EmpirBus™

A Garmin Brand

Terms of Use & Best Practice for Designers and Installers

Table of contents

Terms of Use 4

Digital Switching 5

- Human factors in system design 5
- Physical network design and installation 5
- System security 5
- System safety 5
- System redundancy and fail-safe design 5
- System performance 5
- System testing and commissioning 5
- System documentation and backups 5
- Trademark and patents notice 6
- Fair Use Statement 6
- Software updates 6
- Product handbooks 6

Important Information 7

- EMC installation guidelines 8
- Product disposal 8
- IMO and SOLAS 8
- Technical Accuracy 8

Document overview 9

- Document information 9
- Audience 9
- Limitations 9

Introducing best practice for digital switching systems 10

- Digital switching overview 10
- About “best practice” 11
- Using this document 12

Best practice recommendations 13

- Human factors in system design 13
  - Introduction to touchscreen multifunction displays (MFDs) 13
  - Best practice: consider MFD environmental conditions 14
  - Best practice: consider MFD context 15
  - Best practice: consider user capabilities for MFDs 15

Best practice: when to provide physical switches 16
Best practice: use switch-guards for critical circuits 16
Best practice: use of latched and unlatched switches 17
Physical network design and installation 18
Best practice: install robust CAN-cabling 18
Best practice: use a CAN network bridge to isolate critical components 18
Best practice: do not exceed CAN bus specifications 19
Best practice: dealing with inductive loads 19
System security 21
Best practice: when to use GSM SMS(text message) control interfaces 21
Best practice: consider control panel locks 21
Best practice: consider security of switching components 22
Best practice: configure strong Wi-Fi passphrases for MFDs 22
System safety 23
Best practice: take extra precautions when switching moving equipment 23
Best practice: configure software fuses for every switched circuit 24
System redundancy and fail-safe design 25
Best practice: use redundant switching mechanisms for critical systems 25
Best practice: implement fail-safe mechanisms 25
System performance 26
Best practice: consider NMEA 2000 (CAN bus) bandwidth limitations 26
Best practice: Graphic file size 26
System testing and commissioning 27
Best practice: take appropriate precautions when testing 27
Best practice: perform comprehensive system testing 27
Best practice: perform regression tests 28
System documentation and backups 29
Best practice: provide comprehensive system documentation 29
Best practice: keep system documentation up to date 29
Best practice: provide contextual labelling and emergency instructions 30
Best practice: create system backups,and manage software changes 30
References 30
Support 31

Terms of Use

Please read this entire document. It is important that you fully understand the stated terms.

When installing Digital Switching modules and control interfaces, it is most important to follow best practices for the equipment type being controlled on the installation and its operation and commisioning, to ensure it operates safely in the manner intended. Safety legislation requires that safety risks be assessed and addressed, such that the Digital Switching and equipment being operated or controlled will not put anyone in a position of potential harm or risk of injury.

It is the manufacturer of the installation and/or equipment installers responsibilities to ensure that a full risk assessment of the Digital Switching system design is carried out, and that the system is rigorously checked during commissioning for correct and safe operation. It is strongly recommended that these actions are carried out by appropriately trained personnel and in accordance with ISO 61508: Functional Safety of Electrical and Electronic Programmable Equipment. Particular care should be taken to ensure that appropriate redundancy and localized safety cut-off facilities are built into to the design of the systems. More information about ISO 61508 is available at: www.iec.ch

A file containing technical information relating to the risk assessment of the equipment, and a commissioning conformity assessment should be produced and maintained by the manufacturer of the installation and/ or equipment installer.

Any future modification or changes to the above equipment installation should be fully risk assessed, validated during commissioning and added to the conformity assessment; careful attention should be made to ensure the changes do not impact any other parts of the system.

Digital Switching

Before planning or installing any part of a Digital Switching system, refer to the Digital Switching "Best Practices" information detailed below.

Human factors in system design

Digital Switching user interfaces should be designed to facilitate safe and efficient control and monitoring of those systems.

Physical network design and installation

EmpirBus Digital Switching systems make use of a wired NMEA 2000-compatible CAN bus to transmit switching signals. The linear nature of these systems requires consideration during design.

System security

Appropirate security features in Digital Switching systems are particularly important where moving equipment could cause injury if operated improperly.

System safety

When designing your Digital Switching system, always consider the safety of the system and those using the system.

System redundancy and fail-safe design

Careful and considered design with regard to system redudancy and implementing fail-safe mechanisms, will ensure that your Digital Switching system is robust, and that rare events are less likely to disable critical system functions.

System performance

To ensure that your Digital Switching system operates consistently and reliably, certain limitations of the NMEA 2000 (CAN bus) network and MFDs, should be considered.

System testing and commissioning

Having followed best practice for system design, it is important that all components of your Digital Switching system as implemented, are comprehensively tested.

System documentation and backups

Although a Digital Switching system can greatly reduce the complexity and amount of cabling required compare to an equivalent tradtionally-switched system, it is very important to document the design of each installed system.

