The 61508 Association

Integrated and Separate ?

A document to aid the demonstration of Independence between Control & Safety

by The 61508 Association

Overriding key principle....it must be safe!

www.61508.org

The 61508 Association

Objective

To generate end-user guidance highlighting where increased integration of BPCS and SIS may impact on the fundamental requirement for separation; thereby equipping the end-user to act as an “intelligent customer” when purchasing, operating and maintaining an integrated control and safety system to ensure the requirements of the standard in terms of separation are met through the lifecycle.

The 61508 Association

What does IEC61511-1 Say? 1/2

11.2.2 Where the SIS is to implement both SIFs and non-SIFs then all the hardware, embedded software and application program 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 of any of the SIFs it can impact.

11.2.3 Where the SIS is to implement SIF of different SIL, then the shared or common hardware and embedded software and application program shall conform to the highest SIL.

NOTE 1: Embedded software or application programs of different SIL could coexist in the same device provided it can be demonstrated that the SIF of lower SIL cannot negatively affect the SIF of the higher SIL.

The 61508 Association

What does IEC61511-1 Say? 2/2

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.

The 61508 Association

Why Separate (in the context of IEC 61511)?

A SIS is normally separated from the BPCS for the following reasons:-

1. To reduce common cause, common mode and systematic failures, minimising the impact of BPCS failures on the SIS.
2. To retain flexibility for changes, maintenance, testing and documentation relating to the BPCS.
3. To facilitate the validation and functional safety assessment of the SIS.
4. To support access security and enhance cyber security for the SIS such that revisions to BPCS functions or data do not affect the SIS.
5. To reduce the amount of analysis that should occur to ensure that the SIS and BPCS are properly designed, verified and managed.

The 61508 Association

Separation

Compliance with IEC 61511-1 clause 11.2 requires a number of considerations regarding separation within an end-to-end SIF as part of an overall SIS covering but not limited to: :

a) Field sensors

b) Final control elements

c) Logic solver

d) Wiring

The main focus of this guidance document is c)

The 61508 Association

BPCS & SIS for Logic Solvers (C)

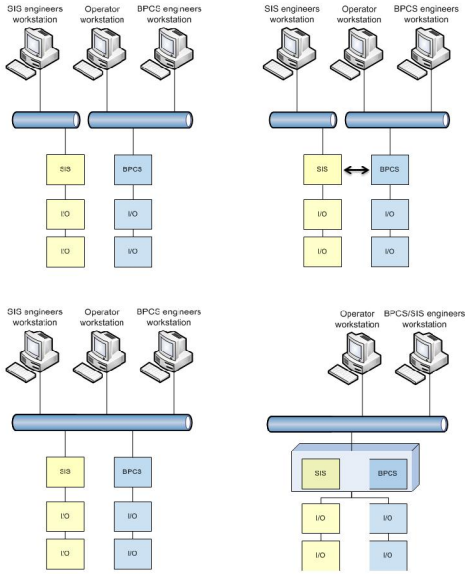
www.61508.org

The 61508 Association

BPCS & SIS Architectures

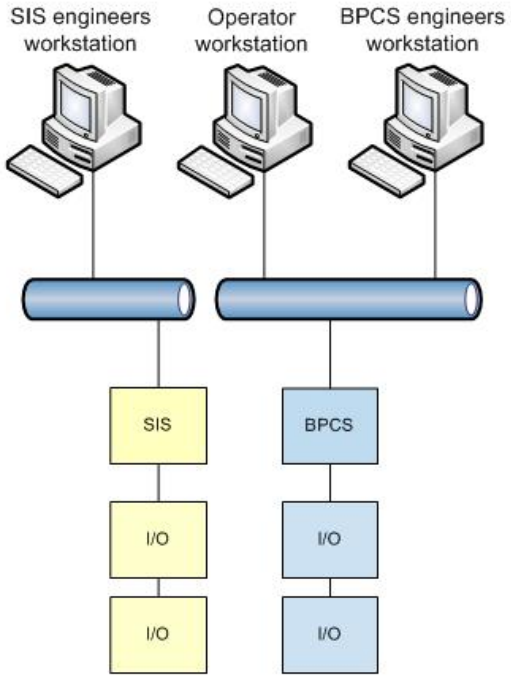
... are often described using the following categories :-

