International Journal of Innovative
Computing, Information and Control
Volume **17**, Number **4**, August **2021**

ICIC International ©2021 ISSN 1349-4198
pp. 1171–1190

SAFETY ENHANCEMENT FOR BASIC PROCESS CONTROL USING 4-20 MILLIAMPERE SIGNAL TRANSMISSION

Amphawan Julsereewong, Phongphiphat Muangmool
and Teerawat Thepmanee

School of Engineering
King Mongkut's Institute of Technology Ladkrabang
Ladkrabang, Bangkok 10520, Thailand
{ amphawan.ju; 61601137; teerawat.th }@kmitl.ac.th

Received February 2021; revised May 2021

Abstract. *To enhance safety of basic process control using traditional 4-20 mA current loops with/without transmitting a return signal of actual actuator position back to a host, this article presents a useful technique to provide fault-state and fault-recovery actions in four patterns. The proposed technique is a design of control drawings configured in a distributed control system (DCS) host for conventional proportional-integral-derivative (PID) loops with/without feedforward path to improve actions of the control loops in response to sensor and actuator failures. The configuration design based on functions of failure status propagation and failure mode shedding for eight control drawings that contain software function blocks for running on the DCS host modeled CENTUM VP is described. Simulation results by employing the DCS virtual test function verify that all designed control drawings can successfully perform the desired fault-state and fault-recovery actions for process safety enhancement.*

Keywords: Current loop, Distributed control system, Fault-state, Fault-recovery, Function block, Process control, Safety

1. **Introduction.** To prevent and/or mitigate hazardous events associated with both normal and abnormal operations for process areas in hydrocarbon processing plants, the need for multiple protection layers is well known because no single safety method can completely eliminate risk [1,2]. Each layer of protection is designed and managed to perform its intended functions for satisfying safety requirements [3-5]. A basic process control, one of protection layers, is generally implemented not only to maintain process performance within specification limits under normal operating conditions, which relate to production facility, but also to react to abnormal events, which occur because of process upsets or instrument failures [6,7]. In general, a response to the detected failure is the continuity of ongoing process operations to minimize downtime for availability goal. On the contrary, the affected control loop must shut the automatic process down to prevent dangerous situations for safety goal. These two conflicting goals can be targeted for each control loop to optimize productivity and risk management of the production plant [8]. A smart transmitter with self-diagnostic capability to detect internal failures and anomalies can improve plant safety and maintenance strategy because its health indication can be useful to enable/disable predetermined safe and alarm actions as well as helpful in troubleshooting effort [9,10]. Alternatively, regulatory control systems using IEC 61158-based digital field instruments such as Foundation Fieldbus (FF) H1 devices are capable of executing

DOI: 10.24507/ijicic.17.04.1171

fault-state actions using quality status of process measurements [11-13]. The status indication of 'Good', 'Uncertain', or 'Bad' measurement is propagated between control system devices for alert notification at an operator/engineering workstation to handle situations and for appropriate response of the receiving device to achieve control purposes [11]. The fault-state action is an effective solution to bring the loop to graceful shutdown when detecting 'Bad' measurement from failure measuring devices used in control [12]. A predefined safe value of an actuator for shutdown functionality can be configured by setting related parameters of an output class function block, which is virtually connected to a control class function block for creating control strategy. However, built-in fault-state functions are available when assigning the control class block to run in H1 field devices that support options of fault-state status processing. In case of assignment of the control class block to execute in a host controller (CONT) module, built-in fault-state functions are unavailable [13]. In addition, FF function blocks based on IEC 61804 standard provide useful option parameters such as input-output options and status options for configuring the block behavior in response to different status conditions [14,15]. Effects of option parameters on function block interlocks and fail-safe mechanisms for FF-based proportional-integral-derivative (PID) and cascade control strategies have been discussed [16]. Recently, a method based on instrument fault diagnosis to improve process safety of an FF-based feedforward control has been suggested [17]. Although there are considerable benefits including material cost saving from digital fieldbus system installation to replace traditional analog instrumentation [18], many existing basic process control systems in hydrocarbon processing plants, especially in Thailand, are currently still in operations based on traditional current loops. Commonly, this is due not only to their capital-intensive production process, which has long system life cycle, but also to lack of plant personnel with digital skills, which is one of serious obstacles to investment in production plants equipped with smart field technologies. In addition, a practical implementation of smart instruments and new communication protocols has a great impact on job descriptions of operators, technicians, and engineers. However, utilizing digitalization technologies is one of transformation steps for plant modernization to enhance competitiveness in global scale in the era of the fourth industrial revolution (Industry 4.0) [19,20]. This becomes a challenge of smooth migration to transform conventional systems into modern systems. Therefore, adequate roadmaps and strategies for successful migration towards the Industry 4.0 should be identified [21]. This article aims to support hydrocarbon processing plants in their modernization at the starting point by improving existing traditional basic control loops for higher degree of safety. Moreover, the proposed improvement also provides an opportunity for plant personnel to be familiar with new tasks in similar way of digital fieldbus systems to mitigate their conservatism in technology adoption.

Most field instruments in standard current loops are connected to conventional input/output (I/O) modules of a distributed control system (DCS) by using 4-20 mA signal transmissions. One hardwired cable is installed for either transmitting a process variable from a measuring device to an analog input (AI) module or sending a manipulated variable from an analog output (AO) module to an actuating device. There is no measure of directly checking the operation status of traditional field instruments from the operator/engineering workstation. Analog current loops do not access instrument diagnostic information. Thus, statuses of the DCS AI module are typically utilized by control strategies to take actions when receiving hardware fault signals from failed field instruments [22]. Usually, the defected loop operation is switched from automatic (AUT) to manual (MAN) control without operator intervention, and the PID function block holds its output at the last 'Good' value. In the event of actuator failure, the failed final element moves to its

mechanical fail-safe position by spring return or its predetermined position by supplemental equipment such as lock-up valve and air lock valve. In order to take additional actions, which are not normally found in basic process control operated as traditional 4-20 mA current loops with/without return signal of actual actuator position, this article proposes a technique to design eight control drawings including software function blocks configured in the DCS host for PID loops, which are common control algorithms in process industry plants. Based on functions of failure status propagation and failure mode shedding in fieldbus-based control loops with increased safety [8,16,17], four patterns to provide fault-state and fault-recovery actions for four interested current loops by employing the CENTUM VP DCS are described. The technical feasibility of the proposed safety enhancement technique is demonstrated through virtual test function of the DCS host used.

The rest of this article is organized as follows. The concepts and descriptions of the proposed safety enhancement for the interested PID control loops with/without feedforward path are detailed in Section 2 and Section 3, respectively. The DCS virtual test results to verify the validity of the proposed technique are given in Section 4. Lastly, conclusions and possible future work are stated in Section 5.

2. **Concepts of Proposed Safety Enhancement.** To clarify the proposed concepts, Figure 1 shows an example of conventional 4-20 mA device installation for PID loops with/without feedforward path to control liquid level in a tank. The level transmitter (LIT) for measuring tank level (PV1), flow transmitter (FIT) for measuring outlet flow rate (PV2), and level control valve (LCV) for manipulating inlet flow rate (MV) are installed in a field site. Usually, most traditional valve positioners do not provide a return signal of actual valve position to be remotely monitored at the operator/engineering workstation. It is, however, possible to check an actual position of the LCV by adding the new

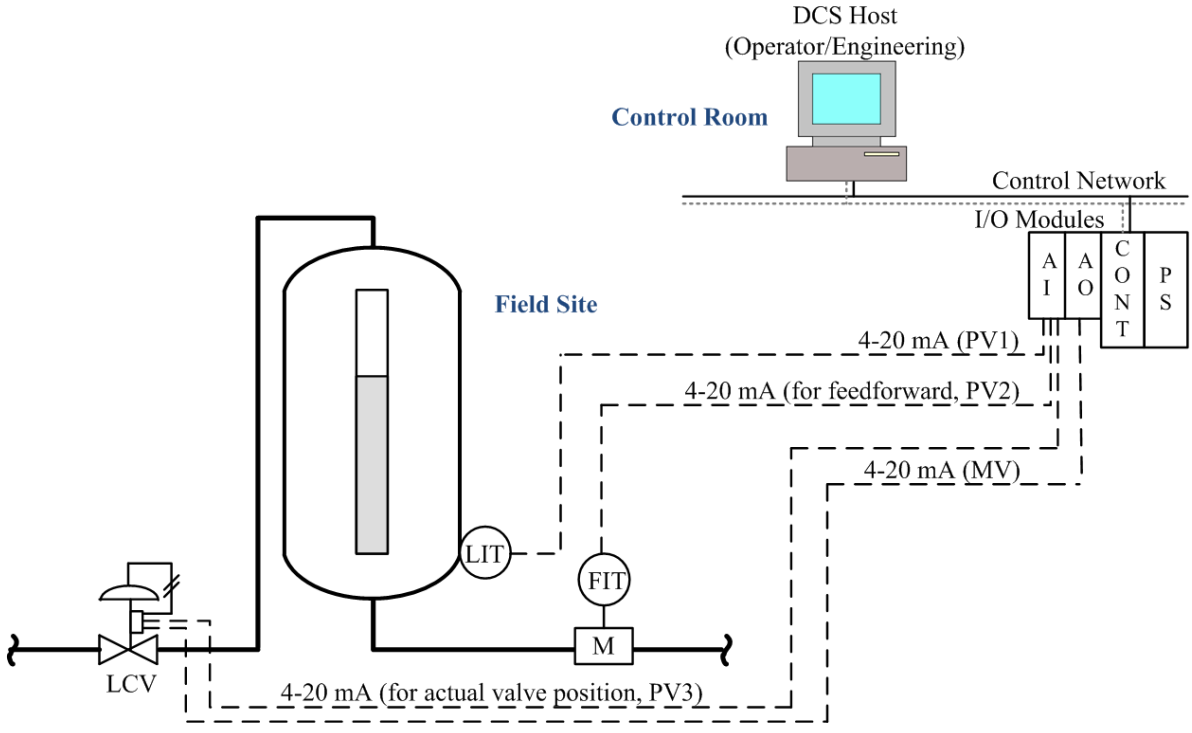


FIGURE 1. Example of device installation for PID loops with/without feedforward path

