Modular Safety Concepts for Marine & Offshore Applications

The current demands from the Marine and Offshore industry require a high amount of flexibility and increasingly faster execution of FPSO projects. Emerson offers the Modular Safety Concept (MSC) assisting customers for meeting these requirements by lowering the overall risk, and allowing for a decrease in the total lead time of the project.

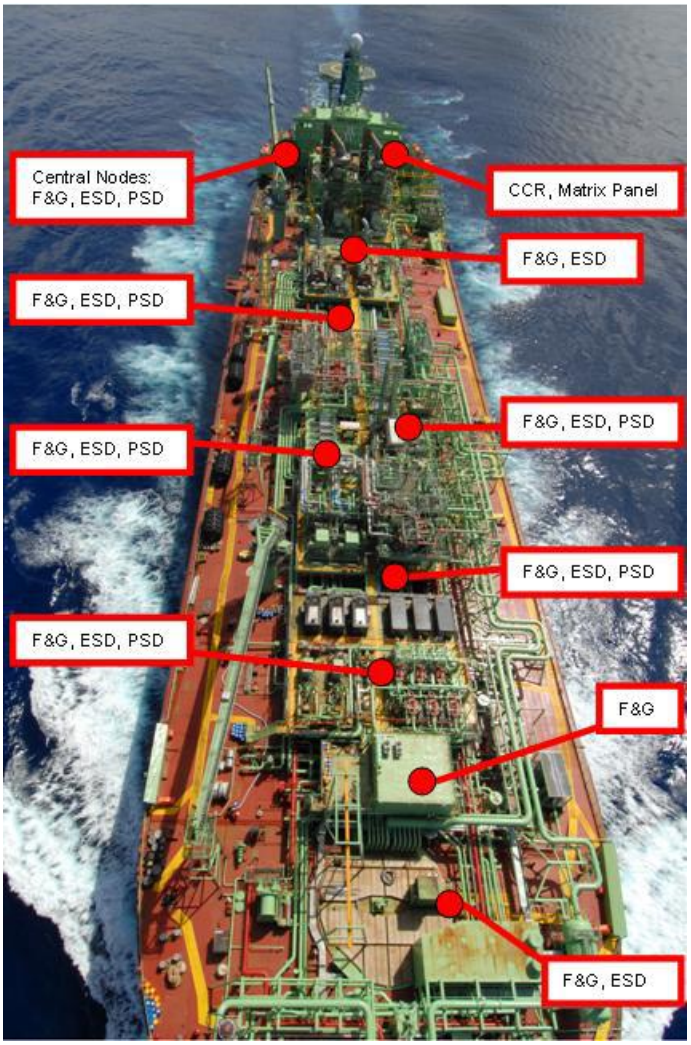


Table of Contents

Introduction

FPSO projects are almost always fast-track projects. For meeting this market requirement Emerson offers the Modular Safety Concept (MSC), which especially when combined with our distributed process control, where the cabinets are installed on Zone classified Modules, results in a faster check out and the Module commissioning can be executed at the OEM's site.

The MSC has the potential to reduce the Total Installed Cost significantly, and improves our clients' Capital Expenditure beyond the cost for automation with pre-engineered hardware and software solutions, reduced commissioning in the shipyard, faster start-up and an increase in flexibility for the implementation of changes late in the project, or once the installation is up and running.

Due to the modular design of the DeltaV SIS safety system, it is possible to locate certain amounts of I/O handling and control on the process modules and thus allow for autonomous automation of the topsides modules. The MSC as it will be applied for Marine and Offshore installations should result in less cabling, pre-commissioned modules arriving in the main shipyard – saving weeks of commissioning time as well as overall project time, and cost savings compared to a centralized solution.

This paper explains the Modular Safety Concept (MSC) for DeltaV SIS applications in the Marine and Offshore (M&OS) industry and will touch on:

- The principles of the MSC.
- The justifications for applying the MSC.
- To which parts of the system the MSC can be applied.
- The acceptance of the MSC by Class Societies.

This paper describes the default solution that Emerson will apply to a project where the MSC is required. Dependant on the actual project requirements as defined by the customer, the Class Society, etc; it might be needed to deviate from this default solution.

This Whitepaper is intended for:

- End-users
- Emerson sales representatives
- Project engineers

Abbreviations and Terminology

Abbreviations

In this paper the following abbreviations will be used.

- AHU Air Handling Unit
- a.k.a. also known as
- AMS Asset Management System
- BD(V) Blow Down (Valve)
- C&E Cause & Effect
- CAAP Critical Alarm and Action Panel
- CCR Central Control Room
- CG Confirmed Gas
- CS Class Society (i.e. DNV, Lloyds, etc)
- DCS Distributed Control System

- DNV Det Norske Veritas
- EER Electrical Equipment Room
- ELD External Layer of Detection
- ESD Emergency Shutdown
- F&G Fire and Gas System (a.k.a. FGS)
- FPSO Floating Production, Storage and Offloading
- FWP Fire Water Pump
- GRP Glass-fibre Reinforced Plastic.
- HART Highway Addressable Remote Transducer
- HVAC Heating, Ventilation and Air Conditioning
- I/O Input / Output
- IEC International Electrotechnical Commission
- JB Junction Box
- LAN Local Area Network
- LER Local Equipment Room
- LOS Line Of Sight Gas Detector
- MAC Manually Activated Call point
- M&OS Marine & OffShore
- MCC Motor Control Centre
- MSC Modular Safety Concept
- OS Operator Station
- PAGA Public Address and General Alarm system
- PAS Process Automation System (a.k.a. DCS, PCS, etc.)
- PCS Process Control System
- PSD Process ShutDown
- RIO Remote I/O
- SAS Safety and Automation System, i.e. PAS, ESD, F&G, etc combined.
- SIL Safety Integrity Level
- SIS Safety Instrumented System
- SLS Safety Logic Solver
- SMP Safety Matrix Panel (a.k.a. CAAP, mimic, etc)
- SOLAS Safety Of Life At Sea
- SOP Standard Operating Procedure
- TBO Total Black Out
- ULCC Ultra Large Crude Carrier

Terminology

In this Whitepaper the following terminology is used.

- Main structure.
  The main structure is often referred to as the “Marine” section and is the basis of the installation, often containing the utility systems. For an FPSO the main structure is either a new build or a converted tanker hull also containing the cargo tanks.

- Module or Unit.
  Most M&OS installations are divided into several process units. Each of these units performs a specific part of the process and is, with respect to the process control, basically stand-alone. Typically process units are also physically separate and built separately from other process units as a complete skid or module. The unit is then lifted onto the main structure and connected to all the other units and piping, thus assembling the entire process installation. In this paper a process module/unit will be referred to as a Module.