- Air gapped
- Interfaced
- Integrated
- Common



The 61508 Association

Air-gapped



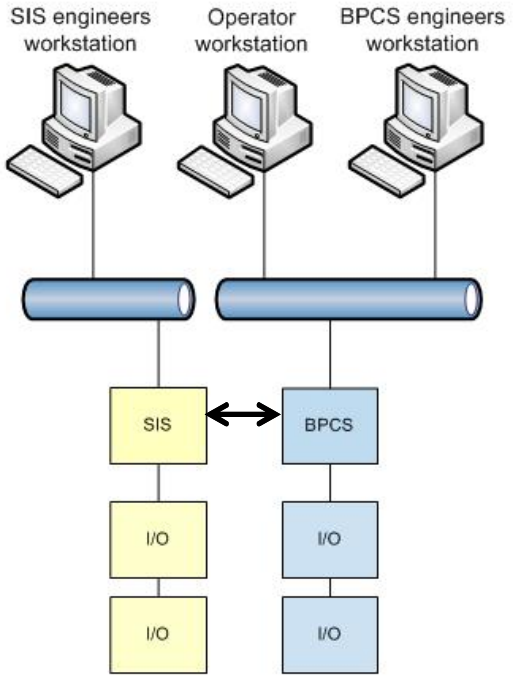
Physically Separate :-

- Engineering Software
- Engineering Workstation
- Networks
- Logic Solvers
- I/O subsystems

- Often from different suppliers
- Legacy concept

The 61508 Association

Interfaced

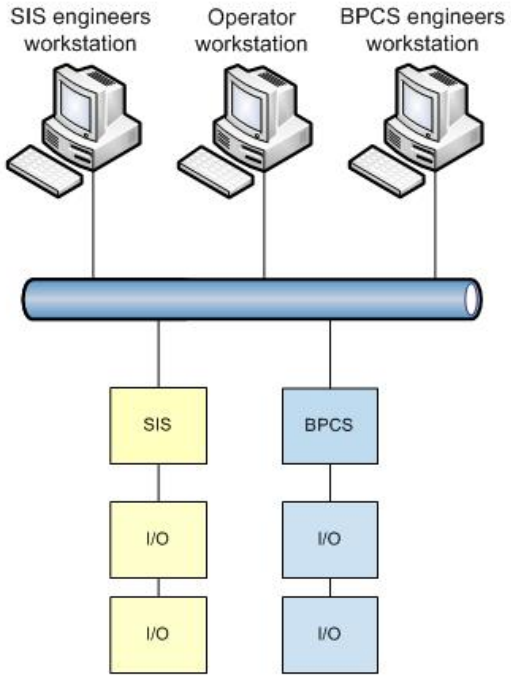


As air-gapped but with a data connection between BPCS and SIS logic solvers

- Typically via a simple RS232 link or modbus
- Typically a non routable protocol