Trademark and patents notice

EmpirBus are registered or claimed trademarks. All other trademarks, trade names, or company names referenced herein are used for identification only and are the property of their respective owners. This product is protected by patents, design patents, patents pending, or design patents pending.

Fair Use Statement

You may print no more than three copies of this manual for your own use. You may not make any furthercopies or distribute or use the manual in any other way including without limitation exploiting the manual commercially or giving or selling copies to third parties.

Software updates

Important: Check the EmpiBus website for the latest software releases for your product.
www.empirbus.com

Product handbooks

The latest versions of handbooks are available to download in PDF format from the website www.empirbus.com. Please check the website to ensure you have the latest handbooks.

Important Information

Warning: Product installation and operation

This product must be installed and operated in accordance with the instructions provided. Failure to do so could result in personal injury, damage to your system and/or poor product performance.

Contact your EmpirBus dealer for further details.

Warning: Product grounding

Before applying power to this product, ensure it has been correctly grounded, in accordance with the instructions provided.

Warning: Positive ground systems

Do not connect this unit to a system which has positive grounding.

Warning: Power supply voltage

Connecting a product to a voltage supply greater than the specified maximum rating may cause permanent damage.

For voltage ratings, refer to the *Technical Specification* section of the product's documentation.

Warning: Switch off power suply

Ensure the system's power supply is switched OFF before starting to install this product. Do NOT connect or disconnect equipment with the
power switched on, unless instructed in this document.

Caution: Do not open the unit

The unit is factory sealed to protect against atmospheric humidity, suspended particulates and other contaminates. It is important that you do not open the unit or remove the casing for any reason. Opening the unit will:

- compromise the seal with possible damage to the unit, and
- void the manufacturer's warranty.

Caution: Power supply protection

When installing this product ensure the power source is adequately protected by means of a suitably-rated fuse or automatic circuit breaker

Caution: Service and maintenance

This product contains no user serviceable components. Please refer all maintenance and repair to authorized EmpirBus dealers. Unauthorized repair may affect your warranty.

EMC installation guidelines

EmpirBus equipment and accessories conform to the appropriate Electromagnetic Compatibility (EMC) regulations, to minimize electromagnetic interference between equipment and minimize the effect such interference could have on the performance of your System.

Correct installation is required to ensure that EMC performance is not compromised.

Note: In areas of extreme EMC interference, some slight interference may be noticed on the product. Where this occurs the product and the source of the interference should be separated by a greater distance.

For **optimum** EMC performance we recommend that wherever possible:

- EmpirBus equipment and cables connected to it are:
    - At least 1m (3ft) from any equipment transmitting or cables carrying radio signals e.g. VHF radios, cables and antennas. In the case of SSB radios, the distance should be increased to 7 ft (2 m).
    - More than 2m (7ft) from the path of a radar beam. A radar beam can normally be assumed to spread 20 degrees above and below the radiating element.
- The product is supplied from a separate battery from that used for engine start. This is important to prevent erratic behavior and data loss which can occur if the engine start does not have a separate battery.
- Cables are not cut or extended, unless doing so is detailed in the installation manual.

Note: Where constraints on the installation prevent any of the above recommendations, always ensure the maximum possible separation between different items of electrical equipment, to provide the best conditions for EMC performance throughout the installation.

Product disposal

Dispose of this product in accordance with the WEEE Directive.

The Waste Electrical and Electronic Equipment (WEEE) Directive requires the recycling of waste electrical and electronic equipment.

IMO and SOLAS

When used in marine applications the equipment described within this document is intended for use on leisure marine boats and workboats NOT covered by International Maritime Organization (IMO) and Safety of Life at Sea (SOLAS) Carriage Regulations.

Technical Accuracy

To the best of our knowledge, the information in this document was correct at the time it was produced. However, Garmin Sweden Technologies AB cannot accept liability for any inaccuracies or omissions it may contain. In addition, our policy of continuous product improvement may change specifications without notice. As a result, Garmin Sweden Technologies AB cannot accept liability for any differences between the product and this document. Please check the EmpirBus website to ensure you have the most up-to-date version(s) of the documentation for your product.

Document overview

Document information

The best practice recommendations in this document apply to generic digital switching systems. This information is not specific to any single manufacturer of digital switching system components.

In addition to reading this document, and before starting work on a digital switching system, you should also refer to the documentation provided by the original manufacturer of individual system components.

Audience

This document is intended to provide guidance to those responsible for designing, installing, testing, commissioning, maintaining, or modifying a digital switching system that uses components supplied by Garmin Sweden Technologies AB.

The guidance provided is relevant to manufacturers, dealers, and support technicians. Owners of systems equipped with a digital switching system, that wish to modify the system, may also find this guidance useful.

> **Important**: Personnel responsible for designing, installing, testing, commissioning, maintaining, or modifying digital switching systems must be appropriately trained and qualified to perform the tasks required.

