

Workover Safety System

The present invention relates to subsea safety systems, more specifically to Workover System (WOS) and equipment, said WOS typically installed on top of the Christmas Tree (XT), allowing safe intervention operations typically in a hydrocarbons containing well. More specifically, the invention concerns a control system for controlling safety functions in a subsea intervention arrangement, as specified in claim 1.

A subsea intervention operation on a hydrocarbon comprising well typically includes,

1. Well Control Package (WCP) – typically comprising two subsea modules, Emergency Disconnect Package (EDP) and Lower Riser Package (LRP), typically surrounding the well bore with safety valves,
2. Riser System – a set of connected riser joints, typically pipes with approximate lengths 30 – 50 m, which connect the WCP and Workover rig or vessel,
3. Workover Control System (WOCS) – typically comprising electric, electronic and hydraulic systems that control practically all operations in WOS, said operations include, opening and closing of valves, measuring of parameters including, temperature and pressure, energy supply to various equipment including, electric and hydraulic.

Nowadays there are increased requirements for the Safety Instrumented Systems (SISs), for example, the Norwegian Petroleum Authority requires stringent implementation of SISs to mitigate risks to personnel, environment and assets. In the Workover business segment, this mainly relates to three safety functions,

- Production Shutdown (PSD),
- Emergency Shutdown (ESD), and
- Emergency Quick Disconnect (EQD).

The above functions strive to protect the rig or vessel from hazardous conditions such as hydrocarbon spill or leakage in the process area or environment, and spill from the riser. These functions further protect the integrity of the well, for example in the event of position loss. Position loss may occur for example, if the vessel/rig drifts outside a given area from the location of the well.

Implementation of the minimum scope of the safety functions is usually regulated through international standards such as IEC61508 and ISO 13628-7, where the latter also includes some Workover specific requirements.

5 In conventional systems, the safety functions are implemented as an integral part of the process control system, wherein some sort of software separation is implemented between the process control system and the SIS. Some safety regulations demand further separation of the Workover Safety System (WSS) from the process control system, such that the WSS is segregated from the process control system.

10 The prior art includes US 2014/374114 A1, which describes a subsea intervention system including at least one control station, at least one programmable logic controller system in each control station, at least one supervisory control and data acquisition system, and at least one safety system capable of interacting with each control station. The safety system is capable of controlling a process shutdown process, an emergency shutdown process, and an emergency quick-disconnect process. The system may also
15 include subsea distribution units, safety manifold subsea control modules, system hydraulic power units, client hydraulic power units, grease skids, flushing and chemical injection units, or umbilical reelers.

The prior art also includes WO 2011/041550 A2, which describes a technique enabling the protection of subsea wells. The technique employs a subsea test tree designed to
20 ensure control over the well in a variety of situations. The subsea test tree is formed with at least one shut-off valve to protect against unwanted release of fluids from the subsea test tree. The subsea test tree also is coupled with and controlled by a control system having a subsea control module mounted to an interior mandrel.

25 The present invention concerns a system of said Workover Safety System (WSS), where the functionality said WSS is implemented independent of the process control system. The present invention, hence achieves a higher degree of separation between the WSS and the process control system, thereby satisfying and exceeding the recent standards and overcoming the limitation of conventional systems, as shown in the accompanying claims.

Figure 1 shows a simplified example of a riser based conventional Workover Control System (WOCS) 100. Such a system comprises a riser 108, a Master Control Unit (MCU) 101 placed, for example, upon a drilling rig deck or platform 110, a Hydraulic Power Unit (HPU) 102, umbilicals, comprising e.g., workover umbilical 103, Subsea Electronics Module (SEM) (see for example 201, Fig. 2) and Workover Control Module (WOCM) typically comprised in WCP 105. Amongst these,

- The MCU 101 is typically a container located on a deck 110. Said container typically comprises operator control panels, logic controller, subsea power and communications unit, and other electrical, electronic or programmable system components. The MCU communicates with the HPU 102 and one or more Subsea Electronics Modules 201.
- The HPU 102 typically comprises accumulators and hydraulic function control valves. The HPU 102 may further comprise pneumatic valves and electrically operated solenoid valves.
- The SEM 201 is typically split in one instrument module and one control function module. The control function SEM comprises driver cards that receive signals from the topside control system and applies power to the corresponding hydraulic control function in the Workover Control Module (WOCM). WOCM, see e.g., 201 is typically located subsea and is a part of the Well Control Package (WCP) 105. Fig. 1 also shows a riser system 108.

In other words, the MCU 101 typically sends digital control signals to the HPU 102 and to the WOCM for controlling the operation of the valves in the Workover System. Other parts shown in fig. 1 are not discussed further as they will be obvious to the person skilled in the art.

Figure 2 shows an alternative diagram of a Workover System. The system comprises 200, a drilling rig derrick, or tower or such for workover, said tower or derrick may for example be aboard a service vessel or rig with a platform or deck 110, and a process plant 202. Said deck 110 may be placed on a drilling rig or it may be placed on a well intervention vessel. On a drilling rig this deck 110 is often named drill floor. On the automation side, the system comprises an MCU 101 and an HPU 102 located on the topside. The figure further shows the Well Control Package (WCP) 105 in more detail.

WCP 105, sometimes also called workover stack, mainly comprises Lower Riser Package (LRP) 204, and Emergency Disconnect Package (EDP) 205. Christmas Tree (XT) 203 is also shown for reference. The LRP 204 and EDP 205 comprise a plurality of valves for controlling and isolating the flow of hydrocarbons. The main functionality of typical valves in the workover system is as follows,

- Surface Production Wing Valve (SPWV) 208 is typically located in the surface flow tree 209. SPWV 208 is used for isolating the vessel process plant from hydrocarbon flow in a riser-based workover system.
- Gate valve, typically named here Retainer Valve (RV) 211 is used for isolating the riser 108 from hydrocarbon flow in a riser-based workover system. RV 211 retains potential hydrocarbons inside the riser, for example, in the event of an Emergency Quick Disconnect (EQD).
- Gate valve, typically called here Production Isolation Valve (PIV) 212 is used for isolating the riser 108 from the hydrocarbon flow in a riser-based workover system. PIV 212 also functions as a secondary well barrier, for example, in the event of an Emergency Quick Disconnect (EQD).
- Valves 231, 232, 233 and 234 illustrate annulus bore valves, crossover valves, and injection valves. These valves are used for functions including, circulating the well and injecting chemicals.
- Typically named EDP Sea Dump Valve, 241 is used for opening the return line for the hydraulic control fluid into the sea in order for the return system to not restrict the control fluid flow from the valves, for example, during an event of Emergency Shutdown (ESD) or Emergency Quick Disconnect (EQD).
- Typically named LRP Sea Dump Valve, 242 is used for opening the return line for the hydraulic control fluid into the sea in order for the return system to not restrict the control fluid flow from the valves, for example, during an event of Emergency Shutdown (ESD) or Emergency Quick Disconnect (EQD).
- EDP Connector Primary Unlock 251 is used for unlocking the EDP connector, allowing the EDP 205 to disconnect from LRP 204.
- EDP Connector Secondary Disconnect 252 is used for backup function to the EDP Connector Primary Unlock 251. The primary function of Secondary Disconnect 252 is to allow the EDP 205 to disconnect from LRP 204.

There are typically two main bore valves in the LRP 204, either two gate valves or one gate valve (e.g. upper and lower PIV) and one shear seal ram (Safety Head (SH)).

The present invention concerns a Workover Safety System (WSS), more specifically a control system for controlling safety functions in a subsea intervention arrangement, as
5 specified in claims 1 – 14, wherein said WSS is physically segregated from the process control system (WOCS) 100. The WSS as proposed in the present invention is designed to be simplistic in sense, only implementing the absolute necessary functionality to achieve shutdown and/or disconnect. In addition, the present invention seeks to reduce the response times for critical events, for example, subsea safety functions ESD and
10 EQD. The system is designed with features including reduced number of critical valves for ESD/EQD, implementing bleed-off function, and eliminating the need for WOCM 104 in shutdown events.

The present invention will now be described in detail below with reference to accompanying drawings, illustrating the invention by way of examples.

15 For the sake of simplicity without limitation or loss of generality, most of the discussion in this specification will use an open-water workover system to describe the present invention. A person skilled in the art will understand that the features of the present invention can be applied to other types of workover, subsea, or other systems where advantages such as an enhanced separation and reliability between the control system
20 and the safety system are required.

Furthermore, for the sake of simplicity, functionality lying within the scope of the same sub-system, for example, blocks representing a WSS function are shown with the same reference sign on all the figures. A person skilled in the art will understand that such WSS shown in different figures does not have to be the exact same module or controller
25 comprising entire functionality shown in all of the attached figures, it may also be a different controller implemented in a distributed control topology or their like. Such distributed controllers, might be communicating with each other, and/or to a main controller by using a communication link. Such variations in implementation have not been shown in the following figures to keep the matter simple, so their absence should

not been deemed limiting or seen as a loss of generality of the present invention. Similar reasoning also applies to other blocks presented in the following figures.

- Fig. 1 illustrates a simplified example of a typical conventional workover system.
- Fig. 2 illustrates an alternative example of a typical conventional workover system.
- 5 Fig. 3 illustrates an embodiment of the system according to the present invention.
- Fig. 4 illustrates an embodiment of the Process Shutdown (PSD) function according to the present invention.
- Fig. 5 illustrates an embodiment of the Emergency Shutdown (ESD) function according to the present invention.
- 10 Fig. 6 illustrates an embodiment of the Emergency Quick Disconnect (EQD) function according to the present invention.
- Fig. 7 illustrates an embodiment of the Uninterruptible Power Supply (UPS) philosophy according to the present invention.
- Fig. 8 illustrates a first embodiment of the accumulator philosophy according to the present invention.
- 15 Fig. 9 illustrates an embodiment of the landing string ESD function according to the present invention when using the first embodiment of the accumulator philosophy.
- Fig. 10 illustrates an embodiment of the landing string ESD function using a second embodiment of the accumulator philosophy according to the present invention.
- 20 Fig. 11 illustrates an alternative embodiment of the UPS philosophy according to the present invention.
- Fig. 12 illustrates an embodiment of the power management system according to the present invention.
- 25

Fig. 13 illustrates an embodiment of the Fail- Safe-Close configuration according to the present invention.

Fig. 14 illustrates an embodiment of the Fail-as-Is configuration for the activation of the final elements according to the present invention.

- 5 The proposed invention is implemented such that it can be retrofitted to any open-water workover system, riser-less workover system and their like. The topside controller and hydraulic safety adapter are compatible to most direct hydraulic in-riser workover systems, or landing string systems.

Now referring to Fig. 3, which illustrates an embodiment of the system shown in
10 Fig. 2 extended with the proposed WSS 301a, 301b and 301c. The proposed WSS 301a, 301a and 301c comprises,

- Topside part 301a,b: Topside part 301a,b of the WSS is implemented such that it is independent of the topside part of the WOCS 100. Only exception is an Uninterruptible Power Supply (UPS) (not shown in Fig. 3), which is shared
15 between the WSS 301a, b and WOCS 100. The WSS topside part 301a is implemented such that it can be retrofitted into existing workover containers, if preferred. Alternatively, the WSS topside part 301a can be installed in a separate container. The topside part 301a of the proposed WSS comprises sequencing logic and communications interfaces as well as the initiators and conditioning
20 monitoring system. In addition, the WSS topside part 301a,b includes a Hydraulic Safety Adapter, said adapter further comprising Directional Control Valves for initiation of direct hydraulic safety functions such as Production Shutdown (PSD) and in-riser workover ESD.
- Workover Safety Module (WSM) 302: In the proposed invention, WSM 302 is typically implemented as a subsea part 301c of the WSS. WSM 302 is mounted
25 on the Emergency Disconnect Package (EDP) 205 and is independent of the Subsea Control Module and Workover Control Module. WSM 302 is the executing part of the WSS. Proposed WSS 301a, b and c is typically supplied with two WSMs for full redundancy in safety function execution.

- Directional Control Valves 303: For de-energized-to-close functions, directional Control Valves 303 inside the WSM 302 normally allow the hydraulic output from the WOCM 201 to pass through. Upon initiation of a critical event, for example, an ESD, the Directional Control Valves 303 shift position, dumping the hydraulic output from the Workover Control Module to return. This causes the main bore valves to close according to the hydraulic system design in a traditional workover stack or WCP. The EDP connector normally requires a different functionality, where the WSM 302 blocks an accumulator supply, and in a critical event opens the line in order for the accumulator to pressurize the EDP connector functions. The DCVs 303 can either be electrically held in position (i.e., de-energize to trip), or more preferably, be normally de-energized (i.e., electrically activated to trip).

There are around fourteen subsea valves and around thirteen topside valves, which are operated by the proposed WSS 301a, b and c in the event of an emergency or critical event. The number of valves depends upon the workover system configuration. Figure 3 shows an embodiment of a standard open water workover configuration in which the proposed WSS 301a, b and c operates eleven subsea- and one topside- valves.

One of the main objectives of the present invention is implementing emergency shutdown functionality in workover systems independent of the WOCS. The emergency shutdown functions are typically, Process Shutdown (PSD), Emergency Shutdown (ESD), and Emergency Quick Disconnect (EQD). These are explained as follows.

Process Shutdown (PSD)

Key features of the PSD function are:

1. PSD closes side outlets in the surface flow tree 209 of a workover system, for example, the Surface Production Wing Valve (SPWV) 208.
2. For riser-based workover systems, PSD is typically executed topside only, and does not as such require communications through the workover umbilical. In riserless workover systems, PSD is a function on the XT, normally controlled by WCP and overridden by WSS in critical events
3. It is usually push-button initiated.

4. PSD can also be initiated by the process facility internal ESD function.
5. PSD can also be initiated by the vessel/rig Safety and Automation System's ESD function.
6. PSD is a fail-safe, usually fail-safe-close, type safety function, upon loss of
5 electrical and/or hydraulic power.
7. PSD is usually a de-energize-to-trip safety function, meaning the final element is opened by powering, for example, by electrical, pneumatic, or hydraulic power, or their combination. Cutting the power to the final element causes the safety function to revert to safe state.
- 10 8. Safe state for the system in this case is, rig/vessel process facility isolated from riser/hydrocarbon return content, typically within 5 seconds of initiation of the PSD event.
9. Electrical power supply, usually sourced through UPS, is shared with the WOCS.
- 15 10. Hydraulic and/or pneumatic power supply is usually not required for the PSD function, however said hydraulic/pneumatic supply is normally used to hold the SPWV 208 open. Without the WSS as proposed in the present invention, electric power keeps a pneumatic valve open, which keeps a DCV open, which further keeps the SPWV 208 pressurized to stay open. With the proposed WSS a second
20 DCV is added; electric power keeps the WSS DCV open (i.e., said DCV is electrically held open), which keeps the SPWV 208 pressurized to stay open.

Figure 4 shows a typical PSD principle sketch according to a preferred embodiment of the present invention. The arrows with solid lines as in 450 represent electrical signals, whereas dashed lines as in 460 represent hydraulic signals. A person skilled in the art
25 will understand that alternative embodiments are possible by extending, reducing, replacing or combining the scope of hydraulic and electric signals. In some embodiments, achieving similar functionality with an alternative power source such as pneumatic is also possible. Specific embodiments are hence, presented in a general sense for the sake of simplicity and without limiting the scope of the invention.