- Node.
  Within the DeltaV system the term node refers to a controller on the DeltaV LAN. For DeltaV controllers associated with the PAS such a node is also used for executing the control logic. For DeltaV controllers associated with DeltaV SIS such a node is only used as a data interface for showing DeltaV SIS data on the displays, and as a download interface. The DeltaV SIS system is in no way dependent on these controllers, hence they are often referred to as Communications Interface. In this paper, when referring to a local node, then this is meant as a Communications Interface combined with the required amount of SLSs.

- Executive action.
  Executive actions are those control actions (effects) that are initiated by the F&G, ESD and PSD systems, such as, for instance, the starting of the firewater pumps, starting of firefighting, activation of the GA system, etc.

- Shutdown levels.
  Within the industry there are various definitions known for the naming of the shutdown levels. The differences are such that it is virtually impossible to define a common shutdown level naming that is applicable to all world areas. In this paper the shutdown levels are therefore generalized, and it will be up to the project engineer to apply it correctly to the project at hand. Whenever this paper refers to shutdown levels then this is based on the following level hierarchy and description:

  - Level 0: Abandon vessel/platform.
    The entire installation is shutdown with only the clearly defined exception of certain emergency systems.
    (a.k.a. TBO or ESD0 in NORSOK Standard).

  - Level 1: Emergency Shutdown.
    Shutdown of the entire process including all utilities.
    Usually the process units will be depressurized by means of blow down valves.
    (a.k.a. ESD1 in NORSOK Standard).

  - Level 2: Total Process Shutdown including electrical isolation.
    Shutdown of the entire process, excluding major utilities.
    Note: The process units will be boxed in, i.e. shutdown of incoming and outgoing process lines thus preventing the failure of equipment within the Module affecting the overall plant integrity.
    (a.k.a. ESD2 in NORSOK Standard).

  - Level 3: Process Unit Shutdown.
    Shutdown of all the devices within the Module in one action.
    (a.k.a. PSD4 in NORSOK Standard).

- Level 4: Local Process Shutdown (similar to standard interlocks and permissive). Shutdown of devices within the Module on an individual basis. (a.k.a. PSD5 in NORSOK Standard).

- ESD System (centralized shutdown system)
  Within the MSC concept the ESD system shall consist of one or more centralized ESD nodes for activation of the ESD executive actions, possibly some local ESD nodes for local shutdown functionality and the ESD related indications and commands on the Safety Matrix Panel. The ESD system is a system that is installed on M&OS installations, providing a means for safeguarding an installation, and the personnel onboard that installation, against hazardous events on the installation. The ESD system is located in the safe area and handles the shutdown functionality related to the L0 to L2 shutdown levels.

- PSD System (distributed shutdown system).
  The main purpose of the PSD system is to bring the process to a safe state in the event of process upsets that may result from the PCS failing to control the process within the determined boundaries or from failure in the process control system and/or equipment itself. The PSD system shall do this by activating controlled shutdown actions that, in most cases are limited to the boundaries of the module that it is monitoring. The PSD system can be located in the safe and hazardous areas and handles the shutdown functionality related to the L3 to L4 shutdown levels.

- F&G system.
  Within the MSC concept the F&G system shall consist of a combination of one or more centralized F&G nodes for activation of the F&G executive actions, several distributed I/O systems interfacing the F&G detectors and the F&G related indications and commands on the Safety Matrix Panel.

  - Centralized F&G system.
    The DeltaV SIS centralized F&G system is that part of the F&G system that takes care of the majority of the F&G logic (C&E), i.e. the initiation of the plant critical executive actions. To this end the centralized F&G system is also connected to the distributed F&G I/O systems, the ESD system (via the safety rated communications network – called SISNet for DeltaV SIS) and the Safety Matrix Panel.

  - Distributed F&G I/O systems.
    The main aim of the distributed F&G I/O systems is to reduce the amount of wiring needed for the F&G detectors. Within the MSC there are two types of distributed F&G I/O systems possible.

    - F&G local nodes (DeltaV SIS).
      DeltaV SIS nodes can be located throughout the installation. These local nodes serve as local I/O handling and voting for the local hardwired F&G detectors. Ideally all detectors wired to DeltaV SIS are HART capable thus ensuring that the data of all the detectors is available on the DeltaV operator stations for operations, as well as in AMS for (preventive) maintenance purposes.

    - Addressable F&G system. An addressable
      F&G system typically consists of one or more controller panels with a variety of detectors connected to it through one or more two wire loops. Each of these loops can hold a number of addressable point detectors of varying types and functions and does not require end of line resistors.

      The proposed default configuration for the MSC is to utilize addressable fire detectors in unclassified areas such as the accommodation and office areas. The addressable fire detection system is effectively used as a remote I/O unit for the centralized F&G system. All other F&G detection on the topsides is hardwired to the F&G local nodes which meet the availability and reliability requirements.

MSC Targets

For many (if not all) M&OS projects it is important that a number of targets are reached for the project to be successful. The MSC has been developed to assist in achieving these targets.

- **Time to start-up as short as possible.**
  A large part of the capital investment for the build of an offshore installation (new-build or conversion) lies with the amount of time spend in the main shipyard. Reducing the amount of time in the main shipyard will therefore not only reduce the investment, but also allow for a shorter overall project execution.

- **Distributed construction.**
  These days the drawing boards hold designs that might very well exceed the capacity of a single main shipyard. By constructing parts of these large projects in parallel at multiple shipyards and/or on-shore construction facilities, one obtains a reduction in investment risk, a reduction in execution time and a reduction in time spent in the main shipyard.

- **Reduce materials needed.**
  Reduction of the types and quantities of materials used will not only reduce the investment, but also simplify logistics and reduce the possibility for issues due to delivery times.

- **Reduce the amount of weight.**
  Reduction of the amount of weight of the installation could result in significant savings in general construction works, and in case of floating installations also in an increased efficiency of the installation.

- **Flexibility for modifications.**
  Once operational, the system design should be as flexible as possible for implementing modifications. Especially the addition of signals should not cause issues with cabling, JBs, etc. All too often modifications that are considered important for operational purposes are not executed due to the immense cost and effort required, which is often due to not enough spare signal capacity in the multicores that run the length of the installation.

- **Distributed responsibility**
  A given topsides Module is usually designed and built by a single company. This company has the full responsibility for the complete module. However, the electrical connections are usually connected in the main shipyard and therefore the responsibility of the yard. Ideally these electrical connections should also be within the scope of the company that builds the Module, thus reducing the responsibility/scope for the main shipyard.

The Modular Safety Concept

Key Principles

Emerson's Modular Safety Concept (MSC) is based on the principle of distributed construction and distributed control. With distributed construction the complete installation is divided into separate Modules. Each of these Modules can be constructed separately at different locations all over the world, complete with the required instrumentation wired to the PAS and SIS cabinets that are located on the Module itself, i.e. the local nodes.