Limitations

> **Important:** Digital switching systems are extremely flexible, and highly configurable. As such, this document does not, and cannot, provide guidelines for every circumstance and eventuality that you may encounter when designing and installing a digital switching system.

Introducing best practice for digital switching systems

Digital switching overview

Digital switching systems enable the creation of highly customizable power distribution, control, monitoring, and alarm management systems.

Data and information supplied from different products connected to the network can be integrated and centralized, increasing the availability of important information. When integrated with multifunction displays(MFDs), dedicated user interfaces can greatly simplify the control and monitoring of the installation.

Additionally, the simplification of power-distribution cabling achievable by implementing a digital switching system can significantly reduce costs.

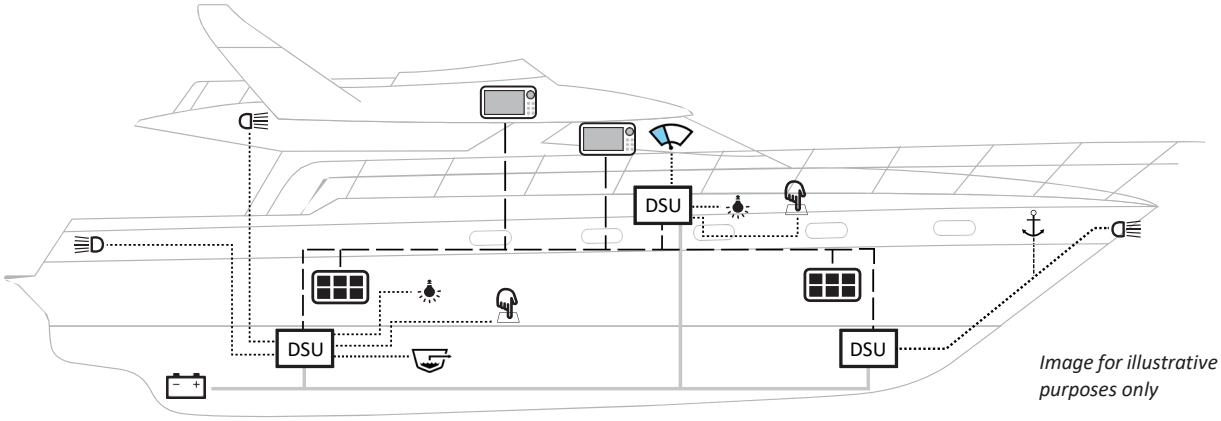


Image for illustrative purposes only

Symbol	Description	Symbol	Description
	DC power cable		Interior light
	NMEA 2000 (CAN bus) Network cable		Contact switch
	Digitally switched input/ output cable		Bilge pump
	DC power supply		Multifunction display (MFD)
DSU	Digital switching unit		Wipers
	Navigation/ search light		Anchor winch
	Switch panel		

About “best practice”

Digital switching systems offer almost unlimited possibilities for monitoring andcontrolling the electrical system.

While this flexibility gives system designers vast scope for implementing bespoke monitoring and control solutions, it is criticalthat these solutions are designed with consideration for the overall safety and security of human beings and the system environment.

To help designers and installers create safe and secure digital switching systems,this document presents a number of “best practice” recommendations. Best practice is guided by the experience of skilled designersand installers with a range of digital switching systems, varying in scope and complexity.

By following best-practice recommendationsduring the design and installation of a new digital switching system, or while modifying an existing system, you can benefit from the checks and processes already proved in the field. Following best practice will result in a safer, more secure, robust, and maintainabledigital switching system.

Note: In addition to this document, always refer to the detailed technical documentationprovided by the original manufacturer

of individual digital switching systemcomponents.

Note: Refer to the international standard IEC 61508 (”Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-relatedSystems”) for comprehen- sive guidelines on developing systems thatcomprise electrical, electronic, or program-mable electronic components that performsafety functions.

Note: As the designer or installer of a digital switching system, you should be appropriatelytrained and have experience of working with both the digital switching system components,and the electrical systems and equipment thatwill be controlled or monitored by the digital switching system.

Using this document

This document groups best-practice recommendations into eightcategories. Each category covers a particular aspect of digital switching system design and implementation:

Category	**Summary**
Human factors in system design	Human factors is a discipline concerned with understanding how people interact with systems, and designing user interfaces that facilitate safe and efficient control and monitoring of those systems.
Physical network designand installation	Your digital switching system makes use of a wired NMEA 2000-compatible Controller Area Network bus (CAN bus) to transmit switching signals. The linear nature of the CAN bus requiresconsideration during design.
System security	The best practice recommendations in this section will help you to design appropriate security features into your digital switching system. This is particularly important where moving equipment could cause injury if operated improperly.
System safety	Designers of digital switching systems must always consider safety, both for human beings as well as the system environment. The best practice recommendations in this section cover safety regarding moving equipment, and electrical fuses.
System redundancy and fail-safe design	Digital switching systems are not immune to failures, particularly when subject to extreme environmental conditions, such as a nearby lightning strike. Careful and considered design with regard to system redundancy and implementing fail-safe mechanisms, will ensure that your digital switching system is robust, and that rare events are less likely to disable critical systems.
System performance	To ensure that your digital switching system operates consistently and reliably, certain limitations of the NMEA 2000 (CAN bus) network,and MFDs should be considered.
System testing and commissioning	Having followed best practice for system design, it is important that all components of the digital switching system as implemented, are comprehensively tested.
System documentation and backups	Although a digital switching system can greatly reduce the complexity and amount of cabling required compared to an equivalent traditionally switched system, it is still important to document the design of each installed system.