wiring (PV3) to achieve less-time consuming troubleshooting for effective maintenance. The DCS components and interfaces are installed in a control room. The CONT module is connected to execute sequential algorithms and logical expressions for regulating control loops. The AI module is used to transfer process data from the field devices to the CONT module, while the AO module is used to transfer executed data from the CONT module to the field devices. The power supply (PS) is installed to distribute energy to the CONT, AI, and AO modules. Table 1 gives four interested PID loops and their related analog signals for controlling the tank level of Figure 1. For 4-20 mA transmission, Figure 2 shows two kinds of signal levels outside a normal range, which are the high/low alarm levels for indicating hardware failures and the high/low saturation levels for indicating out-of-range events. Usually, the low saturation level should be greater than the low alarm level. The high saturation level should be less than the high alarm level. The minimum difference between the saturation and alarm levels should be 0.1 mA. However, many field instrument manufacturers identify the specific alarm and saturation levels for their own products [23-25]. The alarm levels may also differ according to the type of transmitters [26,27]. For the studied loops, 'Bad' measurements are considered by failures of the PV1 and PV2. Typical actions in response to these failures are displayed in Figure 3. In case of the PID loops with/without feedforward path (see Figures 3(a) and 3(c)), there are similar actions in the presence of PV1 failure by switching the operating mode of the PID block to 'MAN' and holding the output of the PID block at the last MV value. However, the presence of PV2 failure has no significant effect on the PID block operation for the loop with feedforward path (see Figure 3(b)) [17]. The PID block still operates in 'AUT' mode by utilizing the last valid 'Good' value of the PV2 for computing its output. Based on functions of failure status propagation and failure mode shedding, two concepts referred to as 'Pattern1' and 'Pattern2' in Figures 4(a) and 4(b), respectively, are specified for improving safety of the PID loops with/without feedforward path when detecting PV1 sensor failure. To enhance safety of the PID control loops with/without feedforward path in combination with actual valve position signal in the event of PV1 and PV3 failures,

Table 1. Four interested PID loops for controlling the tank level of Figure 1

Loop	Description	Related analog signals			
		PV1	PV2	PV3	MV
1	PID loop with feedforward path	√	√		√
2	PID loop without feedforward path	√			√
3	PID loop with feedforward path in combination with actual valve position signal	√	√	√	√
4	PID loop without feedforward path in combination with actual valve position signal	√		√	√

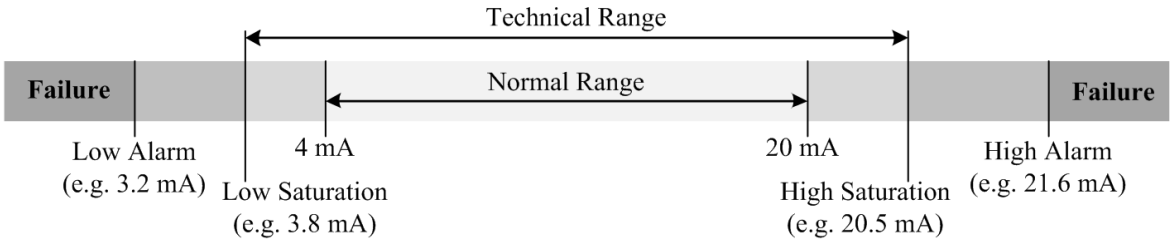
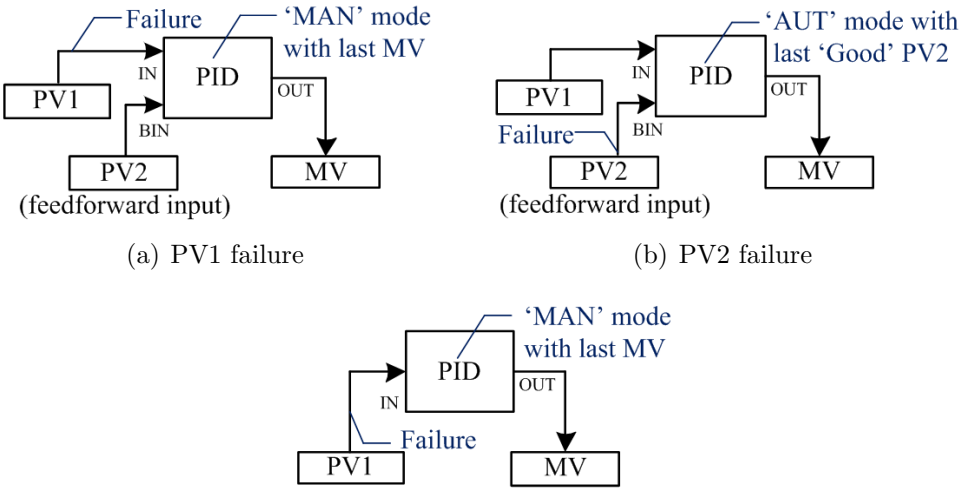


Figure 2. Alarm and saturation levels for 4-20 mA signal transmission

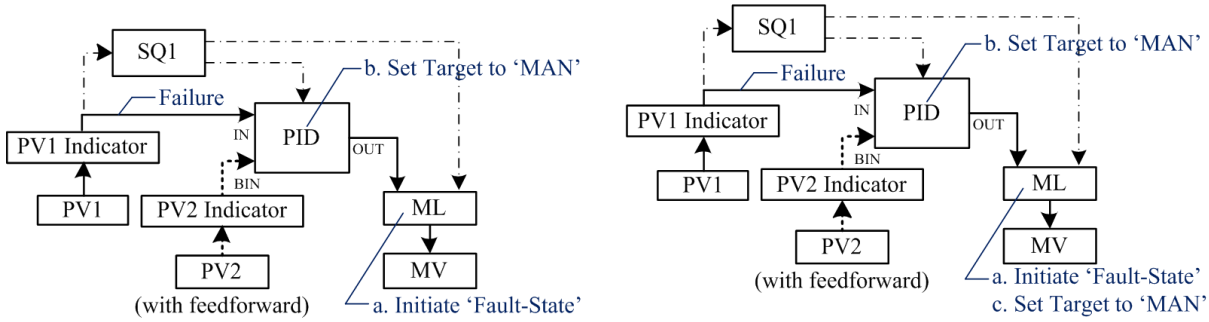


(a) PV1 failure

(b) PV2 failure

(c) PV1 failure

FIGURE 3. Typical actions in response to failures for PID loops with/without feedforward path



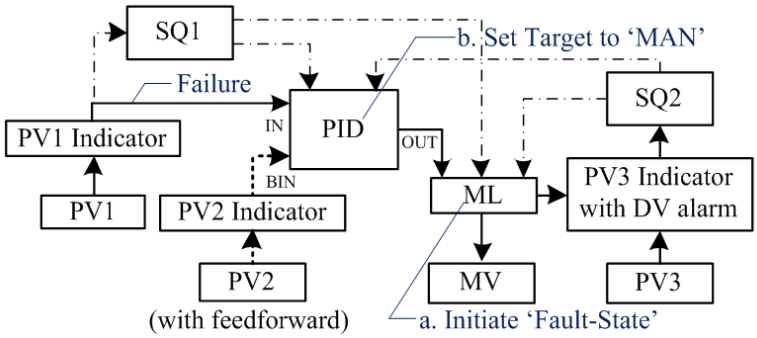
(a) 'Pattern1' for PV1 sensor failure

(b) 'Pattern2' for PV1 sensor failure

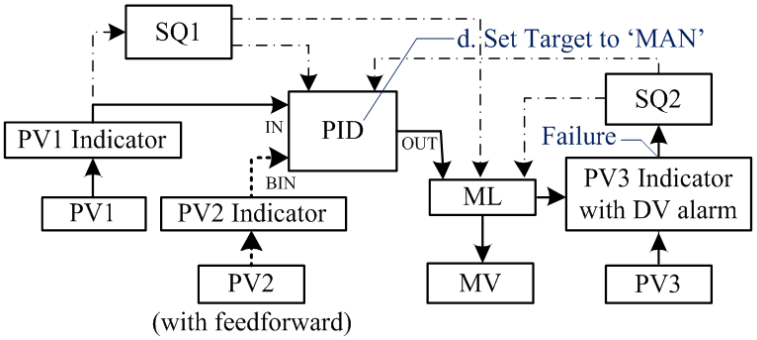
FIGURE 4. Concepts for improving safety of PID loops with/without feedforward path

other two concepts referred to as 'Pattern3' and 'Pattern4' in Figures 5(a) and 5(b), and 5(c) and 5(d), respectively, are also defined.