The 61508 Association

Integrated



Retaining

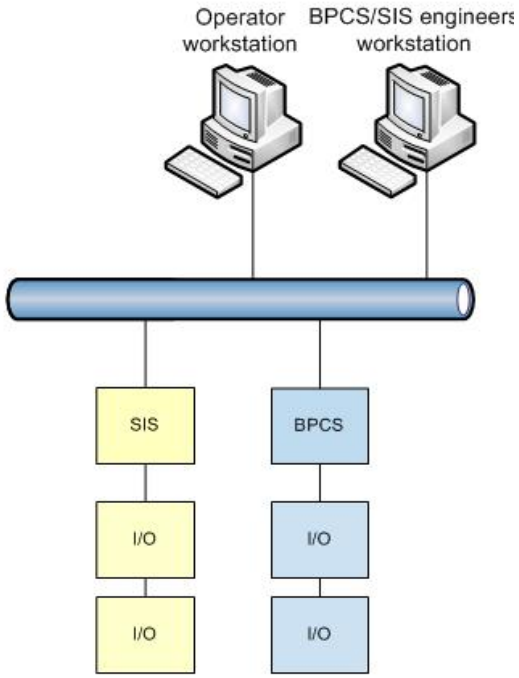
- Separate logic solvers
- Separate I/O

Now connected by common network

- Sometimes accompanied by increased commonality of hardware

The 61508 Association

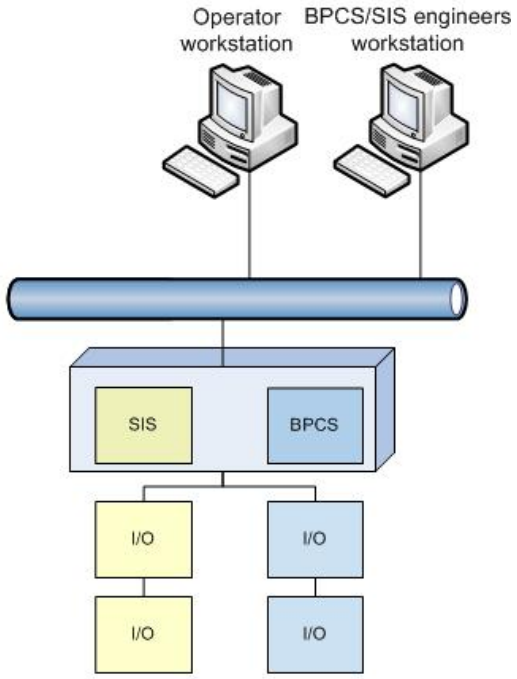
Integrated (a bit more)



Now additionally with a common engineer's workstation
... and therefore increased commonality of engineering tools

The 61508 Association

Common



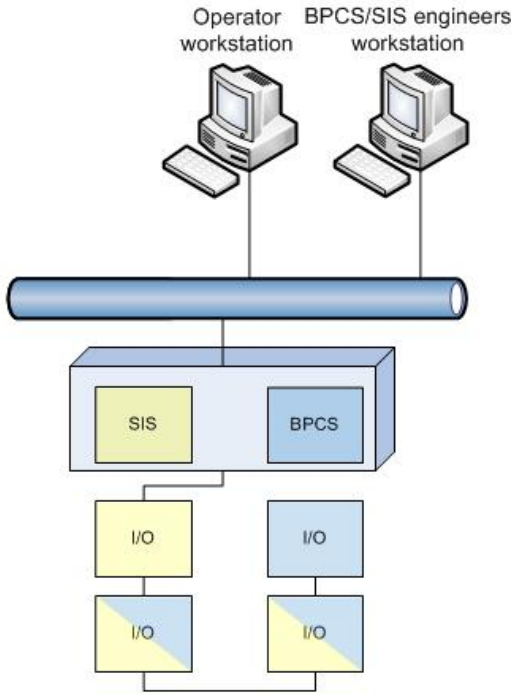
But now with BPCS and SIS functionality in same logic solver

•Retaining
- Separate I/O

•Also (depending on implementation)
- Separate and diverse logic solver CPUs
- Separate safety communications
- Increased diagnostic coverage

The 61508 Association

Common



And with the possibility to put BPCS and SIS I/O modules on the same I/O Network and in the same rack

The 61508 Association

In General

- All of the aforementioned system architectures will have a third-party certification to IEC 61508 Edition 2
- Legacy SISs were typically designed using air gapped and independent architectures"
- Integrated systems are increasingly prevalent
- Common or combined architectures are still few in number

The 61508 Association

Comments on Integrated & Common Architectures

Separation (and therefore independence) at the system level is achieved by a range of techniques :-

- embedded diversity in hardware/software
- Logical and physical separation of CPUs
- Black channel techniques for communications
- Sometimes specific CPUs for SIS (integrated)
- Specific IO modules for SIS
- Includes inherent & diverse Systematic Capability for SIS device development & SIS design / engineering.

The 61508 Association

Reasons to be Separate in the context of IEC 61511 revisited

1. To reduce common cause, common mode and systematic failures, minimising the impact of BPCS failures on the SIS.
2. To retain flexibility for changes, maintenance, testing and documentation relating to the BPCS.
3. To facilitate the validation and functional safety assessment of the SIS.
4. To support access security and enhance cyber security for the SIS such that revisions to BPCS functions or data do not affect the SIS.
5. To reduce the amount of analysis that should occur to ensure that the SIS and BPCS are properly designed, verified and managed.