The rounded blocks, 401, 404 and 407, in Fig. 4 represent the WSS components according to the present invention, whereas the rest of the blocks (rectangular) represent here WOCS components.

As discussed previously, Uninterruptable Power Supply (UPS) 402 is shared between
 5 the WOCS part 405 and WSS part 404.

WOCS is accessible to the operator, typically through a Human Machine Interface (HMI) 403 located in the topside part, for example, the MCU container 101. WOCS HMI interacts with a WOCS logic controller 405, said controller further interacting with a HPU controller 406, preferably a Programmable Logic Controller (PLC), typically
 10 located in an HPU container 102. The HPU PLC 406 controls a Surface Production Wing Valve (SPWV) Directional Control Valve (DCV) 408. Said SPWV DCV 408 controls the hydraulic power supply from WOCS Accumulator Bank 409. Said hydraulic power supply is used for activating SPWV 208 located topside, typically in Surface Flow Tree 209.

15 The WSS part according to the present invention is shown in round shaped blocks, 401, 404 and 407. PSD sequence in WSS is activated through a pushbutton 401 that transmits a PSD event to a WSS logic controller 404. Preferable embodiments of WSS logic controller include PLC. In further embodiments, the system also includes relay to switch in a higher voltage, insulation line monitoring logic, and Ohmmeter for line
 20 monitoring. Relay to switch in a higher voltage is typically not required for PSD, as PSD is usually a de-energize to trip type function. The WSS Logic Controller 404 controls a dedicated PSD DCV 407 to bleed off the hydraulic supply to the Surface Flow Tree Side outlets in order to override the WOCS.

The PSD safety function is typically used when there are major disrupting events in the
 25 process facility, for example hydrocarbon leakages in the production facility, or in hoses from the Surface Flow Tree 209 to the production facility.

Emergency Shutdown (ESD)

Key features of the ESD function are:

1. ESD typically closes all (usually three) main bore valves and all annulus bore valves in the well control package, i.e., the subsea part of the workover system.
2. ESD function typically requires communication through the workover umbilical or through a similar communications cable from topside system to subsea system.
3. ESD is typically pushbutton activated/initiated.
4. ESD function can be initiated by the vessel/rig safety and automation system's ESD function.
5. ESD function is typically provided with an additional spare instrumented initiator port for future automatic initiation functionality.
6. ESD is typically a fail-as-is type safety function upon loss of electrical or hydraulic power. In other words, ESD is fail-safe as is type function upon loss of one of power types subsea. In the event that both electrical and hydraulic powers fail simultaneously, ESD is typically a fail safe close function.
7. ESD is typically an energize-to-trip safety function, meaning that the final element is brought to safe state by applying, power, for example, electrical, hydraulic, pneumatic, or their combination. Cutting the supply of said power does not normally cause the safety function to go to safe state. By safe state, it is here meant that the rig/vessel and environment being isolated from the reservoir content.
8. Electrical power supply, usually sourced through UPS, is usually shared with the WOCS. Upon complete loss of electrical power, e.g., loss of UPS, the system will go to safe state by inherent fail-safe-close functionality, however, not necessarily within the timing requirements for the ESD function.
9. Hydraulic power supply used for close assist for the main bore valves is also typically shared with the WOCS.
10. Hydraulic power supply for pilot functions is typically not required in this function.
11. The ESD function typically further initiates the PSD function described above.

A preferred embodiment of the ESD functionality according to the present invention is shown in Fig. 5. The arrows with solid lines 450 represent electrical signals, whereas dashed lines 460 represent hydraulic signals. A person skilled in the art will understand

that alternative embodiments are possible by extending, reducing, replacing or combining the scope of hydraulic and electric signals. In some embodiments, achieving similar functionality with an alternative power source such as pneumatic is also possible. Specific embodiments are, hence, presented here in a general sense for the
 5 sake of simplicity and without limiting the scope of the invention.

The rounded blocks, 500, 404, 407, 501, 502, 503, 504, and 505 shown in Fig. 5 represent the WSS components according to the present invention, whereas the rest of the blocks represent here WOCS components.

As discussed previously, Uninterruptable Power Supply (UPS) 402 is preferably shared
 10 between the WOCS part 405 and WSS part 404.

WOCS functionality shown in Fig. 5 is similar to that explained in the discussion of Fig. 4 above.

ESD sequence is activated/initiated through a pushbutton 500 that transmits an ESD event to the WSS logic controller 404. The interactions of the WSS controller 404 with
 15 PSD DCV 407 and SPWV 208 are disclosed in the discussion of Fig. 4 above. Proposed embodiments of the WSS logic controller 404 have also been discussed above.

According to the present invention, one or more subsea canisters, mounted on the Emergency Disconnect Package (EDP) 205, usually in the upper part of the Well Control Package 550, typically comprises 14 DCVs (comprising 501 – 505) to enable
 20 an independent control of the final elements, including,

- a. Retainer Valve (RV) 211
- b. EDP Sea Dump Valve 241 (not shown in Fig.5)
- c. Production Isolation Valve (PIV) 212
- d. Safety Head (SH) 515. SH 515 is a ram type valve designed for isolating coiled
 25 tubing. It typically has better isolating/cutting capabilities than gate valves and is used to reduce risk in some systems. Alternatively, other systems use three gate valves, the SH 515 is then absent and a gate valve is inserted to replace it, the inserted gate valve is often called Lower Production Isolation Valve (LPIV)
- e. LRP Sea Dump Valve 242 (not shown in Fig. 5)
- 30 f. Workover Control Module hydraulic supply (not entirely shown in Fig. 5)

- g. Workover Control Module internal hydraulics (not specifically shown in Fig. 5)
- h. Bleed-Off Valve (BOV) (not shown in any figures) – EQD only (used to prevent hydraulic lock (vacuum) when disconnection EDP from LRP)
- i. E.g. Upper Methanol Injection Valve (UMIV) (not shown in figures) – EQD only (redundant to BOV)
- j. Emergency Disconnect Package Connector Primary Unlock 251 – EQD function only (not shown in Fig. 5)
- k. Emergency Disconnect Package Connector Secondary Unlock 252 – EQD function only (not shown in Fig. 5)
- l. Spare functionality

The ESD safety function is typically activated only when there is a major hydrocarbon leakage either on the vessel/rig or in the riser/hydrocarbon return line. The ESD function is initiated typically by a pushbutton 500, thereby sending a signal to the WSS Logic Controller 404, said Logic Controller 404 preferably a PLC, to initiate the shutdown sequence. Upon receiving said signal, the PLC further notifies the process control system of the initiation. The shutdown sequence is performed by the PLC 404. The typical steps are as follows (not necessarily in the same order)

1. Logic Controller 404 sends a signal to the WOCS notifying the process control system of the ESD initiation.
2. Logic Controller 404 sends a signal, preferably an electrical signal, to the DCV 503 bleeding off the pilot pressure on the open side of the RV highflow DCV, thereby causing the RV 211 to close. The same signal is also sent to the DCV bleeding off the pilot pressure on the close side of the EDP Sea Dump Valve, thereby causing the EDP Sea Dump Valve 241 to open. This allows for a shorter closing time for the RV 211.
3. Logic Controller 404 sends a signal, preferably an electrical signal, to the DCV bleeding off the pilot pressure on the open side of the PIV high-flow DCV, thereby causing the PIV 212 to close. The same signal is also sent to the DCV bleeding off the pilot pressure on the close side of the LRP Sea Dump Valve, thereby causing the LRP Sea Dump 242 Valve to open. This allows for a shorter closing time for the PIV 212.

4. Logic Controller 404 sends a signal, preferably an electrical signal, to the two DCVs 501 and 502 bleeding off the low-pressure hydraulic supply to the Workover Control Module, thereby leading all the valves 510 in the Well Control Package 550 to fail-safe.
5. Logic Controller 404 sends a signal, preferably an electrical signal, to the two DCVs bleeding off the internal hydraulics of the Workover Control Module, thereby further enabling a shorter fail-safe response of the Well Control Package 550.
6. Logic Controller 404 sends a signal, preferably an electrical signal, to the DCV bleeding off the pilot pressure on the open side of the Safety Head high-flow DCV, thereby causing the Safety Head 515 to close.

Emergency Quick Disconnect (EQD)

Key features of the EQD function are:

1. EQD typically closes all (usually three) main bore valves and all annulus bore valves in the well control package 550, i.e., the subsea part of the workover system. EQD further disconnects EDP 205 from LRP 204, in other words, the upper and the lower parts of the WCP 550 are disconnected.
2. EQD function typically requires communication through the workover umbilical or through a similar communications cable from topside system to subsea system.
3. EQD is typically pushbutton activated/initiated.
4. EQD function can be initiated by the vessel/rig safety and automation system's ESD function.
5. EQD function is typically provided with an additional spare instrumented initiator port for future automatic initiation functionality.
6. EQD is typically a fail-as-is type safety function upon loss of electrical and/or hydraulic power. This is because in this case it is safer to be in a fail-safe-as-is state and remain connected upon failure rather than to disconnect spuriously.
7. EQD is typically an energize-to-trip safety function, meaning that the final element is brought to safe state by applying, power, for example, electrical,

hydraulic, pneumatic, or their combination. Cutting the supply of said power does not normally cause the safety function to go to safe state.

8. By safe state, it is here meant that the rig/vessel and environment being isolated from the well/reservoir content and further, said rig/vessel being disconnected from the well.
9. Electrical power supply, usually sourced through UPS, is usually shared with the WOCS. Upon complete loss of electrical power, e.g., loss of UPS, the system will go to safe state by inherent fail-safe-close functionality, however, not necessarily within the timing requirements for the EQD function.
10. Hydraulic power supply used for close assist for the main bore valves is also typically shared with the WOCS.
11. Hydraulic power supply for pilot functions of the EDP 205 is preferably supplied through separate accumulators.
12. The EQD function typically further initiates the PSD function as described above.

A preferred embodiment of the EQD functionality according to the present invention is shown in Fig. 6. The arrows with solid lines 450 represent electrical signals, whereas dashed lines 460 represent hydraulic signals. A person skilled in the art will understand that alternative embodiments are possible by extending, reducing, replacing or combining the scope of hydraulic and electric signals. In some embodiments, achieving similar functionality with an alternative power source such as pneumatic is also possible. Specific embodiments are, hence, presented in a general sense for the sake of simplicity and without limiting the scope of the invention.

The rounded blocks, 600, 404, 407, 501, 502, 503, 504, 505, and 601 shown in Fig. 6 represent the WSS sequence according to the present invention, whereas the rest of the blocks represent here WOCS sequence.

As discussed previously, Uninterruptable Power Supply (UPS) 402 is preferably shared between the WOCS part 405 and WSS part 404.

WOCS functionality shown in Fig. 6 is similar to that explained in the discussion of Fig. 4 above.

EQD sequence is activated/initiated through a pushbutton 600 that transmits an EQD event to the WSS logic controller 404. The interactions of the WSS controller 404 with PSD DCV 407 and SPWV 208 are disclosed in the discussion of Fig. 4 above. Proposed embodiments of the WSS logic controller 404 have also been discussed above.

5 According to the present invention, one or more subsea canisters, mounted on the Emergency Disconnect Package (EDP), usually in the upper part of the Well Control Package 550, typically comprises 14 DCVs to enable an independent control of the final elements, including,

- a. Retainer Valve (RV) 211
- 10 b. EDP Sea Dump Valve 241 (not shown in Fig. 5)
- c. Production Isolation Valve (PIV) 212
- d. Safety Head (SH) 515
- e. LRP Sea Dump Valve 242 (not shown in Fig. 5)
- f. Workover Control Module hydraulic supply (not entirely shown in Fig. 6)
- 15 g. Workover Control Module internal hydraulics (not specifically shown in Fig. 6)
- h. BOV – see list in ESD function for description
- i. UMIV – see list in ESD function for description
- j. Emergency Disconnect Package Connector Primary Unlock 251 (shown as a general block, EDP Connector 611, in Fig. 6)
- 20 k. Emergency Disconnect Package Connector Secondary Unlock 252 (shown as a general block, EDP Connector 611 controllable by EDP connector DCV 601, in Fig. 6)
- l. Spare function

The EQD is normally initiated when the rig/vessel loses position (drive off/drift off) or
 25 when a major hydrocarbon leakage is not contained by the ESD and the rig/vessel needs to move off location as soon as possible. The EQD function is initiated typically by a pushbutton 600, thereby sending a signal to the WSS Logic Controller 404, said Logic Controller 404 preferably a PLC, to initiate the shutdown sequence. Upon receiving said signal, the PLC further notifies the process control system of the initiation. The
 30 shutdown sequence is performed by the PLC 404. The typical steps are as follows (not necessarily in the same order)

1. Logic Controller 404 sends a signal to the WOCS notifying the process control system of the EQD initiation.
2. Logic Controller 404 sends a signal, preferably an electrical signal, to the DCV bleeding off the pilot pressure on the open side of the RV high-flow DCV, thereby causing the RV 211 to close. The same signal is also sent to the DCV bleeding off the pilot pressure on the close side of the EDP Sea Dump Valve, thereby causing the EDP Sea Dump Valve 241 to open. This allows for a shorter closing time for the RV 211.
3. Logic Controller 404 sends a signal, preferably an electrical signal, to the DCV bleeding off the pilot pressure on the open side of the PIV high-flow DCV, thereby causing the PIV 212 to close. The same signal is also sent to the DCV bleeding off the pilot pressure on the close side of the LRP Sea Dump Valve, thereby causing the LRP Sea Dump 242 Valve to open. This allows for a shorter closing time for the PIV 212.
4. Logic Controller 404 sends a signal, preferably an electrical signal, to the two DCVs bleeding off the low-pressure hydraulic supply to the Workover Control Module, thereby leading all the valves 510 in the Well Control Package 550 to fail-save.
5. Logic Controller 404 sends a signal, preferably an electrical signal, to the two DCVs bleeding off the internal hydraulics of the Workover Control Module, thereby further enabling a shorter fail-safe response of the Well Control Package 550.
6. Logic Controller 404 sends a signal, preferably an electrical signal, to the DCVs applying pilot pressure to the Connector Primary and Secondary functions.
7. Logic Controller 404 sends a signal, preferably an electrical signal, to the DCV bleeding off the pilot pressure on the open side of the Safety Head high-flow DCV, thereby causing the Safety Head 515 to close.

The present invention results in the following key advantages with respect to the conventional WOCS based systems, the main ones are listed below.

For **PSD** functionality, the present invention results in,

1. The safety related system and functionality physically separated from the process control system and functionality – thereby resulting in an independent, fast and reliable system with enhanced safety.
2. Flexibility for use in different types of workover systems including, openwater workover system (as discussed above), landing string, riserless workover system, through-tubing rotary drilling workover system, and their likes or combinations.

For **ESD** functionality, the present invention results in,

1. The safety related system and functionality physically separated from the process control system and functionality – thereby resulting in an independent, fast and reliable system with enhanced safety.
2. Hardware override of the process control system by the safety system, for example using hydraulic piping as shown in the above discussion. Equivalents in electrical, pneumatic, or other systems are also possible.
3. Relatively simplified safety function, making the safety functionality highly reliable and robust. In addition, any fault detection in the system is also easier, thereby resulting in high availability of the system.
4. Subsea retrievable process control without the loss of safety functionality or integrity.
5. Flexibility for use in different types of workover systems including, openwater workover system (as discussed above), landing string, riserless workover system, through-tubing rotary drilling workover system, and their likes or combinations.

