COMBINED PROCESS CONTROL SYSTEMS AND SAFETY INSTRUMENTED SYSTEMS (SIS) DEMONSTRATION OF INDEPENDENCE

DISCLAIMER

[1] *The Association would welcome any comments on this publication, see http://www.61508.org/contact.htm. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither The 61508 Association nor any of its members will assume liability for any use made thereof.*

[2] These guidelines have been produced by The 61508 Association to assist its members and others to consider how to deal with combined BPSC and SIS systems. *The Association would welcome any comments on this publication, sent to legacy@61508.org. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither The 61508 Association nor any of its members will assume liability for any use made thereof.*

Contents

Revision History

Version	Date	Author	Comments
1	12.10.2015	The 61508 Association	For Publication

1 Introduction

This document is intended primarily for the Duty Holder and for the designers of SIS which includes the end user, Engineering Procurement and Construction (EPC) companies and also System Integrators (Sis), however the content may have relevance to other SIS stakeholders.

Process control systems from reputable automation manufacturers are increasingly available that offer the opportunity to integrate the SIS with the Basic Process Control System (BPCS). For an end user the question remains concerning the demonstration of independence.

Automation manufacturers are able to provide both the hardware and systematic capability information and this must be combined with careful consideration of the needs of each Safety Instrumented Function (SIF) that is to be included in the total system.

The system must show sufficient independence between safety instrumented functions and basic process control has been implemented. This guidance is intended to help identify the areas where independence *may* be compromised by integration and prompt the collation of the information necessary to demonstrate the extent of independence provided by the completed, installed system.

Process control systems currently offered are mainly process plant control systems and so this guidance references both IEC61508 and IEC61511 standards but is primarily focussed on users of IEC61511.

When selecting the architecture of an integrated BPCS & SIS, due consideration of the following points is recommended to ensure the proposed solution is appropriate for the application and the duty holder; and also maintains compliance to the relevant good practice standards;

- Adherence to policy, standards and recommended practices issued by the Duty Holder relating to the specification, design, engineering, installation, verification, operation, validation and maintenance of both BPCS & SIS.
- Evidenced competence of all stakeholders involved in the supply chain for BPCS & SIS.
- Evidenced competence of the duty holder and those responsible for the continued operation and maintenance of the BPCS & SIS after handover.
- Adherence to prevailing international and national regulations, standards and good practice.

Note: - Commercial topics are not considered to be in the scope of this guidance however stakeholders are encouraged to consider the overall total cost of ownership of the BPCS & SIS for the full lifecycle of the plant and not just the up-front purchase cost in isolation.

2 Working Group Deliverables

Background

There is a trend in the Functional Safety World for manufacturers to combine BPCS with SIS into one unit.

Does this go against the advice given in 61508 to always keep them separate? The advice is supported by many technical books on the subject. In general, the advice is to keep the Policeman (the SIS) separate from the executive (The PLC).

Deliverables

- To generate a guidance document on the use of combined BPCS and SIS that summarises the Pros and Cons.
- That compares the risks and benefits conferred by each system
- That gives references for support of any advice given. If the driving force is to save money can this be justified against any increased risk?
- To help engineers decide which course of action to follow. To use combined systems or separate systems.

Factors considered when developing this guide

- Why separate BPCS and SIS?
- Why not separate BPCS and SIS?
- What legal obligations are there (or, are there not) to follow either course of action?
- Comparative costs of the alternatives e.g. capital costs (software and hardware); maintenance costs; design costs;
- Is there any increased risk in a combined system?
- What are the advantages / disadvantages of each system?
- What is the history of the development?
- Who is pushing for the change? Why?
- Who is pushing to retain the status quo? Why?

The working group did not confine themselves to the bullet points above but sought to cover the subject thoroughly and, if possible, give advice on the best (safest ALARP) course of action in accordance with 61508.