Best practice recommendations

Human factors in system design

The best practice recommendations in this section cover design considerations based on human factors.

Human factors is a discipline concerned with understanding how people interact with systems, and designing userinterfaces that facilitate safe and efficient control and monitoring of those systems.

When designing the user interfaces for a digital switching system, you are able to choose from a number of different switching mechanisms. Any one, or a combination of, the following switching mechanisms may be available:

- Soft-switches on a touch-screen multifunction display (MFD) (including toggle buttons, option buttons, and sliders)
- Short-range wireless switches
- Buttons on a NMEA 2000 keypad
- Traditional push-button switches (including momentary, latching, and rotary switches)
- Remote switching using a web application (runningon a smart phone or tablet), or by sending a GSM SMS text message

The most appropriate choice of switching mechanism depends on:

- the type of equipment or system being switched
- the physical environment and location of both the switched equipment and the switch
- the capabilities of the user operating the switch
- a requirement to display status information for the switched equipment or system
- the relationship, if any, between the switched item and other items or systems

Introduction to touchscreen multifunction displays (MFDs)

Touchscreen multifunction displays (MFDs) provide a powerful and flexible method for utilizing soft-switches and bespoke graphical user interfaces to control and monitor systems with digital switching.

Touchscreen displays enable intuitive and efficient interactions with systems and allow for highly contextual presentation of controls and status information.

However, touchscreen displays may not always be appropriate as the primary means to control certain systems or equipment. The detailed design of individual touchscreen displays can also cause problems for users unless individual screen-designs and the components they comprise (for example, soft-buttons, gauges, and background images) are carefully built and tested.

When designing a digital switching system that uses an MFD to control and monitor systems, consider the following best practice recommendations.

Best practice: consider MFD environmental conditions

Environmental conditions where the MFD is located may affect usability. For example:

- Rain, sea spray, condensation, or sweat may make the MFD slippery or difficult to read, and could result in unintentional commands.
- Excessive vibration or motion may prevent users from interacting with the MFD using precise actions.
- Direct sunlight may make it difficult to read and interact with the display.
- In low temperatures, users may need to wear gloves,impacting the usability of the display

To facilitate the safe and effective use of a touchscreendisplay in a variety of conditions:

- Where possible, provide MFDs with physical protection from the environment.
- Ensure that soft-buttons and associated icons and text are sufficiently large and have adequate contrast.
- Consider further distinguishing between important soft-buttons by using different button shapes, and contrasts.
- Allow sufficient space between active parts of the touchscreen display (for example, between individual soft-buttons), to reduce the likelihood that users will touch a button inadvertently.
- Remember that certain types of control may be difficult to use in some conditions. For example, don't use a slider control that requires a precise swiping action as the only means to control a critical system.
- Implement a "long press" feature to protect all buttons controlling important systems or equipment. For example, enforce a three-second press before a soft-button signals that AC shore-power is to be connected or disconnected from the electrical system.

Note: Where rapid operation or power-down of equipment may be required in an emergency, don't enforce a "long press". Also consider providing a physical switch in addition to soft buttons on an MFD (see Best practice: when to provide physical switches).

Best practice: consider MFD context

Contextual placement of touchscreen displays may affect usability. For example:

- Locating a display where it is likely to be knocked or bumped could result in unintentional switching actions.
- A display that is grouped with other controls (for example, an array of physical switches) will form an automatic association between the grouped controls for users.

When locating touchscreen displays:

- Consider the context of the display with respect to other user controls, and with the user's position while operating the display.
- Where space is limited and accidental touchscreen presses may be hard to avoid, consider safeguarding the touchscreen with appropriately positioned physical barriers.
- Consider the context of the display with respect to the systems or equipment under control. In some cases (for example, moving equipment), maintaining line-of-sight between the user operating the MFD and the controlled equipment is important.

Best practice: consider user capabilities for MFDs

User capabilities should be considered when designing touchscreen displays. For example:

- Sight problems, such as reduced visual acuity, or color-blindness, may make it difficult for some users to operate touchscreen displays effectively.
- Lack of experience with touchscreen displays may cause additional problems for some users.

To assist users:

- Ensure that soft-buttons and associated icons and text are sufficiently large and have adequate contrast.
- Consider further distinguishing between important soft-buttons by using different button shapes, and contrasts.
- Do not rely solely on color to distinguish between important system conditions (for example, the operating status of a bilge pump). Color blind users may find it difficult to use systems that rely on visual cues based solely on color.