For **EQD** functionality, the present invention results in,

1. The safety related system and functionality physically separated from the process control system and functionality – thereby resulting in an independent, fast and reliable system with enhanced safety.
2. Physically segregated hydraulic supply for the pilot stages of connector unlock.

3. Hardware override of the process control system by the safety system, for example using hydraulic piping as shown in the above discussion. Equivalents in electrical, pneumatic, or other systems are also possible.
4. Relatively simplified safety function, making the safety functionality highly reliable and robust. In addition, any fault detection in the system is also easier, thereby resulting in high availability of the system.
5. Subsea retrievable process control without the loss of safety functionality or integrity.
6. Flexibility for use in different types of workover systems including, open-water workover system (as discussed above), landing string, riserless workover system, through-tubing rotary drilling workover system, and their likes or combinations.

Another object of the present invention is to enhance the reliability and robustness of the existing components in a typical workover system or in similar systems. The present invention proposes the following changes to the hydraulic supply, electrical power supply, and power management areas for the WSS to enhance the safety and reliability for safety systems, and to meet newer regulatory safety requirements.

Hydraulic Supply

The more recent regulatory requirements demand, for example,

1. IEC 61511-1 11.2.11: For subsystems that on loss of power do not fail to the safe state, all of the following requirements shall be met and action taken according to 11.3
 - a. Loss of circuit integrity is detected (for example, end-of-line monitoring);
 - b. Power-supply integrity is ensured using supplemental power supply (for example, battery back-up, uninterruptible power supplies);
 - c. Loss of power to the system is detected
2. IEC 61511-1 11.2.4: If it is intended not to qualify the basic process control system to this standard, then the basic process control system shall be designed

to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.

NOTE 1 Operating information may be exchanged but should not compromise the functional safety of the Safety Instrumented System (SIS).

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

Item 1 above is interpreted as to require monitoring and surveillance of the hydraulic power supply and the use of accumulators to store power. For SIL2 achievement it is assumed redundant accumulation is required and sufficient. The accumulators shall be monitored for preventive maintenance using the Basic Process Control System (BPCS) and for detection of loss of hydraulic power using the Safety Instrumented System (SIS). The term SIL2 should be known to the person skilled in the art; SIL2 stand for Safety Integrity Level 2 – which means that the probability of failure is in the order between 10^{-2} – 10^{-3} , and certain requirements to system architecture and project execution shall be met.

Item 2 is interpreted as to require the SIS to be segregated from the basic process control system to the extent possible, and that any and all shared elements and/or communication links cannot adversely affect the SIS.

The following realization is proposed to meet and surpass the safety regulations.

Workover Control System Hydraulic System Accumulators

The Workover Control System (WOCS) is provided with redundant accumulator banks, both for low-pressure (LP) and high-pressure (HP) functions; WOCS LP A and WOCS LP B. Both the banks are dimensioned to keep the BPCS live for a minimum of one hour upon loss of vessel/rig power supply, for example, upon loss of power to hydraulic pumps. Due to requirements and margins for the calculations of the accumulator

dimensioning, the accumulators can normally maintain the BPCS live longer than the minimum requirement of one hour.

The WOCS accumulators 409 further ensure the ability of the WOCS Operator to manually take the system to its defined safe state. Depending upon the specific operating conditions, required steps to reach the safe state may vary. The accumulators 409 are normally located in the WOCS Hydraulic Power Unit (HPU) 102.

Now referring to Fig. 7. Due to the overall rig/vessel philosophy the WOCS UPSs 402a and 402b are equipped with an electrically held switch 701a and 701b, Emergency Power Off (EPO), with which the vessel/rig ESD system may override the UPS setting and switch-off all power on the vessel/rig in the event of emergency. This in turn initiates an electrically held dump valve 705 (held directly by the WOCS UPSs 402a and 402b in a two-out-of-two (2oo2) voting using coils 702a and 702b). The dump valve bleeds off the hydraulic pressure in the WOCS HPU, causing the BPCS to go to its defined safe state, i.e., well sealed and all functions de-energized. WOCS redundancy module 704 makes sure that WOCS 405 receives power even if one of the UPSs, 402a or 402b, fails.

In some embodiments, the quick disconnect function is unavailable, but the acoustic back-up, ROV override and riser weak link are normally available. The acoustic back-up and ROV override are means of initiating the EDP connector disconnect when the WCP has lost electric and hydraulic power supply (e.g. after EPO). Riser weak link is a mechanical function wherein one of the riser joints is designed to rupture when overloaded, allowing the rig/vessel to drive off/drift off and bringing the WCP to fail-safe-close due to loss of electric and hydraulic power. These are additional protection layers to the Emergency Quick Disconnect. EQD is the Safety Instrumented Function (SIF) required if the rig/vessel loses position while the workover system is connected to the well.

Workover Safety System Accumulator Philosophy

The Workover Safety System (WSS) includes safety functions relying on topside accumulated hydraulic and electric power to reach safe state, such as direct hydraulic landing string Emergency Shutdown (where the barrier elements within the Sub Surface

Test Tree require hydraulic power to cut, close and seal the high-pressure well bore). Because of this, the proposed WSS provides hydraulic power to this function with sufficiently high reliability for meeting the SIL2 requirements.

The present invention proposes the following two embodiments illustrating the
5 implementation of the accumulator philosophy.

Embodiment 1: Shared Accumulator Banks

A simplified overview of the first embodiment is shown in Fig. 8. Here, the rounded blocks as in the shape of box “801” represent the modules/functionality as proposed in the present invention. The blocks with hexagonal shape as of the block “802” represent
10 here Basic Process Control System (BPCS) functionality. BPCS is another name for the WOCS. The rest of the blocks, as in “803”, represent here shared functionality between SIS and BPCS. For the sake of simplicity, single components are shown in Fig. 8, however the same philosophy applies also to a plurality of components, for example accumulator 409 can also be a plurality of accumulators.

15 As shown in Fig. 8, the accumulator 409 supplies hydraulic power for both the WSS functions 806, and WOCS functions 805. An isolation valve 808 is placed between the accumulator 409 and the WOCS functionality 805 according to the present invention. Said isolation valve 808 is controlled by the WSS controller 404 that also monitors the parameters of the accumulator 409. Said parameters monitored by the WSS controller
20 404 include pressure and accumulator level. When said parameters reach their predetermined limit, for example when the pressure falls below a certain limit, the WSS controller 404 closes the isolation valve 808 such that the hydraulic capacity stored in the accumulator 409 is reserved for critical functions, i.e. WSS function 806. By doing so, the system is able to ensure that enough hydraulic supply will be available to
25 execute the safety functions and thereby securing the vessel or plant. When the parameters come back within safe limits, the WSS controller 404 opens the isolation valve 808 to allow WOCS functions 805 to be executed.

When the SIS cuts off supply to the BPCS ensuring ability to control safety critical functions, the BPCS is normally forced to go to safe state automatically due to loss of
30 hydraulic power to hold barrier valves open.

The accumulator 409 is monitored by the SIS and monitoring information is shared with the BPCS/WOCS using a communication link, preferably the existing one-way Modbus link, between SIS and BPCS (not shown in Fig. 8).

Figure 9 shows a typical overview of system as it will look as implemented, in this case
 5 for controlling a high-pressure well bore 900 through ball-valves 910a and 910b, according to the present embodiment of accumulator philosophy. The accumulators 409aa, 409ab, 409ba, and 409bb are shared between the SIS and the BPCS functionality. Also, valves 904aa, 904ab, 904ba, and 904bb, as well as 910a and 910b are shared between the SIS and BPCS functions. The hydraulic pumps 909aa, 909ab,
 10 909ba, and 909bb are controlled and monitored by the BPCS. This is done to keep the SIS simple and limited to safety critical functions, thereby achieving advantages including increased robustness and reduced response time of the system. As can be seen from Fig. 9, the BPCS accumulators are fully redundant, and the hydraulic system designed such that redundant barrier element safety functions are controlled from
 15 separate hydraulic power supplies. This further ensures robustness and simplicity in the safety system design.

Embodiment 2: Segregated Accumulation for the Safety System

A simplified overview of the second embodiment is shown in Fig. 10. The Workover Safety System in this embodiment utilizes a separate set of accumulators 1009aa,
 20 1009ab, 1009ba, and 1009bb charged by the WOCS pumps 909aa, 909ab, 909ba, and 909bb respectively. As in the first embodiment, the pumps are not part of the safety function to keep the safety system lean. The system ensures that there is enough accumulated capacity and power at all times sufficient to reach safe state. In specific events, such as an initiation of a safety function, the Workover Safety System
 25 accumulators 409aa, 409ab, 409ba, and 409bb are teed-in to the hydraulic function line to apply hydraulic power to the barrier elements upon said safety function initiation.

The first embodiment discussed above is the preferred embodiment due to advantages such as reduced number of accumulators in the system, and the first embodiment being relatively simpler implementation over the second embodiment.

30 Electrical Supply

Now referring again to the recent regulatory requirements,

1. IEC 61511-1 11.2.11: For subsystems that on loss of power do not fail to the safe state, all of the following requirements shall be met and action taken according to 11.3
 - d. Loss of circuit integrity is detected (for example, end-of-line monitoring);
 - e. Power-supply integrity is ensured using supplemental power supply (for example, battery back-up, uninterruptible power supplies);
 - f. Loss of power to the system is detected
2. IEC 61511-1 11.2.4: If it is intended not to qualify the basic process control system to this standard, then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.

NOTE 1 Operating information may be exchanged but should not compromise the functional safety of the Safety Instrumented System (SIS).

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

Item 1 here is interpreted as to require monitoring and surveillance of the power supply and the use of Uninterruptible Power Supply (UPS). For SIL2 requirement it is assumed redundant UPS is required and sufficient. The UPSs shall be monitored for preventive maintenance using the basic process control system (BPCS) and for detection of loss of power supply using the Safety Instrumented System (SIS).

Item 2 here is interpreted as to require the SIS to be segregated from the basic process control system to the extent possible, and that any and all shared elements and/or communications links cannot adversely affect the SIS.

The following realization is proposed to meet and surpass the safety regulations.

Workover Control System UPS

Now referring again to Fig. 7, the Workover Control System (WOCS) is provided with two redundant UPSs, WOCS UPS A 402a and WOCS UPS B 402b. Both the UPSs are
5 specified such that the BPCS can be kept live for a minimum of one hour upon loss of vessel/rig power supply. Due to requirements and margins for the calculations of the UPS specifications, such as capacity, the UPSs can normally maintain the BPCS live longer than the minimum requirement of one hour.

The WOCS UPSs 402a and 402b further ensure the ability of the WOCS Operator to
10 manually take the system to its defined safe state. Depending upon the specific operating conditions, required steps to reach the safe state may vary.

Due to the overall rig/vessel philosophy the WOCS UPSs 402a and 402b are equipped with an electrically held switch 701a and 701b, Emergency Power Off
- 27 - P4914NO00-TS
15 (EPO), with which the vessel/rig ESD system may override the UPS setting and switch-off all power on the vessel/rig in the event of emergency. This in turn initiates an electrically held dump valve 705 (held directly by the WOCS UPSs 402a and 402b in a two-out-of-two (2oo2) voting). The dump valve bleeds off the hydraulic pressure in the WOCS HPU, causing the BPCS to go to its defined safe state, i.e., well sealed and all
20 functions de-energized.

Workover Safety System UPS Philosophy

For making the Workover Safety System aware of the initiation of the safe state defined in the WSS Emergency Shutdown (ESD) and Process Shutdown SIFs, for example, caused by Vessel EPO signal or failure of both WOCS UPS A 402a and WOCS UPS B
25 402b, the present invention proposes that the Workover Safety System should use the WOCS UPSs as back-up power supply. By doing this, the proposed system avoids instances such as when the WOCS has shut down, for example due to power loss, and the WSS does not know if system has reached safe state.

In the unlikely event that both WOCS UPSs should fail, it is a possibility for the 20 WSS to include a third, independent UPS to maintain the ability to initiate Emergency Quick Disconnect (EQD). Please note that this third UPS too will be subject to the rig/vessel EPO signal, rendering the EQD function unavailable due to the global safety
 5 strategy. As in the previous section, the back-up initiators (acoustic, ROV and riser weak link) are still available because they do not rely on topside accumulated power (electric or hydraulic).

Fig. 11 shows another embodiment of the power management system according to the present invention. In this embodiment, the WSS 404 is supplied power in addition
 10 through a dedicated UPS 1102. The first redundancy module 704a provides redundancy between UPS A 402a and UPS B 402b. The second redundancy module 704b provides redundancy between the output from the first redundancy module and the dedicated WSS UPS 1102. In this embodiment the WSS can keep EQD available even after loss of WOCS UPSs 402a,b, but still has connection to WOCS UPSs 402a,b such that WSS
 15 is aware of loss of power to the WOCS and inherent fail-safe of the workover system.

Power Management

Now referring again to one of the recent regulatory requirements,

1. IEC 61511-1 11.2.11: For subsystems that on loss of power do not fail to the safe state, all of the following requirements shall be met and action taken
 20 according to 11.3
 - g. Loss of circuit integrity is detected (for example, end-of-line monitoring);
 - h. Power-supply integrity is ensured using supplemental power supply (for example, battery back-up, uninterruptible power supplies);
 - i. Loss of power to the system is detected

25 Item 1 a here is interpreted as to require line monitoring of subsea lines and the high-voltage power supply unit (HVPSU) output lines

Item 1 c here is interpreted as to require monitoring and surveillance of the 20 HVPSU condition, i.e. detection of internal failures.

Workover Safety System Power Management Philosophy

It is the main object of the present invention to make the Workover Safety System be simplified, robust and reliable. A key element recognized by the inventors for achieving this objective is to control subsea functions directly using hardwired electrical power.

The subsea functions typically require 4 W at 24 V DC to operate, and are configured to be electrically energized to activate. In other words, the safety functions require electrical power within a given range, for example, at a given voltage to reach safe state. Some requirements such as ISO 13628-7 for workover systems, are important to adhere to.

As an example, direct operation of the subsea DCV coils through cables in the umbilical with lengths of the order of 3600 m will encounter voltage drop over the length of the power carrying cable. The length of umbilical varies depending upon the depth of the actual field where the system is deployed. For supplying 24 VDC to a 4 W 24 VDC coil located subsea connected topside through a 3600 m long AWG 19 cable, a topside voltage of around 190 VDC is required. The voltage drop in the cable depends on several factors, including cable material, length, cross-section, resistivity, and even temperature, which typically alters the resistivity of the material.

The inventors propose the following method and system in yet another embodiment of the present invention, for improving the power supply conditions for the subsea components, including DCVs.

