detected and outvoted. (If you have three watches and one of them disagrees with the other two, it's pretty easy to decide which one has the problem.) When one slice fails on one module, the

system does not “switch”; the module and the rest of the system continue operating. *Multiple* modules can all have single slice failures, and the modules and system will continue operating. If process uptime is critically important, triplicated systems offer the highest level of fault tolerance and online availability.

2oo4D

While quad certainly sounds better than triplicated, some of these systems only offer quad processors; the I/O modules are still simplex or dual redundant. Therefore, some of these are really just enhanced dual systems designed to get around the weakness of early 1oo2D systems and their degraded run-time restriction.

Score a fail-safe 1oo2 system as -1, hot back-up and 1oo1 systems as 0, 1oo2D and 2oo4D as +1, and 2oo3 as +2.

-2	-1	0	+1	+2
----	----	---	----	----

Configuration Flexibility

Most systems have a mixture of different SIL and fault tolerance requirements. Some portions of the system may have a low safety requirement, some a high requirement. Some portion may require fault tolerance, other portions may not. However, most redundant logic systems incorporate the same level of redundancy throughout (i.e., every module is dual or triple redundant). This means some functions may have more safety and fault tolerance (and the associated cost) than is really necessary. At least one system allows the user to select for *each* module (processors and I/O), the level of fault tolerance actually required. One input module could be simplex, another dual, and yet another triplicated. The user can mix and match portions of the system to their exact requirements and avoid the costs associated with over-designing certain portions of the system.

-2	-1	0	+1	+2
----	----	---	----	----

Size

Size is critical in some applications (e.g., offshore platforms, FPSOs: Floating, Production, Storage, Offloading vessels). In general, the more redundant a system gets, the larger it gets. Most dual redundant systems require identical redundant chassis (i.e., mirror images of each other), even if you have only a few modules in a chassis. Not all triplicated systems are the same size. Some configurations have a ‘module – spare slot – module – spare slot’ arrangement (with the spare slots used to replace an active module online without affecting the process). One system offers a much more compact arrangement with only one or a few empty slots needed to replace any I/O module in the system. This can result in a 50% reduction in system size.

If size is not important for your application, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Distributiveness

Some systems (and most triplicated systems) were designed for relatively large I/O applications. The systems are relatively expensive and difficult to justify for low I/O count systems (e.g., < 100 I/O). In order to justify and implement such systems in the past, many users combined separate smaller systems into one larger centralized system. This may have added costs associated with more field wiring and potential common cause problems (where a failure of the single centralized system now impacts many different process units). One monolithic system may be suitable for your needs. However, some systems are available with small I/O counts making them now cost effective to implement in the originally desired distributed manner. Such systems will utilize standard networks to pass data back and forth between them. It may be too early to tell whether one large monolithic system is easier to maintain and has lower life cycle costs than multiple smaller distributed systems.

-2	-1	0	+1	+2
----	----	---	----	----

Environmental Ruggedness

Some systems are designed to be remote mounted in the field with little power draw and no forced cooling (i.e., fans). Some systems are too large or not rugged enough to mount locally. Field mounting equipment usually results in lower field device wiring and installation costs. Evaluate the systems immunity to EMI/RFI interference, vibration and shock limits, temperature limits, etc.

If environmental ruggedness is not important for your application (e.g., it will be mounted in an environmentally controlled internal rack room), score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Scan Time

Speed of response is important for some applications such as high speed exothermic reactors and turbomachinery control. It may not matter at all if you're closing valves with 30 second travel times. Throughput (response) time of most PLCs ranges between two and three scans. Most safety PLCs will have scan times ranging between 50 and 500 msec. Scan time is not necessarily determined by processor type, clock or bus speed, so don't evaluate something that doesn't really matter. Rather than a scaled ranking, this choice is a binary yes/no decision as a system will either meet your speed requirement or it won't.

Acceptable	Not Acceptable
------------	----------------

SOE Resolution

When something shuts your process down, you want to know what happened and in what order. Most systems offer some form of SOE (Sequence Of Events) recording. Some systems time tag the events at the I/O modules with true 1 msec resolution. Some systems time tag the events at the main processor and therefore only have the resolution of the processor scan time (as the clock is read once per scan, no matter whether the clock itself has 1 msec resolution or not). In such systems, if four inputs change state during one scan, they will all be given the same time stamp. If you have a high speed process (e.g., an exothermic reactor with dozens of temperature inputs) this may be very important. If you have low speed process (e.g., tank levels) this may not be important at all.