Once the Module is mechanically complete it is commissioned to the fullest extent possible, approximately 90% of the I/O (e.g. related to PAS, local F&G detectors and L3 to L4 shutdown signals).

Only after completing this part of the commissioning will the Module be shipped to the main shipyard. In the main shipyard all Modules are assembled onto the main structure, hooked up to the various networks and piping, and then the remaining 10% of the I/O (F&G executive actions and L0 to L2 shutdown signals) are commissioned.

Note that this stepwise testing and commissioning only covers the basic logic functionality and the field device loop testing. As with all systems, distributed and centralized, a full functional test of the F&G and shutdown systems shall still be required once everything is hooked up as a complete system.

A fully constructed Module complete with system cabinets and signal wiring is hoisted onto a main structure

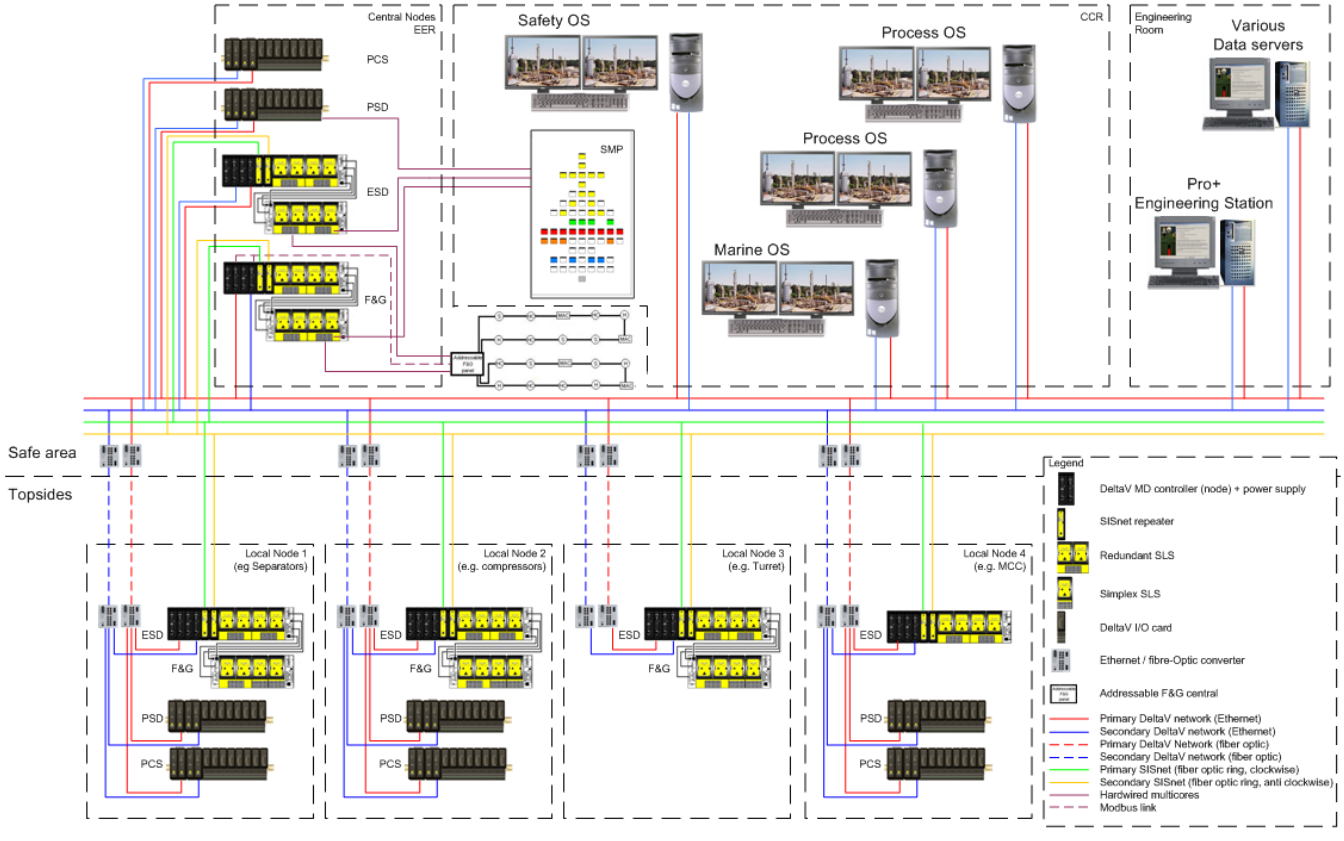
Once the software is downloaded in the SLSs (L3-L4 shutdown, F&G) and controllers (PCS) that are located in the local nodes, it is in principle possible, dependant on customer/end-user requirements, to operate the process on the Module completely autonomous. The only required connections for operations are to the CCR for operator monitoring and/or control and possibly changing of setpoints.

With distributed control, the logic functionality that comprises the safety systems is to some extent allocated to the local node. The allocation of the logic execution to the local node shall be strictly limited in such a way that, combined with the design of DeltaV SIS, the loss of a single (local) node shall result the relevant trips to revert to the fail safe state. Any subsequent action is then executed as defined in the project C&Es.

In very extreme situations with multiple successive plant failures, a certain amount of data loss relevant to the local instruments and logic functions might occur. However operations will at all times have the ability to initiate ESD and F&G executive actions related to the affected Module as well as the entire installation.

The distributed control also allows for precise parts of the application to be tested in the construction yard, thus reducing the amount of time needed for the final validation once the Modules are installed on the main structure.

In short, local shutdowns can only trip elements related to the module integrity. Elements that affect the plant integrity shall be tripped by the plant level shutdowns.



A simplified, general architecture of a system according to the MSC, indicating the main items

Central Node(s)

Central nodes are those nodes that are located in the safe area, usually in an EER in the accommodation, adjacent (or very close) to the CCR. The central nodes will, dependent on the size of the application, consist of one or more DeltaV SIS nodes for ESD and F&G (minimum one node for each system) and a node for PSD. Dependent on the project specific SIL requirements for the PSD system, this PSD node can either be a regular DeltaV node or a DeltaV SIS node.

The central ESD and F&G nodes contain the critical safety functions, so they must remain functioning at all times and will only be powered down (timer delayed) during a L0 shutdown situation.

Central ESD node

The central ESD nodes shall be used for the execution of the safety logic such as:

- High level shutdown logic with trips that affect the entire installation (L0-L2).
- Control of L0-L2 initiated shutdown valves.
- Control of L0-L2 initiated blow down valves.
- Interaction with the F&G system.
- Activation of L3-L4 shutdown as per C&Es.
- ESD related inputs from the SMP.
- ESD related indications on the SMP.
- L0-L2 related indications on the SMP.
- Control that also directly affects other Modules (e.g. ESD valve between Modules)
- Interaction with the GA system.