3 Objective

The IEC61508 group of standards all write that the complete independence of the SIS from the BPCS is the ideal but simultaneously recognise that this cannot always be done. Thus the standards themselves recognise that there may exist genuine reasons why the two should be interlinked or combined. In such circumstances the standards ask for sufficient independence:

IEC 61508-2: 2010 states:

"7.4.2.3 Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is **sufficiently independent** (i.e. that the failure of any non-safety-related functions does not cause a dangerous failure of the safety-related functions).

NOTE 1 *Sufficient independence of implementation is established by showing that the probability of a dependent failure between the non-safety and safety-related parts is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.*

NOTE 2 *Caution should be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. While this is allowed in the standard, it may lead to greater complexity and increase the difficulty in carrying out E/E/PE system safety lifecycle activities (for example design, validation, functional safety assessment and maintenance)."*

Similarly IEC61511-1 states:

11.2.2 Where the SIS is to implement both safety and non-safety instrumented function(s) then all the hardware and software that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL.

NOTE 1: Wherever practicable, the safety instrumented functions should be separated from the non-safety instrumented functions.

NOTE 2: Adequate independence means that neither the failure of any non-safety functions nor the programming access to the non-safety software functions is capable of causing a dangerous failure of the safety instrumented functions.

11.2.3 Where the SIS is to implement safety instrumented functions of different safety integrity levels, then the shared or common hardware and software shall conform to the highest safety integrity level unless it can be shown that the safety instrumented functions of lower safety integrity level cannot negatively affect the safety instrumented functions of higher safety integrity levels.

11.2.4 If it is intended not to qualify the basic process control system to this standard, then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.

NOTE 1: Operating information may be exchanged but should not compromise the functional safety of the SIS.

NOTE 2: Devices of the SIS may also be used for functions of the basic process control system if it can be shown that a failure of the basic process control system does not compromise the safety instrumented functions of the safety instrumented system."

When assessing a process control system that contains safety functions, it is necessary to assess the hardware, the architecture, the installation, the software, the defences against control alterations

affecting safety systems, the management of change and other factors. This is not simply a matter of assessing the manufacturer's product information but also includes aspects of concern to the designer of the safety instrumented function, the systems integrator, the installer and the operator/maintainer of the system.

The objective of this guidance is to provide an overview of the different considerations for independence and provide a means to formally document the responses.

4 Independent Protection Layers

A safety instrumented protection function is forming an independent protection layer and therefore must conform to the basic requirements of an IPL:

- Specific
- Independent
- Dependable
- Auditable
-

For example, IEC61511 Part 3 clause F.2 states:

F.9 Independent Protection Layers (IPL)

…. The criteria to qualify a Protection Layer (PL) as an IPL are:

– *The protection provided reduces the identified risk by a large amount, that is, a minimum of a 100-fold reduction;*
– *The protective function is provided with a high degree of availability (0,9 or greater);*
– *It has the following important characteristics:*

a) Specificity: An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (for example, a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event; and, therefore, multiple event scenarios may initiate action of one IPL

b) Independence: An IPL is independent of the other protection layers associated with the identified danger.

c) Dependability: It can be counted on to do what it was designed to do. Both random and systematic failure modes are addressed in the design.

d) Auditability: It is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system is necessary.

Only those protection layers that meet the tests of availability, specificity, independence, dependability, and auditability are classified as independent protection layers.

Specificity: Each safety instrumented function must be specifically designed to be capable of preventing the consequence under consideration.

Independence: The protection layer must operate completely independently of all other protection layers.

Dependability: The device must be able to dependably either prevent the consequence from occurring or mitigate the unwanted event down to an acceptable level.

Auditability: The device should be proof tested and maintained. Its configuration should allow for proper audit of the installed system compared to design and for audit of all proof testing and maintenance activities.

5 Considerations for demonstrating independence

The following table is intended to guide and support the end user with a series of prompts when considering areas where independence might be compromised by an integrated BPCS and SIS. It is intended that the response column be used to document whether the point raised in the first column has been addressed and, if so, how.

- If the response is positive then supporting information should be provided.
- If the response is negative but the point has been addressed in some other way then the response box can be used to indicate this and supporting information provided.
- If the point in question is not relevant then the response box can be used to indicate why it is not relevant.