Best practice: when to provide physical switches

Although well designed touchscreen displays offer intuitive, flexible, and compact switching solutions for multiple systems and equipment, some cases are better implemented with (or supplemented with) physical switches, including NMEA keypads.

Consider that touchscreen displays:

- lack tactile feedback
- are sensitive to accidental touches
- can be hard to use in adverse environmental conditions
- can be hard to use when wearing gloves
- may require additional touches (for example, using menus and page jumps) to reveal the required control button
- may be hard to navigate quickly, especially in emergency situations, or by users unfamiliar with the installation

If the user needs to switch systems or equipment in response to urgent conditions, or repeatedly operate a switch while looking away from the touchscreen display,consider providing a physical switch in place of (or in addition to) a soft-button on a touchscreen.

Physical switches are also recommended when it is important that the switch location maintains the operator's line-of-sight with the switched-equipment.

Some examples where provision of a physical switch is recommended:

- operating the horn
- operating internal lighting positioned to illuminate controls
- operating an emergency stop feature (for example,to immediately stop a moving piece of equipment that is within the switch operator's line of sight)

Best practice: use switch-guards for critical circuits

For cases where inadvertent use of a switch could impact the safety of the installation or its occupants,ensure that the switch is guarded.

For example, a switch controlling power to a primary DC bus should be guarded to prevent accidental powering down of multiple systems. Similarly, a soft-switch on a touchscreen display that operates a moving item of equipment (such as a powered hatch cover), should be designed with a software guard.

For physical switches, install a purpose-built guard (such as an integral flip-cover).

For soft-switches on a touchscreen display, consider implementing:

- a "long press" feature. For example, enforce a three-second press before a soft-switch signals that AC shore-power is to be connected or disconnected from the electrical system.
- a confirmation message that the user must acknowledge to complete the action (for example,"Power-off the primary DC bus? <Yes>/<No>).
- an access code (PIN code) that the user must enter before gaining access to a soft switch.

Best practice: use of latched and unlatched switches

The choice of a latched or unlatched (momentary) switch to control a particular system or piece of equipment may have a direct impact on user safety.

Always consider the nature of the equipment under control when deciding which type of switch to use:

- A latched switch may be appropriate when a continuously closed (or open) switch-state is unlikely to impact user or system safety.

Note: Remember that a physically latched switch **cannot be overridden** by other switches within the digital switching system.

- Use an unlatched (momentary) switch for moving equipment that may present an entrapment hazard.

Physical network design and installation

Your digital switching system makes use of a wired NMEA 2000-compatible Controller Area Network bus(CAN bus) to transmit switching signals.

The linear bus topology comprises a central cable (the backbone), with tee-connections and multi-way connectors to CAN-compatible devices (including digital switching components, and multifunction displays). Each end of the backbone is terminated with an appropriate resistor.

The linear nature of the CAN bus means that a break or bad connection in the backbone could degrade or disable a digital switching system. A CAN bus also has an upper limit to the bandwidth available to distribute messages; if the maximum supported data rate is exceeded, this may result in delayed messages, and unreliable operation. It is therefore important to consider the following best practice recommendations when designing and installing the CAN-bus wiring to support a digital switching system.

Best practice in physical network design is not restricted to the CAN bus. Power-circuit design also needs careful consideration, particularly when switching devices that may place an additional strain on components, such as inductive loads.

Best practice: install robust CAN-cabling

Ensure that:

- all CAN-bus cables (including the backbone, device drops, and power insertion cables) are securely fixed. Excessive play in cable runs can lead to intermittent or broken connections. Similarly, very tight cable runs in situations where some play is required,can also cause connection problems.
- the linear topology of the CAN bus is maintained.

Best practice: use a CAN network bridge to isolate critical components

For complex digital switching systems comprising a number of digital switching control units, connected via a long central cable (backbone), consider using a CAN network bridge to split the CAN network into multiple independent subnets.

CAN subnets must also have separate power connections.

When designing a CAN network comprising bridged subnets, consider how best to distribute CAN-compatible devices between the subnets. For example:

- multiple digital switching control units could be placed on different subnets
- critical systems controlled by digital switching should be placed on a separate subnet from non-critical systems (for example, switching associated with engine monitoring and control on a separate subnet from all other digital switching components and other components using the CAN bus)

Best practice: do not exceed CAN bus specifications

Ensure that the following limits are not exceeded for an individual CAN network (or subnet):

- maximum of 50 connected CAN devices
- maximum 5 m drop (spur) to each CAN device;maximum 30 m total drop (spur) length
- maximum 100 m total backbone length

Also ensure that:

- correct termination is applied to each end of the CANbus
- where possible, power is applied near to the center of the backbone
- the CAN bus is not overloaded with data; overloading may result in delayed or unreliable responses from devices

Best practice: dealing with inductive loads

Inductive loads may require special handling when incorporated into a digital switching system.