The 61508 Association

1)To reduce common cause, common mode and systematic failures, minimising the impact of BPCS failures on the SIS.

- In Air gapped/Independent the BPCS and SIS components are likely to come from different vendors and have different design teams giving some assurance that common cause issues have been implicitly addressed.
- In Integrated/Common the BPCS & SIS logic solvers may well come from a single vendor. Common cause issues relating to hardware and system are explicitly addressed, typically by embedding diversity. Third party certification attests to this.
- Integrated often allows for physical separation of controllers which can help avoid physical common cause stressors (EMC, Fire, Heat etc)
- Integrated and Common runs the risk of BPCS and SIS being engineered, modified, maintained etc by the same person/team - so more care needs to be taken to ensure independence of these aspects throughout lifecycle in line with IEC 61511 (separate documentation, separate teams, separate procedures etc)

The 61508 Association

2) To retain flexibility for changes, maintenance, testing and documentation relating to the BPCS.

Frequency of changes to BPCS is generally far greater than for SIS.

Integrated is comparable to air-gapped and independent in this regard. Physical separation of BPCS and SIS logic solvers and associated IO sub systems is normal and allows SIS assets to be physically identified and secured.

Integrated may have a single engineering workstation (EWS) for both BPCS and SIS but this would normally include access protection to prevent inadvertent changes to the SIS. If desired then dedicated BPCS and SIS workstations could be used.

This is more of a challenge for Common which can make physical separation for maintenance reasons more difficult, especially at the CPU level because BPCS and SIS code may well be running in the same CPU. Separation of BPCS and SIS IO racks may be possible and should be considered if Common is employed.

Again a shared EWS with access protection for the SIS code would be most likely and BPCS and SIS code would be logically separated but in the same controller. Tools will exist to help keep the systems separate but actually demonstrating independence is more challenging with 3rd party certification .

The 61508 Association

3)To facilitate the validation and functional safety assessment of the SIS.

This highlights the importance of treating BPCS and SIS separate from an engineering perspective.

Implementation of Integrated and Common can often be done by a single organisation so it is particularly important to ensure throughout the realisation stage of the lifecycle.

- IEC 61511 should be followed for the SIS scope
- Functional Safety Management should be in place and, therefore...
- All documentation for the SIS should be separate from the BPCS documentation.
- V & V activities should also be performed and documented separately.
- Separate teams/engineers for designing BPCS and SIS HW & SW preferable.
- Separate test procedures used for BPCS and SIS software
- Separate test methods should be used at FAT, SAT, commissioning and there should be sufficient independence of the people involved.

The 61508 Association

4)To support access security and enhance cyber security for the SIS .....

General observations: -

- Risks related to cyber security increase with increased integration.
- Integrated allows for a separate SIS Zone but firewalls will be required.
- Common result in a shared zone for BPCS and SIS.
- Shared EWS is a challenge if BPCS and SIS are in separate zones.
- Need to weigh up risk and countermeasures and evaluate according to best practise standards.

Guidance on achieving cyber security for the SIS (covered in upcoming IEC61511 Ed 2.0) is already comprehensively covered by other standards such as IEC 62443 (formerly ISA 99).

The 61508 Association

5)To reduce the amount of analysis that should occur to ensure that the SIS and BPCS are properly designed, verified and managed.

General observations :-

- Compliance with 61511 goes a long way to ensuring this - particularly for Air-Gapped, Independent & Integrated.
- Some extra checks may be required at FSA to check for independence of engineering, testing and validation activities.
- Extra practicality analysis of operation and maintenance procedures may be required for sharing of instruments and for Common architectures

The 61508 Association

Summary

- Separation is self evident for traditional Air Gapped/Interfaced architectures.
- Separation is less self evident for Integrated architectures even though BPCS and SIS are physically separate.
- Combining BPCS and SIS in the same logic solver in a Common architecture may have advantages in some circumstances but doing this may require significant additional organisational and technical measures.
- Use of the checklist for both Integrated and Common architectures will help identify potential areas of concern and also help in providing a framework for documenting how such concerns have been addressed.

www.61508.org