Central F&G node

The central F&G nodes shall be used for the execution of dedicated parts of the F&G logic such as:

- Control of automated firefighting functionality related to the process Modules such as deluge, foam, firewater/foam pumps, etc.
- Control of fire containment actions related to the accommodation and engine room such as door closers, dampers, HVAC, etc.
- F&G related inputs from the SMP.
- F&G related indications on the SMP.
- Interaction with the ESD system.
- Interaction with the distributed F&G I/O systems.
- Limited amount of monitoring and voting of topsides F&G detectors for which the central nodes happen to be the closest node.
- Interaction with the GA system.
- If required, monitoring and voting of topsides F&G detectors that are part of the ELD for a given Module.

Central L3-L4 shutdown node

The central L3-L4 shutdown node (if any) shall be an interface between the local nodes for L3-L4 shutdown and the SMP (if required).

Local node(s)

Local nodes are nodes that are located on the Modules. Local nodes will contain limited safety functionality, in such a way that the loss of a given local node will only impact the safety integrity of the installation in a pre-defined manner. Upon loss of communication with the local nodes the signals communicated on the SISNet will be marked with a bad integrity flag. The configuration of the central nodes shall be such that any such signal going to the bad state will be considered as the signal being voted to trip.

In all practicality this means that:

- The loss of a local F&G node shall result in all the relevant voted confirmed fire and confirmed gas signals to trip as if a fire or gas was present on the module.
- The loss of a local ESD node should normally result in a level 2 shutdown. This in order to avoid cascade effects in other Modules that would result from the local node tripping.

For the local nodes the following philosophies are fundamental:

Allocation of logic functionality to a local node
The local node shall only contain that part of the safety logic/control that relates to the Module on which the local node is installed. If a local node is powered down then the system therein will revert to the de-energized (safe) state. The local nodes may contain the following functionality:

Local shutdown functionality
The local shutdown nodes will be used for execution of the local Module L3 and L4 shutdown logic. This means that all trip causes and effects must remain within the Module's process boundaries. Any signal that interacts with process functionality beyond the Module's boundaries must be allocated to a higher shutdown level in the centralized shutdown nodes. Note that this does not apply to, for instance, trips to the MCC for stopping pumps/motors that are located on the Module itself, since these are an integral part of the Module's process. Such signals will be secure parameter stop requests over the SISNet to the node that is controlling the MCC equipment.

Local F&G functionality
The F&G local nodes will be used for the F&G detection on the Module (detectors as well as MACs) and a limited amount of F&G initiated shutdown actions. The single/confirmed fire and/or single/confirmed gas voting will be performed within the local node based on the data of these detectors. The voted results are then communicated to the central F&G node for execution of the F&G C&E logic, and thus initiation of the executive actions.

As mentioned, it is to some extent allowed that F&G initiated shutdown actions get allocated to the F&G local node. Allocating F&G shutdown actions to the F&G local node is allowed if:

- These local shutdown actions are in no way needed for the mitigation of an F&G event, nor shall they be designated as essential functions, i.e. they could only affect local integrity but not plant integrity.
- These local shutdown actions do not require control from the CCR in case of an F&G event.
- In the event that the local node is powered down, for instance due to extreme F&G circumstances, then these shutdown actions will be tripped automatically due to the node reverting to the fail safe state. De-energizing of these local shutdown actions should not have any adverse effect on the Module or plant integrity.

Typical examples for shutdown actions that can be allocated to the F&G local node are:

- The control of F&G actions related to the environmentally controlled enclosure (i.e. an LER or GRP container) in which the F&G local node is located. Such control actions could be the tripping of AHU/HVAC/dampers of that enclosure, activation of external "loss of containment" indicators, etc.
  Under normal F&G circumstances the local node should have sufficient time to detect a local F&G event and initiate the containment of the LER. Should the local node get powered down, then these containment actions will be tripped.
- The shutdown of local non-Ex sockets and/or equipment.

Please refer to the ***Redundancy*** section on page 17 for specific redundancy requirements/solutions for the F&G local nodes.

Please refer to the ***F&G System Design Considerations*** section on page 18 for more specific design considerations for the F&G system

Local node quantity
For any given Module there will typically be at least one local node for shutdown levels L3/L4 combined with local F&G detection.

Local node housing
The MSC can be implemented with one of three optional local node housings:

- Stainless steel cabinets. All equipment will be located in stainless steel cabinets that are installed on the Modules. These cabinets will only contain Zone 2 compliant equipment. For these cabinets one should consider the environmental conditions, such as heat radiation from the sun, flare and cargo, sea water corrosion, etc.

- Ex-p container. The local nodes will consist of regular safe area enclosures that will be installed in a GRP Ex-p container located on the module. These containers will only contain Emerson equipment for the local DeltaV and DeltaV SIS nodes. Inside these purged enclosures all the components of the DeltaV SIS node itself, as well as those components supporting the DeltaV SIS node (network, etc), will be Zone 2 compliant, thus avoiding the need to power the local node down should the purge of the container fail. Any regular DeltaV node in these Ex-p containers shall not be zone compliant and shall powered down in such a situation. Ex-p containers shall only be used in Zone 2 or above. Normally the local nodes shall not be installed in Zone 1 locations. If location of local nodes in a Zone 1 area cannot be avoided, then LERs or EX-d housings should be used instead.

- LER. In some instances there could be a LER already present on the Module. Such a LER is normally foreseen for electrical equipment such as switchgears, power distribution, etc, and may also be utilized to house a number of DeltaV and/or DeltaV SIS nodes. The LER is considered as safe area; the cabinets and all the equipment therein is suitable for safe area. This implies that the DeltaV and DeltaV SIS nodes will be electrically isolated if there is confirmed gas detected within the LER. Should the customer require this then Zone 2 compliant equipment can be applied for the DeltaV SIS nodes located in the LER, thus avoiding the requirement to power the SIS nodes down.

The actual selection process for the preferred local node housing should at least consider all of the following criteria with respect to the location of the local node and the type of housing used:

- Weather protection
- Blast protection
- Heat radiation from surrounding equipment, sun, flare, cargo, etc.
- IP rating
- Maintenance access

Local node functional segregation
I/O counts permitting, it is allowed to locate the F&G and shutdown local nodes of a given Module in the same cabinet. Similarly it is also allowed to install the SLSs of the L3/L4 shutdown levels and F&G under the same node (i.e. one redundant set of Communications Controllers) using the same SISNet repeaters.

However, under no circumstances shall F&G and ESD logic be combined in the same SLS; there shall be a strict functional segregation by SLS.