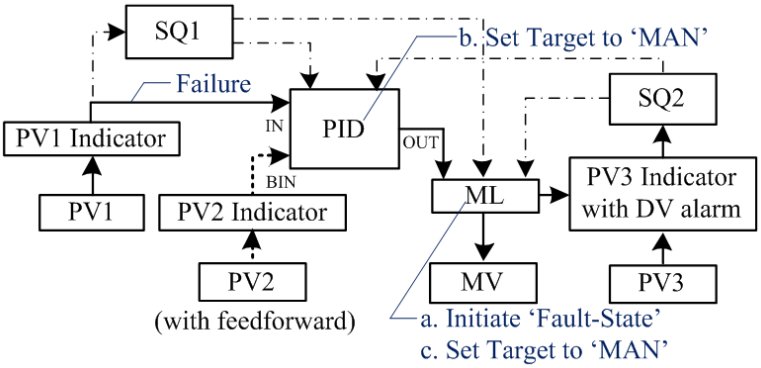
From Figures 4 and 5, the solid and dash-dotted lines represent the wiring and virtual interconnections between blocks for data transfers, respectively, while the dotted line represents the PV2 input connection for feedforward path. The PV1 and PV2 indicator blocks perform the input and alarm processing to detect failures of the LIT and FIT transmitters, respectively. The PV3 indicator with deviation (DV) alarm executes the input and alarm processing to detect the deviation of the PV3 from the desired MV value for indicating failure of the LCV positioner. To generate the MV, the manual loader (ML) block performs the operating mode selection between cascade (CAS) mode and 'MAN' mode. The output of the PID block becomes the MV when setting the target mode of the ML block to 'CAS', whereas the MV is manually set by the operator when setting the target mode of the ML block to 'MAN'. The SQ1 and SQ2 blocks are used to manage sequential operations in response to PV1 and PV3 failures, respectively. Table 2 shows four patterns specified for safety enhancement of the interested control by adding fault-state and fault-recovery actions, which are software-based mechanisms for upgrading capabilities of traditional loops. The 'Pattern1' and 'Pattern2' provide the actions specified in



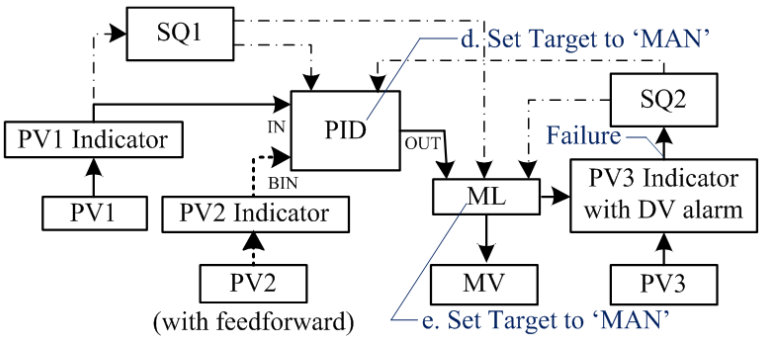
(a) 'Pattern3' for PV1 sensor failure



(b) 'Pattern3' for PV3 actuator failure



(c) 'Pattern4' for PV1 sensor failure



(d) 'Pattern4' for PV3 actuator failure

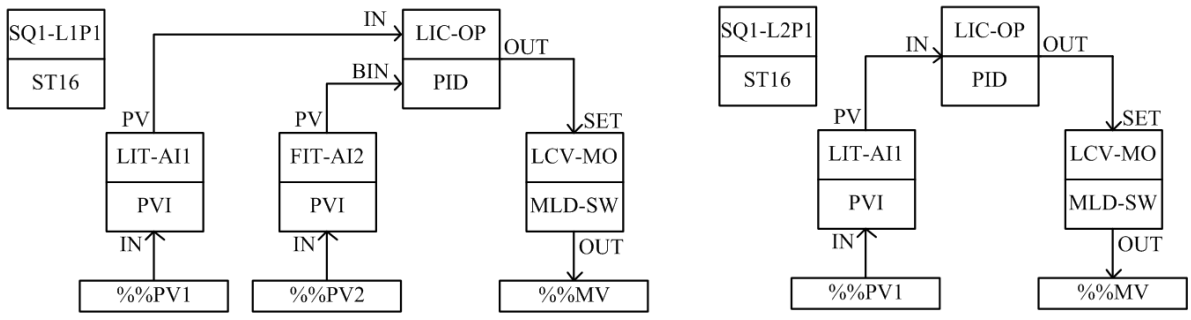
FIGURE 5. Concepts for improving safety of PID loops with/without feedforward path in combination with actual valve position signal

TABLE 2. Four patterns specified for safety enhancement of the interested process control

Pattern	Fault-state action	Fault-recovery action
1	a. Force the preset safe value to be the MV signal when detecting PV1 failure.	b. Force the target mode of the PID block into 'MAN' when detecting PV1 failure.
2	a. Force the preset safe value to be the MV signal when detecting PV1 failure.	b. Force the target mode of the PID block into 'MAN' when detecting PV1 failure.
		c. Force the target mode of the ML block into 'MAN' when detecting PV1 failure.
3	a. Force the preset safe value to be the MV signal when detecting PV1 failure.	b. Force the target mode of the PID block into 'MAN' when detecting PV1 failure.
		d. Force the target mode of the PID block into 'MAN' when detecting PV3 failure.
4	a. Force the preset safe value to be the MV signal when detecting PV1 failure.	b. Force the target mode of the PID block into 'MAN' when detecting PV1 failure.
		c. Force the target mode of the ML block into 'MAN' when detecting PV1 failure.
		d. Force the target mode of the PID block into 'MAN' when detecting PV3 failure.
		e. Force the target mode of the ML block into 'MAN' when detecting PV3 failure.

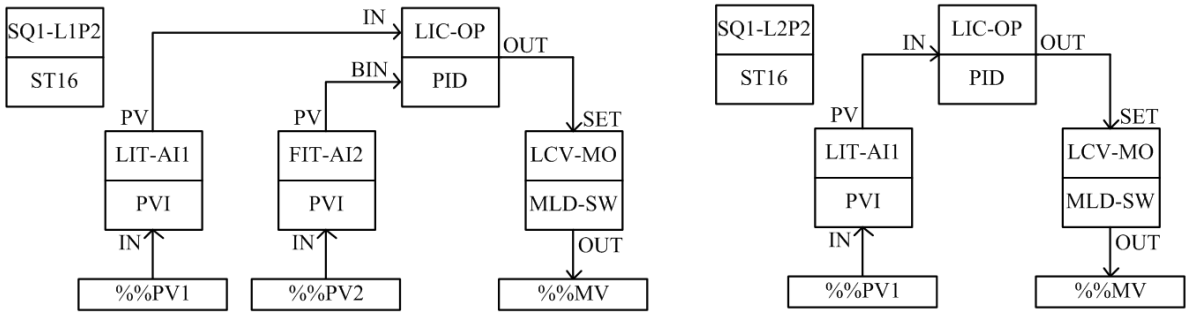
response to PV1 failure for the Loop1 and Loop2. The 'Pattern3' and 'Pattern4' provide the actions specified in response to PV1 and PV3 failures for the Loop3 and Loop4. It should be noted that, for fault-recovery action implemented in the PID block in the event of PV1 failure, the block itself automatically forces its desired target mode of operation into 'MAN'.

3. **Descriptions of Proposed Safety Enhancement.** To design control drawings based on the specified patterns shown in Table 2 for improving safety of four interested PID control loops in Table 1, the CENTUM VP DCS (version R6.02.00) [28] with the CONT module (or field control station) modeled AFV10D is utilized as an illustrative host system. Eight control drawings designed by using function blocks available in the DCS host are depicted in Figures 6-9. Based on 'Pattern1' and 'Pattern2', four control drawings referred to as L1P1, L2P1 and L1P2, L2P2 are displayed in Figures 6(a) and 6(b), and 7(a) and 7(b), respectively. For safety improvement based on 'Pattern3' and 'Pattern4',



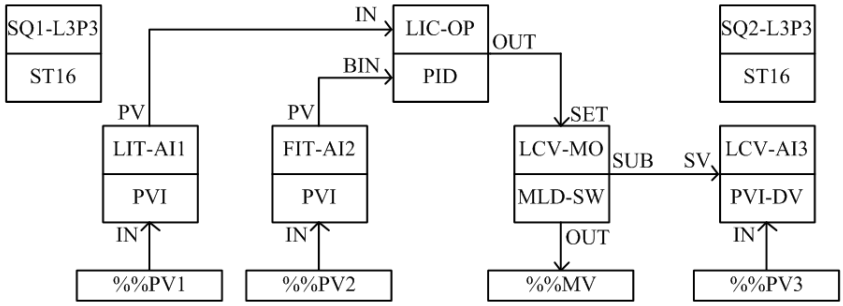
(a) Loop1 using 'Pattern1' (L1P1) (b) Loop2 using 'Pattern1' (L2P1)

FIGURE 6. Control drawings designed for safety enhancement using 'Pattern1'

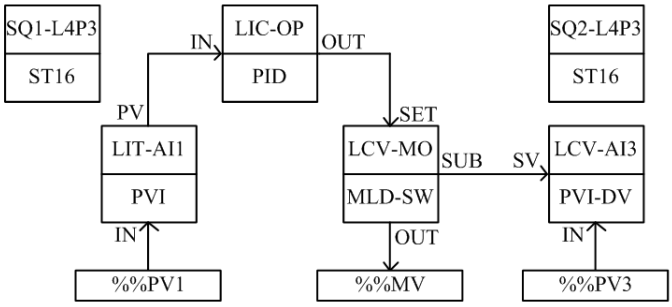


(a) Loop1 using 'Pattern2' (L1P2) (b) Loop2 using 'Pattern2' (L2P2)

FIGURE 7. Control drawings designed for safety enhancement using 'Pattern2'



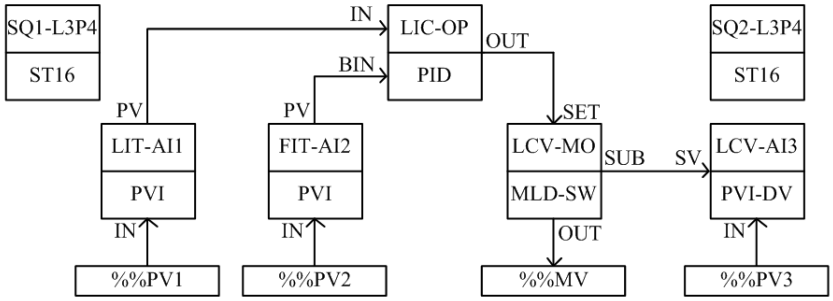
(a) Loop3 using 'Pattern3' (L3P3)