-2	-1	0	+1	+2
----	----	---	----	----

Range of I/O Modules

Does the system only offer 24Vdc digital inputs and outputs? Does it incorporate the range of analog (e.g., current, voltage, thermocouple, RTD) and high voltage modules you may need? Requiring interposing relays just adds to the complexity and cost of the system and will degrade overall system performance.

-2	-1	0	+1	+2
----	----	---	----	----

Certification Restrictions

Merely knowing that a system has a TÜV (or other agency) certificate is not enough. The modules you want to use may not be certified for safety applications. There may be restrictions on the time limit and conditions associated with changing modules that you may not be happy with. There may be restrictions on additional hardware you may need to add, or online software changes that you may not be allowed to make. Read the vendor's full certification report and safety manual to gain a better understanding of their restrictions.

-2	-1	0	+1	+2
----	----	---	----	----

Module DIP Switches or Settings

Some modules of some systems require DIP switches and/or jumpers to be set prior to use (e.g., different analog input ranges, RTD settings, etc.). Systems have failed and caused damage because technicians were unaware of the settings that needed to be made. Systems that do not require any switch or jumper settings offer greater resistance to human error.

-2	-1	0	+1	+2
----	----	---	----	----

Ease of Changing a Processor and I/O Module

When a module fails – and they will – how easy are they to change? Some are as simple as “pull the old one out, plug a new one in and you're done – while the system and the process continue running the entire time”. Replacing a processor in some other systems can be a rather convoluted process with potential for human error. One vendor has a 14 page procedure! Have your vendor actually demonstrate this for you. How easy is it? How long does it take? What are the chances of error? Check out the same capability for replacing an I/O module.

-2	-1	0	+1	+2
----	----	---	----	----

Time Synchronization

Many safety systems today are large and distributed. Each system will usually be performing its own sequence of events recording and there may be one events viewer or collector grabbing data from all the different systems. One issue to consider is how closely the clocks can be synchronized between the different systems. If you know events must have happened in a certain order, but the time stamps between different systems indicate otherwise, then the clocks are not synchronized closely enough for much of the data to be useful. One method of synchronizing clocks in multiple safety systems has been to have the control system pulse the safety systems in some manner (e.g., once per day at noon). Depending upon the method used, this may still offer a resolution no better than a few scans or possibly seconds. A better method would be to have all the systems utilize clock signals from global satellites. This allows multiple systems to all be synchronized to within 1 msec of each other. There are systems with this capability. Another method would be to use Windows time servers and SNTP (Simple Network Time Protocol).

If you will not be having *multiple* systems jointly providing sequence of events information, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Same modules for Remote I/O and Line Monitoring?

Many systems offer remote I/O capabilities and modules that have line monitoring capabilities (the ability to detect open and short circuits in normally de-energize loops). However, some systems require different modules for local vs. remote I/O and different modules for line monitoring. Some systems utilize the *same* modules, thus simplifying spares and eliminating potential errors of installing an incorrect module.

If you do not require remote I/O or line monitoring, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Certified Safety Communications

Some systems consist of multiple safety controllers. In such cases it is usually necessary for the systems to share data amongst themselves (e.g., if one unit shuts down, others may need to go to reduced capacity or shut down also). Rather than hard wiring I/O between them (which is very expensive), many systems offer some form of certified communications between them, some independent of the actual media (i.e., wire or radio).

If you do not plan on having multiple systems share data, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Connectivity

What are the connectivity choices to your control system, human machine interfaces and other third party equipment? Ethernet, serial, OPC, Modbus? How many connections do you need and what can the system support? Are redundant communications possible? Are separate gateways required (adding to the complexity, engineering and overall cost of the system)? Does the safety system have a direct highway connection to the control system?