Also the 8-wide carriers shall be functionally segregated ensuring that all SLSs on a given 8-wide carrier (and the spare slots thereon) belong to the same system, i.e. F&G or shutdown.

Local node integrity

All F&G detectors and MACs on the Module shall be wired to the local node. These detectors shall serve as the initial detection means as well as a means of tracking the F&G event as it evolves on the Module. Under extreme circumstances (multiple faults, long ongoing F&G events, etc) it could happen that the local node is powered down or becomes non-operational. This could, for instance, occur due to a catastrophic (large explosion demolishing the entire module) or long ongoing event (ongoing fire). In such situations, the data from the devices that are connected to the local node is no longer available.

A similar situation could potentially also occur on centralized systems, if for instance a cable duct or junction box is destroyed due to the F&G event. With centralized systems the installations SOPs will almost always require a shutdown of that location by manual action of the operator.

In the MSC the F&G voting functionality is located in the local node, so a loss of the local node voids the F&G voting of that Module. Therefore the F&G configuration of the centralized F&G systems will be configured such, that upon loss of integrity of a confirmed fire or gas signal from a local node, this will be considered as a confirmed fire or gas, thus automatically tripping the required safety actions.

If so defined in the shutdown requirements, the L2 shutdown level will be activated by the F&G system and initiate the required shutdown actions. The L3 and L4 shutdown systems located in the effected local node shall be fail-safe, so they will automatically go to the safe state.

SISNet

Conventional safety systems often require hardwired signals for communicating trip signals from one location to another location. More advanced systems can use additional safety rated data links but these often require additional configuration efforts.

DeltaV SIS has an embedded infrastructure consisting of a safety critical communications network (SISNet), which can be extended to SIS nodes in other locations without the need for any additional configuration work.

Between nodes, the DeltaV SISNet will be installed as a dual redundant counter-rotating fiber-optic ring network, thus ensuring that even the loss of an entire node will still not cause a failure of the SISNet communication between the remaining nodes. DeltaV SISNet communications are covered by the TÜV IEC 61508 certification for DeltaV SIS. It is therefore allowed to use the SISNet for communicating trip signals with a SIL rating as high as SIL 3.

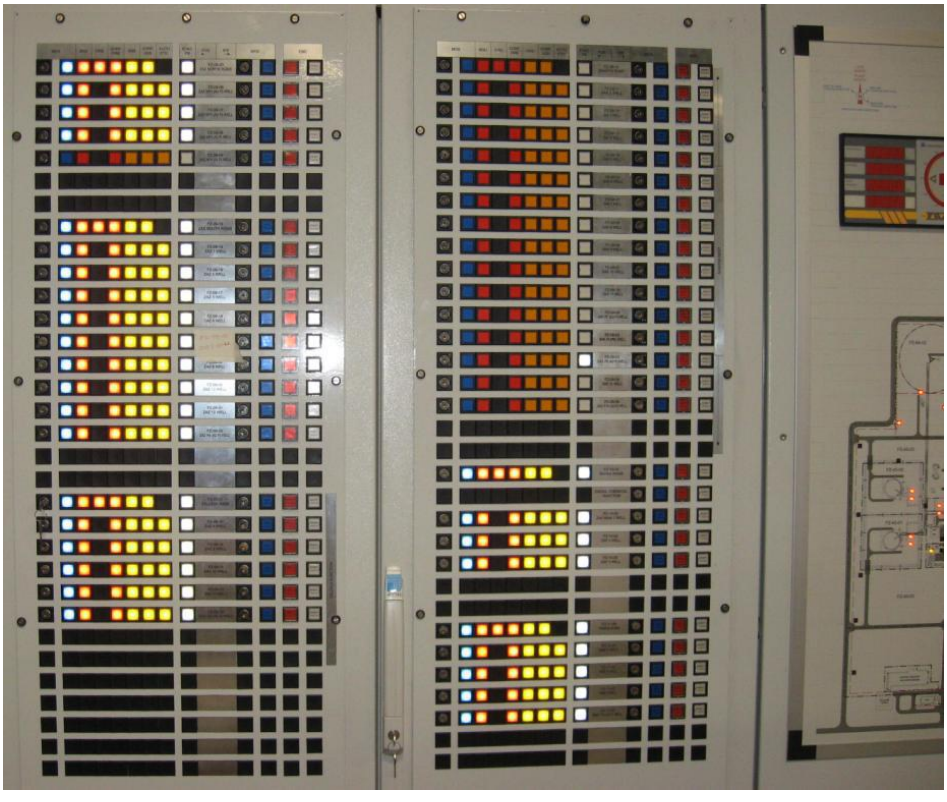
Note that the entire DeltaV SIS configuration will be configured in the software as normally energized. The SISNet is merely an extension of the SISNet internal to the DeltaV SIS node. As such any parameter communicated over the SISNet will also be normally energized.

By default DeltaV SIS is capable of detecting a loss of communication on the SISNet. When a communications loss occurs then the affected parameters are flagged as bad. By default the MSC is based on the fact that any communications loss will result in a failsafe action. This action is especially so for the confirmed fire and confirmed gas signals from the local node(s) to the central node(s). Should the application require normally de-energized outputs then this is dealt with in the final SLS that is driving the output.

Safety Matrix Panel

The DeltaV SIS safety system is also connected to the basic, non-safety rated DeltaV process control network for presentation of the SIS data on the displays. Although the DeltaV network will be installed in a fully redundant setup, it is still required that the operator should be able to have an overview of the most critical data should the DeltaV network fail completely. For this purpose it is required to have a Safety Matrix Panel (SMP) that shows all the critical (summarized) information and allows for the initiation of the most critical commands.

The SMP will be provided with a cover preventing accidental activation of any of the command buttons. This cover can be a single one over the entire panel or individual covers for each command button.



Example of an SMP.

SMP commands

Commands will be latching pushbuttons with a physical and visual difference between the activated and not activated state. All command buttons will be line-monitored for open loop and short circuit.

The SMP will typically provide in the following commands:

- ESD
  - Individual activation of each shutdown level. As a minimum this will include the levels L0 to L2. Shutdown level L3 could be included for activation from the SMP or alternatively only from the screens (depending customer requirements)
  - Activation of blow down (levels).
  - Activation of electrical isolations.
- F&G
  - Activation of deluge per fire area.
  - Activation of foam per fire area.
  - Activation of other automated firefighting (if any) per fire area.
  - Start firewater pumps.
  - Start foam pumps.
  - Duty/Standby selection (depending customer requirements)
- General
  - Lamp test.
  - The SMP can also be equipped with buttons and indications for other safety critical functions such as water tight doors, ballast trips, etc. This should however be limited to safety critical data only, thus preventing that the criticality of the SMP is downgraded into an interface for everyday use.