Now referring to Fig. 12, a general form of system and method according to the present invention is proposed as follows,

1. Verify a theoretical model for calculating required topside power for energizing subsea components, such as solenoids, with variable cable lengths, cable cross-section, ambient temperature, and the number of components or solenoids connected in parallel on each cable.
2. Use the theoretical model to generate initial values for the power system settings and initialize the WSS Logic Controller 404, preferably a PLC with said settings.
3. Monitor the subsea line parameters, for example, using electrical measurement equipment 1202, and use said parameters, including voltage

applied and current supplied in the subsea line to dynamically adjust the High Voltage Power Supply Unit (HVPSU) 1201 settings. Said settings adjusted, for example, using a control interface or bus 1211 between the PLC 404 and the HVPSU 1201.

- 5 4. Use the measured parameters from the electrical measurement equipment 1202 to verify and correct the HVPSU 1201 settings, i.e., performing a comparison and correction between the commanded and actual settings.
5. Continuously monitor the HVPSU 1201 for internal diagnostics using the communications link, or bus 1211. Said communication link comprising, for
10 example, a serial communication medium.
6. If a failure is detected in the HVPSU 1201, notify WOCS operator, for example, through SCADA HMI and SIL2 compatible WSS status lamps or displays accessible by the operator. Said lamps visible for the operator even when BPCS or SCADA HMI is not operational.

- 15 A person skilled in the art will understand that in practice there will be at least one HVPSU 1201 each for the A-branch, and for the B-branch for providing clean redundancy from the power supply to the final element in the system.

An important advantage of this embodiment is that the system may be built using off-the-shelf components to nevertheless achieve a highly reliable, robust and simplistic
20 safety system. In other words, the High-Voltage Power Supply Units 1201 (HVPSU A and HVPSU B) can be selected as relatively inexpensive off-theshelf components. This implies that they do not need to be pre-certified for use in SIL2 safety functions. The closed-loop monitoring and correction mechanism as proposed above results in a highly reliable safety system that can be developed using general purpose components, or
25 without custom made components, thereby saving costs.

In further an embodiment of the present invention, the activation of specific final elements as referred in the above description will be discussed. To achieve the object of physical independency of the safety system as discussed above, following method and system of operating the final elements is proposed in the present invention.

It is proposed that the WSS control be placed in series between the hydraulic source, for example, accumulators 402, and the final element, where said final elements is a Fail-Safe-Close (FSC) final element. It is further proposed that the WSS controlled be placed in parallel to the final element, where said final element is a Fail-As-Is (FAI) element.

5 By doing so WSS is made the dominant system for control of the final elements.

Figure 13 shows a simplified overview of a Fail-to-Safe or fail-safe-close configuration. Here WOCM 201 controls a DCV module 1301, both WOCM 201 and DCV module 1301 preferably installed subsea. The DCV module 1301 comprises at least one DCV controlled by the WSS, said DCVs in the DCV modules preferably electrically driven values such as solenoid valves, for example 1302. In this case, the solenoid valve 1302 is a WSS controlled DCV used for implementing the ESD and EQD functions. As shown, the solenoid valve 1302 is connected in series to the WOCM 201. In Fig. 13, the DCV 1302 operated by the WSS is shown activated, therefore WOCM 201 is not in control of the final elements 1330. When the WSS is activated, said DCV 1302 in the WSS will bleed off the hydraulic pressure in the line 1307, thus blocking off the control of the final elements 1330 from the WOCM 201. The final elements 1330 shown in Fig. 13 show a typical mainbore valve setup, for example, for RV, PIV and SH. Block 1330 shows an accumulator 1308 supplying hydraulic power to DCV 1310 through line 1309. The second DCV 1320 also receives a hydraulic supply through line 1319. The hydraulic supply to the valves 1310 and 1320 can either be supplied by the same accumulator or separate ones. The DCVs 1310 and 1320 are controlling the valve 1340 by routing the hydraulic supplies in lines 1310 and 1319 through ports C and O of the valve 1340.

Note that even though Fig. 13 shows a fail-safe-close configuration, the WSS fails-as-is, i.e., if e.g. the DCV module 1301 fails, the final element 1330 will not change state. This design is selected according to the present invention to avoid spurious trips of the safety functions, as spurious trips is equally dangerous to not achieving a trip on demand. Note that the DCV valve 1302 is illustrated activated in Fig. 13.

Figure 14 shows a simplified overview of a Fail-as-IS configuration. The DCV module 1301 is similar to as discussed in Fig. 13, and is controlled by the WSS. As shown, the WSS uses a solenoid valve 1402 to interface with the inner pilot 1407 of the DCVs

1410 and 1420. The WOCM 201 interfaces with the outer pilot 1437 of the DCVs 1410 and 1420. When a safety sequence, for example, WSS EQD is activated, the pressure from the WSS, supplied through line 1406 by an accumulator 1408 is applied which leads the DCVs 1410 and 1420 to unlock the connector by applying hydraulic supplies
5 through ports CUL and CL of the valve 1440.

A system preferably used for controlling a subsea intervention operations arrangement, is described, said arrangement preferably handling hydrocarbons from a subsea well. Said system comprises a first controller adapted for controlling functions including, opening and closing of various valves in said subsea intervention operations
10 arrangement. Said first controller also measures parameters including temperature and pressure at various points within said subsea intervention operations arrangement. Said first controller also controls energy supply to various equipment and valves in said subsea intervention operations arrangement. Said valves and said various equipment are operated electrically, hydraulically, pneumatically, or such, alone or in combination.
15 Said system further comprises a second controller adapted to be physically separated in terms of hardware from the first controller. By physically separated it is meant that the first controller and the second controller are realized as two different entities, for example as two different electronic modules. In the preferred embodiment of the present invention, at least one of the first controller, and the second controller are realized as
20 logic controllers such as Programmable Logic Controllers (PLCs). Said second controller is capable of executing safety functions in said subsea intervention operations arrangement by operating at least some of said various equipment and valves independent of said first controller.

By independent of said first controller it is meant that the second controller is capable of
25 functions such as, bypassing, taking over the functionality of, ignoring the commands from, said first controller. The second controller uses said functions for bringing at least some of the said various equipment and valves to a safe state.

Said subsea intervention operations arrangement may further include topside and associated functionality located elsewhere, besides the subsea located equipment.

Said first controller may either be realized as a single electronic module or as a distributed arrangement comprising a plurality of modules. In another embodiment, said plurality of modules are communicating with each other over a communications medium such as a bus or a wireless link.

- 5 Also, said second controller may either be realized as a single electronic module or as a distributed arrangement comprising a plurality of modules. In another embodiment, said plurality of modules are communicating with each other over a communications medium such as a bus or a wireless link.

In another embodiment, said second controller is capable of communicating with the
10 first controller.

In another embodiment, said subsea intervention operation comprises a process plant processing hydrocarbons from a subsea well, a Well Control Package (WCP) preferably located subsea, said WCP further comprises an Emergency Disconnect Package (EDP) and a Lower Riser Package (LRP). Said EDP and LRP further comprise a plurality of
15 valves for controlling the flow of said hydrocarbons in said subsea intervention operations arrangement. Said subsea intervention operation also comprises a riser system, a drilling deck, platform or similar, a Master Control Unit (MCU) preferably located on said deck or platform, and a Hydraulic Power Unit (HPU) preferably located on said deck or platform.

- 20 In yet another embodiment, said drilling deck or platform is at least partially a watercraft or a part of said watercraft. Said watercraft can be a floating object such as a marine vessel or boat.

In yet another embodiment, said second controller takes over control of a plurality of final elements, said plurality of final elements comprising at least some of the various
25 equipment and valves in the subsea intervention operations arrangement. In a preferred embodiment, said second controller takes over said control, irrespective of the control commands from said first controller to said plurality of final elements. The second controller, hence, is able to achieve prioritized control over said at least some of the various equipment and valves in the subsea intervention operations arrangement.

In a preferred embodiment, the second controller brings each final element within said plurality of final elements to the respective predetermined safe state of said each final element. By final elements it is meant elements such as, solenoids, valves, regulators, circuit breakers, or relays.

- 5 In another embodiment, the second controller takes over control of said plurality of final elements upon detection or initiation of a safety event. Said safety events include Production Shutdown (PSD), Emergency Shutdown (ESD), or Emergency Quick Disconnect (EQD).

- In yet another preferred embodiment, the system further includes a plurality of
10 Uninterruptable Power Supply (UPS). Said plurality of UPS are electrically coupled to the first controller to supply electrical power for the execution of control functions of said first controller. At least some portion of said plurality of UPS is also electrically coupled to said second controller. The second controller is adapted to monitor predetermined parameters, including voltage, current, and remaining power or energy
15 within said plurality of UPS. The second controller is further adapted to isolate at least a portion of the various equipment and valves from drawing power from said plurality of UPS under predetermined conditions.

- In another embodiment, said predetermined conditions include initiation of a safety event and remaining power or energy in said plurality of UPS below a predetermined
20 range or limit.

- In yet another embodiment, the system further comprises, at least one Control Valve, for example a DCV. Said Control Valve is controlled by said second controller and is adapted to control the flow or pressure in a fluid-carrying supply line. Said fluid-carrying supply line can be a hydraulic supply line, or pneumatic supply line, or similar.
25 Said fluid-carrying supply line is configured to supply power from fluid under pressure within said fluid-carrying supply line. The power, due to pressure of said fluid within said fluid-carrying supply line, is used for operating a plurality of equipment. Said equipment includes final elements such as valves. The second controller includes at least one power supply used by said second controller for controlling said at least one
30 Control Valve. The controller also comprises at least one initiation unit configured for

generating a trigger event. Said trigger event notifies the second controller that a specific safety event has initiated. Upon receiving said trigger event, the second controller is configured to send a signal to said at least one Control Valve for adapting the flow or pressure of fluid within said fluid-carrying supply line such that at least
5 some of the equipment within said plurality of equipment is set to a safe state. The system adapts the pressure within said fluid-carrying supply line by for example, bleeding off, blocking, or injecting additional fluid to, the fluid within said fluid-carrying supply line.

In yet another embodiment, the system further comprises a power management system,
10 and said power management system comprises at least one electrical cable for electrically coupling a power supply unit to at least one electrical consumer. Said power supply unit can be a high voltage power supply unit. Said power supply unit is used for supplying electrical power into the at least one electrical cable. Said at least one electrical consumer preferably located remotely from the location of said power supply
15 unit. Said at least one electrical consumer is adapted to draw electrical power supplied by the power supply unit through said at least one electrical cable. The proposed power management system further comprises a measurement unit adapted to measure electrical parameters including voltage, current and power at predetermined locations on said electrical cable. The preferable location of measurement of electrical parameters is close
20 to the power supply unit. The system further comprises a configuration unit, said configuration unit comprising at least one switching element, such as relay or high voltage semiconductor. Said at least one switching element is preferably serially connected between the power supply and the at least one cable. The preferred location of said configuration unit is also close to the location of the power supply unit. Said
25 configuration unit is adapted to configure parameters of the electrical power supplied by the power supply unit. Said second controller is adapted to communicate with said power supply unit, said configuration unit and said measurement unit, and the second controller is further adapted to dynamically configure the configuration unit such that electrical power received by said at least one electrical consumer is within
30 predetermined limits at all times. Thus, by monitoring said electrical parameters, the proposed power management system is able to configure the power supplied to the said at least one consumer such that the power received by the said at least one consumer is

always within favorable limits. The system may be configured to monitor a plurality of consumers individually such that power parameters of each consumer are individually tracked and maintained within desired limits.

The present invention includes an embodiment of a control system for controlling safety
5 functions in a subsea intervention arrangement, as set out in claims 1 to 14. Said control system comprises at least one Control Valve (DCV) adapted to control the flow or pressure of a fluid-carrying supply line. Said fluid-carrying supply line is configured to supply power from fluid under pressure within said fluid-carrying supply line for operating a plurality of equipment. Said equipment include final elements such as
10 valves, at least one logic controller, preferably a Programmable Logic Controller (PLC), adapted for controlling said at least one Control Valve. Said control system also comprises at least one power supply used by said at least one logic controller for controlling said at least one Control Valve. The control system also includes at least one initiation unit, such as a pushbutton, configured for generating a trigger event, said
15 trigger event notifies the at least one logic controller that a specific safety event has initiated. Upon receiving said trigger event, the at least one logic controller is configured to send a signal to said at least one Control Valve for adapting the flow or pressure of fluid within said fluid-carrying supply line such that at least some of the equipment within said plurality of equipment is set or brought to a safe state.
20 In the preferred embodiments, said fluid-carrying supply line is a hydraulic supply line, or a pneumatic supply line, or their combinations.

In another embodiment, the control system adapts the pressure of said fluid-carrying supply line by bleeding off the pressure within said fluid-carrying supply line.

In yet another embodiment, the control system adapts the pressure of said fluid-carrying
25 supply line by injecting additional fluid within said fluid-carrying supply

In yet another embodiment, the control system adapts the pressure of said fluid-carrying supply line by blocking or redirecting fluid within said fluid-carrying supply line.

In another embodiment of said control system, at least one logic controller executes a plurality of safety function steps. Said safety function steps comprise a set of commands

executed by said at least one logic controller in a predetermined sequence for controlling at least some of the equipment within said plurality of equipment.

In yet another embodiment of the control system, said at least one power supply also comprises a power source and at least one energy storage unit. Said control system is
5 further adapted to monitor parameters of said power source and said at least one energy storage unit. Said parameters include remaining stored energy within said energy storage unit, forecast of required power or energy for successfully executing remaining safety function steps, and operational parameters of said power source. Under
predetermined conditions, the control system is adapted to isolate, trip, or shutdown,
10 any non-critical equipment drawing power from said at least one power supply. The proposed control system, is thus able to reserve remaining power for executing critical functions such as said safety function steps.

In one embodiment, said at least one energy supply is hydraulic, said power source is a hydraulic pump and said at least one energy storage unit is a hydraulic accumulator.

15 In another embodiment, said at least one energy supply is electric, said power source is a generator or a switchboard and said at least one energy storage unit is a UPS.

In yet another embodiment, said at least one energy supply is pneumatic, said power source is a pump, and said at least one energy storage unit is a pneumatic accumulator.

In another embodiment of the proposed control system, said predetermined conditions
20 include said power source unavailable, and said remaining stored energy below a predetermined limit.

In yet another embodiment, said control system is related to subsea intervention operations including a movable platform, and said initiation unit further comprises a measurement unit for measurement of parameters including the position of said
25 platform. Said initiation unit is adapted to generate a trigger event notifying said logic controller that a safety event has initiated if said parameters drift beyond predetermined limits.

In another embodiment, said control system further comprises a relay to switch in a higher voltage, insulation resistance line monitoring logic, and ohmmeter for line monitoring.

An embodiment of a power management system, preferably for application in a subsea intervention arrangement, is also described. Said power management system comprises at least one electrical cable for electrically coupling a power supply unit to at least one electrical consumer. Said power supply unit can be a high voltage power supply unit. Said power supply unit is used for supplying electrical power into the at least one electrical cable. The at least one electrical consumer is preferably located remotely from the location of said power supply unit. The at least one electrical consumer is adapted to draw electrical power supplied by the power supply unit through said at least one electrical cable. The proposed power management system further comprises a measurement unit adapted to measure electrical parameters including voltage, current and power at predetermined locations on said electrical cable. The preferable predetermined location on said electrical cable is close to the location of the power supply unit. The power management system further comprises a configuration unit, said configuration unit also comprising at least one switching element. Possible embodiments of said switching element include relay, and high voltage semiconductor device. Said at least one switching element is preferably serially connected between the power supply and the at least one cable. The configuration unit is preferably located close to the power supply unit. Said configuration unit is adapted to configure parameters of the electrical power supplied by the power supply unit into the at least one electrical cable. The power management system also comprises a logic controller, preferably a Programmable Logic Controller (PLC). Said logic controller is further adapted to communicate with said power supply unit, said configuration unit and said measurement unit. The logic controller is capable of dynamically configuring the configuration unit such that electrical power received by said at least one electrical consumer is within predetermined limits at all times.