Please also refer to the guidance notes toward the end of this document to aid completion

Competence/training/safety culture	**Response**
1. Are the hardware designers trained to understand the causes and consequences of common cause failures between BPCS & SIS hardware? Is this training recorded as part of overall competency management?	
2. Are the application program designers trained to understand the causes and consequences of common cause failures between BPCS & SIS software? Is this training recorded as part of overall competency management?	
3. Are the operators trained to understand the distinction between BPCS and SIS functions within operator graphics? 4. Is this training recorded as part of overall competency management?	
5. Are the maintainers trained to understand the causes and consequences of common cause failures between BPCS & SIS and associated field devices? ? Is this training recorded as part of overall competency management?	
6. Are the implications of an integrated/common architecture understood by maintenance and engineering for the purposes of maintenance and management of change?	
Safety, Security and Manufacturer guidelines	**Response**
1. Is the SIS component of the system fully certified to IEC 61508 in the proposed BPCS/SIS architecture (i.e. the total SIF that includes all parts)?	
2. Does the IEC 61508 certification, the safety manual and any standard documentation address separation of the SIS to ensure that BPCS is non-interfering with the SIS in the proposed architecture?	
3. If cyber security is to be considered then are there manufacturers' "Defence in Depth" cyber security policy and processes which will be followed for the proposed architecture?	
4. If security requirements are identified for this application and are in the integrator's scope then have the requirements of manufacturer security policy been adhered to sufficiently to provide required protection for the SIS?	
Location and Access Control	**Response**
1. Do the engineering tools support the differentiation of roles for BPCS and SIS engineer?	
2. Are there barriers in place to prevent unauthorised access to safety system application program during the realisation phase of the lifecycle?	

3. Are there barriers in place to prevent unauthorised access to safety system application program during the operation and maintenance phase of the lifecycle?	
4. Are personnel limited in their physical access to the safety instrumented systems (for example locked cabinets)?	
Procedures/human interface	**Response**
1. Is there separation/segregation of all SIS documentation in line with FSM requirements of IEC61511?	
2. Is there separation/segregation of access control to functions which interact with the SIS such as the ability to apply and change bypasses, overrides, trip limits??	
3. Is there auditability and traceability of user actions?	
4. Do the documented maintenance procedures specify that all parts of independent BPCS and SIS systems (for example, cables, etc.) intended to be separate are kept separate?	
5. Can the systems integrator provide certified evidence of their systematic capability to design & engineer the SIS?	
Separation/Segregation	**Response**
1. Is there appropriate separation/segregation of BPCS & SIS power supplies?	
2. Is there physical or logical separation/segregation of BPCS and SIS logic subsystems?	
3. Is there physical or logical separation/segregation of BPCS and SIS networks at the logic subsystem level?	
4. Is there separation/segregation of BPCS and SIS I/O bus if not one and the same?	
5. Is there separation/segregation of BPCS and SIS modules within an I/O rack?	
6. Is there separation/segregation of BPCS and SIS I/O racks?	
7. Is there separation/segregation of signal cables for BPCS & SIS I/O?	
8. Is there separation/segregation of safety and non-safety (i.e. standard) I/O subsystems?	
9. Is there separation/segregation of BPCS & SIS sensors and final elements? Is there clear, visible differentiation and assessment between safety and non-safety related items?	
10. Is there separation/segregation of engineering workstations for SIS and BPCS?	
11. Are the safety instrumented systems sensors / final elements connected to dedicated remote I/O stations i.e. not shared with BPCS	
12. If the safety instrumented systems have their own remote I/O stations are they within their own physically separate cabinets?	
13. Do remote I/O stations for safety instrumented systems have their own UPS and power supplies?	
14. Are all signal and power cables separate at all positions?	