Notes:

1. By default the manual SMP activation of a L0 to L2 level trip, or the automated firefighting in a fire area, will also remove all active output overrides for that shutdown level or fire area. In order to allow the yearly shutdown testing it will be possible to inhibit this override removal from the DeltaV screens. Optionally it is also possible to add override removal command buttons to the SMP should the customer/end-user require this.
2. Optionally the SMP could also be equipped with alarm buttons for the activation of the various GA alarms. This could be used for manual activation of these alarms in case of drills or actual events.

SMP indications

The SMP will typically provide the following status indications. All status indications will be off in normal (not tripped) situation and lit if the logic has tripped the associated outputs or shutdown level.

- ESD
  - Trip of each individual shutdown level (red). As a minimum L0 to L2, other levels depending on customer requirements.
  - Status of ESD valves that are tripped by the L0 to L2 shutdown levels (green). There shall be one summarized indication per shutdown level. It shall be blinking when the shutdown level is activated and steady when the trip is confirmed by the feedback of the associated ESD valves.
  - Status of BD valves that are tripped by the L0 to L2 shutdown levels (green). There shall be one summarized indication per blowdown (level). It shall be blinking when the blowdown (level) is activated, and steady when the trip is confirmed by the feedback of the associated BD valves
- F&G
  - Single fire per fire area (yellow).
  - Confirmed fire per fire area (red).
  - Single gas per fire area (yellow)
  - Confirmed gas per fire area (red).
  - Deluge activated per fire area (green).
  - Foam activated per fire area (green).
  - Activation of any other automated firefighting system (green).
  - Per firewater and foam pump:
    - General fault (includes failed to start), (red).
    - Not available/remote status (yellow).
    - Running status (green).
    - Duty (optional, green or by position of switch)
  - Ring main pressure low (red).

Notes:

1. Indication colors are selected such that:
   - Pre-alarms are yellow.
   - Errors and trips are red.
   - Correct execution of trip actions is green.
   - All colors indicated are indicative and subject to customer/end-user preferences and/or safety/operational philosophy.
2. Depending customer requirements the SMP could also include indications for common fault and/or common override for ESD as well as F&G

SMP wiring considerations

The following wiring principles will be applied in order to comply with the various rules and regulations. With reference to SMP commands and SMP indications:

- L0-L2 shutdown signals will be wired to the central ESD node(s).
- F&G signals will be wired to the central F&G node(s).

- The pushbuttons for the FWP start commands will be equipped with a dual contact. The first contact is line monitored, and hardwired to the central F&G node for starting the firewater pump under normal operational conditions, as well as execution of any other executive actions required by the C&Es, such as ESD, GA, etc. The second contact will most likely not be line monitored, and is hardwired directly to the associated FWP controller, thus providing a means of starting the FWP for the unlikely event that the central F&G node has stopped functioning.
- Depending customer requirements the dual contact solution can also be considered for any of the other command buttons on the SMP.
- L3-L4 shutdown signals will be wired to the central L3-L4 shutdown node.
- The lamp test command shall be hardwired to the central F&G, ESD and L3-L4 shutdown nodes, and the logic within these nodes shall light the lamps. Lamp test shall not be hardwired to all lamps internally within the SMP.

Redundancy

By default the MSC provides an availability that is in line with the requirements of the industry, as well as the Class Societies. This in effect means that the below redundancy features shall by default be applied.

Nodes and communication:

- For every safety node (ESD, L3-L4 Shutdown, and F&G) full redundancy is applied to the DeltaV LAN and the communications controller.
- The SISNet shall have full redundancy as per the DeltaV SIS design.
- The serial communications link between the addressable F&G detection and the centralized F&G system shall be redundant.

ESD:

- ESD nodes will have full redundancy for the SLSs with the exception of:
  - SMP indications can be wired to a simplex SLS.
  - Valve position feedbacks can be wired to a simplex SLS.

F&G:

- F&G nodes may have a mix of redundant and simplex SLSs following the principle of redundant processors and simplex I/O. This means that:
  - For each F&G node there will be a minimum of one set of redundant SLSs.
    The redundant SLSs are used for executing the voting logic based on detectors that are wired to the simplex SLSs.
  - For each redundant SLS there is a maximum of two simplex SLSs.
    The simplex SLSs will function as “I/O cards” to the redundant SLSs. There should not be any data processing or logic functionality configured in the simplex SLSs. The I/O of the simplex SLSs is read directly by the redundant SLS via the I/O bus, and all associated logic shall be configured in the redundant SLS.
  - Any SLS containing logic (e.g. voting or C&E) shall be redundant.
  - For the central F&G node any SLS driving an F&G output (other than SMP indications) shall be redundant.
  - SMP commands that directly activate the F&G logic shall be wired to a redundant SLS.
  - SMP indications can be wired to a simplex SLS.
  - Valve position feedbacks can be wired to a simplex SLS.

Operator interfaces:

- The safety operator station shall be simplex. Redundancy for this station shall be obtained by assigning the SIS areas to one (or more) of the other operator stations as well. Should the safety operator station stop functioning then the control of the safety system shall be capable through the backup process operator station.
  Note: At all times it is possible to view the safety data on any operator station. The above mentioned redundancy applies only to safety control actions such as applying/removing overrides/resets, etc.
- All critical safety control actions shall also be available on the SMP.

F&G System Design Considerations

F&G systems often have additional design requirements. By default the MSC is based on the following design features for the F&G system:

- All fire detectors in the safe areas such as accommodation, offices, LERs, etc will be wired to an addressable fire detection system.
- All fire detectors and MACs on the topsides will be wired to the F&G local nodes.
- All LOS and point gas detectors will be wired to the F&G local nodes.
- The DeltaV operator interface will be the primary control interface for the entire F&G system including the distributed I/O systems.
  All commands to the addressable system shall be possible through the DeltaV screens. Physical access to the addressable system should only be required in extreme (complete failure of redundant Modbus link) or extensive maintenance situations.

The possible use of addressable F&G systems for F&G detection on the topsides is rather limited due to the fact that the current design of most (if not all) addressable F&G systems contains multiple single point of failure. This means that currently none of the Addressable F&G system vendors can meet the availability requirements without doubling certain components and executing some careful designs.