In a preferred embodiment of the proposed power management system, said logic controller is adapted to control said configuration unit using at least one electrical

output. Said electrical output is preferably digital, but in another embodiment, said electrical output can also be at least partially analog.

In another preferred embodiment of the power management system, said logic controller is adapted to monitor status and settings of said configuration unit using at least one
5 electrical input. Said electrical input is preferably digital, but in another embodiment, said electrical input can also be at least partially analog.

In another embodiment of the power management system, said configuration unit is located within said power supply unit.

In another embodiment of the power management system, the logic controller maintains
10 nearly constant current flowing through said at least one electrical cable.

In yet another embodiment of the power management system, the logic controller maintains near constant voltage across said at least one consumer.

In yet another embodiment of the power management system, the parameters of the power received by said at least one consumer are independent of the voltage drop across
15 and resistance variations in the said at least one electrical cable.

In a preferable embodiment of the power management system, the logic controller is instantiated with an initial model or nominal values of the components within the power management system. Said nominal values and model include, electrical parameters of the cable, physical parameters of the at least one electrical cable, and electrical
20 parameters of the at least one consumer.

In yet another embodiment of the power management system, the logic controller records variations in the said electrical parameters over time and said logic controller is adapted to generate a signal that a specific component within said power management system is probable to fail soon.

Claims

1. A control system for controlling safety functions in a subsea intervention arrangement, wherein said control system is **characterized by**:
 - at least one Control Valve (DCV) (408) adapted to control the flow or pressure of a fluid-carrying supply line (460), said fluid-carrying supply line being configured to supply power from fluid under pressure within said fluid-carrying supply line for operating a plurality of equipment, said equipment including final elements such as valves;
 - at least one logic controller (PLC) (406), adapted for controlling said at least one Control Valve (408);
 - at least one power supply (409) used by said at least one logic controller for controlling said at least one Control Valve; and
 - at least one initiation unit configured for generating a trigger event, said trigger event notifying the at least one logic controller that a specific safety event has initiated,wherein upon receiving said trigger event, the at least one logic controller is configured to send a signal to said at least one Control Valve for adapting the flow or pressure of fluid within said fluid-carrying supply line such that at least some of the equipment within said plurality of equipment is set to a safe state.
2. Control system according to Claim 1, wherein said fluid-carrying supply line is a hydraulic supply line.
3. Control system according to Claim 1, wherein said fluid-carrying supply line is a pneumatic supply line.
4. Control system according to any of the Claims 1 – 3, wherein said at least one Control Valve adapts the flow or pressure within said fluid-carrying supply line by reducing the pressure of the fluid within said fluid-carrying supply line.

5. Control system according to any of the Claims 1 – 3, wherein said at least one Control Valve adapts the flow or pressure within said fluid-carrying supply line by increasing the pressure within said fluid-carrying supply line.
- 5 6. Control system according to any of the Claims 1 – 5, wherein the at least one logic controller executes safety function steps, said safety function steps comprising a set of commands executed by said at least one logic controller in a pre-determined sequence for controlling at least some of the equipment within said plurality of equipment.
- 10 7. Control system according to any of the Claims 1 – 6, wherein said at least one power supply also comprises a power source and at least one energy storage unit, and said control system is further adapted to monitor parameters of said power source and said at least one energy storage unit, said parameters including
15 remaining stored energy within said energy storage unit, forecast of required power or energy for successfully executing remaining safety function steps, and operational parameters of said power source; wherein under predetermined conditions the control system is adapted to isolate any non-critical equipment drawing power from said at least one power supply.
- 20 8. Control system according to Claim 7, wherein said at least one energy supply is hydraulic, said power source is a hydraulic pump and said at least one energy storage unit is a hydraulic accumulator.
- 25 9. Control system according to Claim 7, wherein said at least one energy supply is electric, said power source is a generator or a switchboard and said at least one energy storage unit is a UPS.
- 30 10. Control system according to Claim 7, wherein said at least one energy supply is pneumatic, said power source is a pump, and said at least one energy storage unit is a pneumatic accumulator.

11. Control system according to any of the Claims 6 – 10, wherein said predetermined conditions include said power source unavailable, and said remaining stored energy below a predetermined limit.
- 5 12. Control system according to any of the Claims 1 – 11, wherein said initiation unit includes at least one pushbutton (401).
13. Control system according to any of the Claims 1 – 12, wherein said control system is related to subsea intervention operations including a movable platform,
10 and said initiation unit further comprising a measurement unit for measurement of parameters including the position of said platform, wherein said initiation unit is adapted to generate a trigger event notifying said logic controller that a safety event has initiated if said parameters drift beyond predetermined limits.
- 15 14. Control system according to any of the Claims 1 – 13, wherein said control system further comprises a relay to switch in a higher voltage, insulation resistance line monitoring logic, and ohmmeter for line monitoring.

Patentkrav

1. Et kontrollsystem for styring av sikkerhetsfunksjoner i et undervanns intervensjonsarrangement, der kontrollsystemet er **karakterisert ved**:
5 minst én styreventil (control valve; DCV) (408) tilpasset for å regulere strømmingen eller trykket i en fluidførende tilførselsledning (460), der den fluidførende tilførselsledningen er konfigurert til å tilføre kraft fra trykksatt fluid i nevnte fluidførende tilførselsledning for å drive et flertall utstyr, der utstyret inkluderer sluttelementer så som ventiler;
10 minst én logisk styreenhet (logic controller; PLC) (406), tilpasset for å styre i det minste én styreventil;
minst én krafttilførsel (409) benyttet av nevnte minst ene logiske styreenhet for å styre nevnte minst én styreventil; og
minst én initieringsenhet konfigurert for å generere en utløserhendelse, der
15 nevnte utløserhendelse meddeler den minst ene logiske styreenheten at en spesifikk sikkerhetshendelse er initiert,
hvor den minst ene logiske styreenheten er konfigurert til, når den mottar nevnte utløserhendelse, å sende et signal til nevnte minst ene styreventil for å tilpasse strømmingen eller trykket i fluid i nevnte fluidførende tilførselsledning slik at i
20 det minste noe av utstyret i nevnte et flertall utstyr settes til en sikker tilstand.
2. Kontrollsystem som angitt i krav 1, der nevnte fluidførende tilførselsledning er en hydraulisk tilførselsledning.
- 25 3. Kontrollsystem som angitt i krav 1, der nevnte fluidførende tilførselsledning er en pneumatisk tilførselsledning.
4. Kontrollsystem som angitt i et hvilket som helst av kravene 1 - 3, der nevnte minst ene styreventil tilpasser strømmingen eller trykket i nevnte fluidførende
30 tilførselsledning ved å redusere trykket i fluidet i nevnte fluidførende tilførselsledning.

5. Kontrollsystem som angitt i et hvilket som helst av kravene 1 - 3, der nevnte minst ene styreventil tilpasser strømmingen eller trykket i nevnte fluidførende tilførselsledning ved å øke trykket i fluidet i nevnte fluidførende tilførselsledning.
- 5
6. Kontrollsystem som angitt i et hvilket som helst av kravene 1 - 5, der den minst ene logiske styreenheten utfører sikkerhetsfunksjonstrinn, der nevnte sikkerhetsfunksjonstrinn omfatter et sett kommandoer utført av nevnte minste ene logiske styreenhet i en predefinert sekvens for å styre i det minste noe av utstyret i nevnte et flertall utstyr.
- 10
7. Kontrollsystem som angitt i et hvilket som helst av kravene 1 - 6, der nevnte minst ene krafttilførsel også omfatter en kraftkilde og minst én energilagringsenhet, og nevnte kontrollsystem videre er tilpasset til å overvåke parametere i nevnte kraftkilde og nevnte minst ene energilagringsenhet, der parameterne inkluderer gjenværende lagret energi i nevnte energilagringsenhet, prognose for kraft- eller energibehov for vellykket å kunne utføre gjenværende sikkerhetsfunksjonstrinn, og operasjonelle parametere ved nevnte kraftkilde; i det kontrollsystemet er tilpasset for, ved på forhånd bestemte betingelser, å isolere ethvert ikke-kritisk utstyr som trekker kraft fra nevnte minst ene krafttilførsel.
- 15
- 20
8. Kontrollsystem som angitt i krav 7, der nevnte minst ene krafttilførsel er hydraulisk, nevnte kraftkilde er en hydraulisk pumpe og nevnte minst ene energilagringsenhet er en hydraulisk akkumulator.
- 25
9. Kontrollsystem som angitt i krav 7, der nevnte minst ene krafttilførsel er elektrisk, nevnte kraftkilde er en generator eller en instrumenttavle og nevnte minst ene energilagringsenhet er en UPS.
- 30

10. Kontrollsystem som angitt i krav 7, der nevnte minst ene krafttilførsel er pneumatisk, nevnte kraftkilde er en pumpe og nevnte minst ene energilagringseenhet er en pneumatisk akkumulator.
- 5 11. Kontrollsystem som angitt i et hvilket som helst av kravene 6 - 10, der nevnte på forhånd bestemte betingelser inkluderer at nevnte kraftkilde er utilgjengelig, og nevnte gjenværende lagret energi er under en forhåndsbestemt grense.
- 10 12. Kontrollsystem som angitt i et hvilket som helst av kravene 1 – 11, der nevnte initieringsenhet inkluderer minst én trykknapp.
- 15 13. Kontrollsystem som angitt i et hvilket som helst av kravene 1 – 12, der nevnte kontrollsystem vedrører undervanns intervensjonsoperasjoner inkludert en bevegelig plattform, og nevnte initieringsenhet videre omfatter en målingsenhet for måling av parametere inkludert nevnte platfforms posisjon, idet nevnte initieringsenhet er tilpasset for å generere en utløserhendelse som notifiserer nevnte logiske styreenhet at en sikkerhetshendelse er initiert dersom nevnte parametere vandrer ut over forhåndsbestemte grenser.
- 20 14. Kontrollsystem som angitt i et hvilket som helst av kravene 1 – 13, der nevnte kontrollsystem videre omfatter et relé for å bytte til en høyere spenning, monitoreringslogikk for isolasjonsresistans, og ohm-meter for linjemonitorering.