-2	-1	0	+1	+2
----	----	---	----	----

Remote I/O Capabilities

Field wiring of sensors and final elements to termination assemblies is very expensive. If I/O modules can be mounted remotely (i.e., closer to the field devices), thousands of dollars can be saved per loop by eliminating much of the field wiring. Remote I/O modules only requires a single cable between the I/O chassis and controller. Some systems are small enough to have I/O and processing mounted in the field, with a network connection between controllers for sharing data.

-2	-1	0	+1	+2
----	----	---	----	----

Automatic, Built-in Valve Testing

Using a logic solver rated for use in SIL 2 or 3 does not provide you with a SIL 2 or 3 system. Field devices play a major role in overall system performance. The fault tolerance tables included in the IEC 61511 standard show that sensors and valves will typically need to be redundant even for SIL 2. However, it is possible to design SIL 2 systems with simplex, non-redundant field devices. One way of doing this with valves is using partial stroke testing (to determine if a valve is stuck, the predominant failure mode in dormant safety applications where valves are left in single positions for long periods of time). There are over a dozen different methods of partially stoking a valve. Some methods are manual and labor intensive. Some methods are automatic, but require additional hardware and software (increasing hardware, engineering and overall costs). Some methods do not fully test the entire output shutdown path and all the devices. Some methods do test all the devices in the path and do not require additional hardware or software.

If you are not implementing partial stroke valve testing, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Capability of Adding Modules Online

Just as programs will change over time, hardware may also need to be changed (e.g., added to) over time due to plant expansion. Some systems do not allow online changes and must be restarted in order to recognize the new hardware. Some systems can have missing modules configured for 'simulate', and will accept the actual module when inserted (although it's unlikely that you'll know what modules you're going to add years in the future). Some systems allow you to add modules online (although some systems have been known to accidentally and unintentionally shut down when doing so). Working on, or adding to, any system 'live', poses a higher level of risk that many are unwilling to accept.

-2	-1	0	+1	+2
----	----	---	----	----

Conformal Coating of Modules

Systems located in tropical environments may benefit from conformal coating. However, conformal coating usually retains heat and can make the modules run hotter and cause other problems and premature failures.

Unless your system is located in a severe tropical environment, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Busses

If you are using Profibus and Profisafe, can the safety system accept such data? (There are relatively few field devices available in the process industries that incorporate Profisafe.) Foundation Fieldbus is not yet available for safety applications (as of the summer of 2008). Many field devices implement HART, yet only a few safety logic solvers are able to utilize such information.

-2	-1	0	+1	+2
----	----	---	----	----

Ability to Detect Field Device Failures

Can an input module detect a transmitter going out of range and indicate a failure, rather than cause a spurious trip? Can modules detect open and short circuit wiring problems? Can an output module read back current and voltage and detect load problems and impending faults (e.g., a solenoid coil is about to burn out).

-2	-1	0	+1	+2
----	----	---	----	----

Size of Installed Base

A product with a larger installed base often means that vendor is doing something right, whether their hardware is superior or not. However, one vendor may dominate in one area of the world (e.g., Siemens in Europe), yet another may dominate elsewhere (e.g., Rockwell in North America). A brand new product may offer key features not available with any other system, yet offer no or little installed base early in its life cycle.

-2	-1	0	+1	+2
----	----	---	----	----

Years the Product has been in Service

A brand new product may offer features no one else may have, yet its use will entail some risk. What if the product flops and is pulled off the market (which has happened)? A product in the middle of its life cycle has the greatest chance of being around for a while longer. A product near the end of its life cycle may be 'long in the tooth' and run into support difficulties.

-2	-1	0	+1	+2
----	----	---	----	----

Documentation

Check out the products technical documentation and training materials. Does the level of detail of the system integration drawings meet your needs?

-2	-1	0	+1	+2
----	----	---	----	----

SOFTWARE ISSUES

Programming Languages

The IEC 61131-3 standard defines five PLC programming languages (ladder logic, function block, structured text, instruction list and sequential function chart). Some systems offer only one language, some offer several, some offer all five. Some systems offer additional languages not defined in the standard (e.g., cause & effect programming, flow chart). While cause & effect programming has certain advantages, most detailed logic cannot be programmed that way. Different languages are suitable for different tasks. Force fitting a sequential operation into ladder logic can be difficult and awkward. Performing math calculations in function blocks is also awkward. Using the most appropriate language can reduce development and testing time, as well as make the program easier to read, understand and maintain by others. Does the software offer you the flexibility you desire?