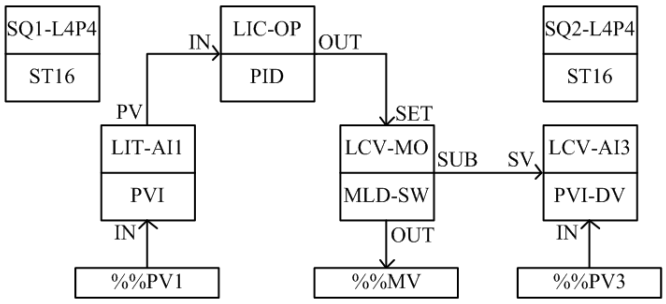
(b) Loop4 using 'Pattern3' (L4P3)

FIGURE 8. Control drawings designed for safety enhancement using 'Pattern3'

the remaining four control drawings referred to as L3P3, L4P3 and L3P4, L4P4 are illustrated in Figures 8(a) and 8(b), and 9(a) and 9(b), respectively. Table 3 gives assignments of the addresses for receiving analog inputs from the AI module and transmitting analog output to the AO module as well as the function blocks for representing logical processing units. For each function block, the tag is represented in upper part, whereas the type is represented in lower part. Five different types of function blocks, which are supported by the CENTUM VP DCS, include the input indicator block (PVI), input indicator block with deviation alarm (PVI-DV), PID block, manual loader block with operating mode switching (MLD-SW), and sequence table block (ST16). The 'AUT' is the normal operating mode for the PVI, PVI-DV, ST16, and PID blocks, and the 'CAS' is the normal operating mode of the MLD-SW block. The 'LIT-AI1' and 'FIT-AI2' blocks perform the input and alarm processing to detect sensor failures of the PV1 and PV2 signals, respectively. During normal conditions, the 'LIC-OP' block's output is determined by the target



(a) Loop3 using 'Pattern4' (L3P4)



(b) Loop4 using 'Pattern4' (L4P4)

FIGURE 9. Control drawings designed for safety enhancement using 'Pattern4'

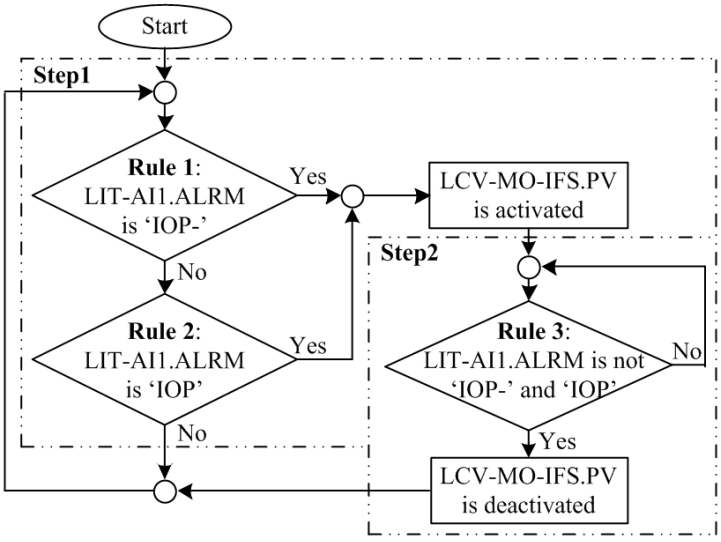
TABLE 3. Address/function block assignments for eight designed control drawings

Address/Tag	Block type	Description
%%PV1		Input connection address to get the LIT measurement
%%PV2		Input connection address to get the FIT measurement
%%PV3		Input connection address to get the return of actual LCV
%%MV		Output connection address to set the LCV position
LIT-AI1	PVI	Indicating the LIT output (PV1) and its failure status
FIT-AI2	PVI	Indicating the FIT output (PV2) and its failure status
LCV-AI3	PVI-DV	Indicating the LCV position (PV3) and its failure status
LIC-OP	PID	Executing control computation to adjust the MV value
LCV-MO	MLD-SW	Selecting the source of the MV to be sent to the LCV
SQ1-L1P1, SQ1-L2P1, SQ1-L3P3, SQ1-L4P3	ST16	Executing fault-state action in the 'LCV-MO' block in response to PV1 sensor failure
SQ1-L1P2, SQ1-L2P2, SQ1-L3P4, SQ1-L4P4	ST16	Executing fault-state and fault-recovery actions in the 'LCV-MO' block in response to PV1 sensor failure
SQ2-L3P3, SQ2-L4P3	ST16	Executing fault-recovery action in the 'LCV-MO' block in response to PV3 actuator failure
SQ2-L3P4, SQ2-L4P4	ST16	Executing fault-recovery action in the 'LIC-OP' and 'LCV-MO' blocks in response to PV3 actuator failure

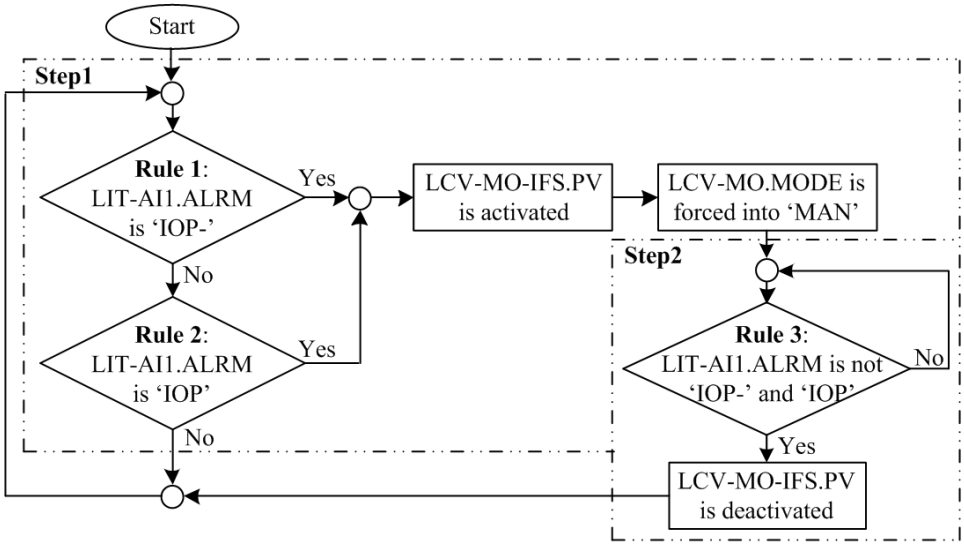
mode. The outputs of the 'LIC-OP' blocks in 'AUT' mode for 'Loop2' and 'Loop4' are computed by PID algorithms based on the deviation of the PV1 from the desired control setpoint. For 'Loop1' and 'Loop3', the PV2 feedforward inputs are added to control outputs of PID computations for providing the 'LIC-OP' blocks' outputs in 'AUT' mode. However, the outputs of the 'LIC-OP' blocks in all interested loops in 'MAN' mode are manually set by the operator through a process visualization program running on the DCS host. The 'LCV-AI3' block detects actuator failure by calculating the difference between the PV3 return signal of the actual LCV position and the output of the 'LCV-MO' block, which is used for selecting the source of the MV signal to be sent to the LCV positioner. This means that the MV signal is determined by target operating mode of the 'LCV-MO' block. In 'CAS' mode, the MV is equal to the 'LIC-OP' block's output, while the operator sets the MV value directly in 'MAN' mode. In order to establish fault-state and fault-recovery actions in response to sensor and actuator failures detected by the 'LIT-AI1' and 'LCV-AI3' blocks, respectively, the sequence control functions are realized by utilizing the ST16 blocks. In the presence of PV1 failure, the 'low-alarm' and 'high-alarm' statuses of the LIT-AI1.ALRM parameter are stated as 'IOP−' and 'IOP' (or 'IOP+'), respectively. In the event of PV3 failure, the 'low-alarm' and 'high-alarm' statuses of the LCV-AI3.ALRM parameter are stated as 'DV−' and 'DV+', respectively. Table 4 illustrates the steps and rules programmed in the ST16 blocks in the designed control drawings to provide the actions specified in Table 2, which are based on functions of status propagation and mode shedding during failure conditions. Figures 10(a)-10(d) show the flowchart diagrams for sequential operations of the ST16 blocks. In addition, based on

Table 4. ST16 block assignments for providing safety enhancement of Table 2

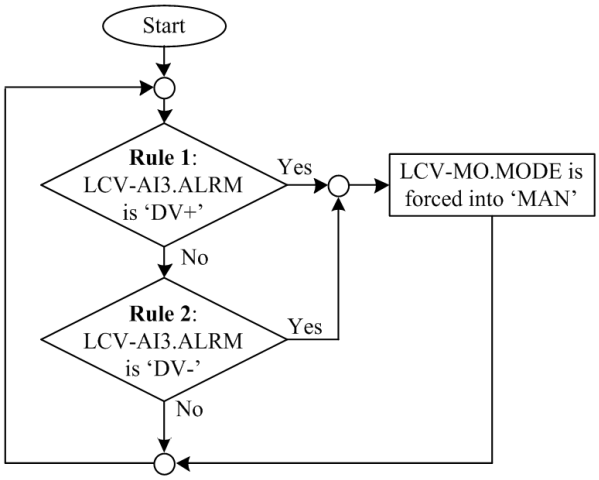
Block tag	Step	Rule	Block input condition	Block output action	Action in Table 2
SQ1-L1P1, SQ1-L2P1, SQ1-L3P3, SQ1-L4P3	1	1	If LIT-AI1.ALRM is 'IOP−'.	LCV-MO-IFS.PV is activated (or 'high'). Go to Step2.	a. Fault-state
		2	If LIT-AI1.ALRM is 'IOP'.		
	2	3	If LIT-AI1.ALRM is not 'IOP−' and 'IOP'.	LCV-MO-IFS.PV is deactivated (or 'low'). Go to Step1.	
SQ1-L1P2, SQ1-L2P2, SQ1-L3P4, SQ1-L4P4	1	1	If LIT-AI1.ALRM is 'IOP−'.	LCV-MO-IFS.PV is activated (or 'high'). LCV-MO.MODE is forced into 'MAN'. Go to Step2.	a. Fault-state c. Fault-recovery
		2	If LIT-AI1.ALRM is 'IOP'.		
	2	3	If LIT-AI1.ALRM is not 'IOP−' and 'IOP'.	LCV-MO-IFS.PV is deactivated (or 'low'). Go to Step1.	
SQ2-L3P3, SQ2-L4P3	–	1	If LCV-AI3.ALRM is 'DV+'.	LCV-MO.MODE is forced into 'MAN'.	d. Fault-recovery
		2	If LCV-AI3.ALRM is 'DV−'.		
SQ2-L3P4, SQ2-L4P4	–	1	If LCV-AI3.ALRM is 'DV+'.	LCV-MO.MODE and LIC-OP.MODE are forced into 'MAN'.	d. Fault-recovery e. Fault-recovery
		2	If LCV-AI3.ALRM is 'DV−'.		