1/14

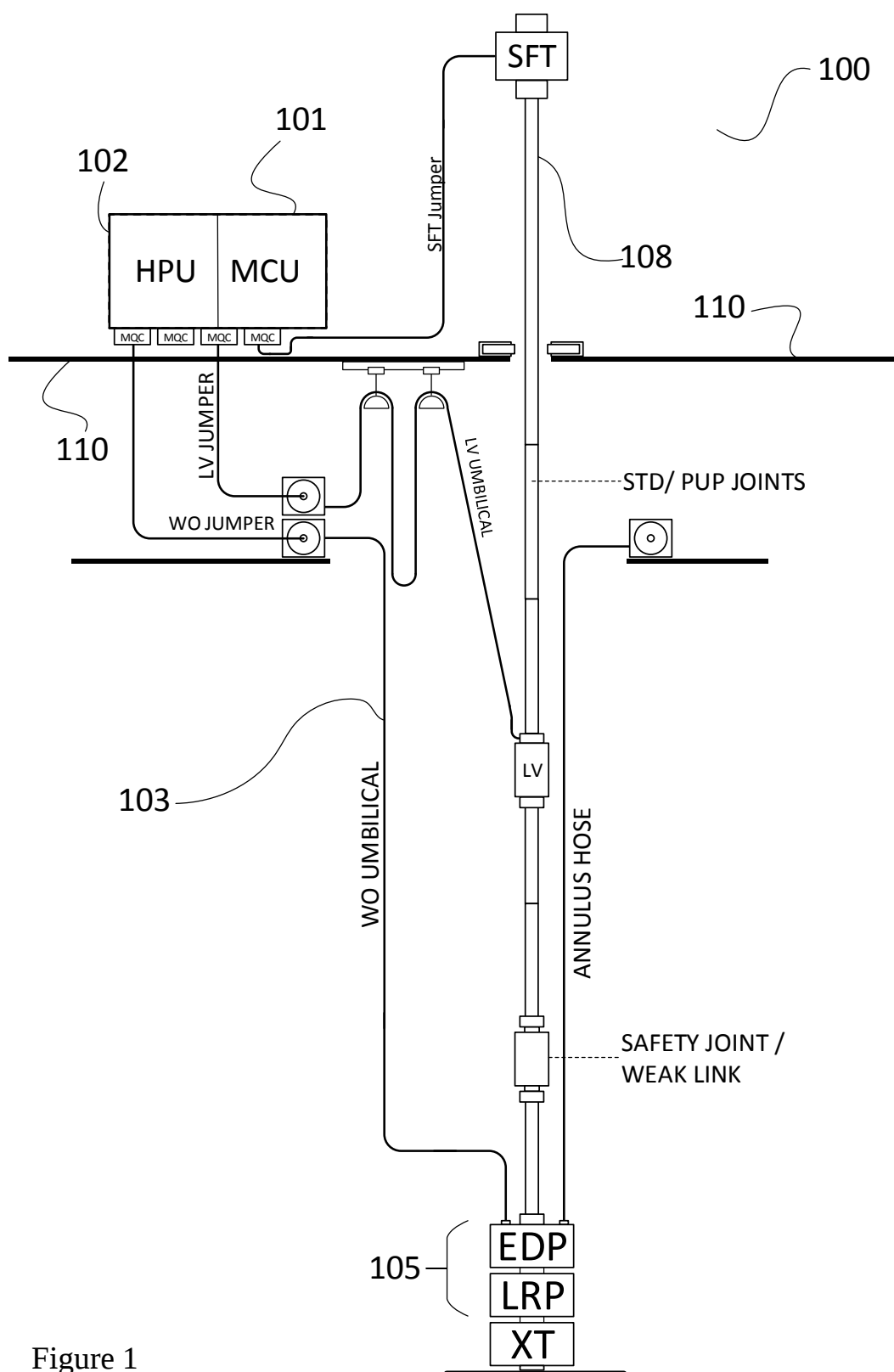


Figure 1

2/14

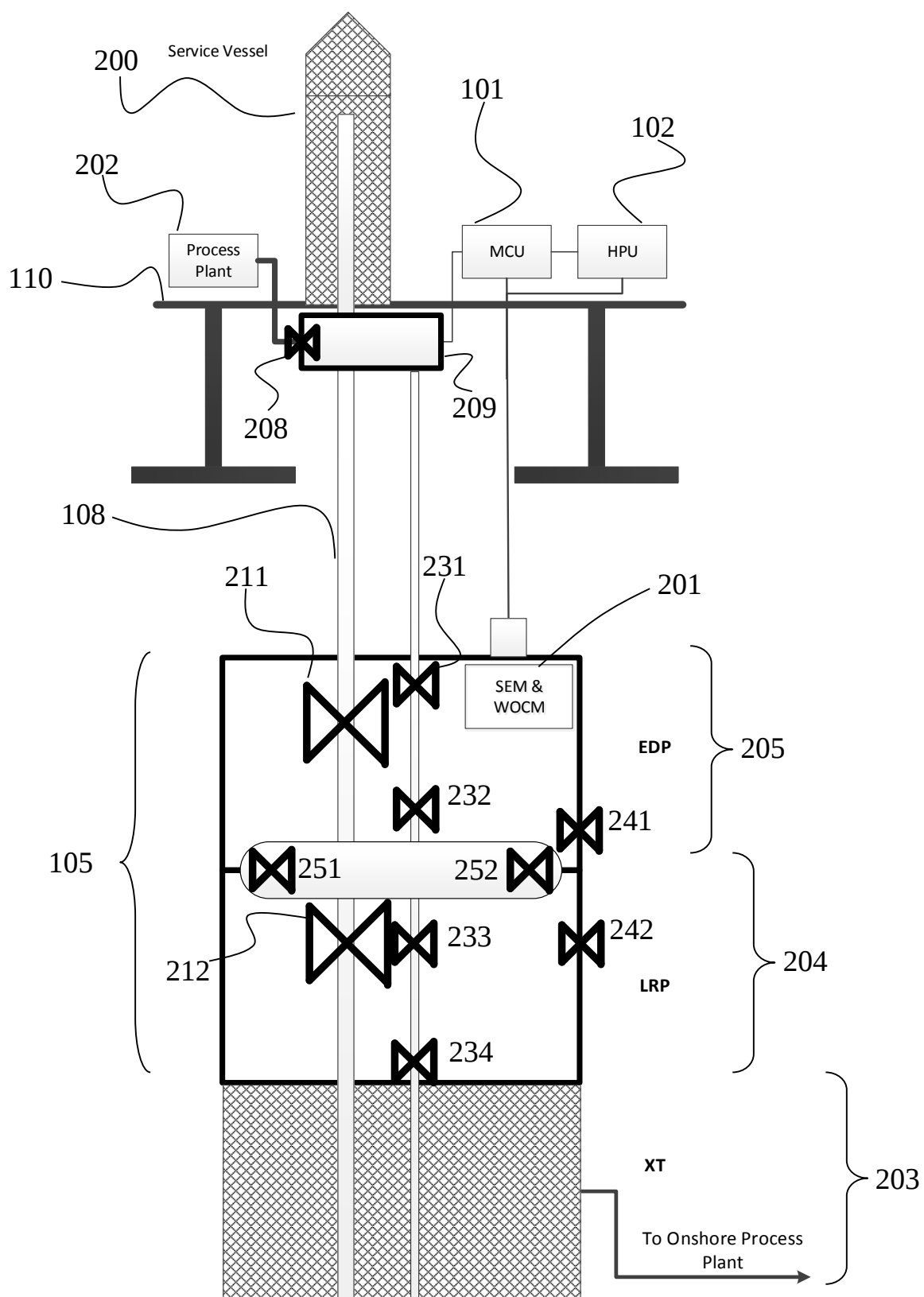


Figure 2

3/14

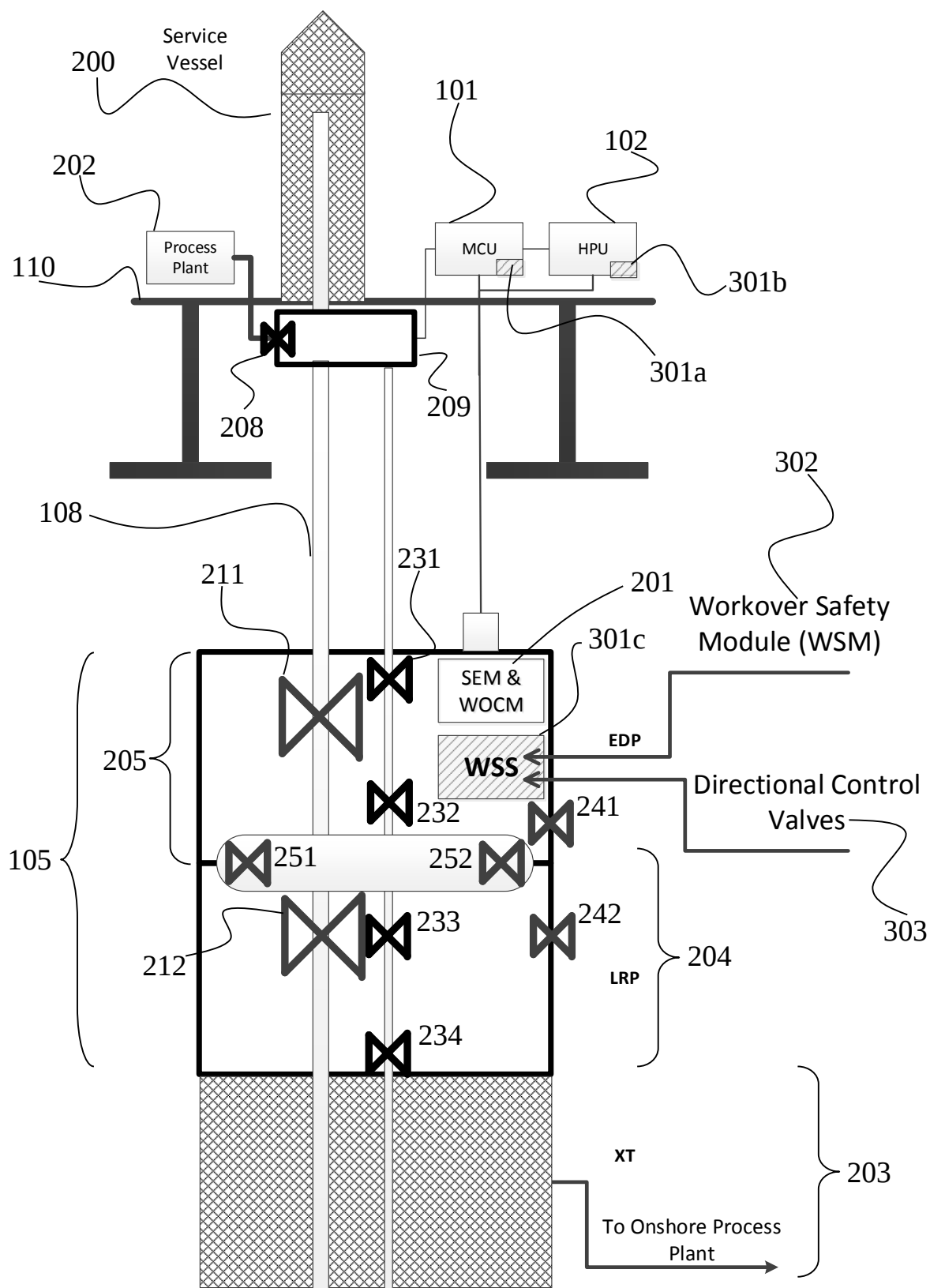


Figure 3

4/14

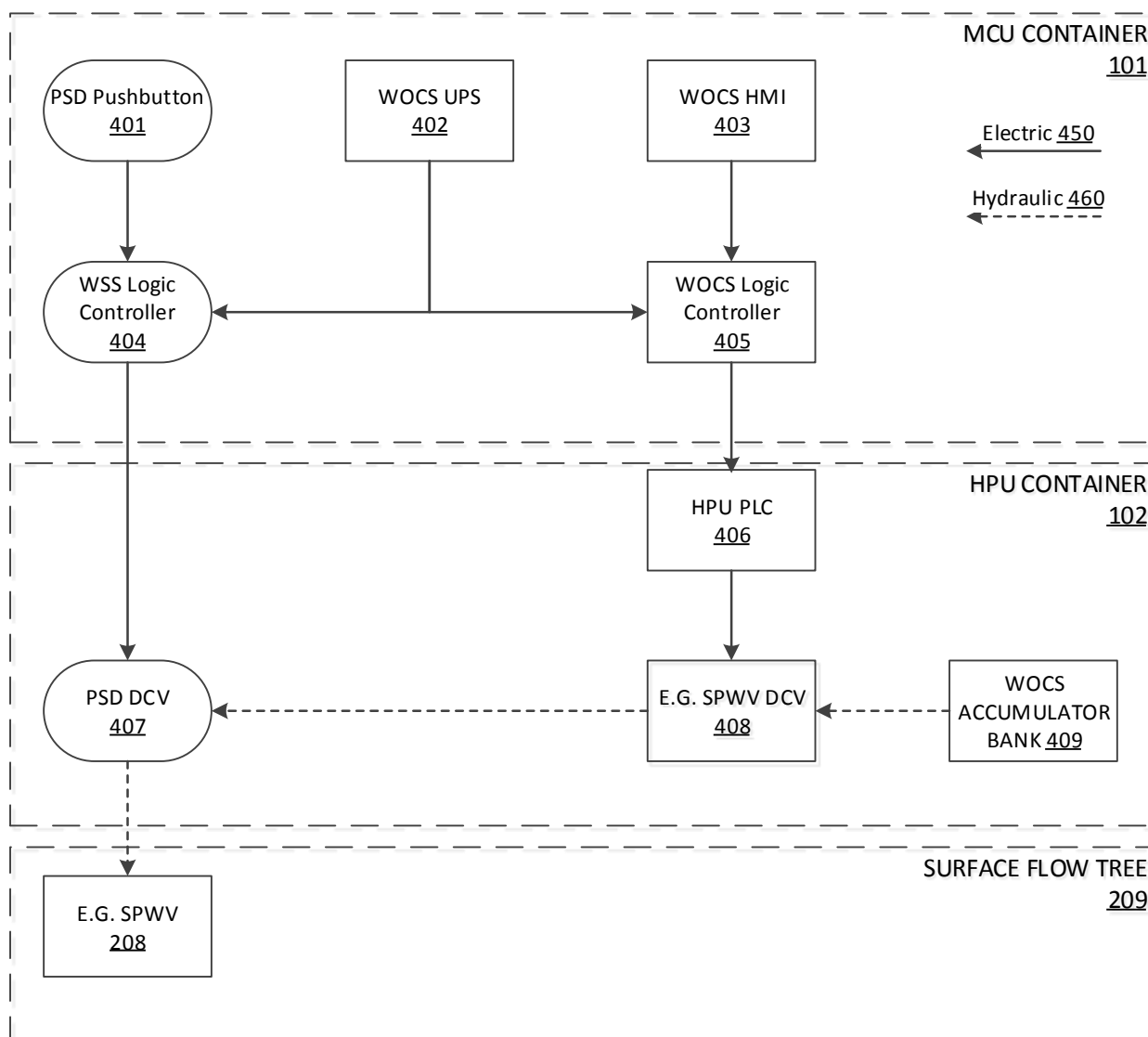


Figure 4

5/14

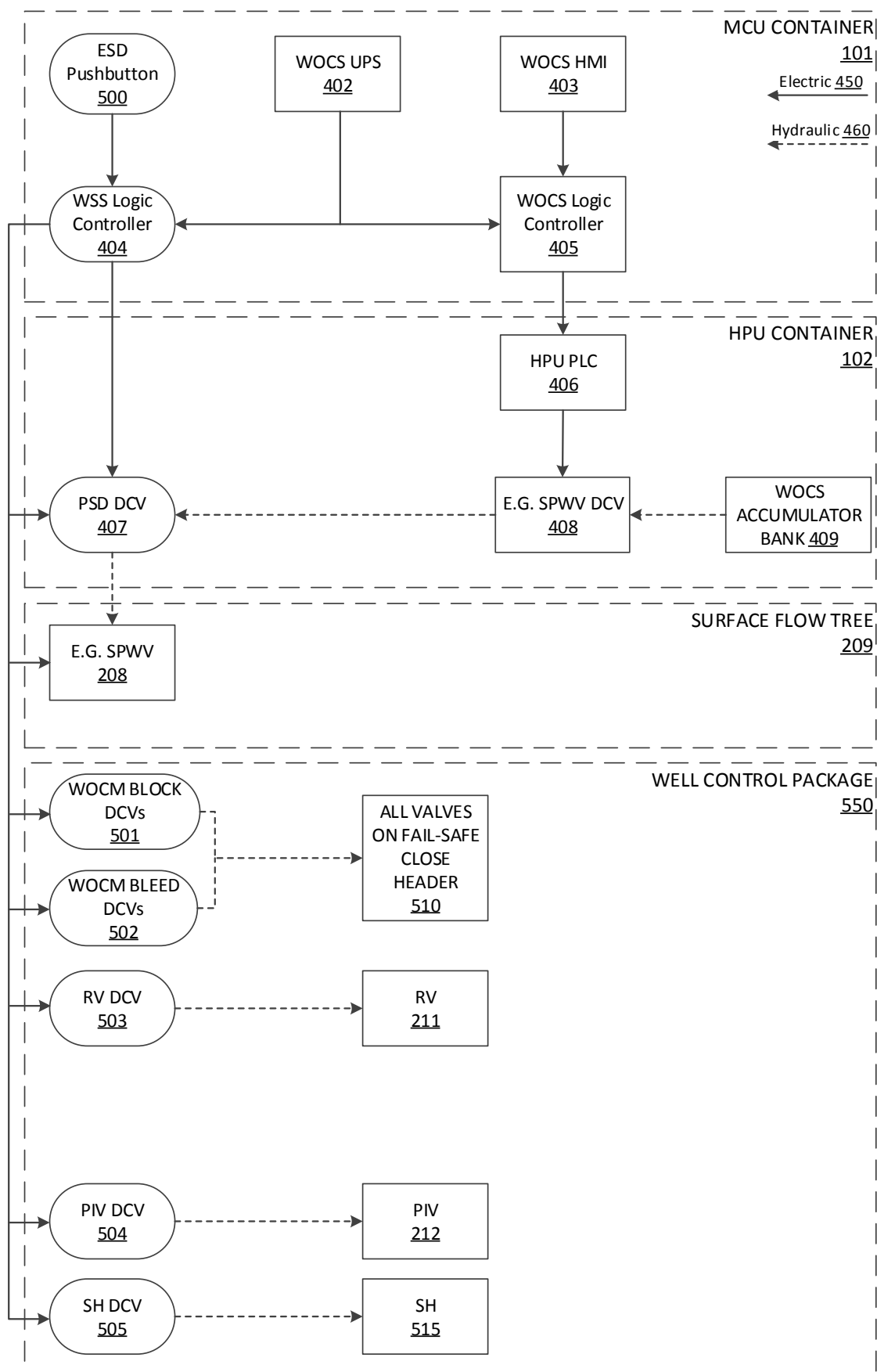