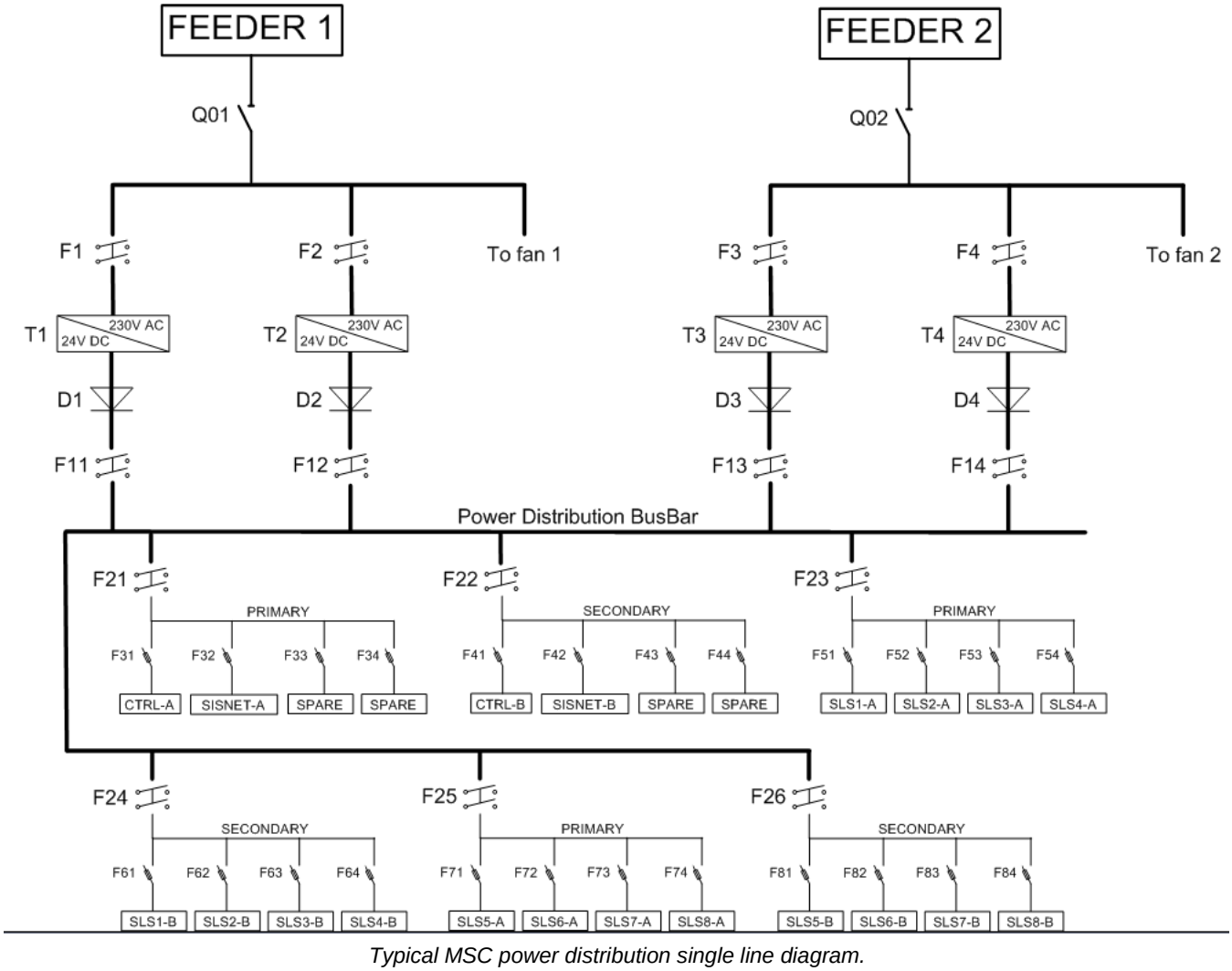
Power Distribution

As with most M&OS installations there are strict requirements with respect to the power distribution for the MSC nodes, centralized as well as local.

Some of the main considerations are:

- A power failure to (a part of) one of the safety systems should not affect the other (parts of the) safety system(s),
- The failure of a single feeder or power supply shall not affect the integrity of a safety system, not by shutting parts of the node down, nor by reverting to a degraded mode of operation.
- The failure of (parts of) the power distribution internally to the node shall generate an alarm.

In order to meet these requirements the power distribution principle as shown in 0 has been adopted for the MSC nodes, centralized as well as local.



Typical MSC power distribution single line diagram.

Cost of MSC and Optimizing the Modularity

Keeping the overall cost of any given project down is always one of the most important factors for the project's success. This is one of the main reasons for introducing the MSC. Although the initial purchase cost of a distributed arrangement of the system, as proposed in the MSC, may be higher than that of a centralized solution, this additional cost can be quickly recovered as the project progresses.

The additional costs can be easily explained by a simple example for a system of 30 redundant I/Os for four Modules.

- In a centralized setup it would, amongst other items, require one safe area cabinet containing one set of communications controllers, one 8-wide carrier and 2 redundant SLSs.

- Applying the MSC, this would then require 4 hazardous area cabinets, each containing one set of communications controllers, one 8-wide carrier and 2 redundant SLSs.

From the simple example above it is clear that when purely looking at the system cost, the MSC option is more expensive. However, by introducing the MSC there will be savings in other areas that will result in a positive overall cost calculation. These cost savings become more and more beneficial if the size of the project exceeds a certain size, or when the plant is engineered and built using the modular approach.

When applying the MSC to a project design, one should make a careful weighing of all the factors that will in the end contribute to the final cost of the entire project. These factors are:

- Size of the installation
  The bigger the installation, the longer the cables, and the bigger the effort of designing and installing these cables, so the larger the savings with the MSC.

- Amount of I/O per module.
  Regardless of the amount of I/O per local node, each local node will require a certain amount of basic materials such as cabinet, carriers, controllers, etc. The lower the I/O count for a given Module, the higher the average cost per I/O for applying the MSC.

- Locations of the Module construction sites.
  The more distributed the locations of the Module construction sites, the greater the possibility for parallel construction and commissioning as made possible by the MSC, thus providing cost and time savings for the project.

Considering the above factors one should determine the optimum level of modularity for a given project. This might mean that it will be better to combine one or more Modules of a single construction site into one local node instead of a local node for each.

However, the advantages of the MSC can only be assessed to achieve the full benefit when one looks at the overall cost for the installation. It might well be that just on the system level it looks beneficial to combine two Modules into one single node, but if for instance one Module is constructed in the USA, the other in South Korea and the main shipyard is in Singapore, then it could very well turn out that full modularity is more cost effective on the total project scope.

MSC Advantages

Distributed Construction

Using a single shipyard for the entire construction is often not possible or advisable due to various reasons, among which:

- Many Module vendors have their own/dedicated construction locations.
- Some main shipyards cannot handle the complete construction of multiple Modules at the same time. A single supplier for all Modules would then most likely stagger the construction successively thus increasing the build time for the entire installation
- Allocating the construction of a large number of Modules to a single construction site increases the risk for delays. A mishap during the construction of one Module can easily have follow up implications for the other Modules under construction at the same site.
- Distributing the construction of the Modules over several sites allows for the optimum use of specific unit knowledge at the various construction sites.

Applying the MSC deals with all this and allows for the most efficient use of construction capacity and scheduling.