Important: Failure to correctly install adequately rated flyback diodes could result in overheating of circuit components, and subsequent fire.

Important: Failure to correctly install adequately rated flyback diodes could result in damage to digital switching modules.

Examples of loads which may result in high inductance during switching include:

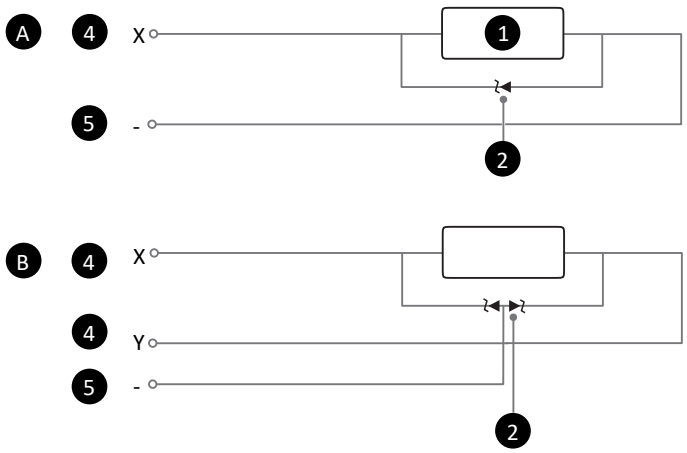
- dc motors (for example, a motor that comprises part of a fan or compressor)
- transformers, relays, and coils

When removing power from an inductive load, a large reverse-voltage may develop, which has the capacity to cause damage to digital switching modules. In extreme cases, excess reverse voltage may cause overheating ofcircuit components, and subsequent fire.

To enable this reverse-voltage to be dissipated safely, you must install a “flyback” diode in the power circuit for the inductive load. Consider the following points when installing a flyback diode:

- position the diode as close as possible to the inductive load
- ensure that the diode is suitably specified for the expected reverse-voltage and current, and for the standard power-supply voltage of the circuit in which it will be installed.
- if protecting a bi-directional load, use an appropriate diode (the following circuit diagram includes an example for bi-directional loads)
- ensure that the diode circuitry is appropriately housed and secured. For example, install the diode securely within a waterproof junction box, to provide adequate environmental protection.

The following illustration shows examples of flyback-diode circuits suitable for most uni-directional and bi-directional inductive loads:



Item	Description
A	Protection circuit for unidirectional loads
B	Protection circuit for bi-directionalloads
1	Inductive load
2	Single TVS diode. For 12V system use GPN 010-12913-01 For 24V system use GPN 010-12912-03
3	Dual TVS diodes. For 12V system use GPN 010-12913-02 For 24V system use GPN 010-12913-04
4	Named digitally switched channel('X' or 'Y')
5	'Minus' connection on digitalswitching unit

Note: The diodes specified above will safely dissipate reverse power up to 5 kW. However, to ensure that the diodes are sufficiently specified for your installation, consult the original equipment manufacturer's documentation for both the equipment that presents an inductive load, and for the digital switching units.

System security

The best practice recommendations in this section will help you to design appropriate security features into your digital switching system. Digital switching systems facilitate both the concentration of data and control mechanisms (for example, multiple systems can be managed using a single MFD screen), and a wider distribution (for example, by using peer-to-peer WiFi between an MFD and a tablet computer, or by providing a GSM SMS text interface to certain systems).

Although this concentration and distribution of data and control enables more efficient management and monitoring, you should ensure that your digital switching system is designed such that only authorized personnel can access and use data and control mechanisms.

This is particularly important where moving equipment could cause injury if operated improperly.

Best practice: when to use GSM SMS(text message) control interfaces

Do not implement GSM SMS (text message) controlinterfaces for equipment whose improper use maycompromise the security or safety, or of personnel.

Although GSM SMS text messaging is not inherently insecure, opening up control of critical equipment to a GSM interface without good cause is not recommended.

For example, providing a GSM SMS interface to controlthe opening and closing of a motorized hatch cover, isnot advisable. However, using SMS to control selectedinterior lighting, would be unlikely to create a safety hazard or security concern; remote control of interior lighting may actually enhance security, by giving the impression that an installation is occupied.

Best practice: consider control panel locks

If system control panels are located where non- authorized personnel may be able to access them, ensure that features controlling systems critical to thesafety of the installation, cannot be accessed without providing appropriate authorization.

Note: It is important to balance the security of system controls, with ease-of-use by authorized personnel. For example, where an important system or item of equipment is protected by a control-panel lock because unauthorized users may have physical access to the panel, authorized users should be given unhindered access to control the same system or item of equipment from at least one other, more secure, location.

Best practice: consider security of switching components

Some of the hardware components of your digital switching system may incorporate physical manual-override switches that can be used to directly control individual circuits.

Ensure that these components are positioned in a secure location, while maintaining easy access for authorized personnel.