Figure 5

6/14

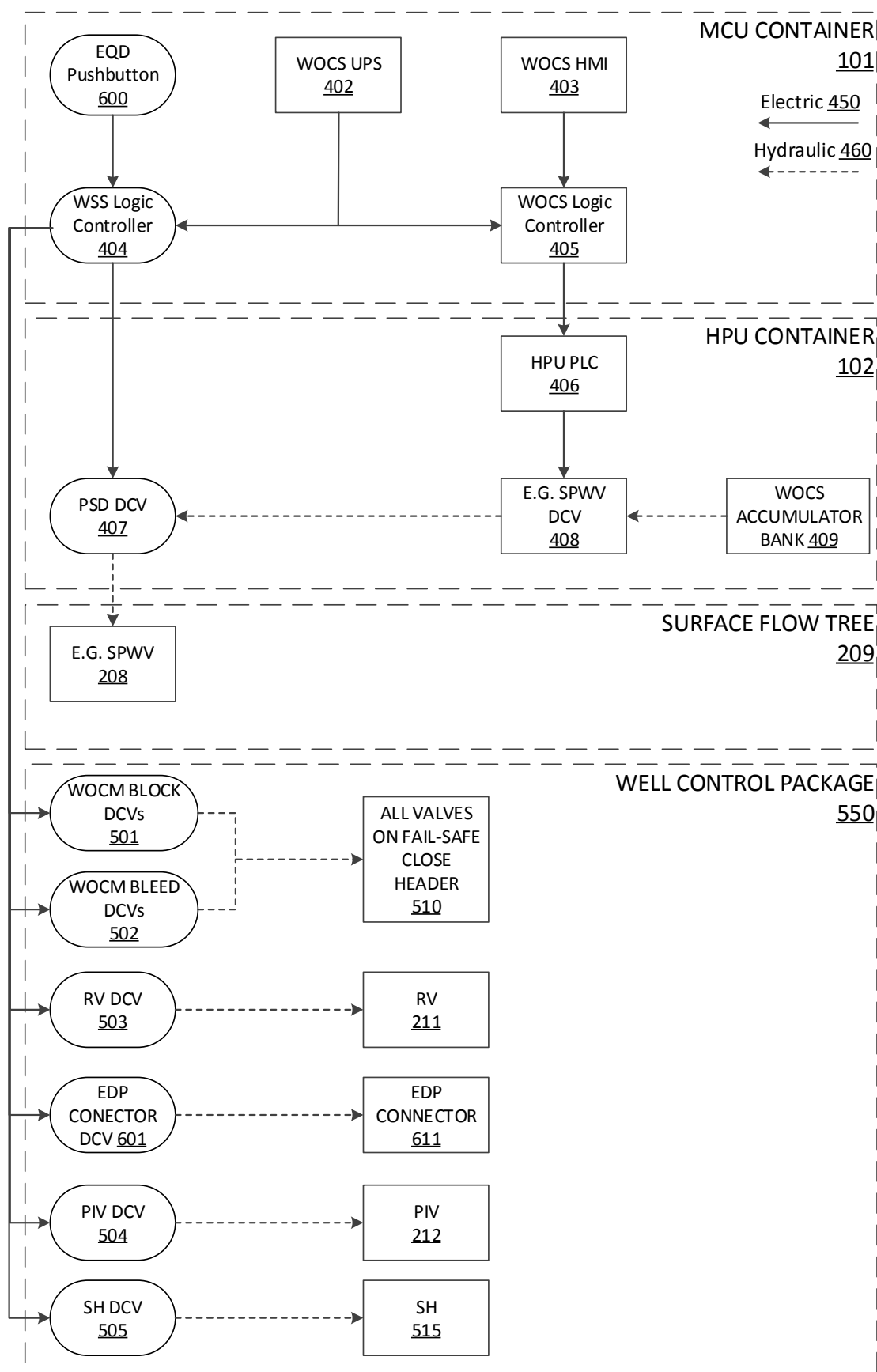


Figure 6

7/14

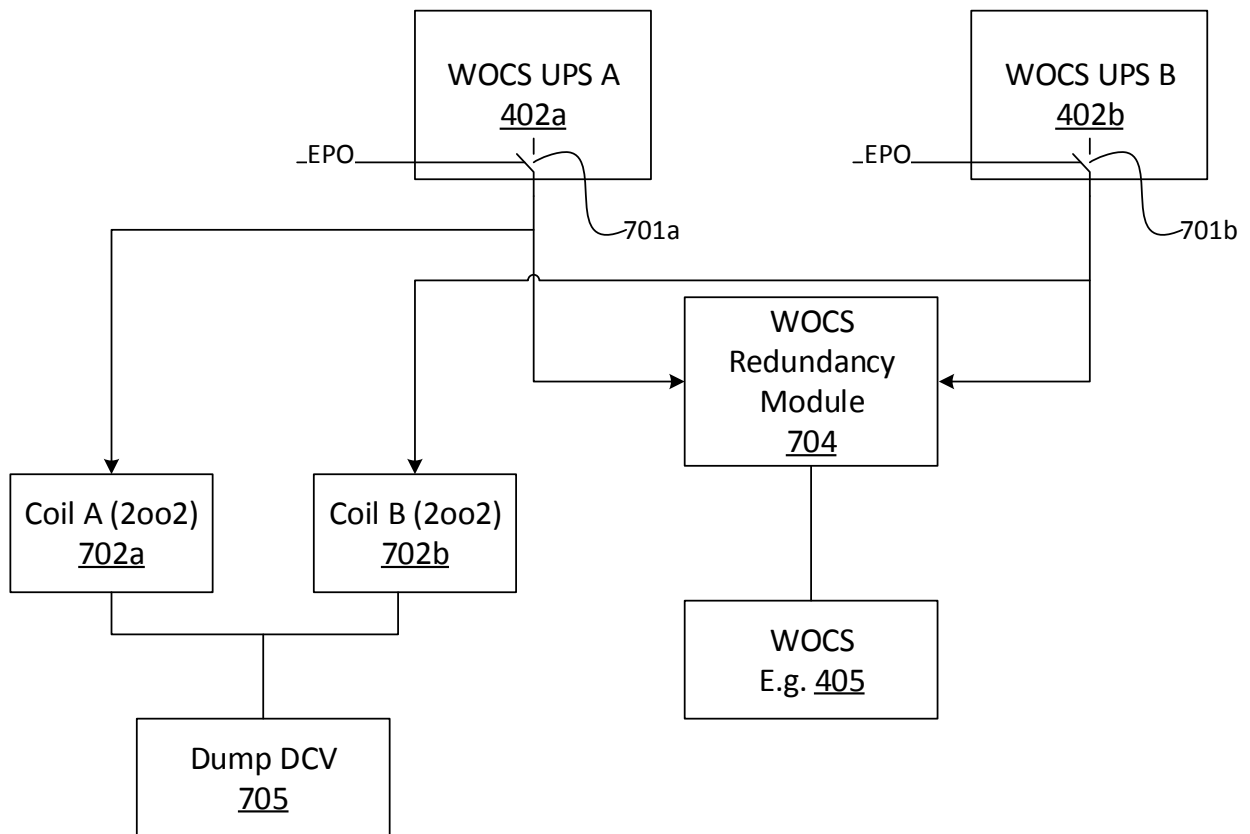


Figure 7

8/14

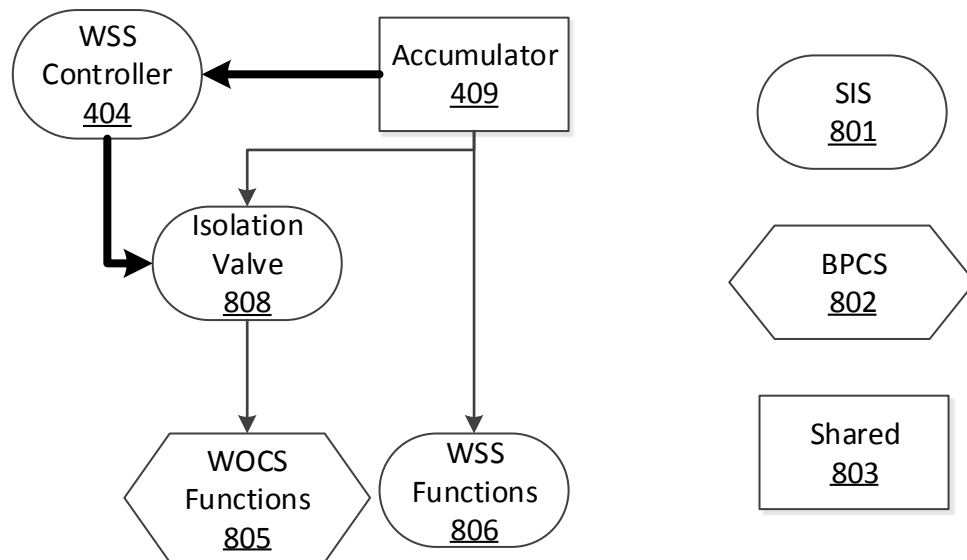


Figure 8

9/14

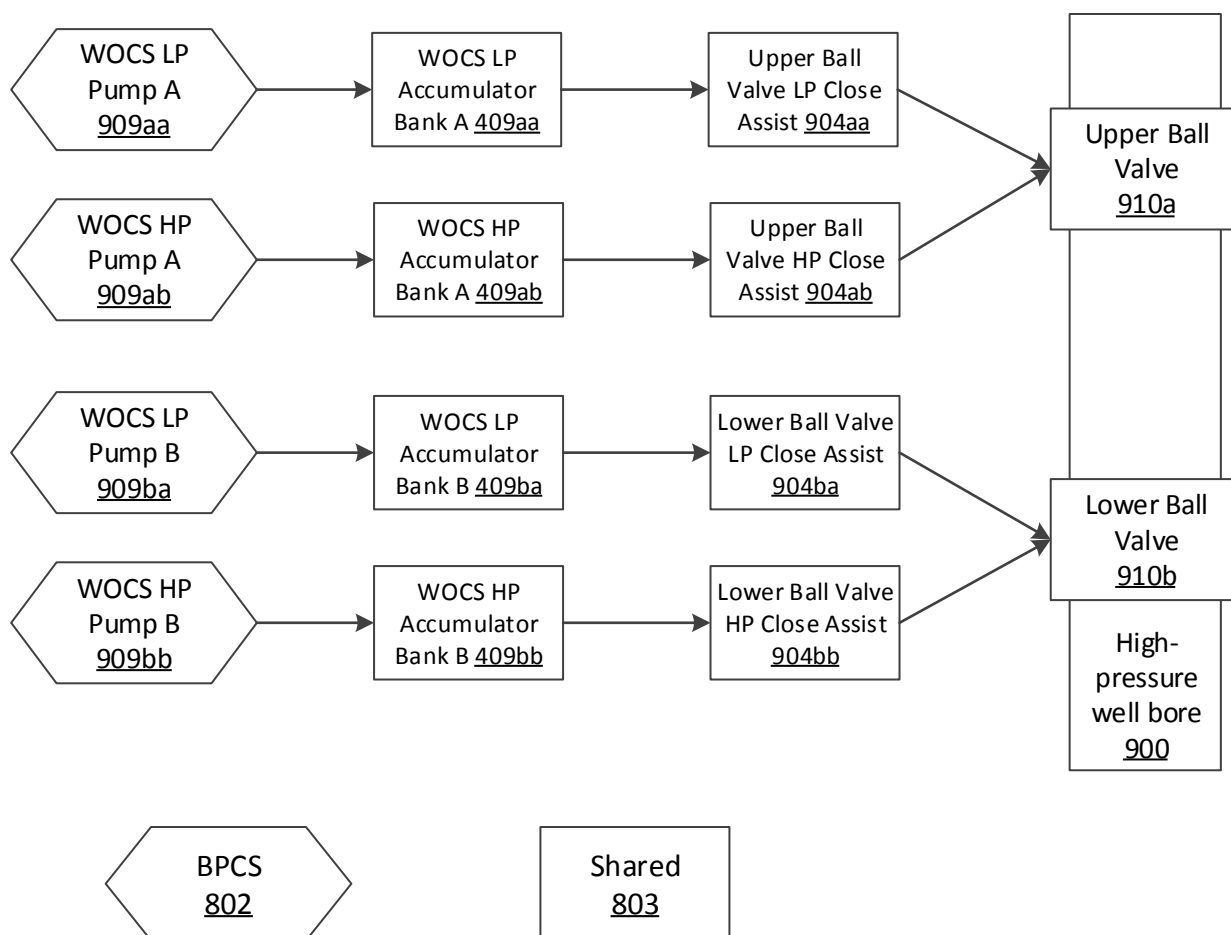


Figure 9

10/14