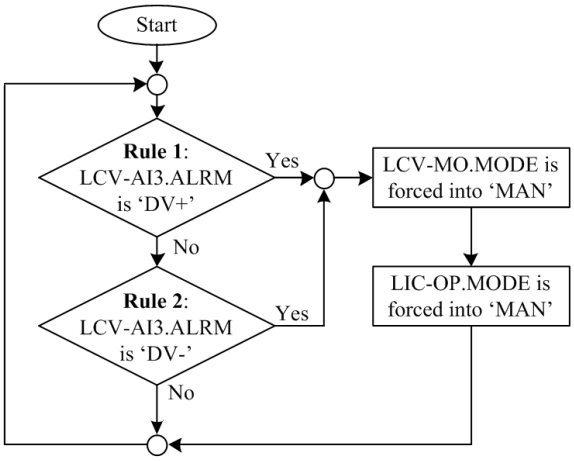
(a) SQ1-L1P1, SQ1-L2P1, SQ1-L3P3, and SQ1-L4P3 blocks



(b) SQ1-L1P2, SQ1-L2P2, SQ1-L3P4, and SQ1-L4P4 blocks



(c) SQ2-L3P3 and SQ2-L4P3 blocks



(d) SQ2-L3P4 and SQ2-L4P4 blocks

FIGURE 10. Flowchart diagrams for sequential operations of the ST16 blocks used

its default algorithm, the target mode of the 'LIC-OP' block is automatically set to 'MAN' when detecting the 'IOP−' or 'IOP' status (b. in Table 2). After the PV1 failure has been resolved, the target mode of the 'LIC-OP' block remains in 'MAN'. Until the operator sets 'AUT' for the target mode, the 'LIC-OP' block can resume its automatic control function.

To activate the fault-state action (a. in Table 2) when detecting the 'IOP−' or 'IOP' status by performing operations of the 'SQ1-L1P1', 'SQ1-L2P1', 'SQ1-L3P3', and 'SQ1-L4P3' blocks as shown in Figure 10(a), the LCV-MO-IFS.PV parameter is set to 'high' logic state. The actual mode of the 'LCV-MO' block automatically changes to the tracking (TRK) mode and then the MV signal is forced to equal the predefined safe value. After the PV1 failure has been fixed, the LIT-AI1.ALRM is not the 'IOP−' and 'IOP'. Then the LCV-MO-IFS.PV is set to 'low' state to deactivate the specified fault-state action. To provide the fault-state and fault-recovery actions (a. and c. in Table 2) during the detected 'IOP−' or 'IOP' status by running functions of the 'SQ1-L1P2', 'SQ1-L2P2', 'SQ1-L3P4', and 'SQ1-L4P4' blocks as depicted in Figure 10(b), the LCV-MO-IFS.PV and LCV-MO.MODE parameters are set to 'high' and 'MAN', respectively. Then the preset safe value becomes the MV signal, and the target mode of the 'LCV-MO' block is forced into 'MAN'. After the PV1 failure has been corrected, the LIT-AI1.ALRM is not 'IOP−' and 'IOP'. Then the fault-state action is deactivated by setting the LCV-MO-IFS.PV to 'low'. The 'LCV-MO' remains in 'MAN' actual operating mode, while the 'LIC-OP' block remains in initialization manual (IMAN) mode. To initiate the fault-recovery action (d. in Table 2) when detecting the 'DV+' or 'DV−' status by running operations of the 'SQ2-L3P3' and 'SQ2-L4P3' blocks as illustrated in Figure 10(c), the LCV-MO.MODE is set to 'MAN'. Therefore, the target mode of the 'LCV-MO' block becomes 'MAN'. After the PV3 failure has been fixed, the 'LCV-MO' remains in its 'MAN' actual mode. Until the operator sets 'CAS' for the target mode of the 'LCV-MO', the MV signal then is equal to the 'LIC-OP' block's output. To provide the fault-recovery actions (d. and e. in Table 2) during the detected 'DV+' or 'DV−' status by executing functions of the 'SQ2-L3P4' and 'SQ2-L4P4' blocks as displayed in Figure 10(d), the LCV-MO.MODE and LIC-OP.MODE parameters are set to 'MAN'. The target modes of the 'LIC-OP' and 'LCV-MO' blocks then become 'MAN'. This means that the actual modes of these two blocks are 'IMAN and 'MAN', respectively, until the operator intervenes by changing the target modes to be their normal operating modes.

4. **Simulation Results from DCS Test Function.** To confirm the feasibility of the proposed safety enhancement, all control drawings designed for providing the fault-state and fault-recovery actions were simulated by utilizing virtual test function of the DCS host used. Simulations were carried out to test the configured functions of four control drawings in the presence of PV1 failure and four control drawings in the presence of PV1 and PV3 failures. The values for failure detections were chosen as: 'IOP−' = −6.3%, 'IOP' (or 'IOP+') = 106.3%, 'DV+' = 10%, and 'DV−' = 10%. The preset safe value for fault-state action was set to 10%, and the setpoint of tank level control was set to 50%.

Table 5 gives the conditions defined for simulations to observe the operability of all designed control drawings. Figure 11 illustrates an example of graphic displays created for user interface in simulations. Figures 12(a) and 12(b) show the examples of 'Set Data' window used to set data status of the LIT-AI1.RAW for simulating the 'PV1-IOP−' and 'PV1-IOP' conditions, respectively. To save space, only the test results of the L3P4 control drawing that provides the highest possible degree of safety among the interested current loops are illustrated in Figures 13-16 for examples of observation of fault-state and fault-recovery actions when detecting PV1 and PV3 failures.

TABLE 5. Conditions for simulations of the designed control drawings

Condition	Description
PV1-NR	Set data status of LIT-AI1.RAW to be normal by using 'Set Data' window.
PV1-IOP−	Set data status of LIT-AI1.RAW to be 'IOP−' by using 'Set Data' window.
PV1-IOP	Set data status of LIT-AI1.RAW to be 'IOP+' by using 'Set Data' window.
PV3-NR	Set the difference between LCV-AI3.RAW and LCV-MO.MV to be less than 10%.
PV3-DV−	Set LCV-AI3.RAW to be less than LCV-MO.MV, and their difference is greater than 10%, then 'DV−' is detected.
PV3-DV+	Set LCV-AI3.RAW to be greater than LCV-MO.MV, and their difference is greater than 10%, then 'DV+' is detected.

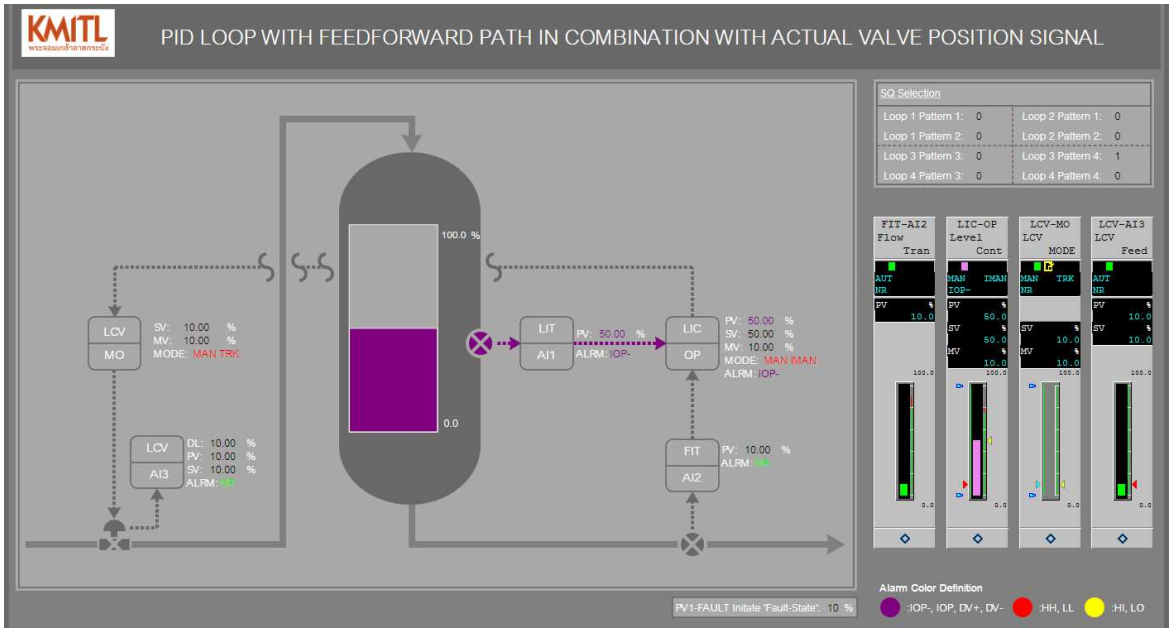
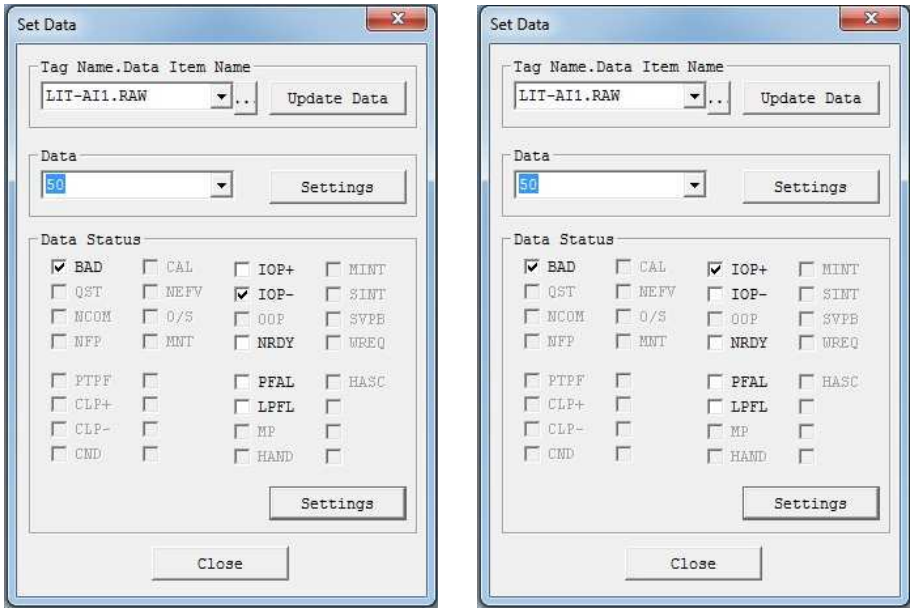