15. Is there separation/segregation of engineering of application programs for BPCS and SIS i.e. different teams, different engineers? If not is there provision for peer review to help avoid common cause errors between BPCS and SIS application programs?	
16. Is there visual differentiation between the BPCS and SIS application programming as displayed in the engineering environment?	
17. Is there separation/segregation of verification and validation activities at the application program level?	
18. Is there separation/segregation of test procedures at the application program level and do different engineers do the BPCS & SIS testing	
19. Is there identification of SIS field hardware elements such that can they be easily distinguished?	
20. Is there separation/segregation of SIS logic solvers in separate, lockable cabinets?	
21. Are the SIS IO modules and terminations separate from BPCS?	
22. Are there documented procedures to ensure that BPCS and SIS elements which are designed to be separate and independent are not to be physically relocated such that this is compromised?	
23. Is dedicated earth grounding provided for the integrated system?	
Diversity/Redundancy	**Response**
1. Is there redundancy of cables for redundant networks for both BPCS and SIS? Are redundant cables physically separated?	
2. Is there redundancy of cables for redundant IO buses if carrying data for both BPCS and SIS? Are redundant cables physically separated?	
3. Is there sufficient redundancy of BPCS & SIS sensors and final elements to meet the HFT requirements?	
4. Where applicable do the sensors for safety systems employ different principles /designs from those used for the BPCS? For example, digital and analogue, different manufacturer or different technology?	
5. Is there redundancy of common controller hardware?	
6. Is there redundancy of common controller racks?	
7. Is there redundancy of common power supplies?	
8. Are the SIS HW designers autonomous from the BPCS HW designer during the design activities?	
9. Are the requirements to avoid common cause failures between SIS and BPCS hardware specified in the safety requirement specification?	
10. Are separate test methods and procedures used for BPCS and SIS respectively during commissioning?	
11. Are the SIS application program designers autonomous from BPCS application programmer designers during the design activities?	
12. Is there sufficient independence to facilitate maintenance of both BPCS and SIS?	

6 Appendix 1

Relevant Extracts from the standard

IEC61511 Part 1 says:

9.5 Requirements for preventing common cause, common mode and dependent failures

9.5.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between protection layers and between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative.

NOTE *For a definition of dependent failure, see 3.2.12*.

9.5.2 The assessment shall consider the following:

- independency between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS (for example, can plugging of relief valves cause the same problems as plugging of sensors in a SIS?).

11 SIS design and engineering

11.1 Objective

The objective of the requirements of this clause is to design one or multiple SIS to provide the safety instrumented function(s) and meet the specified safety integrity level(s).

11.2 General requirements

11.2.1 The design of the SIS shall be in accordance with the SIS safety requirements specifications, taking into account all the requirements of this clause.

11.2.2 Where the SIS is to implement both safety and non-safety instrumented function(s) then all the hardware and software that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL.

NOTE 1 *Wherever practicable, the safety instrumented functions should be separated from the non-safety instrumented functions*.

NOTE 2 *Adequate independence means that neither the failure of any non-safety functions nor the programming access to the non-safety software functions is capable of causing a dangerous failure of the safety instrumented functions*.

11.2.3 Where the SIS is to implement safety instrumented functions of different safety integrity levels, then the shared or common hardware and software shall conform to the highest safety integrity level unless it can be shown that the safety instrumented functions of lower safety integrity level cannot negatively affect the safety instrumented functions of higher safety integrity levels.

11.2.4 If it is intended not to qualify the basic process control system to this standard, then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.

NOTE 1 *Operating information may be exchanged but should not compromise the functional safety of the SIS.*

NOTE 2 *Devices of the SIS may also be used for functions of the basic process control system if it can be shown that a failure of the basic process control system does not compromise the safety instrumented functions of the safety instrumented system.*

…..

11.2.9 The design of the SIS shall take into consideration all aspects of independence and dependence between the SIS and BPCS, and the SIS and other protection layers.

11.2.10 A device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE *When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand for the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared component because if the shared component fails, a demand will be created immediately to which the SIS may not be capable of responding . For that reason, additional analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.*

IEC 61508 Part 2: 2010 says:

"7.4.2.3 Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is **sufficiently independent** (i.e. that the failure of any non-safety-related functions does not cause a dangerous failure of the safety-related functions).