-2	-1	0	+1	+2
----	----	---	----	----

Ease of Programming / Configuration

Most systems today offer a Windows based development station and at least one of the IEC 61131-3 programming languages. However, this does not mean all systems offer the same ease of configuration and programming!

Ask your vendors to demonstrate the following, while you time how long it takes to complete. Define/configure an input and output tag name; configure an input module and output module; write a simple application program that when the input turns on, the output turns on; compile the program; simulate the program. That can be done in some systems in less than five minutes. The exact same steps may take *ten times* longer in some other systems! Rather than watch them do it for you, have them coach you through the steps while you do it yourself. (After all, you'd rather personally drive a new car you're considering buying yourself rather than merely being driven around as a passenger.)

While this criterion may be subjective, try to compare apples to apples. Any new system will be different than the one you may be used to. Safety PLCs will generally have some configuration and programming restrictions compared to general purpose PLCs or DCSs.

-2	-1	0	+1	+2
----	----	---	----	----

Version Control & Comparison

All programs will change over time. MOC (Management Of Change) practices requires documentation and an impact study of any change. Some programming workstations do not save previous program versions (although this can always be done manually). Some do not have any version comparison features to determine what is actually different between program versions. Checking the differences manually is both time consuming and prone to human error. Some workstations automatically save all program versions and offer extensive comparison features, even printing out the difference between versions. This greatly eases recordkeeping and troubleshooting.

-2	-1	0	+1	+2
----	----	---	----	----

Online Changes (Programs and Firmware)

All programs will change over time. Some systems do not allow online program changes (the ability to update a program without bypassing or shutting the system or process down). Some systems allow only limited changes. Some systems allow virtually unlimited changes.

The *ease* of making changes is also very important. Some redundant systems require connecting to and loading each processor separately, usually taking one offline during the process. Such an update is prone to error. Other systems require only a single connection and a single download without taking anything offline. Have the vendor demonstrate this capability for you with a real system. Better yet, have them coach you through the process while *you* do it.

All systems also go through firmware (operating system level) changes. Most systems need to be shutdown in order to change firmware. At least one system allows even firmware changes to be done *online*.

-2	-1	0	+1	+2
----	----	---	----	----

Simulation Capabilities

There are different levels of simulation. Some systems do not offer any offline (PC based) simulation capabilities. Most offer off-line simulation where logic can be tested on a PC before downloading and running it in the actual controller. Some offer a more advanced level of simulation including connectivity with operator training simulators (OTS), where a simulation of the plant running on a computer can send data to a DCS and SIS simulator so operators can be trained using real dynamic scenarios of plant problems.

-2	-1	0	+1	+2
----	----	---	----	----

Ability to see Field and Logic Values of Forced Variables

All PLCs offer the ability to force I/O, often done during times of maintenance (e.g., if you're going to disconnect a sensor, you need to lock the input energized in order to prevent a shutdown). Forcing is done differently in each system, but one thing to consider is whether you can see both the logic and field values. Seeing only the logic value (e.g., the input is locked in logic) does *not* tell you whether the technician has correctly connected the wires or what state the device is actually in. Seeing *both* conditions will let you know what will (or will not) happen when you release the force.

-2	-1	0	+1	+2
----	----	---	----	----

Security / Access Control

What level of security and access control does the system provide? How many password access levels are there and how configurable are they? Does the system have a method of preventing unauthorized downloads or changes?

-2	-1	0	+1	+2
----	----	---	----	----

Diagnostic Reporting & Asset Management

One key to achieving high safety is extensive diagnostics. Field devices constantly become more powerful and provide higher levels of diagnostics than in the past. Diagnostics can be used to alarm to operators when devices are degrading and in need of repair. Diagnostics can be used to indicate which sensor in a redundant pair may not be functioning properly and alter the voting configuration. Diagnostic information may be available via HART or other busses and used directly by the system. How capable is your system of incorporating this data, either directly or as a pass-through device to other systems for recording and trending purposes?