FIGURE 11. Example of graphic displays created for user interface in simulations

The operations of the 'SQ1-L3P4' block in response to PV1 failure before detecting the 'IOP−', when detecting the 'IOP−', and after clearing the 'IOP−' are illustrated in Figures 13(a)-13(c), respectively. Before and after experiencing the PV1 failure (see Figures 13(a) and 13(c)), the online statuses of the C01 and C02 conditions during normal operation are 'N' (shown in the red font color), and the current operation of the 'SQ1-L3P4' is in 'Step1' ('01' shown in green background) to check whether 'Rule1' (C01) or 'Rule2' (C02) is true. If the 'IOP−' status is detected under 'PV1-IOP−' condition (see Figure 13(b)), the online statuses of the C01 and C02 are 'Y' and 'N' (shown in red font color), respectively, and the current operation of the 'SQ1-L3P4' is in 'Step2' ('02' shown in green background).

The online statuses of function blocks in the L3P4 from virtual test in response to PV1 failure are displayed in Figures 14(a)-14(c). Before detecting 'IOP−' status under 'PV1-NR' condition (see Figure 14(a)), all function blocks operate in their normal modes, and the operation of the 'SQ1-L3P4' is in 'Step1' (01). During 'PV1-IOP−' condition (see Figure 14(b)), the 'SQ1-L3P4' can detect the 'IOP−' status, and its operation is switched to 'Step2' (02). The 'LIT-AI1' block propagates the 'IOP−' status to the 'LIC-OP' block,



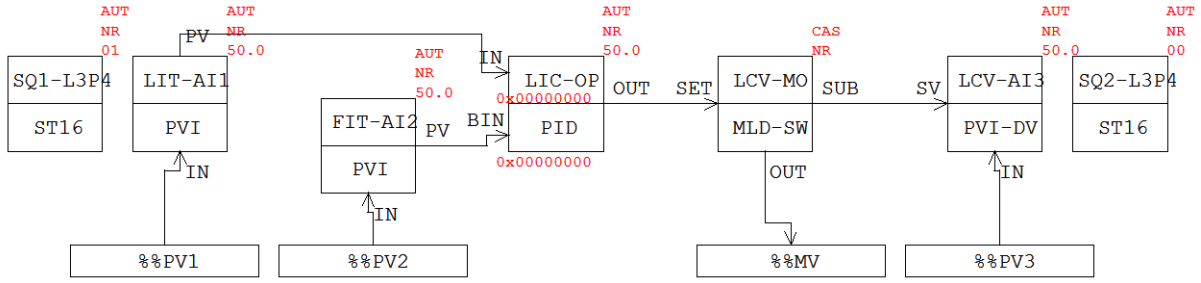
(a) 'PV1-IOP−' condition (b) 'PV1-IOP' condition

FIGURE 12. Examples of 'Set Data' window used for PV1 failure simulations

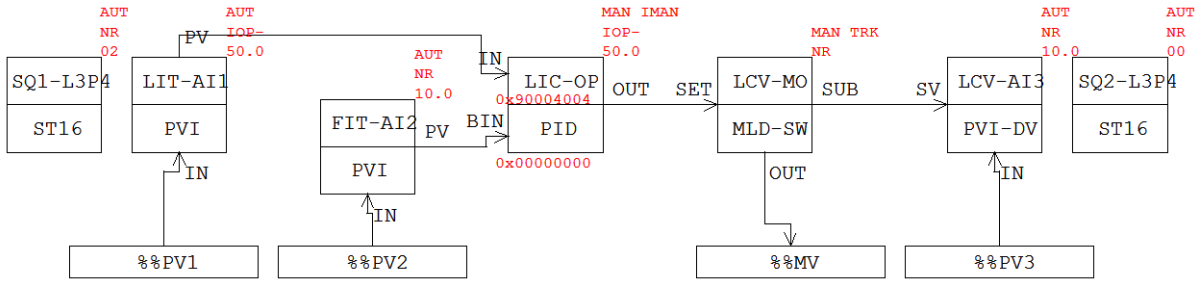
(a) Before detecting 'IOP−' (b) When detecting 'IOP−' (c) After clearing 'IOP−'

FIGURE 13. (color online) Operations of the 'SQ1-L3P4' block in response to PV1 failure

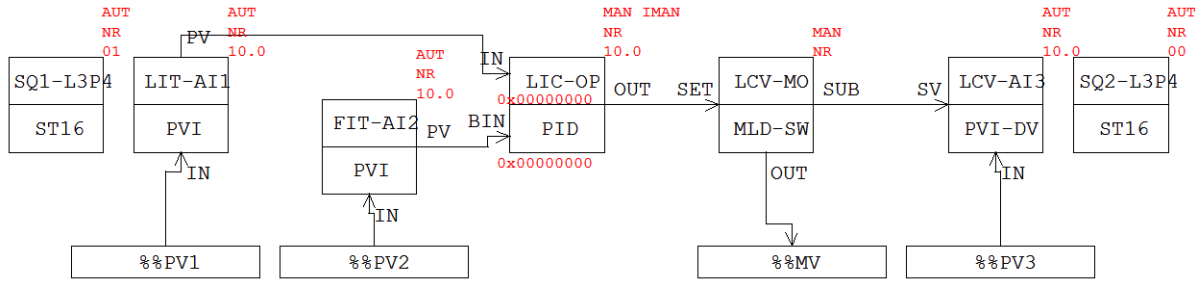
and the fault-state action in the 'LCV-MO' block is initiated by forcing the preset value of 10% to be the MV. The correctness of the desired fault-state action is determined by the 'LCV-AI3' block's output, which equals the actual LCV position signal. It is seen that the output of the 'LCV-AI3' block is also 10%. In addition, the target modes of the 'LIC-OP' and 'LCV-MO' blocks are forced into 'MAN'. Based on mode shedding in response to PV1 failure, the actual modes of the 'LIC-OP' and 'LCV-MO' blocks change to 'IMAN' and 'TRK', respectively. After clearing the 'IOP−' status, the actual mode of the 'LCV-MO' returns back to 'MAN' mode (see Figure 14(c)). The predefined safe value is used as the initial value to restart the LCV valve positioner. If the operator sets the target mode of the 'LCV-MO' block to 'CAS', the actual mode of the 'LIC-OP' will be placed in 'MAN'. Until the operator changes the target mode of the 'LIC-OP' to 'AUT', the L3P4 can return to its automatic control function.



(a) Before detecting 'IOP−' status under 'PV1-NR' condition



(b) When detecting 'IOP−' status under 'PV1-IOP−' condition



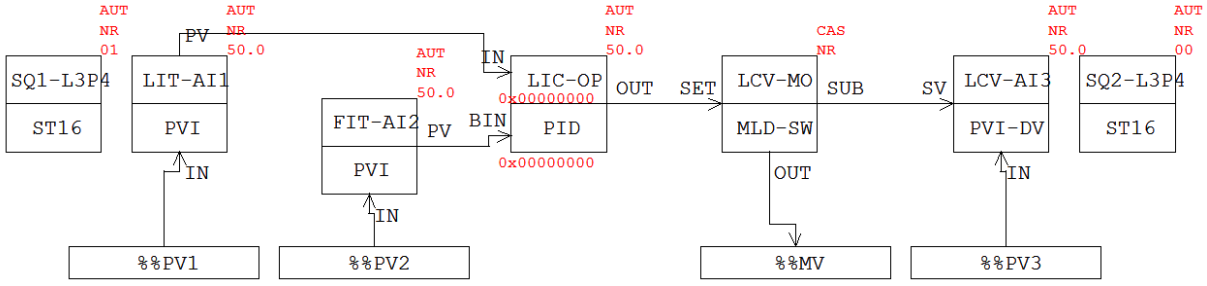
(c) After clearing 'IOP−' status under 'PV1-NR' condition

FIGURE 14. Online statuses of function blocks in the L3P4 in response to PV1 failure