NOTE 1 *Sufficient independence of implementation is established by showing that the probability of a dependent failure between the non-safety and safety-related parts is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved.*

NOTE 2 *Caution should be exercised if non-safety functions and safety functions are implemented in the same E/E/PE safety-related system. While this is allowed in the standard, it may lead to greater complexity and increase the difficulty in carrying out E/E/PE system safety lifecycle activities (for example design, validation, functional safety assessment and maintenance)."*

IEC 61508-1: 2010 says, in connection with safety requirements allocation:

"7.6.2.7 The allocation shall proceed taking into account the possibility of common cause failures. If the EUC control system, E/E/PE safety-related systems and other risk reduction measures are to be treated as independent for the allocation, they shall:

- be independent such that the likelihood of simultaneous failures between two or more of these different systems or measures is sufficiently low in relation to the required safety integrity;
- be functionally diverse (i.e. use totally different approaches to achieve the same results);
- be based on diverse technologies (i.e. use different types of equipment to achieve the same results);

NOTE 1 It is recognised that, however diverse the technology, in the case of high safety integrity systems with particularly severe consequences in the event of failure, special precautions will have to be taken against low probability common cause events, for example aircraft crashes and earthquakes.

- not share common parts, services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;
- not share common operational, maintenance or test procedures.

7.6.2.8 If not all of the requirements in 7.6.2.7 can be met then the E/E/PE safety-related systems and the other risk reduction measures shall not be treated as independent for the purposes of the safety allocation. Instead, the allocation shall take into account relevant common cause failures between the EUC control system, the E/E/PE safety-related systems and the other risk reduction measures.

NOTE 1 *For further information on analysing dependent failures see references [13] and [14] in the Bibliography.*

NOTE 2 *Sufficient independence is established by showing that the probability of a dependent failure is sufficiently low for the E/E/PE s*afety-related systems in comparison with the overall safety integrity requirements (see 7.6.2.7)."

7 Appendix 2

Additional guidance notes

Competence/training/safety culture	
1.	It is envisaged that hardware engineers may be tasked to work on either BPCS or SIS or both. They should understand the potential for common cause errors particularly if asked to work on both aspects of the system.
2.	It is envisaged that application programmers may work on either BPCS or SIS and, although not ideal from a separation standpoint, may work on both. Application programmers should understand the potential for common cause errors if asked to work on both aspects of the system and full peer review should be used as a defence against common cause errors being introduced in both BPCS and SIS.
3.	Operators should be able to easily differentiate between SIS and the BPCS within the HMI. Graphic elements relating to the SIS should be readily identifiable. Interaction with SIS functionality such as overrides, bypasses etc should be carefully controlled and restricted appropriately.
4.	Maintenance staff should easily be able to identify the SIS and its associated sensors and final elements. They should also understand the need to avoid adversely affecting the SIS when maintaining the BPCS. They should know to follow specific procedures when maintaining and proof testing the SIS. It is recommended that maintenance and testing of the SIS be covered by separate procedures.
5.	It is recommended that management of change (MOC) for BPCS and the SIS be covered by two separate procedures. MOC for the SIS should involve an impact analysis which may require earlier stages of the IEC 61511 lifecycle to be followed for any changes made.
Safety, security and manufacturer guidelines	
1.	Integrated systems currently available on the market typically have a third party certification to IEC 61508. Even the most integrated systems are designed in accordance with IEC 61508 to be capable of meeting SIL requirements. This has led to their increasing levels of acceptance in industry. Evidence of certification and associated reports and safety manuals should be kept.
2.	Documentation should address how to implement the system in such a way as to maintain separation of BPCS and SIS. Manufacturer's recommendations (in the form of the safety manual and other associated documentation) will need to be complied with.
3.	Manufacturers should have a documented approach to applying a 'Defence in Depth' concept for security. Cyber security concerns requirements shall be addressed for both interfaced and separate systems. This policy document will likely show how to implement a "safety" zone associated with the SIS with the necessary separation from the BPCS from a security perspective. End users should ascertain that such requirements exist and ensure that it has been complied with to the extent necessary to address any security threats.
4.	Any available manufacturer guidance should be followed during the system integration phase to ensure that security threats have been addressed in the design in accordance with the appropriate techniques and measures. The end user should also comply with any guidance relating to the operation phase of the lifecycle (e.g. patch management, anti-virus updates, use of memory sticks etc)
Location and Access Control	
1.	It may be that software configuration for BPCS and SIS is done on separate engineering workstations but, for some integrated systems, engineering can be done in a common engineering tool on a single engineering workstation. In either scenario it is important that access to safety application programming can be restricted such that only authorised, competent staff can make changes to SIS.
2.	For example by password protection of the safety program, via specific logins on a single workstation or by dedicated separate workstations each with separate logins. Use this response to elaborate on what techniques are used.
3.	This might be addressed by the point above but sometimes additional mechanisms exist to prevent inadvertent changes to the SIS i.e. a physical switch on the controller to make the SIS read-only and prevent any unauthorised or inadvertent changes to safety code. Again if such mechanisms exist then use this response to describe them.
4.	Where possible SIS cabinets should be locked and physical access controlled to prevent unauthorised access to the SIS. This is intended to protect against unauthorised or inadvertent changes of the SIS primarily during operation and maintenance.