Distribution of Scope

For centralized projects a large part of the scope related to the SAS system, such as cabling, is part of the scope of the main shipyard. The current increase in size and complexity of these installations puts a higher strain onto these shipyards.

By applying the MSC, sizeable chunks of this scope get allocated to the Module vendors thus reducing the risks for delays in the main shipyard.

Reduction of Commissioning Time

By applying the MSC, a project can be in a position to drastically reduce the amount of time that is needed for the commissioning of the system. With the average M&OS project, commissioning of the majority of the instrumentation is executed in the main shipyard, which is often a very long process and in conflict with the construction of the main structure itself. Due to various delays the commissioning period often shifts and then gets extended well into the sail-away.

With the MSC, the bulk of the commissioning work no longer takes place in the main shipyard, but is moved out to the various construction yards where the Modules are being build. Only those I/O points that go beyond the Modules boundaries will need to be tested when the Module is installed on the main structure, thus drastically reducing the commissioning time in the main shipyard.

In fact, even the overall construction time can potentially be reduced since the MSC allows for the various units to be commissioned in different locations at the same time. The MSC also reduces the amount of work with regards to cabling thus requiring less effort and time for the construction of the main structure itself.

Reduction of Materials and Weight Needed for the Main Structure.

Applying the MSC to a project can potentially result in less cabling being required, and could therefore also decrease the amount and/or size of the cable trays and support structures. These reductions will obviously result in less weight for the Modules and the topsides in general.

Improving Flexibility for Modifications

The MSC improves the flexibility for future modifications:

- Given the design of the SLS there is a lot of flexibility for expanding local functionality. The I/O channels of the SLS are freely configurable for AI, DI and DO, so the classical situation where the addition of a single channel requires the addition of a complete I/O card is much less likely. As long as there are spare channels, then a signal can be wired to the SLS and used in the logic.

- By assigning I/O to the local nodes, one no longer has to consider the spare capacity within the multicores to the central node. Often these are a limiting or high cost factor whenever a minor expansion is considered.
- Adding an SLS also adds processing capacity, so there is little chance that expansion of the system will result in an increased response time.

Decrease of Central Node Size

With many offshore installations, the amount of space available for installation of the central nodes is very limited. This is already the case for new build installations but even more so for FPSO conversion projects. The amount of EER space available is already limited and there is hardly any free space for creating a new EER.

By applying the MSC a given amount of I/O and logic is relocated to the local nodes in the field thus reducing the size of the central nodes.

Quantity of LERs

When using the Zone 2 compliant stainless steel cabinets or GRP containers one might no longer need to install large and costly LERs for locating parts of the system on the Module.

MSC versus RIO

Most of the currently available solutions for modularity involve the use of Remote I/O (RIO).

In a RIO setup there will be a number of RIO modules located in the field. These RIO modules are basically classic I/O modules without any control capacity. The connected I/O is monitored and the data is transmitted onto a network link that can be made redundant, and for some systems also safety rated (ProfiSafe). The actual control functionality is then located in the safe area and handled by standard control units.

The table below provides a comparison of the MSC versus RIO

Subject	MSC	RIO
Loss of communication on data link,	Communication will still be available on the SISNet with summarized data on the SMP so much higher availability. Communication will be lost and node will be de-energized as soon as the data link as well as the SISNet fails (a total failure requires 4 simultaneous faults).	Communication will be lost and node will be de-energized as soon as the data link fails (a total failure requires 2 simultaneous faults).
Loss of communication on data link, DO control	Control of local node outputs still possible through the SISNet.	No control of local node outputs.
Loss of communication on data link, control	If so desired, the MSC allows for the local node to continue the process in a safe way as long as the process does not go beyond the limits as defined in the L3 and L4 shutdown specifications.	No autonomous control possible, local node will be de-energized and go to a shutdown situation.
Loss of communication on data link, integrity data	Local node trips, alarms and first-up details are buffered in the SLSs of the local node. Once the data link get's reconnected the data will be automatically uploaded to the centralized alarms and events chronicle.	Local node trips and alarm data is generated by the local node controller in the safe area. Loss of communication will therefore result in this data not being available and a loss of first-up information.

Commissioning	Commissioning of local node includes related to the local node. This allows for a package or module to be fully tested and accepted by the customer including the automation. Responsibility for the package/module (scope of work) incl. automation will be with the supplier	Commissioning of the local node is limited to the I/O landing. Responsibility for the installation, test and commissioning of the automation related to package or module will be with the customer
Operator station on the Module.	The functionality of the Control Network is available on the Module. It is therefore possible to connect an operator, maintenance or engineering station for (for instance) commissioning, even if the rest of the system is not yet up and running. It is also possible to permanently connect a local operator workstation without requiring any additional hardware.	Only the I/O bus is available on the Module. To be able to execute commissioning without the main system up and running one will also need to provide in the controller and all other associated hardware. For a permanent operator station an additional network link will need to be installed.
F&G and high level ESD shutdown actions	The MSC ensures that control of the essential F&G and ESD trip actions remains available to the operator, even if a certain amount of the I/O is located in the local node.	RIO will by definition only locate the landing of the I/O in the zone classified areas. For the I/O and logic handling RIO relies completely on the controller module that is located in the safe area. The use of RIO for ESD or F&G is generally not permitted.
Communication speed and SIF cycle time	When adding SLSs for expanding the functionality then each of those additional SLSs comes with its own build-in CPUs, memory, diagnostics, etc. The expansion of the local node will therefore have hardly any impact on the SIF response time or the system cycle time	RIO solutions are dependent on centralized CPUs. The cycle and response time of those CPUs are very dependent on the size and complexity of the local node application. Any additional I/O or functionality is likely to increase the response and cycle time.
Time stamping of alarms & events	The time stamping of alarms and events is provided by, and buffered in, the SIS Logic Solvers in the local node. As such even if the communication to the centralized event history database has failed, the time stamping of the events will still maintain the required resolution.	The SOE time stamping is handled by the local node controller in the safe area. As such when the communication fails the events following this failure will no longer be time-stamped. Temporary events will be lost all together, and events still active during re-establishing of communications will all be time stamped with that time and not the actual event time.

Revision Table Revision Date	Revision Description
July 2009	First official edition. Base document for DNV issuing the Aip on the MSC principle.
October 2009	Re-format of the DeltaV branding. Minor textual corrections not affecting content. Renamed to Whitepaper.
March 2011	Minor textual corrections not affecting content. Removed invalid references.

This Whitepaper was prepared by Rafael Lachmann, Emerson Process Management, Rijswijk, The Netherlands, in cooperation with Det Norske Veritas, Høvik, Norway.

For further clarifications on the contents of this Whitepaper please refer to the MSC your local sales representative.