Best practice: configure strong Wi-Fi passphrases for MFDs

For application remote use to view and remotely control MFD screens, ensure that all MFDs are set up with a strong Wi-Fi passphrase, and WPA2 Wi-Fi security.

System safety

Digital switching systems enable distributed control and monitoring of electrical systems and equipment.

Combined with bespoke touchscreen user interfaces, and additional means of triggering switching operations(for example, using GSM SMS text messages, or via Wi-Fi using smart phone or tablet applications), a digital switching system offers greater ease-of-use and efficiency when compared to a traditional wiring system.

However, the flexibility available to designers of digitalswitching systems must be considered alongside the safety of the system and those on board.

The following best practice recommendations cover a number of safety features that you should consider when designing a digital switching system.

Best practice: take extra precautions when switching moving equipment

Electrically controlled moving equipment installed presents special safety concerns.

In particular, moving equipment has the potential to cause pinching or crushing injury, entrapment of clothing or body parts, and may cause trips or falls.

Examples of electrically controlled moving equipment include:

- retractable platforms, or steps
- hatch covers
- winches
- doors
- passerelles (gangways)

To mitigate against personal injury caused by moving equipment:

- position switches such that users can maintain line-of-sight with the controlled equipment.
- install a kill switch or dead-man's switch in close proximity to the switched equipment, the closing of which is necessary to operate the equipment, irrespective of any other switching signals received.
- install audible and visual warning devices (for example, a buzzer and strobe light) that are automatically activated before a piece of equipment starts to move, and during use.
- install a safety limit switch (for example, an appropriately positioned micro-switch) to automatically stop equipment that is moved beyond fixed limits.
- implement current detection and limiting, to automatically cut power to a moving piece of equipment that has stalled due to a physical obstruction.
- never allow electrically powered moving equipment to be activated or controlled at a distance from the installation, such as via GSM SMS text messages.

Best practice: configure software fuses for every switched circuit

The switching and control modules that comprise your digital switching system may include software fuses for each switched circuit.

Always ensure that the software fuse is correctly configured for each circuit in use; do not leave software fuses set to their default rating, unless the default rating is appropriate for a specific circuit.

Failure to configure software fuses correctly may result in damage to the installation caused by excessive resistive heating, or in extreme cases, fire.

System redundancy and fail-safe design

Digital switching systems are generally very reliable. The reduction in cabling when compared to a traditionally switched system reduces the likelihood that cable connection faults will degrade or disable the control of systems and equipment.

However, digital switching systems are not immune to failures, particularly when subject to extreme environmental conditions, such as a nearby lightning strike.

Careful and considered design with regard to system redundancy and implementing fail-safe mechanisms, will ensure that your digital switching system is robust, and that rare events are less likely to disable critical systems.

Best practice: use redundant switching mechanisms for critical systems

Do not rely on a single switching mechanism to control critical systems and equipment.

For example, if bridge wipers can be controlled and monitored via soft-switches on a touchscreen display,also provide an appropriate physical switch, wired to a digital switching channel, that offers a degree of bridge-wiper control.

If the touchscreen display fails (and no alternative touchscreens are available) or becomes difficult to use due to harsh environmental conditions, a physical switch provides an important backup control.

Best practice: implement fail-safe mechanisms

The components used to build a digital switching system(for example, switching modules and control modules) may include built-in functionality to provide sensible default switching states, given the failure of the CAN bus(in whole or in part), partial failure of power supply, or failure of other digital switching modules.

Ensure that you specify and program appropriate settings for default switching states (often referred to as “limp home” settings), for all critical circuits under the control of the digital switching system.

System performance

To ensure that your digital switching system operates consistently and reliably, certain limitations of the NMEA 2000 (CAN bus) network, and MFDs should be considered.

These limitations concern the bandwidth of the NMEA 2000 backbone (that is, the amount of data that can be transferred across the network within a given time), and the maximum memory available to the digital switching application running on MFDs.

Best practice: consider NMEA 2000 (CAN bus) bandwidth limitations

The NMEA 2000 (CAN bus) backbone is capable of reliably transmitting digital switching data between elements of a complex system at a high rate.

However, the rate at which data can be reliably transmitted is not unlimited. In particular, graphical animations on an MFD's digital switching pages may require a large amount of data to be transmitted across the NMEA 2000 network. For example, you may wish to animate the position of a bathing platform, as the platform position changes.

To avoid overloading the NMEA 2000 network, minimize the number of animated elements in your MFD page designs.

Best practice: Graphic file size

When designing graphics for WDU applications, make sure to limit the width and height for all graphical assets based on the target device that will be used.
Limit Graphics file size for Raymarine MFDs to 15 mb.

System testing and commissioning

Having followed best practice for system design, it is important that all components of the digital switching system as implemented, are comprehensively tested.

Testing should take place during system build, and also when the installation is commissioned, to ensure that the digital switching system operates as designed alongside and in conjunction with all other systems.