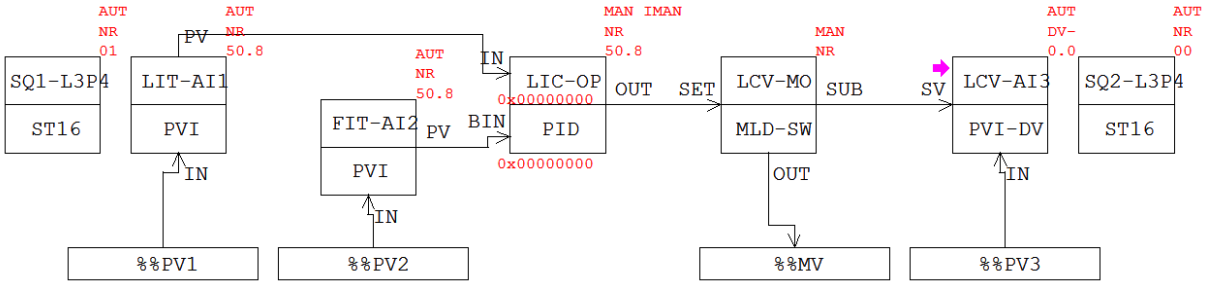
The operations of the 'SQ2-L3P4' block in response to PV3 failure before detecting the 'DV−', when detecting the 'DV−', and after clearing the 'DV−' are displayed in Figures 15(a)-15(c), respectively. In the event of the 'DV−' under 'PV3-DV−' condition (see Figure 15(b)), the online (red) status of the C02 input condition is 'Y' (shown in the red font color). Before and after experiencing the failure (see Figures 15(a) and 15(c)), the online (green) statuses of the C01 and C02 conditions during normal operation are 'Y' (shown in the light blue font color). The online statuses of function blocks in the L3P4 in response to PV3 failure are illustrated in Figures 16(a)-16(c). From Figure 16(a), all function blocks perform in their normal modes under 'PV3-NR' condition. In the presence of the 'DV−' status by setting the PV3 to zero and the MV to 50% (see Figure 16(b)), the 'SQ1-L3P4' forces the target modes of the 'LIC-OP' and 'LCV-MO' blocks into 'MAN'. Based on mode shedding in response to PV3 failure, the actual modes of the 'LIC-OP' and 'LCV-MO' blocks are 'IMAN' and 'MAN', respectively. From Figure 16(c), after clearing the 'DV−' status, the 'LCV-MO' block still remains in 'MAN'. Until the target modes of the 'LCV-MO' and 'LIC-OP' are changed to 'CAS' and 'AUT', respectively, the L3P4 can resume to its normal control operation. Additionally, the online statuses of function

(a) Before detecting 'DV−' (b) When detecting 'DV−' (c) After clearing 'DV−'

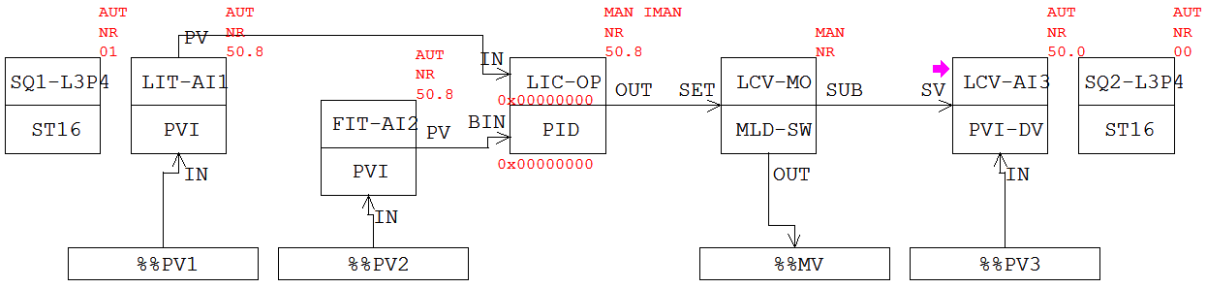
FIGURE 15. (color online) Operations of the 'SQ2-L3P4' block in response to PV3 failure



(a) Before detecting 'DV−' under 'PV3-NR' condition



(b) When detecting 'DV−' under 'PV3-DV−' condition



(c) After clearing 'DV−' under 'PV3-NR' condition

FIGURE 16. Online statuses of function blocks in the L3P4 in response to PV3 failure

blocks in the L1P1, L2P1, L1P2, and L2P2 from virtual tests in response to PV1 failure as well as the online statuses of function blocks in the L3P3, L4P3, and L4P4 from virtual tests in response to PV1 and PV3 failures agree very well with the expected results.

Table 6 presents the virtual test results of eight control drawings designed for safety enhancement of two PID loops with/without feedforward path in response to PV1 failure and two PID control loops with/without feedforward path in combination with actual valve position signal in response to PV1 and PV3 failures. It is evident that fault-state and fault-recovery actions provided by the designed control drawings are in good agreement with the desired actions in Tables 2 and 4. Table 7 shows the changes of target and actual modes of the 'LIC-OP' and 'LCV-MO' blocks when detecting and after resolving

TABLE 6. Test results of eight control drawings designed for safety enhancement

Control drawing	Defined condition	Fault-state action	Fault-recovery action
L1P1, L2P1	PV1-IOP−	LCV-MO-IFS.PV is high.	LIC-OP.MODE is 'MAN'.
	PV1-NR	LCV-MO-IFS.PV is low.	LIC-OP.MODE remains in 'MAN'.
	PV1-IOP	LCV-MO-IFS.PV is high.	LIC-OP.MODE is 'MAN'.
	PV1-NR	LCV-MO-IFS.PV is low.	LIC-OP.MODE remains in 'MAN'.
L1P2, L2P2	PV1-IOP−	LCV-MO-IFS.PV is high.	LCV-MO.MODE and LIC-OP.MODE are 'MAN'.
	PV1-NR	LCV-MO-IFS.PV is low.	LCV-MO.MODE and LIC-OP.MODE remain in 'MAN'.
	PV1-IOP	LCV-MO-IFS.PV is high.	LCV-MO.MODE and LIC-OP.MODE are 'MAN'.
	PV1-NR	LCV-MO-IFS.PV is low.	LCV-MO.MODE and LIC-OP.MODE remain in 'MAN'.
L3P3, L4P3	PV1-IOP−	LCV-MO-IFS.PV is high.	LIC-OP.MODE is 'MAN'.
	PV1-NR	LCV-MO-IFS.PV is low.	LIC-OP.MODE remains in 'MAN'.
	PV1-IOP	LCV-MO-IFS.PV is high.	LIC-OP.MODE is 'MAN'.
	PV1-NR	LCV-MO-IFS.PV is low.	LIC-OP.MODE remains in 'MAN'.
	PV3-DV−	–	LIC-OP.MODE is 'MAN'.
	PV3-NR	–	LIC-OP.MODE remains in 'MAN'.
	PV3-DV+	–	LIC-OP.MODE is 'MAN'.
	PV3-NR	–	LIC-OP.MODE remains in 'MAN'.
L3P4, L4P4	PV1-IOP−	LCV-MO-IFS.PV is high.	LCV-MO.MODE and LIC-OP.MODE are 'MAN'.
	PV1-NR	LCV-MO-IFS.PV is low.	LCV-MO.MODE and LIC-OP.MODE remain in 'MAN'.
	PV1-IOP	LCV-MO-IFS.PV is high.	LCV-MO.MODE and LIC-OP.MODE are 'MAN'.
	PV1-NR	LCV-MO-IFS.PV is low.	LCV-MO.MODE and LIC-OP.MODE remain in 'MAN'.
	PV3-DV−	–	LCV-MO.MODE and LIC-OP.MODE are 'MAN'.
	PV3-NR	–	LCV-MO.MODE and LIC-OP.MODE remain in 'MAN'.
	PV3-DV+	–	LCV-MO.MODE and LIC-OP.MODE are 'MAN'.
	PV3-NR	–	LCV-MO.MODE and LIC-OP.MODE remain in 'MAN'.

TABLE 7. Target and actual modes of the 'LIC-OP' and 'LCV-MO' in case of PV1 failure

Control drawing	When detecting PV1 failure				After resolving PV1 failure			
	LIC-OP (PID)		LCV-MO (ML)		LIC-OP (PID)		LCV-MO (ML)	
	Target	Actual	Target	Actual	Target	Actual	Target	Actual
L1P1	MAN	IMAN	CAS	TRK	MAN	MAN	CAS	CAS
L2P1	MAN	IMAN	CAS	TRK	MAN	MAN	CAS	CAS
L1P2	MAN	IMAN	MAN	TRK	MAN	IMAN	MAN	MAN
L2P2	MAN	IMAN	MAN	TRK	MAN	IMAN	MAN	MAN
L3P3	MAN	IMAN	CAS	TRK	MAN	MAN	CAS	CAS
L4P3	MAN	IMAN	CAS	TRK	MAN	MAN	CAS	CAS
L3P4	MAN	IMAN	MAN	TRK	MAN	IMAN	MAN	MAN
L4P4	MAN	IMAN	MAN	TRK	MAN	IMAN	MAN	MAN

TABLE 8. Target and actual modes of the 'LIC-OP' and 'LCV-MO' in case of PV3 failure

Control drawing	When detecting PV3 failure				After resolving PV3 failure			
	LIC-OP (PID)		LCV-MO (ML)		LIC-OP (PID)		LCV-MO (ML)	
	Target	Actual	Target	Actual	Target	Actual	Target	Actual
L3P3	MAN	MAN	CAS	CAS	MAN	MAN	CAS	CAS
L4P3	MAN	MAN	CAS	CAS	MAN	MAN	CAS	CAS
L3P4	MAN	IMAN	MAN	MAN	MAN	IMAN	MAN	MAN
L4P4	MAN	IMAN	MAN	MAN	MAN	IMAN	MAN	MAN

PV1 failure. This ensures that the affected loops with PV1 failure shut their automatic operations down safely by fault-state action. Similarly, Table 8 gives the changes of target and actual modes of the 'LIC-OP' and 'LCV-MO' blocks when detecting and after resolving PV3 failure. It is confirmed that the control loops with failed actuator are not operated in 'AUT' mode, and they cannot immediately resume their automatic control function after the failure has been resolved until the operator unlocks. Therefore, functions of status propagation and mode shedding in response to sensor and actuator failures are particularly useful in basic process control. Table 9 summarizes the comparison results between the actions of the ML, PID, and ST16 blocks in the designed control drawings and the parameter options of FF function blocks in the FF-based PID control with/without feedforward [8,16,17]. The ST16 blocks are the 'SQ1-LiPk', 'SQ1-LiPm', 'SQ2-LjPn', and 'SQ2-LjP4', where i $(= 1, 2, 3, 4)$ and j $(= 3, 4)$ are the 'Loop' numbers, and k $(= 1, 2, 3, 4)$, m $(= 2, 4)$, and n $(= 3, 4)$ are the 'Pattern' numbers. It is clearly seen that the fault-state and fault-recovery actions provided by all designed control drawings are in similar way as the built-in fault-state and fault-recovery options provided by the digital FF-based PID loops. Hence, the proposed technique for configuration design of control drawings of four studied PID loops with/without feedforward path can be an alternative solution for existing production plants using conventional wiring to improve their control operations for additional level of safety.