Procedures/human interface
1. SIS documentation should be separate from that associated with the BPCS throughout the lifecycle. This should be the expected outcome if following an IEC 61511 lifecycle approach. Use the response to confirm.
2. Graphic elements relating to the SIS should be readily identifiable. Interaction with SIS functionality such as overrides, bypasses etc should be carefully controlled and restricted appropriately.
3. Operator action logs, traceability of changes etc are a useful tool in deterring unauthorised changes. Are such facilities available within the system, are they used and are they checked?
4. If certain elements of an integrated system are originally engineered to be physically separate for reasons of independence then this should not be compromised during maintenance or modification to the system.
5. Errors, omissions & faults during design should be avoided by following a structured, robust and systematic process utilising the appropriate techniques and measures as identified within IEC 61508. Competency assurance coupled with a compliant FSM which could be independently 3rd party certified is required for additional confidence during SIS design & engineering.
Separation/Segregation
1. For a traditional de-energise to trip ESD type system the power supply is not typically safety relevant but continuity of power may be an issue for energise to trip systems and separation and redundancy of SIS power supplies should be considered.
2. Integrated systems (that are partly or wholly integrated) typically have physically separate CPUs for BPCS and SIS. Often these are diverse but in some cases common (the same controller can be used for SIS or BPCS) but with extra functionality being invoked to provide embedded diversity and resistance to common cause. Appropriate separation may be best demonstrated by the third party accreditation of the system to IEC61508.
3. Integrated systems may have the option to use a single, common network for BPCS and SIS communications to the operator workstation and between controllers. Shared network solutions will typically use a black channel approach to achieve safety. Appropriate separation of this aspect may be best demonstrated by the third party accreditation of the system to IEC61508.
4. Some integrated systems use the same technology for communication between logic solver and I/O and, if I/O is mixed then a single bus or network can carry BPCS and SIS traffic. Safety protocols are used to ensure separation. Appropriate separation of this aspect may be best demonstrated by the third party accreditation of the system to IEC61508.
5. Even in a common/combined system it may make sense to separate BPCS and SIS I/O into separate racks to simplify identification and maintenance. If BPCS and SIS IO modules are placed in a common rack it should be ensured that a failure of the rack itself is not a common mode failure. Response to indicate what approach is taken and why it gives the necessary separation.
6. Even in a common/combined system it may make sense to separate BPCS and SIS I/O into separate racks to simplify identification of SIS assets as an aid to maintenance.
7. If there is a risk of a common cause error affecting the BPCS and SIS simultaneously it may make sense to separate I/O signal cables. If there is a risk of physical damage (e.g. from a forklift or other heavy equipment) then separation may be worthwhile.
8. Even in a common system it may make sense to separate BPCS and SIS I/O subsystems to simplify identification of SIS assets as an aid to maintenance
9. Generally BPCS and SIS should not share the same sensors and final elements. If they do then this should be justified in accordance with the standard through a quantitative analysis. Care should be taken not to take undue credit for risk reduction from both BPCS and SIS where there is an overlap.
10. Some systems give the possibility of a shared engineering workstation and provide additional levels of access control for the SIS functionality. This may be sufficient but there may be reason to consider separate engineering workstations for BPCS and SIS if such facilities do not exist or if BPCS and SIS need to be in separate zones for cyber security purposes.
11. Some systems will allow for BPCS and SIS I/O modules to co-reside in the same remote I/O station or rack. Where this functionality is provided then appropriate separation will likely be demonstrated by the third party accreditation of the system to IEC61508 however there may be merit in having separate remote I/O stations for BPCS and SIS to avoid BPCS maintenance adversely affecting the SIS.
12. If the remote I/O stations need to be placed in a cabinet then having a physically separate, lockable panel for field mounted SIS I/O again helps avoid BPCS maintenance adversely affecting the SIS.
13. No additional guidance
14. No additional guidance
15. No additional guidance