Note: Refer to the international standard IEC 61508 (”Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”) for comprehensive guidelines on developing systems that comprise electrical, electronic, or programmable electronic components that perform safety functions.

Best practice: take appropriate precautions when testing

When testing a system, take precautions to prevent unintended injuries to personnel or damage to the installation.

In particular, moving equipment or system components could cause entrapment injuries if they were to move unexpectedly. This could happen if, for example, a connector is incorrectly wired, or an output channel is incorrectly allocated.

Precautions to take when testing, include:

- ensuring personnel keep clear of moving equipment
- checking that the correct output channels are activated as expected before connecting equipment power plugs

Best practice: perform comprehensive system testing

A comprehensive description of how to test your digital switching system is beyond the scope of this document. However, as a minimum, the following points should be considered:

- carefully document all tests and test results,including information about:
    - when each test was performed
    - who performed each test
    - the exact version of the software and firmware installed on system components during testing
    - the configuration files used during testing
- before starting tests or commissioning, ensure that the latest firmware and software is installed on all devices (such as MFDs, and digital switching units);manufacturers may release frequent firmware or software updates to fix issues with components.
- test every circuit that is under the control of the digital switching system; ensure that each switching mechanism operates the equipment or system that it is designed to operate, and only that equipment or system.
- comprehensively test all bespoke touchscreen user interfaces.

- run tests to simulate the failure of digital switching system components, and of partial power and CANbus network failures; ensure that any fail-safe logic designed into the system operates correctly and maintains adequate control systems.

When commissioning, you should make suitable user documentation available to the personnel that will be using the digital switching system while operating the installation. For more complex systems, bespoke user training may also be appropriate.

Best practice: perform regression tests

Whenever you make any changes to an existing system, always re-test the entire system to ensure that all features and components continue to operate as expected.

System documentation and backups

Although a digital switching system can greatly reduce the complexity and amount of cabling required compared to an equivalent traditionally switched system, it is still important to document the design of each installed system.

System documentation, copies of which should be stored available in the installation/system environment, can be invaluable when troubleshooting switching problems, orwhen modifying and upgrading a system.

Best practice: provide comprehensive system documentation

Digital switching systems comprise numerous components, in addition to the items of equipment or systems that are being switched.

To aid troubleshooting and upgrades, document the following:

- CAN-bus cabling, including the connectivity and locations of the main backbone, terminators, tee-pieces and adapters, drops (spurs), power connections, and CAN-compatible units. Create circuit diagrams as appropriate.
- Connections (both power cables, and CAN-bus cables) between all digital switching system components (such as switching modules, and control modules), switched equipment and systems. Create circuit diagrams as appropriate.
- Switching-channel data (listing, for example, switching-module channel numbers, along with channel functions, associated touchscreen display switches and indicators, software-fuse settings, and fail-safe fallback settings).

Much of this documentation can be based on the initial design documents for a digital switching system.

Consider making documentation available electronically,as well as providing physical printed copies. For example, help materials could be built into the digital switching MFD pages, providing contextual help.

Best practice: keep system documentation up to date

Whenever you make changes to a digital switching system, always update the system documentation to keep it in-line with the changes.

Best practice: provide contextual labelling and emergency instructions

In a troubleshooting scenario, clear and comprehensive labeling of physical components can be of great assistance.

Contextual labeling (physical labels applied directly to, or adjacent to, system components) supplements separate system documentation, and will make troubleshooting less prone to error, and more efficient.

Where space is limited, or individual labeling of switching-channel connections is inconvenient, provide a comprehensive list of switching-channel data on a separate sheet, and affix this adjacent to the relevant digital switching modules.

Direct tagging and labeling of individual cables will also assist when troubleshooting or upgrading a system.

In the unlikely case that a digital switching system suffers a major failure while in operation, provision of emergency operation instructions and checklists will be of great benefit. This material should always be available and focused on operating the most critical systems in the event that digital switching components are not working correctly (for example, navigation lights, communication systems, and engine control andmonitoring).

Best practice: create system backups,and manage software changes

In addition to the physical hardware and cabling, your digital switching system may include configuration files and software (for example, specific versions of firmware) that are essential for the correct operation ofthe system.

It is important that any required configuration files and additional software are backed-up to a safe location, and that any changes are carefully managed. Maintaining backups and managing changes to configuration files and software will be helpful when recovering or troubleshooting a digital switching system, or if re-installation is required.

References

- “Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems”(IEC 61508)
- “NMEA 2000 Standard” (Edition 3.101, March 2016) 30

Support

A lot of useful information can be found on our website. In case answers can't be found there, feel free to contact us anytime by phone or email.

Website
https://www.EmpirBus.com/#faq
https://www.EmpirBus.com/#support

Email:
Support@EmpirBus.com

Phone:
+46 522 44 22 22
8 am to 5 pm (CET/CEST), Monday to Friday

Address:
Garmin Sweden Technologies AB
Spikvägen 1
S-451 75 Uddevalla
SWEDEN