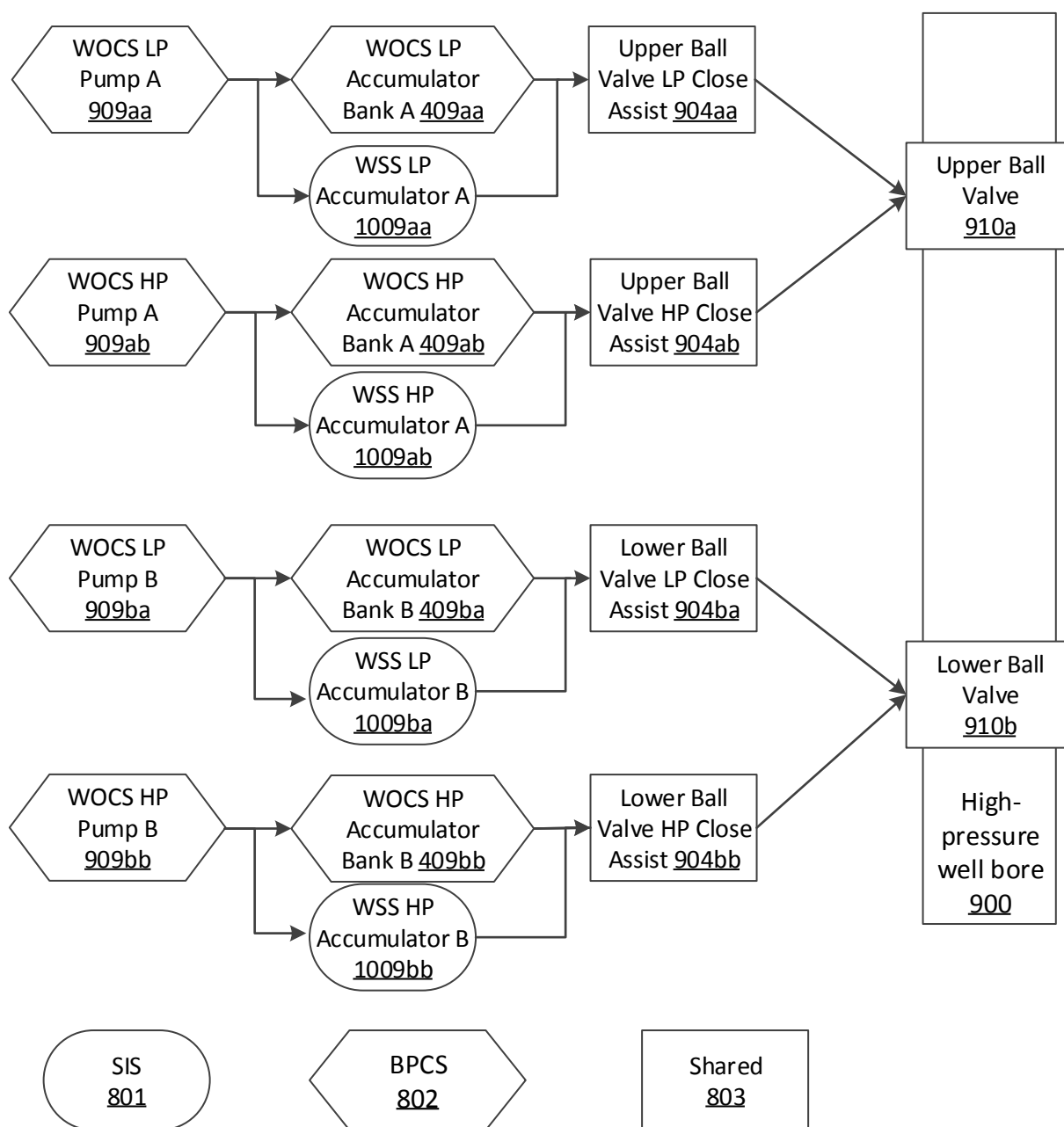


Figure 10

11/14

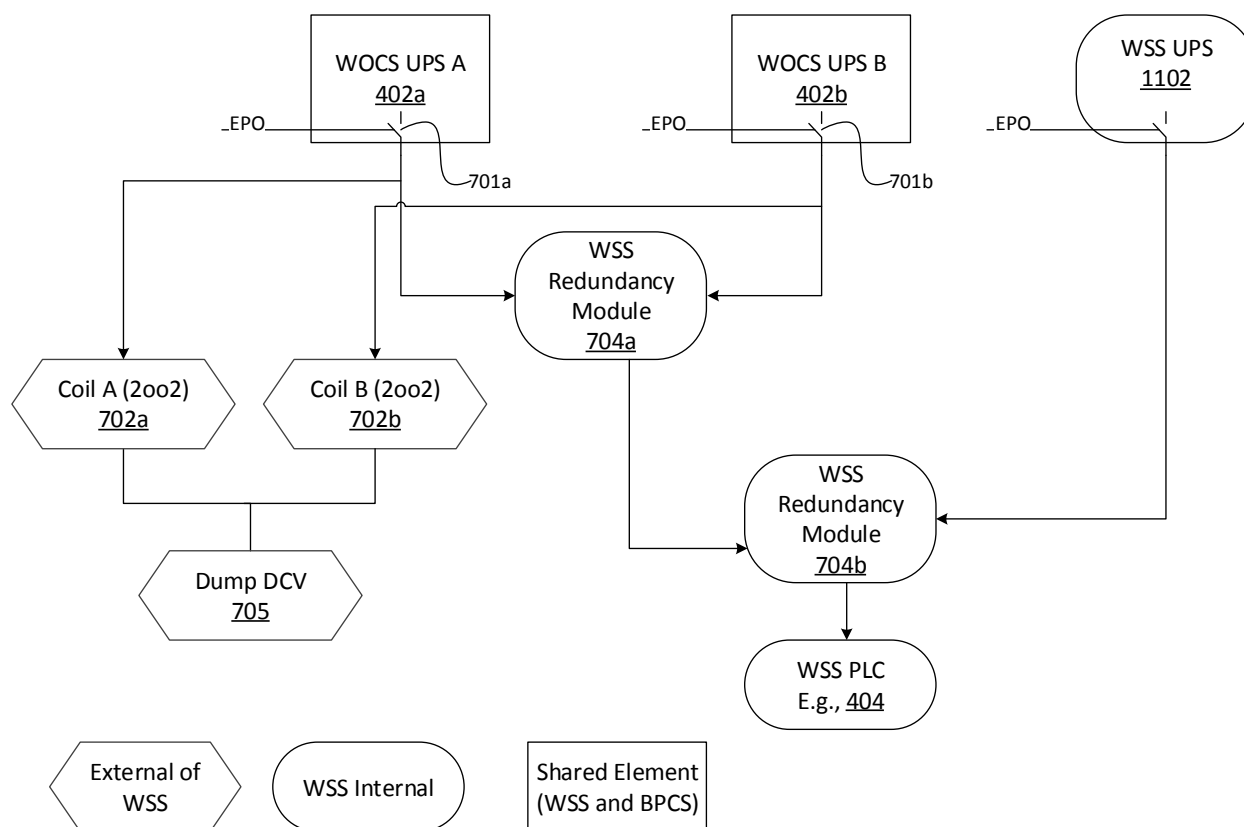


Figure 11

12/14

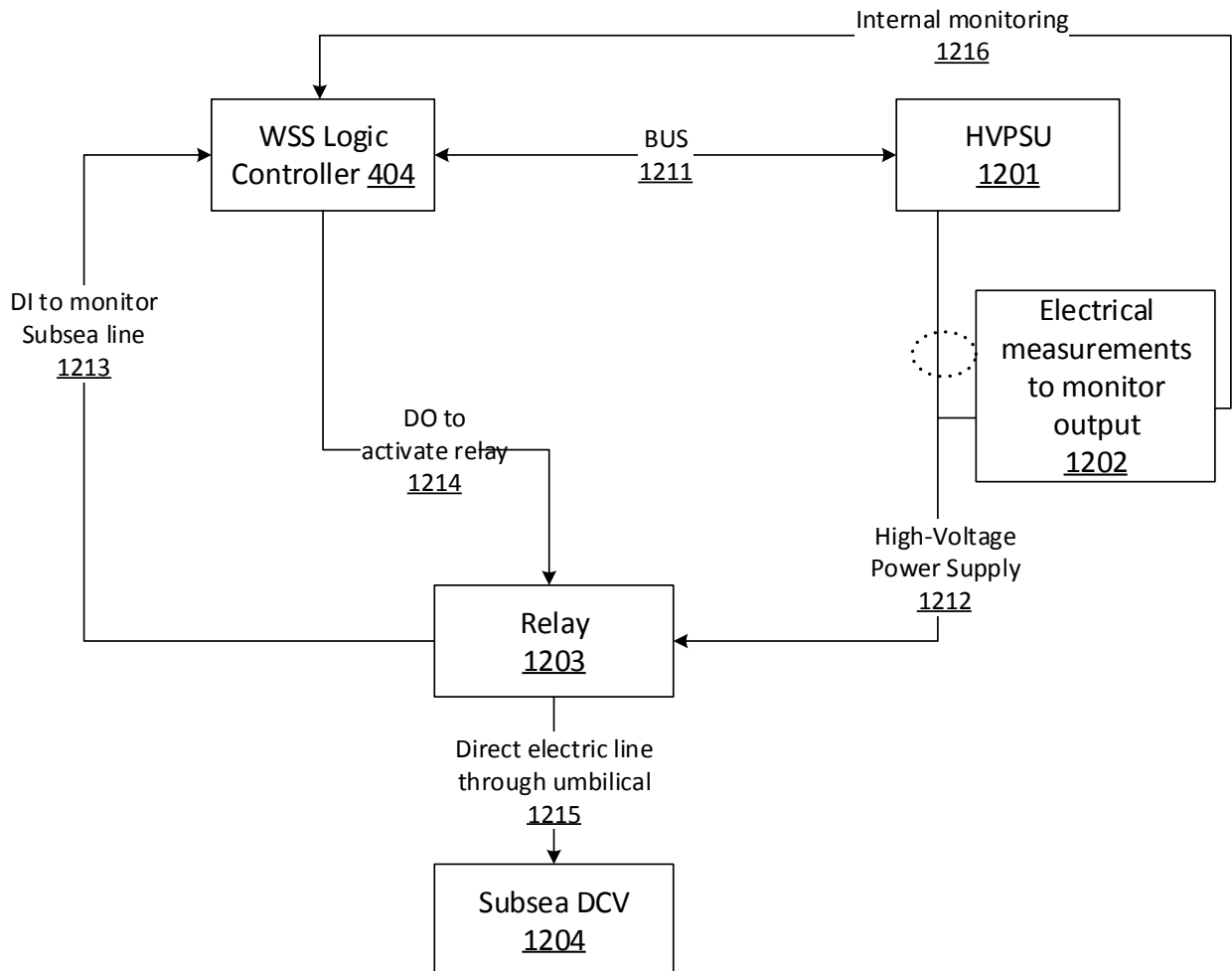


Figure 12

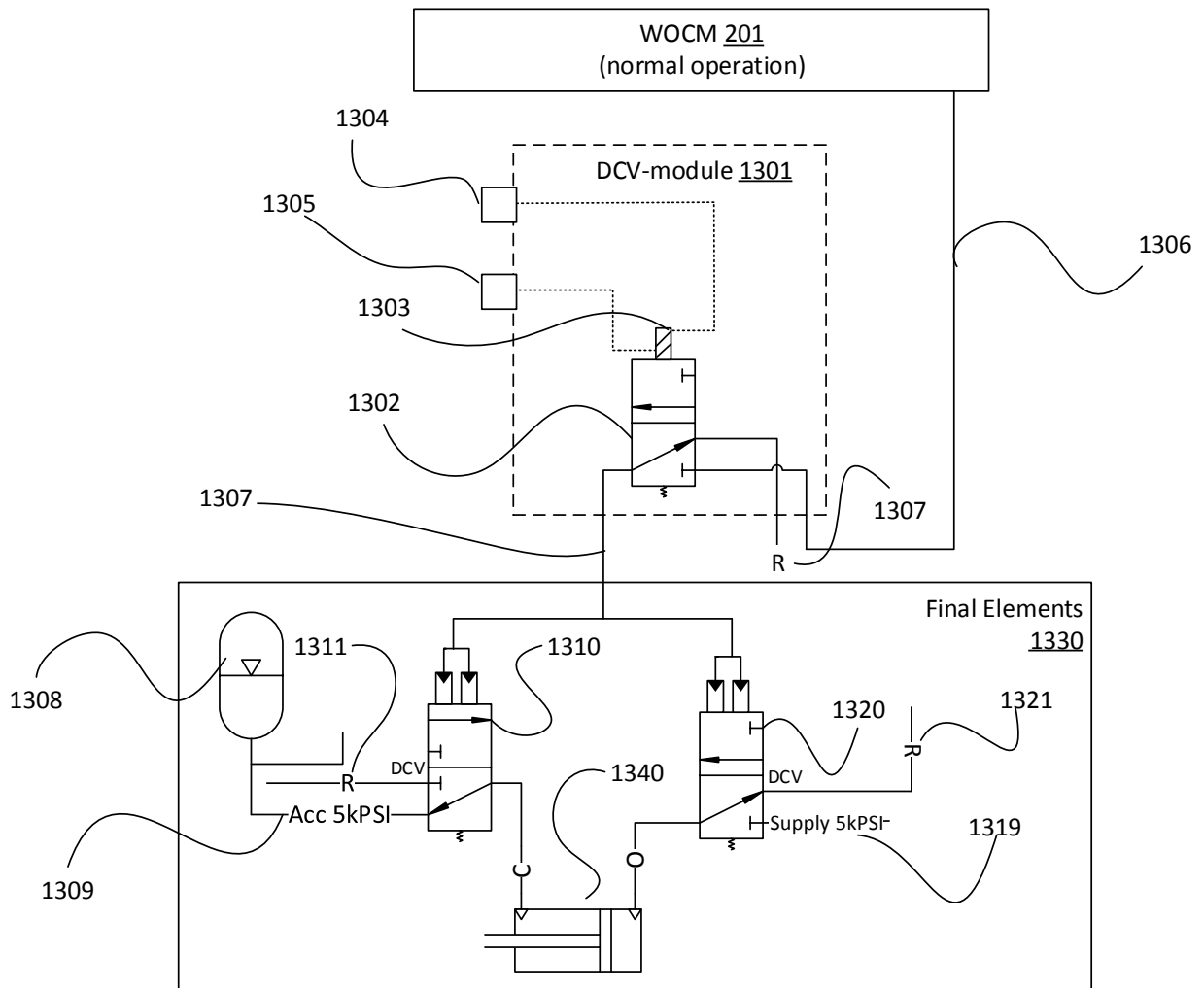


Figure 13

14/14

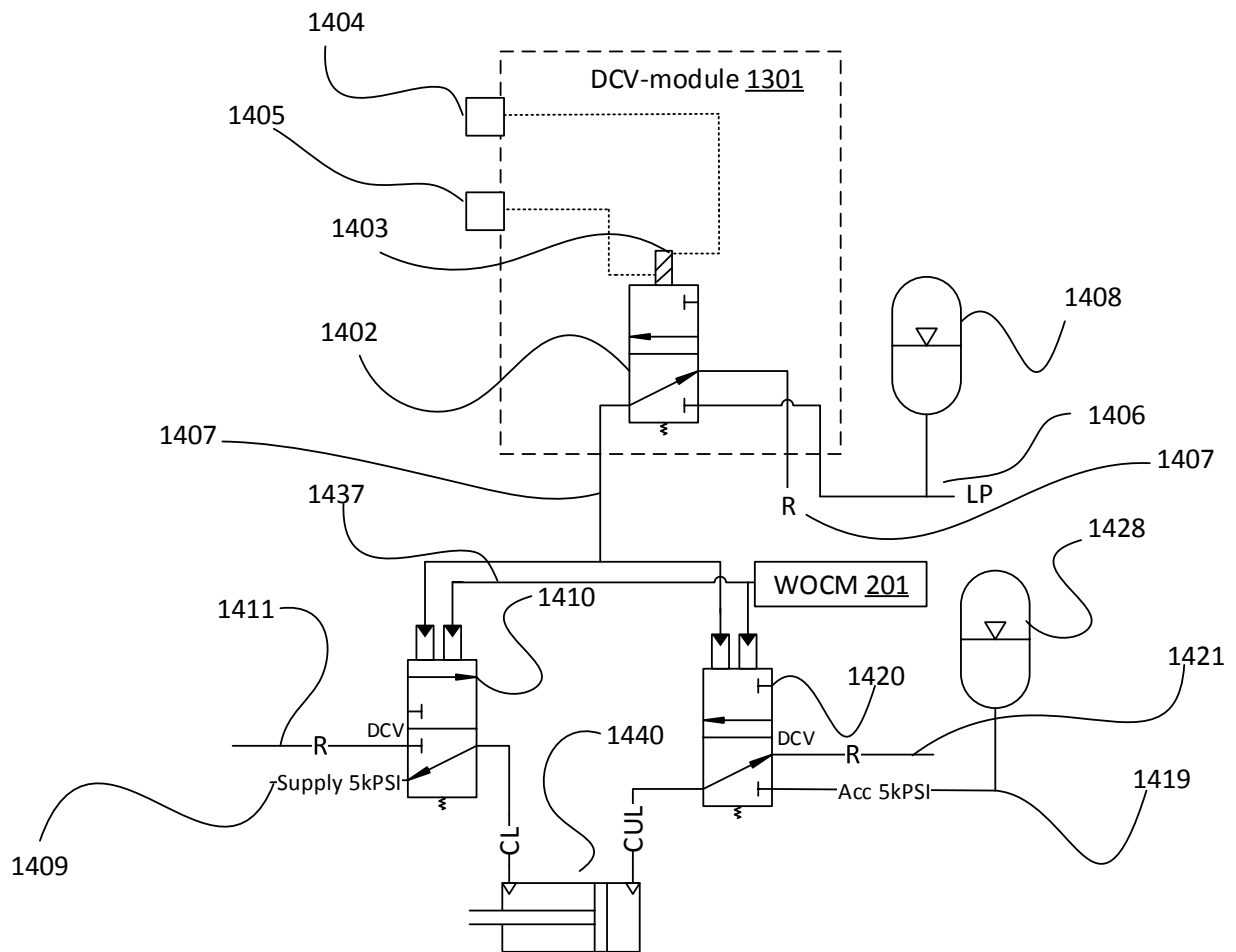


Figure 14