16.	No additional guidance
17.	No additional guidance
18.	No additional guidance
19.	Response should indicate how SIS field devices are clearly identified as safety critical elements,
20.	Access to SIS cabinets should ideally be controlled to prevent unauthorised access to the SIS. This is possible if controllers are physically separate but not possible if BPCS and SIS functionality in running in the same controller. In this latter scenario extra measures should be considered to address the lack of physical separation and justification for this approach should be made in the response.
21.	If logic solvers are physically separate then the I/O modules and terminations will also likely be separate. If BPCS and SIS functionality in running in the same controller then there may still be scope for physical separation of the I/O modules and terminations. If not separate then justification should be made in the response.
22.	Items which are designed to be separate should be kept separate. This should be stipulated in documented procedures.
Diversity/Redundancy	
1.	Plant availability and resistance to spurious trips can be achieved by use of redundancy. Spurious trips may not affect SIL but can often be detrimental to safety. Manufacturers and OEMs should be able to provide details regarding system availability as well as safety.
2.	If BPCS and SIS share the same network it is usual to make the network redundant and run cables physically separate to avoid spurious trips. Not separating them will likely not impact directly on the SIF but, by avoiding spurious trips, separation can also contribute to safety.
3.	Redundancy of sensors and final elements can be required to meet the requirements of IEC61511 in terms of hardware fault tolerance (HFT). Use of diverse technologies can be advantageous in helping avoid common cause - although this is not specifically an issue specific to integrated systems.
4.	Use of diverse technologies can be advantageous in helping avoid common cause - although this is not an issue specific to integrated systems.
5.	Some systems can use the same CPU hardware for BPCS and SIS functionality. This would typically be covered by diversity in the way in which the safety program is executed and covered by third part certification to IEC 61508 but, if used, these mechanisms should be understood by the engineer to ensure they are used correctly
6.	Some systems can use the same rack hardware for BPCS and SIS functionality. This would typically be covered by the third part certification to IEC 61508 but any special considerations should be taken into account during hardware design
7.	The power supply is seldom an issue for de-energise to trip applications but is important for energise to trip type applications. Sufficient integrity of power supply may require redundancy. In these circumstances diversity of power supply may also be helpful in avoiding common cause failures.
8.	For small projects it may be impractical to use different engineers but where the same engineer is working on the hardware design for both BPCS and SIS they should be particularly aware of the potential for common cause errors. Nevertheless, independence requirements shall be applied and demonstrated. Peer review may be a useful tool in helping ensure independence in this scenario.
9.	No additional guidance
10.	No additional guidance
11.	For small projects it may be impractical to use different engineers but where the same engineer is working on the application programming for both BPCS and SIS they should be particularly aware of the potential for common cause errors. Nevertheless, independence requirements shall be applied and demonstrated. Peer review may be a useful tool in helping ensure independence in this scenario.
12.	No additional guidance

10 61508 Association Recommended Practices

This document suggests one way of demonstrating the independence of a combined BPCS and SIS but does not seek to prescribe specific measures, since these will depend on the application, and any existing constraints of the installation.