5. **Conclusions.** To enhance safety of conventional 4-20 mA current loops with/without actual actuator position signal in the presence of instrument failures for PID control with/without feedforward path, a configuration design technique by using software function blocks available in the CENTUM VP DCS host has been proposed. Eight control

TABLE 9. Comparison of the proposed technique and the previous works [8,16,17]

Designed control drawings		PID control with/without feedforward	
Block	Action of function block	Block	Option of FF function block
SQ1-L*i*P*k* (ST16)	If LIT-AI1.ALRM is 'IOP−' or 'IOP', LCV-MO-IFS.PV is activated.	PID	'IFS if Bad IN' for setting 'Initiate Fault State' status on its output in the event of 'Bad' input [16,17].
LCV-MO (ML)	If LCV-MO-IFS.PV is activated, its actual mode becomes 'TRK' and its output equals the preset safe value.	AO	'Fault State to value' for forcing its output to equal the preset safe value when receiving the 'Initiate Fault State' status from the PID [16,17].
LIC-OP (PID)	If LIT-AI1.ALRM is 'IOP−' or 'IOP', its default algorithm sets the target mode to 'MAN'.	PID	'Target to Manual if Bad IN' for setting its target mode to 'MAN' in the event of 'Bad' input [16,17].
SQ1-L*i*P*m* (ST16)	If LIT-AI1.ALRM is 'IOP−' or 'IOP', LCV-MO.MODE is forced into 'MAN'.	AO	'Target to Manual if Fault State Act' for setting its target mode to 'MAN' in case of fault-state action [17].
LCV-MO (ML)	If LCV-MO.MODE is forced into 'MAN', its target mode becomes 'MAN'.		
SQ2-L*j*P*n* (ST16)	If LCV-AI3.ALRM is 'DV+' or 'DV−', LCV-MO.MODE is forced into 'MAN'.	AO	Option is unavailable, but its default algorithm sets 'Bad' status on its BKCAL_OUT and forces the actual mode to change in response to the detected actuator failure [8].
LCV-MO (ML)	If LCV-MO.MODE is forced into 'MAN', its target mode becomes 'MAN'.		
SQ2-L*j*P4 (ST16)	If LCV-AI3.ALRM is 'DV+' or 'DV−', LIC-OP.MODE is forced into 'MAN'.	PID	Option is unavailable, but its default algorithm forces the actual mode into 'IMAN' in the event of 'Bad' status of its BKCAL_IN [8].
LIC-OP (PID)	If LIC-OP.MODE is forced into 'MAN', its target mode becomes 'MAN'.		

drawings designed for providing not only fault-state action to bring the affected loop to predefined safe state when detecting the failure but also fault-recovery action to return the affected loop back to normal operation with operator intervention after clearing the failure in four patterns have been introduced. With the proposed safety enhancement, four specified patterns based on functions of failure status propagation and failure mode shedding can also be applied to creating control drawings that contain function blocks running on other DCS platforms. Simulation results have been utilized to demonstrate the operability of four control drawings in the presence of sensor failure and four control drawings in the presence of sensor and actuator failures. A configuration design technique to provide greater safety of multi-loop control employing traditional 4-20 mA wiring is the future work.

Acknowledgment. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] P. Gruhn and H. L. Cheddie, *Safety Instrumented Systems: Design, Analysis and Justification*, ISA Press, USA, 2006.

[2] J. Poomhuang, P. Julsereewong and T. Thepmanee, SIL assessment for tail gas treating process using layer of protection analysis, *ICIC Express Letters, Part B: Applications*, vol.9, no.6, pp.525-531, 2018.

[3] R. J. Willey, Layer of protection analysis, *Procedia Engineering*, vol.84, pp.12-22, 2014.

[4] J. Jin, B. Shuai, X. Wang and Z. Zhu, Theoretical basis of quantification for layer of protection analysis (LOPA), *Annals of Nuclear Energy*, vol.87, pp.69-73, 2016.

[5] A. Gabriel, Design and evaluation of safety instrumented systems: A simplified and enhanced approach, *IEEE Access*, vol.5, pp.3813-3823, 2017.
[6] T. Vollmer, K. Borcherding, G. Hellriegel and R.-D. Penzhorn, Process control under safety aspects, *Fusion Engineering and Design*, vol.48, nos.1-2, pp.57-61, 2000.
[7] T. Blevins and M. Nixon, *Control Loop Foundation-Batch and Continuous Processes*, ISA Press, USA, 2011.
[8] J. Berge, *Fieldbuses for Process Control: Engineering, Operation and Maintenance*, ISA Press, USA, 2004.
[9] B. G. Liptak, *Instrument Engineers' Handbook: Process Control and Optimization*, CRC Press in Cooperation with ISA Press, USA, 2006.
[10] S. Kummool, T. Thepmanee and S. Pongswatd, Condition monitoring based on failure modes and effects analysis using SCADA software for WirelessHART devices, *ICIC Express Letters*, vol.12, no.4, pp.393-400, 2018.
[11] T. Blevins and W. Wojsznis, Fieldbus support for process analysis, *ISA Transactions*, vol.35, pp.177-183, 1996.
[12] J. Chen, Z. Wang and Y. X. Sun, How to improve control system performance using FF function blocks, *Proc. of the IEEE International Conference on Control Applications*, Scotland, U.K., pp.1022-1026, 2002.
[13] A. Julsereewong, N. Whatphat, T. Sangsuwan, J. Chanwuttitum and T. Thepmanee, Comparative analysis between control in the host and control in the field in terms of safety and availability for Foundation Fieldbus-based process control, *International Journal of Innovative Computing, Information and Control*, vol.14, no.2, pp.737-745, 2018.
[14] C. Diedrich, F. Russo, L. Winkel and T. Blevins, Function block application in control system based on IEC 61804, *ISA Transactions*, vol.43, pp.123-131, 2004.
[15] Fieldbus Foundation, *FF-890-1.10: Foundation Specification-Function Block Application Process, Part 1*, USA, 2012.
[16] T. Sangsuwan, T. Thepmanee and A. Julsereewong, Safety and availability of basic process control using Foundation Fieldbus with control in the field – An experimental analysis, *International Journal of Intelligent Engineering & Systems*, vol.10, no.4, pp.135-146, 2017.
[17] A. Julsereewong and S. Kummool, Process safety enhancement of feedforward control using Foundation Fieldbus, *International Journal of Innovative Computing, Information and Control*, vol.16, no.2, pp.621-630, 2020.
[18] T. Thepmanee, A. Julsereewong, P. Julsereewong and C. Jetanacheawchankij, Replacement of existing analog with digital Fieldbus: A case study of raw cane sugar production, *ICIC Express Letters*, vol.7, no.3(B), pp.1157-1162, 2013.
[19] T. Nguyen, R. G. Gosine and P. Warrian, A systematic review of big data analytics for oil and gas Industry 4.0, *IEEE Access*, vol.8, pp.61138-61201, 2020.
[20] T. R. Wanasinghe, R. G. Gosine, L. A. James, G. K. I. Mann, O. de Silva and P. J. Warrian, The Internet of Things in the oil and gas industry: A systematic review, *IEEE Internet of Things Journal*, vol.7 no.9, pp.8654-8672, 2020.
[21] A. Cala, A. Luder, F. Boschi, G. Tavola and M. Taisch, Migration towards digital manufacturing automation – An assessment approach, *Proc. of the 2018 IEEE Industrial Cyber-Physical Systems*, St. Petersburg, Russia, pp.714-719, 2018.
[22] N. Khochasin, T. Trisuwannawat, P. Julsereewong and A. Julsereewong, Comparative study on cascade control configuration in engineering phase for analog system and FF system, *Proc. of the IEEE/SICE International Symposium on System Integration*, Sapporo, Japan, pp.881-886, 2016.
[23] Azbil Corporation, *CM2-GTX100-2001: Advanced Transmitter Electronic Differential Pressure/ Pressure Transmitter*, 2020.
[24] Emerson, *00809-0100-4007: Rosemount^{TM} 3051 Pressure Transmitter with 4-20 mA HART® Revision 5 and 7 Selectable Protocol*, 2020.
[25] Endress+Hauser, *TI00383P/00/EN/34.20: Technical Information Cerabar S PMC71, PMP71, PMP75 Process Pressure Measurement*, 2020.
[26] Yokogawa, *IM 01C50T01-02EN: YTA610 and YTA710 Temperature Transmitters (HART Protocol)*, 2020.
[27] Yokogawa, *GS 01C31C01-01EN: EJA210E Flange Mounted Differential Pressure Transmitter*, 2020.
[28] Yokogawa, *GS 33K01A10-50E: Integrated Production Control System CENTUM VP System Overview (Vnet/IP Edition)*, 2017.