-2	-1	0	+1	+2
----	----	---	----	----

Author Bio: Paul Gruhn is the Training Manager at ICS Triplex in Houston, Texas. Paul is an ISA Fellow, a member of the ISA 84 standard committee, the developer and instructor of ISA courses on safety systems and co-author of the ISA textbook on the subject. He has a B.S. degree in Mechanical Engineering from Illinois Institute of Technology, is a licensed Professional Engineer (PE) in Texas, and a Certified Functional Safety Expert (CFSE).

Safety Logic Solver Ranking Criteria Summary

System: _____

Note: Criteria that are not important should be rated 0. Criteria that are more important should have an additional multiplication or weighting factor applied (i.e., be rated -4 to +4, or -6 to +6) to show their greater significance.

Company Issues:

Knowledgeable Staff

-2	-1	0	+1	+2
----	----	---	----	----

Relationship with Vendor

-2	-1	0	+1	+2
----	----	---	----	----

Support

-2	-1	0	+1	+2
----	----	---	----	----

Integration by Third Parties

-2	-1	0	+1	+2
----	----	---	----	----

Hardware Issues:

Fault Tolerance

Score a fail-safe 1oo2 system as -1, hot back-up and 1oo1 systems as 0, 1oo2D and 2oo4D systems as +1, and 2oo3 as +2.

-2	-1	0	+1	+2
----	----	---	----	----

Configuration Flexibility

The ability to match module safety and fault tolerance to the requirements of each function.

-2	-1	0	+1	+2
----	----	---	----	----

Size

If size is not important for your application, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Distributiveness

-2	-1	0	+1	+2
----	----	---	----	----

Environmental Ruggedness

If environmental ruggedness is not important for your application (e.g., it will be mounted in an environmentally controlled, internal rack room), score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Scan Time

Acceptable	Not Acceptable
------------	----------------

SOE Resolution

-2	-1	0	+1	+2
----	----	---	----	----

Range of I/O Modules

-2	-1	0	+1	+2
----	----	---	----	----

Certification Restrictions

-2	-1	0	+1	+2
----	----	---	----	----

Module DIP Switches or Settings

DIP switches or jumpers are considered a negative.

-2	-1	0	+1	+2
----	----	---	----	----

Ease of Changing a Processor and I/O Module

-2	-1	0	+1	+2
----	----	---	----	----

Time Synchronization

If you will not be having *multiple* systems jointly providing sequence of events information, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Same modules for Remote I/O and Line Monitoring

If you do not require remote I/O or line monitoring, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Certified Safety Communications

If you do not plan on having multiple systems share data, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Connectivity

-2	-1	0	+1	+2
----	----	---	----	----

Remote I/O Capabilities

-2	-1	0	+1	+2
----	----	---	----	----

Automatic, Built-in Valve Testing

If you are not implementing partial stroke valve testing, score this a 0.

-2	-1	0	+1	+2
----	----	---	----	----

Capability of Adding Modules Online

-2	-1	0	+1	+2
----	----	---	----	----

Conformal Coating of Modules

-2	-1	0	+1	+2
----	----	---	----	----

Busses

-2	-1	0	+1	+2
----	----	---	----	----

Ability to Detect Field Device Failures

-2	-1	0	+1	+2
----	----	---	----	----

Size of Installed Base

-2	-1	0	+1	+2
----	----	---	----	----

Years the Product has been in Service

-2	-1	0	+1	+2
----	----	---	----	----

Documentation

-2	-1	0	+1	+2
----	----	---	----	----

Software Issues:

Programming Languages

The more languages, the better.

-2	-1	0	+1	+2
----	----	---	----	----

Easy of Programming / Configuration

-2	-1	0	+1	+2
----	----	---	----	----

Version Control & Comparison

-2	-1	0	+1	+2
----	----	---	----	----

Online Changes (Programs and Firmware)

-2	-1	0	+1	+2
----	----	---	----	----

Simulation Capabilities

-2	-1	0	+1	+2
----	----	---	----	----

Ability to see Field and Logic Values of Forced Variables

-2	-1	0	+1	+2
----	----	---	----	----

Security / Access Control

-2	-1	0	+1	+2
----	----	---	----	----

Diagnostic Reporting & Asset Management

-2	-1	0	+1	+2
----	----	---	----	----

Total Score: