Safety and Availability of Basic Process Control Using Foundation Fieldbus with Control in the Field – An Experimental Analysis

Thaksin Sangsuwan [1], Teerawat Thepmanee [1], Amphawan Julsereewong [1]*

[1]*Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, 10520, Thailand*
* Corresponding author's Email: amphawan.ju@kmitl.ac.th

Abstract: Detailed knowledge of how to balance between safety and availability for instruments is essential to successful design and implementation in fieldbus-based process control systems. The configuration correctness is crucial to actually obtain the benefits of digital fieldbus technology used. In actuality, a number of device parameters must be set to provide the required functionalities. This paper focuses on improving safety and availability for the proportional-integral-derivative (PID) and cascade control strategies using Foundation Fieldbus (FF) with control in the field. The aim of this paper is to analyze the logical behaviors of PID and cascade loops in two conflicting purposes for studying how different configuration options affect the interlocks between function blocks located in instruments as well as the initialization and fail-safe mechanisms in response to invalid measurements. For safety purpose, the interested control loops are configured to bring the process to a safe state in the presence of a fault. For availability purpose, the interested control loops are configured to keep the process running in the event of a failure. A water tank process is utilized as a case study for control loop implementations. Interactions between the status propagation and mode shedding for demonstrating the studied control loop behaviors are examined experimentally in Petri net models. In addition, the function block options for bumpless transfer and setpoint tracking are also described. The proved configuration method for proper operations in balancing the interests of safety and availability is proposed.

Keywords: Foundation fieldbus, Safety, Availability, Process control, Function block, Control in the field.

1. Introduction

If a device, a module, a unit, or a system fails to execute its intended function, then a failure will occur [1]. As the analysis phase of the IEC 61511 safety life-cycle, end users in process industries such as refineries and chemical plants are required to perform hazard and risk analysis as well as consider the potential demands on the independent protection layers [2]. For hazardous process units, the safety protection is implemented by using an approved safety instrumented system (SIS) in addition to a basic process control system (BPCS) used for the control loops associated with the danger to reduce the risk of harming people, property, environment, and so on [3]. The BPCS is responsible to operate functions required for production within its normal operating range. If the BPCS fails to maintain control

strategies, alarms will indicate a problem that the operator intervention is needed to reestablish control within specified limits. If the operator cannot make the specified corrections, the SIS must take actions to bring the process to safe conditions and mitigate the hazards. In order to avoid common cause faults and reduce systematic error, the BPCS and the SIS must be completely independent [4]. These two systems are designed and implemented to meet different risk reduction requirements, so there is a large gap between the high-level safety provided by the BPCS and that provided by the SIS. As the advances in technology continued, however, end users can employ digital fieldbus technologies to fill this void by improving the response of the BPCS to failures [5-8]. There are various failure modes applicable to the BPCS such as process variable indication erratic, control output frozen, and control output indication saturated low [4]. Because the process control loop

136

operates with signals that are relative dynamic, these failures can then be detectable by diagnostic and measurement validation methods. However, level of self-diagnostics and method of self-validation for field devices vary greatly by manufacturer. The capabilities of digital field instruments used within the process industry sector such as PROFIBUS PA and Foundation Fieldbus (FF) are based on function blocks for performing the monitoring and control applications [9]. The function blocks are logical grouping of variables, parameters, and their execution algorithms that are defined to meet specific functionality requirements. The major difference between PROFIBUS PA and FF is that no control function blocks are available in PROFIBUS PA field devices. Only the FF specification has the ability to perform control functionality distributed into the field instruments, which is called 'Control in the Field' (CIF). Because of its decentralized feature, the CIF provides various performance benefits such as improved control loop performances, increased reliability and availability, and reduced loading on the network and host system [10]. The CIF shall be utilized for building the basic proportional-integral-derivative (PID) and cascade control loops when installing all field devices associated the loop within the same segment [11].

Based on the ability to report the diagnostic and measurement validity data, the FF-based BPCS can perform its function that is targeted toward either high level of process safety or high degree of production availability in the event of instrument failures. The safety and availability are generally two conflicting purposes for the BPCS [12]. In order to enhance process safety, the affected control loops must be shut down in the presence of a fault for preventing hazards or equipment damages. On the other hand, the affected control loops must be able to execute even in case of failure for reducing losses of raw materials and finished products to increase production availability.

When embarking on a greenfield or brownfield project, the project stakeholders must understand the benefits of the fieldbus technology used and how it can be employed to transform the plant operations. Although standardized technology, FF is based on relatively complex concepts such as instrumentation, data communications, computerized automation controllers, and engineering software, thus it has a slow learning curve [13]. In shortening the time for the implementation phase of project work, a useful suggestion on using FF function blocks to enable failure-safe mechanism for safe loop action of the

PID control is reported [14]. Nevertheless, there are no experimental results that confirm this proposed suggestion. A practical guideline for configuring FF function blocks to create the cascade control with high system safety is also introduced in an author's previous work [15], which proves that different configurations of three groups of function block options (including status options, control options, and input/output options) affect the cascade control loop actions in the event of device failure. However, the mode shedding and return upon fault recovery of the function blocks are not examined.

In this paper, the logical behaviors of PID and cascade control loops using FF with CIF are intensively investigated in detail in terms of safety and availability improvements during control strategy and device configuration in order to realize the configuration method for proper operations to provide the required safety and availability attributes. A case study for building the interested control strategies with different function block options is the level control of water tank process, which consists of three FF H1 field instruments. More specifically, not only the interactions between status propagation and operating mode shedding, but also the fault recovery of interested control loops in response to transmitter failures are represented using Petri net models.

This paper is organized into six sections. After this introduction, Section 2 briefly describes how to create the basic control loops using FF with CIF. Section 3 and Section 4 provide the details of water tank process used as a case study and the experimental analysis in case study, respectively. Section 5 gives the results and discussion. Finally, Section 6 summarizes the content and purpose of this article.

2. Basic process control using FF with CIF

2.1 FF function blocks

Function blocks within FF field devices perform various functions required in a process monitoring and control system such as analog input (AI) and analog output (AO) functions as well as PID function. The FF-based control strategies then can be created by selecting, linking, and parameterizing the function blocks. The Fieldbus Foundation (recently become FieldComm Group) has published specifications of function blocks to provide a common structure for defining block elements (such as inputs, outputs, modes, scaling information, and back calculation), whereby, the Foundation does not
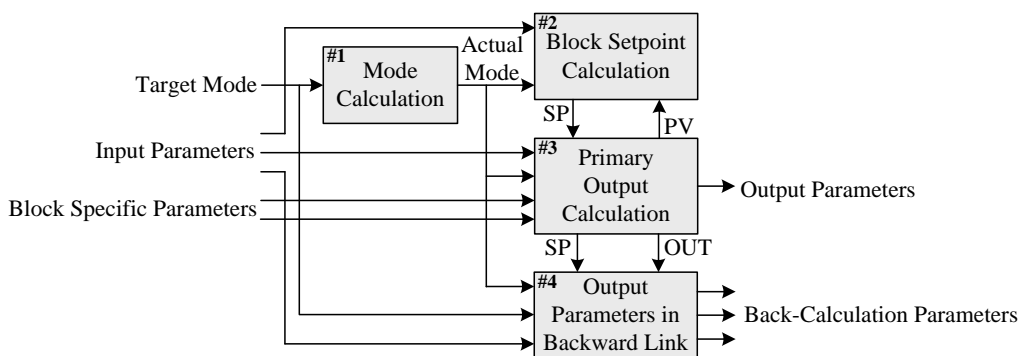
Figure.1 Basic processing sequence of function blocks

define how each device manufacturer is to realize the block execution algorithms to complete the functions [16-17]. This allows the manufacturers to differentiate their product for expanding competitive advantage such as increased device diagnostics.

Fig. 1 shows a basic processing sequence of FF function blocks, which can be divided into four steps as follows.

1) Determine the actual block mode.
2) Calculate the block setpoint (SP).
3) Execute the block algorithm to generate output parameters in the forward path.
4) Calculate the output parameters in the backward path.

The target mode indicates what mode of operation is desired for the block, while the actual mode reflects the mode of operation that the block is able to achieve. Comparison of the actual mode against the target mode indicates whether the target mode was obtained. In addition, the actual mode may change without operator intervention during the events of error conditions, which is called 'mode shedding' [12]. Table 1 summarizes the effect of mode on the operation of function blocks [16].

2.2 PID and cascade control loops

Fig. 2 shows the function block diagrams for implementing PID and cascade control strategies with CIF concept. The PID control loop is configured by using three function blocks; AI, PID, and AO. The cascade control loop is created by utilizing five function blocks; two AI blocks, two PID blocks, and one AO block. These function blocks are sequentially executed. The AI function blocks are assigned to the measuring devices, while
the AO function block is located in the final control element. The PID blocks can be in the measuring devices or the final control element. However, their locations have implication on loading of the communications network. With the aim of reducing the number of scheduled communications between

field devices, the PID function blocks are preferably placed in the final control element [18-19]. Table 2 and Table 3 illustrate the operation and normal mode of the function blocks used in the PID and cascade control loops as shown in Fig. 2(a) and Fig. 2(b), respectively. The normal mode is typically used by a human interface application to help guide the process engineer or plant operator in setting the desired target mode of the block during normal operation.

Table 1. Effect of mode on the block operation

| Mode	Description
Out of Service (O/S)	Block execution is disabled.
Initialization Manual (IMan)	Block output (OUT) parameter is being set in response to the status of the back-calculation input (BKCAL_IN) parameter.
Local Override (LO)	This mode applies to control and output class blocks that support a track value input (TRK_VAL) parameter. The OUT is set to track the value of the TRK_VAL.
Manual (Man)	The OUT is set by the operator through an interface device.
Automatic (Auto)	The block setpoint (SP) is set by the operator. The block itself calculates the value of the OUT.
Cascade (Cas)	The block SP is received from the upper function block through the cascade setpoint input (CAS_IN) parameter. The block itself calculates the value of the OUT.
Remote-Cascade (RCas)	The block SP is received from another application through the remote cascade setpoint input (RCAS_IN) parameter. The block itself calculates the value of the OUT.
Remote-Output (ROut)	The block OUT is received from another application through the remote output input (ROUT_IN) parameter.

(a)

(b)
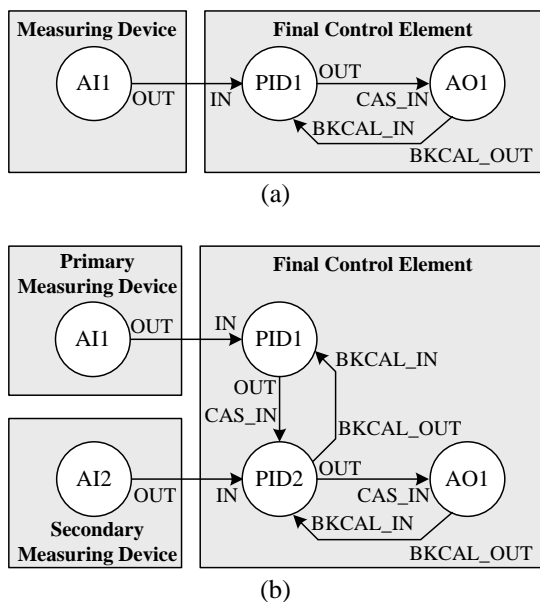
Figure.2 Function block diagrams for CIF applications:
(a) PID control and (b) cascade control

Table 2. Operation and normal mode of the blocks used
in PID control loop of Fig. 2(a)

Block	Operation	Normal mode
AI1	Processing measurement data received from the transducer block to be available for the PID1.	Auto
PID1	Receiving the operator-entered setpoint and the AI1 output, and calculating the block output.	Auto
AO1	Processing the PID1 output, and passing to the transducer block for manipulating the process.	Cas

Table 3. Operation and normal mode of the blocks used
in cascade control loop of Fig. 2(b)

Block	Operation	Normal mode
AI1	Processing measurement data received from the transducer block of the primary transmitter to be available for the PID1.	Auto
AI2	Processing measurement data received from the transducer block of the secondary transmitter to be available for the PID2.	Auto
PID1	Receiving the operator-entered setpoint and the AI1 output, and calculating the block output.	Auto
PID2	Receiving the block cascade setpoint and process variable from the PID1 and the AI2, respectively, and determining the block output.	Cas
AO1	Processing the PID2 output, and passing to the transducer block for manipulating the process.	Cas

3. Case study on water tank process

Fig. 3 illustrates a schematic diagram of the FF-based water tank process connected with the DeltaV host system, which is used as a case study in this paper. There are three FF field devices installed in H1 segment with tree topology at the field-level network running at 31.25 kbps. The LIT_101 level transmitter is used to measure the water level in the tank, whereas the FIT_101 flow transmitter is employed to measure the volume flowrate of water through the inlet pipe. The FCV_101 control valve is used as the final control element to regulate the fluid flow. Table 4 shows the details of the FF H1 field instruments used including physical device tag, vendor, model, device revision, numbers of AI, PID, and AO function blocks resided in the device, and block execution time. The DetlaV host system connected on the control network running at 100 Mbps is utilized for device and control configuration, device commissioning, and segment operation.

Based on the function block diagrams for configuring the control loops of Fig. 2, Table 5 summarizes the function block assignments to the H1 field instruments used in the PID and cascade control loops. In order to control the water level in the tank by using PID control strategy, only the LIT_101 level transmitter and the FCV_101 control valve are configured in the control loop. In the case of level-to-flow cascade control strategy, the LIT_101 level transmitter and FIT_101 flow

Table 4. Details of H1 field devices used in Fig. 3

Device Tag	LIT_101	FIT_101	FCV_101
Vendor	Yokogawa	EMP	Azbil
Model	EJX110A	8732E	AVP303
Revision	3	2	2
AI count	3	1	-
AI time	30 ms	10 ms	-
PID count	1	1	2
PID time	45 ms	10 ms	125 ms
AO count	-	-	1
AO time	-	-	75 ms

Table 5. Function block assignments to the instruments

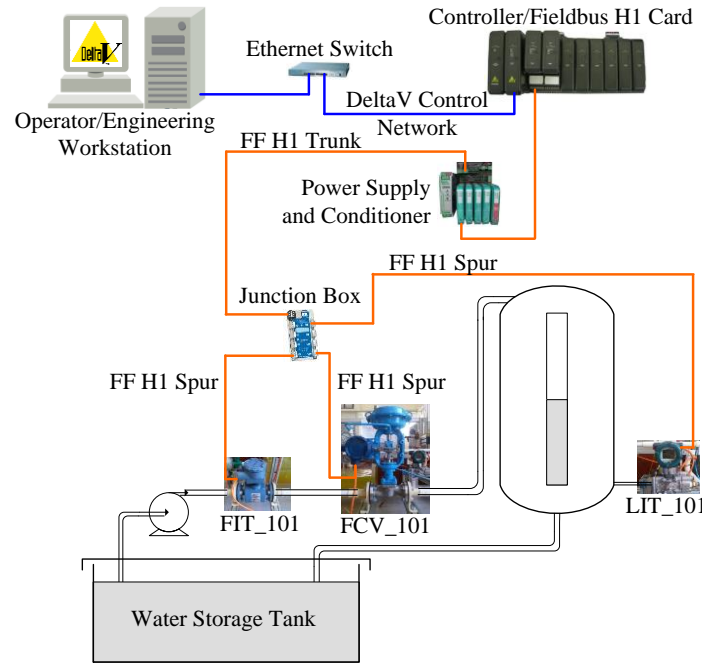| Control Loop	Block	Instrument
PID	AI1	LIT_101
	PID1	FCV_101
	AO1	FCV_101
Cascade	AI1	LIT_101
	AI2	FIT_101
	PID1	FCV_101
	PID2	FCV_101
	AO1	FCV_101

Figure.3 Schematic diagram of the water tank process connected with the DeltaV host system

transmitter are used as the primary and secondary measuring devices, respectively. Because of supporting two PID function blocks resident in the device, both primary and secondary PID blocks are located in the FCV_101 control valve.

4. Experimental analysis in case study

4.1 Interested function block options

Input and output parameters of FF function blocks consist of two elements; value and status. The parameter status contains additional validation information about the value for indicating hardware, communication, configuration, and other fault. The quality portion of the status element is 'Good', 'Bad', or 'Uncertain' to identify the general validity of the value. For example, the 'Good' quality means that the value may be used for control. The 'Bad' with substatus of 'Device failure' means that the associated output hardware has failed, and the 'Bad' with substatus of 'Sensor failure' means that the associated sensor has failed. The 'Uncertain' quality means the value is questionable, when the measured value is out of measurement range or inaccurate for some reason.

As observed in [15], there are three groups function block options that at detailed system design time allow the interests of safety and availability to be specified with respect to failures; status options, control options, and input/output options. The status options in the function blocks provide options for

handling and processing the block output status, whereas the control options allow the behavior of the control class function blocks like PID block to be customized. The input/output options activate the options for processing the input and output values of

Table 6. Interested status options in AI block

Option	Description
Uncertain if Limited	Set the output status to 'Uncertain' if the measured value is higher or lower than the sensor limits.
Bad if Limited	Set the output status to 'Bad' if the measured value is higher or lower than the sensor limits.
Uncertain if Man mode	Set the output status to 'Uncertain' if the actual mode of the block in Man.

Table 7. Interested status options in PID block

Option	Description
IFS if BAD IN	Set 'Initiate Fault State' status in the OUT parameter if the status of the IN parameter is BAD.
IFS if BAD CAS_IN	Set 'Initiate Fault State' status in the OUT parameter if the status of the CAS_IN parameter is BAD.
Use Uncertain as Good	If the status of the IN parameter is Uncertain, consider it as Good. (0: status handled as Bad, 1: status handled as Good).
Target to Manual if BAD IN	Set the target mode to Man if the status of the IN parameter is BAD. This handles the block into Man mode if the IN ever goes BAD.

Table 8. Interested control options in PID block

Option	Description
Bypass Enable	Allow 'BYPASS' to be set. Some control applications cannot perform closed-loop control if bypassed.
SP-PV Track in Man	Permit the setpoint (SP) to track the process variable (PV) when the target mode of the block is Man.
SP-PV Track in LO or IMan	Permit the SP to track the PV when the actual mode of the block is LO or IMan.

Table 9. Interested input/output options in AO block

Option	Description
SP-PV Track in Man	Permit the SP to track the PV when the target mode of the block is Man.
SP-PV Track in LO	Permit the SP to track the PV when the actual mode of the block is LO.
Fault State to value	Determine the output operation to take when a fault occurs (0: freeze the last value, 1: go to preset value).
Use Fault State value on restart	Use the value of FSTATE_VAL parameter if the device is restarted. Otherwise use the final output value restored in non-volatile memory.
Use PV for BKCAL_OUT	The value of BKCAL_OUT parameter is normally the working SP. This option changes it to the PV.

the function blocks. The interested options to be set in the AI, PID, and AO function blocks used for creating control loops in our experiments are summarized in Tables 6-9.

4.2 Bumpless transfer and setpoint tracking

For feedback control loops, a change in the controller operation mode from manual (Man) to automatic (Auto), or from Auto to Man, should be made without suddenly changing the position of the final control element, which is called 'bumpless transfer' [20]. One procedure that obtains bumpless transfer involves setpoint tracking. The built-in setpoint tracking options such as 'SP-PV Track in Man' are available in the PID and AO blocks as shown in Tables 8-9, respectively.

In the PID control loop (See Fig. 2a), the PID1 block obtains the operator-entered setpoint (SP). Its IN parameter, the process variable (PV), is linked to the OUT parameter of the AI1 block, while its OUT parameter is linked to the CAS_IN and becomes the AO1 block setpoint for subsequently controlling the control valve positioner. Similarly, the desired valve position is the SP, and the actual valve position is the

PV. The BKCAL_OUT parameter of the AO1 block is backward linked to the BKCAL_IN parameter of the PID1 block. This backward link is used to initialize its output to prevent reset windup as well as to provide bumpless return from Man to Auto mode. If the control valve is hand-operated, the actual mode of the AO1 block is not its usual cascade (Cas) mode. This is informed to the PID1 block through the backward BKCAL_OUT-BKCAL_IN link. Additionally, if the input/output option 'Use PV for BKCAL_OUT' is set in the AO1 block, thus the actual stem position, the process variable, is used for the BKCAL_OUT parameter. The status of the AO1 block feedback link will force the actual mode of the PID1 block into initialization manual (IMan). This initialization mechanism not only assures the bumpless transfer, but also prevents the reset windup of the PID1 block in the event that the valve stem is limited with hardware or software.

In the cascade control loop (See Fig. 2b), this mechanism is extended to the secondary PID2 block to the primary PID1 block. The BKCAL_OUT from the PID2 block is sent to the BKCAL_IN of the PID1 block. If actual mode of the secondary PID2 block is not Cas mode (for example, in Auto). The BKCAL_OUT-BKCAL_IN feedback link will force the actual mode of the primary PID1 block into IMan, and its setpoint is then forced to follow the process variable, if the 'SP-PV Track in LO or IMan' is enabled. Moreover, when the PID1 actual mode is IMan, it also initializes its OUT parameter to the value of BKCAL_IN, which is the same value as the secondary PID2 setpoint. This prevents reset windup of the primary PID1 block. In consequent, the CAS_IN of the PID2 block will be identical to its own SP value. As a result, any time the PID2 block mode is switched back to Cas mode, there will be no bump. Therefore, the initialization mechanism can provide the procedure that obtains bumpless transfer during operation mode switches.

With the purpose of providing bumpless transfer and setpoint tracking, Table 10 summarizes the enabled function block options for configuring the PID and cascade loops with CIF in experiments.

4.3 PID control with CIF architecture

4.3.1 Improving Safety

For safety purpose, the PID control must be shut the process down in case of failure. In order to enhance process safety in response to invalid measurements, two safe actions by setting the function block options as given in Table 11 are defined as follows.

Table 10. Enabled options for bumpless transfer and setpoint tracking of PID and cascade controls with CIF

Loop	Block	Parameter	Option
PID	PID1	CONTROL_OPTS	SP-PV Track in Man
			SP-PV Track in LO or IMan
	AO1	IO_OPTS	SP-PV Track in Man
			SP-PV Track in LO
			Use PV for BKCAL_OUT
Cas-cade	PID1, PID2	CONTROL_OPTS	SP-PV Track in Man
			SP-PV Track in LO or IMan
	AO1	IO_OPTS	SP-PV Track in Man
			SP-PV Track in LO
			Use PV for BKCAL_OUT

Table 11. Enabled block options for improving safety of the PID control with CIF

Block	Parameter	Option
AI1	STATUS_OPTS	Uncertain if Limited
		Bad if Limited
		Uncertain if Man mode
PID1	STATUS_OPTS	IFS if BAD IN
		Target to Manual if BAD IN
AO1	IO_OPTS	Fault State to value
		Use Fault State value on restart

1) The 'Uncertain' status quality of the LIT_101 transmitter is used to switch the PID control loop to Man mode of operation by freezing the FCV_101 control valve in the last position. After the problem has been fixed, the PID loop can continue its control function immediately.

2) The 'Bad' status quality of the LIT_101 transmitter is utilized to bring the FCV_101 control valve to its predetermined safe position. After the failure has been fixed, the PID loop remains the 'failed' state in Man mode of operation (by using the fault state value as the initial value for restarting the FCV_101 valve) until the operator unlocks by changing the PID1 block to operate in Auto mode.

4.3.2 Improving Availability

For availability goal, the PID control loop must be able to perform even in the presence of failure. However, it is not possible to automatically control the process if the information of measurement validity is 'Bad', and this 'Bad' information always shuts the control loop down. But, it is possible to maintain the automatic control by using the 'Uncertain' status quality such as measurement

readings are slightly out of range for improving availability.

With the intention of increasing availability in response to invalid measurements, two actions by enabling 'Use Uncertain as Good' status option in the PID1 block only are specified as follows.

1) The 'Uncertain' status quality of the LIT_101 transmitter is treated as 'Good' status, and the PID1 block is operated in Auto mode. Thus the water level in the tank is still automatically controlled by the control loop.

2) The 'Bad' status quality of the LIT_101 level transmitter is used to switch the PID1 block from Auto mode to Man mode by freezing the FCV_101 valve in the last position. After the fault has been solved, the PID loop can resume control instantly.

4.4 Cascade control with CIF architecture

4.4.1 Improving Safety

For improving process safety in response to invalid primary and secondary measurements of the CIF-based cascade control, four actions by setting the function block options in Table 12 are specified as follows.

1) The 'Uncertain' status quality of the LIT_101 level transmitter is used to switch the primary PID1 block to Man mode by freezing its OUT parameter, driving the setpoint of the secondary PID2 block, in the last value, while the secondary flow control loop can be still performed. After the problem has been fixed, the primary PID1 block can return to operate in Auto mode instantly.

2) The 'Bad' status of the LIT_101 transmitter is employed to switch the primary PID1 block to Man mode by freezing its OUT parameter loop can be still operated. After the problem has been solved, the primary PID1 block remains its operation in Man mode by setting the fault state value as the initial

Table 12. Enabled block options for improving safety of the cascade control with CIF

Block	Parameter	Option
AI1, AI2	STATUS_OPTS	Uncertain if Limited
		Bad if Limited
		Uncertain if Man mode
PID1	STATUS_OPTS	Target to Manual if BAD IN
PID2	STATUS_OPTS	IFS if BAD IN
		IFS if BAD CAS_IN
		Target to Manual if BAD IN
AO1	IO_OPTS	Fault State to value
		Use Fault State value on restart

Table 13. Enabled block options for enhancing availability of the cascade control with CIF

Block	Parameter	Option
PID1	STATUS_OPTS	Use Uncertain as Good
PID2	STATUS_OPTS	Use Uncertain as Good
	CONTROL_OPTS	Bypass Enable

position for restarting the FCV_101 control valve. Until the operator changes the target mode of the primary PID1 block to Auto mode, the cascade control loop is then returned to its normal operation.

3) The 'Uncertain' status quality of the FIT_101 flow transmitter is used to switch the secondary PID2 block to Man mode by freezing its OUT parameter, driving the setpoint of the AO1 block, in the last value. After the fault has been corrected, the secondary control loop can continue its operation immediately.

4) The 'Bad' status quality of the FIT_101 flow transmitter is utilized to switch the target mode of the secondary PID2 block from Cas mode to Man mode and to bring the FCV_101 control valve to its predetermined safe position. After the failure has been fixed, the PID2 block remains in Man mode of operation by using the fault state value as the initial position for restarting the FCV_101 control valve. Until the operator changes the PID2 block target mode to Cas mode, the cascade control loop is returned to its regular function.

4.4.2 Improving Availability

With the aim of enhancing process availability in response to invalid primary and secondary measurements from the measuring devices of the cascade control with CIF, three actions by enabling the function block options as summarized in Table 13 are defined as follows.

1) The 'Uncertain' status quality of the LIT_101 and FIT_101 transmitters is considered as 'Good' status, and the water level in the tank can be still automatically controlled by the cascade loop.

2) The 'Bad' status quality of the LIT_101 level transmitter is used to switch the primary PID1 block to Man mode by freezing its OUT parameter in the last value, while the secondary flow control loop can be still operated. After the problem has been solved, the primary PID1 block can return to operate in Auto mode immediately.

3) The 'Bad' status quality of the FIT_101 flow transmitter is utilized to switch the secondary PID2 block from CAS mode to Man mode by freezing the FCV_101 control valve in the last position. After the fault has been corrected, the secondary PID2 block returns back to CAS mode, thus the primary level control loop can continue its function instantly.

5 Results and discussion

In order to investigate the interlocks between function blocks as well as the initialization and fail-safe mechanisms in PID and cascade control loops using FF with CIF, many experiments were conducted in four different parameter configurations as discussed in Section 4 for controlling the water level in the tank of Fig. 3 in case study. In experiments, the air tube of the LIT_101 pressure sensor input and the power supply of the water pump were turned off to mimic the failures for 'Uncertain' status of the AI1 and AI2 function blocks, respectively. The FF H1 spur cables of the LIT_101 and FIT_101 transmitters were taken off from the junction box to mimic the failures for 'Bad' status of the AI1 and AI2 blocks, respectively. The experimental results were analyzed to examine how different configuration options affect the safety and availability improvements of the studied control loops.

Fig. 4 shows the simple Petri net models for representing the logical behaviors of the interested PID control loop of Fig. 2(a) in response to measurement validation information. Their place (P) and transition (T) descriptions are given in Table 14, where the input place 'P₁' is the initial state of the system, and the transition 'T₁' is enabled by the arc 'Status of AI1 OUT'. As depicted in Fig. 4(a), the model displays the status propagation and mode

(a)   (b)

Figure.4 Simple Petri net models for representing behaviors of the FF-based PID control loop: (a) with increased safety and (b) with increased availability

Table 14. Descriptions of the places and transitions of Figs. 4(a) and 4(b)

| Fig.4(a) for PID control with increased safety		Fig. 4(b) for PID control with increased availability	
Item	Description	Item	Description
P_1	Control loop is configured using function block options discussed in Sections 4.2 and 4.3.1	P_1	Control loop is configured using function block options discussed in Sections 4.2 and 4.3.2
T_1	If the OUT status of AI1 is 'Good' then P_2. If the OUT status of AI1 is 'Uncertain' then P_3. If the OUT status of AI1 is 'Bad' then P_4.	T_1	If the OUT status of AI1 is 'Good' then P_2. If the OUT status of AI1 is 'Uncertain' then P_2. If the OUT status of AI1 is 'Bad' then P_3.
P_2	Target mode/Actual mode of PID1 is Auto/Auto. Target mode/Actual mode of AO1 is Cas/Cas.	P_2	Target mode/Actual mode of PID1 is Auto/Auto. Target mode/Actual mode of AO1 is Cas/Cas.
P_3	Target mode/Actual mode of PID1 is Auto/Man. Target mode/Actual mode of AO1 is Cas/Cas. For fault recovery, the control loop can resume control immediately.	P_3	Target mode/Actual mode of PID1 is Auto/Man. Target mode/Actual mode of AO1 is Cas/Cas. For fault recovery, the control loop can resume control immediately.
P_4	Target mode/Actual mode of PID1 is Man/IMan. Target mode/Actual mode of AO1 is Cas/LO. Fail-safe action is active to predefined safe value. For fault recovery, the process remains 'failed' state until the operator unlocks.		
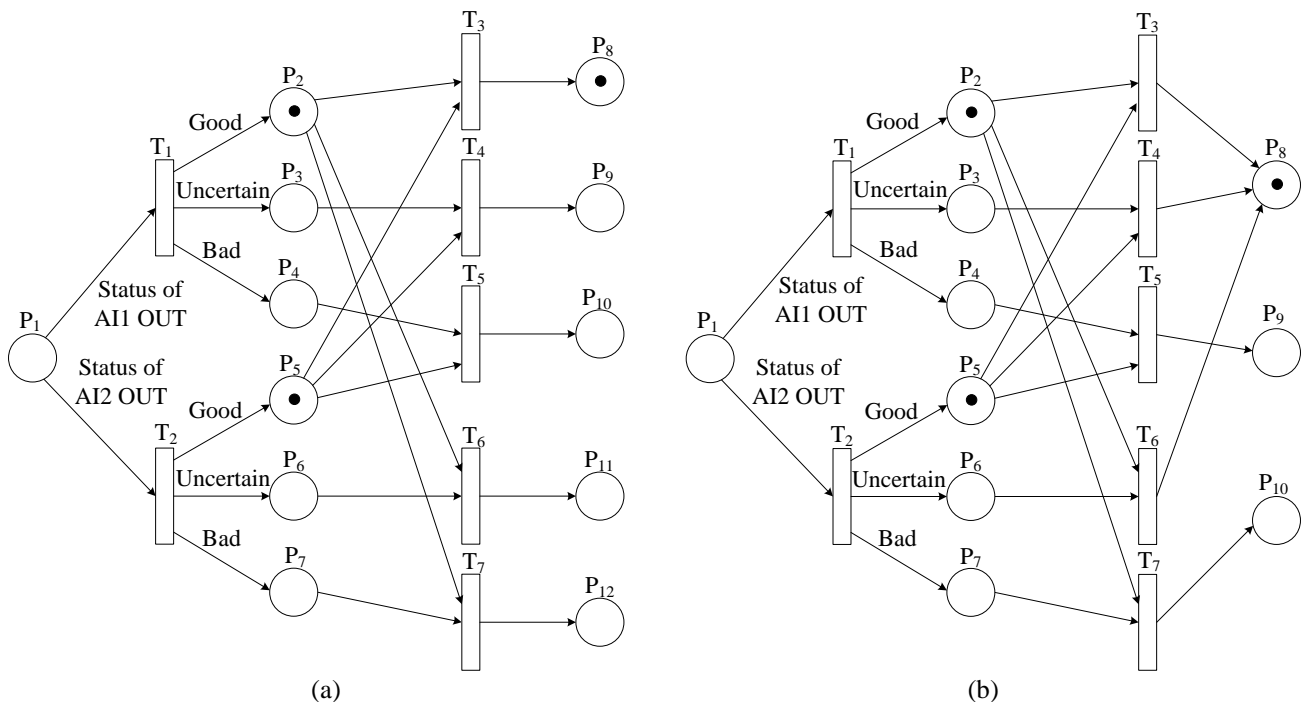
Figure.5 Simple Petri net models for representing behaviors of the FF-based cascade loop: (a) with increased safety and (b) with increased availability

shedding of the FF-based PID loop with increased safety. It is seen that the output places of the transition 'T_1' (P_2, P_3, and P_4) the do not occur simultaneously, which are agreed with the expected actions as defined in subsection 4.3.1 for responding to the status 'Good', 'Uncertain', and 'Bad' of the OUT parameter of the AI1 block. Similarly, the model of Fig. 4(b) shows the status propagation and mode shedding of the FF-based PID loop with increased availability, which are conformed to the requirements specified in subsection 4.3.2 for enabling 'Use Uncertain as Good' status option. If the

status of the OUT of the AI1 block is 'Uncertain', the system will consider it as 'Good' status.

In the case of the interested cascade control loop of Fig. 2(b), its logical behaviors in response to measurement validation results are represented by the simple Petri net models as illustrated in Fig. 5. The descriptions of their places and transitions are summarized in Table 15, where the input place 'P_1' is the initial state of the loop, and the transitions 'T_1' and 'T_2' are let by the arcs 'Status of AI1 OUT' and 'Status of AI2 OUT', respectively. The output places of the transition 'T_1' (P_2, P_3, and P_4) as well as the

144

Table 15. Descriptions of the places and transitions of Figs. 5(a) and 5(b)

Fig. 5(a) for cascade control with increased safety		Fig. 5(b) for cascade control with increased availability	
Item	Description	Item	Description
P_1	Control loop is configured using function block options discussed in Sections 4.2 and 4.4.1	P_1	Control loop is configured using function block options discussed in Sections 4.2 and 4.4.2
T_1	If the OUT status of AI1 is 'Good' then P_2. If the OUT status of AI1 is 'Uncertain' then P_3. If the OUT status of AI1 is 'Bad' then P_4.	T_1	If the OUT status of AI1 is 'Good' then P_2. If the OUT status of AI1 is 'Uncertain' then P_3. If the OUT status of AI1 is 'Bad' then P_4.
T_2	If the OUT status of AI2 is 'Good' then P_5. If the OUT status of AI2 is 'Uncertain' then P_6. If the OUT status of AI2 is 'Bad' then P_7.	T_2	If the OUT status of AI2 is 'Good' then P_5. If the OUT status of AI2 is 'Uncertain' then P_6. If the OUT status of AI2 is 'Bad' then P_7.
P_2	The OUT status of AI1 is 'Good'.	P_2	The OUT status of AI1 is 'Good'.
P_3	The OUT status of AI1 is 'Uncertain'.	P_3	The OUT status of AI1 is 'Uncertain'.
P_4	The OUT status of AI1 is 'Bad'.	P_4	The OUT status of AI1 is 'Bad'.
P_5	The OUT status of AI2 is 'Good'.	P_5	The OUT status of AI2 is 'Good'.
P_6	The OUT status of AI2 is 'Uncertain'.	P_6	The OUT status of AI2 is 'Uncertain'.
P_7	The OUT status of AI2 is 'Bad'.	P_7	The OUT status of AI2 is 'Bad'.
T_3	If both P_2 and P_5 are true then P_8.	T_3	If both P_2 and P_5 are true then P_8.
T_4	If both P_3 and P_5 are true then P_9.	T_4	If both P_3 and P_5 are true then P_8.
T_5	If both P_4 and P_5 are true then P_{10}.	T_5	If both P_4 and P_5 are true then P_9.
T_6	If both P_2 and P_6 are true then P_{11}.	T_6	If both P_2 and P_6 are true then P_8.
T_7	If both P_2 and P_7 are true then P_{12}.	T_7	If both P_2 and P_7 are true then P_{10}.
P_8	Target mode/Actual mode of PID1 is Auto/Auto. Target mode/Actual mode of PID2 is Cas/Cas. Target mode/Actual mode of AO1 is Cas/Cas.	P_8	Target mode/Actual mode of PID1 is Auto/Auto. Target mode/Actual mode of PID2 is Cas/Cas. Target mode/Actual mode of AO1 is Cas/Cas.
P_9	Target mode/Actual mode of PID1 is Auto/Man. Target mode/Actual mode of PID2 is Cas/Cas. Target mode/Actual mode of AO1 is Cas/Cas. For fault recovery, the control loop can resume control immediately.	P_9	Target mode/Actual mode of PID1 is Auto/Man. Target mode/Actual mode of PID2 is Cas/Cas. Target mode/Actual mode of AO1 is Cas/Cas. For fault recovery, the control loop can resume control immediately.
P_{10}	Target mode/Actual mode of PID1 is Man/Man. Target mode/Actual mode of PID2 is Cas/Cas. Target mode/Actual mode of AO1 is Cas/Cas. For fault recovery, the process remains 'failed' state until the operator unlocks.	P_{10}	Target mode/Actual mode of PID1 is Auto/IMan. Target mode/Actual mode of PID2 is Cas/Man. Target mode/Actual mode of AO1 is Cas/Cas. For fault recovery, the control loop can resume control immediately.
P_{11}	Target mode/Actual mode of PID1 is Auto/IMan. Target mode/Actual mode of PID2 is Cas/Man. Target mode/Actual mode of AO1 is Cas/Cas. For fault recovery, the control loop can resume control immediately.		
P_{12}	Target mode/Actual mode of PID1 is Auto/IMan. Target mode/Actual mode of PID2 is Man/IMan. Target mode/Actual mode of AO1 is Cas/LO. Fail-safe action is active to predefined safe value. For fault recovery, the process remains 'failed' state until the operator unlocks.		

output places of the transition 'T₂' (P_5, P_6, and P_7) do not happen concurrently. The models in Figs. 5(a) and 5(b) depict the status propagation and modeshedding of the FF-based cascade loop with increased safety and the FF-based cascade control with increased availability, respectively, which are in good agreement of the expected actions for improving safety and availability as discussed in subsection 4.4.

Experimental results obtained from both control loops verify that the capacity for detecting device failures and the parameter options for handling measurement status provide the user the ability to improve the safety and availability. The FF H1 field devices with self-diagnostic and self-validation capabilities can distinguish between less serious problems and serious problems by notifying 'Uncertain' and 'Bad' status, respectively. The 'Uncertain' status can be configured to be treated either as 'Good' to continue the process for availability reason or as 'Bad' to shut down the process (or to bring the control to manual of

Table 16. Enabled parameter options for balancing the interests of safety versus availability

Loop	Block	Parameter	Option	Safety	Availability
PID	AI1	STATUS_OPTS	Uncertain if Limited	√	
			Bad if Limited	√	
			Uncertain if Man mode	√	
	PID1	STATUS_OPTS	IFS if BAD IN	√	
			Target to Manual if BAD IN	√	
			Use Uncertain as Good		√
	AO1	IO_OPTS	Fault State to value	√	
			Use Fault State value on restart	√	
Cascade	AI1, AI2	STATUS_OPTS	Uncertain if Limited	√	
			Bad if Limited	√	
			Uncertain if Man mode	√	
	PID1	STATUS_OPTS	Target to Manual if BAD IN	√	
			Use Uncertain as Good		√
	PID2	STATUS_OPTS	IFS if BAD IN	√	
			IFS if BAD CAS_IN	√	
			Target to Manual if BAD IN	√	
			Use Uncertain as Good		√
		CONTROL_OPTS	Bypass Enable		√
	AO1	IO_OPTS	Fault State to value	√	
			Use Fault State value on restart	√	

operation) for safety reason. This makes it possible to be selective when balancing process safety against production availability for each individual control loop. In addition, the fail-safe shutdown for the 'Bad' status can be obtained. The actual mode of the PID block becomes 'Man' mode to stop automatic control, and the control valve positioner becomes 'Initiate Fault State' status to bring it to its preset fail-safe position (or 'Fault State to value'). Moreover, there are options for deciding the fault recovery by using the 'Target to Manual if BAD IN'. By not enabling this option, the affected loop can resume control instantly after the fault has been fixed to achieve higher availability, whereas by enabling this option, the affected loop can remain the 'failed' state in 'Man' mode until the operator changes to 'Auto' mode to obtain higher safety.

Table 16 summarizes the function block options to strike the appropriate balance between safety and availability for the PID and cascade loops using FF with CIF. The safety and availability improvements of FF-based basic control strategies can be conveniently performed by configuring function block options to provide the desired actions.

6   Conclusion

To achieve the real benefits of FF technology based on powerful function blocks resided in field devices, improving the safety and availability of the PID and cascade control loops with CIF has been described in this paper. How different parameter option configurations affect the function block interlocks as well as the initialization and fail-safe mechanisms of the interested control loops has been analyzed. Based on experimental results, the interactions between status propagation and operating mode shedding and the fault recovery of two studied control loops have been represented by the Petri net models. The proved configuration method for achieving appropriate balance between process safety against production availability for the FF-based PID and cascade control with CIF has been proposed. The reliability of these process control strategies needs to be evaluated in a future work.

Acknowledgments

References

[1] W. M. Goble, *Control Systems Safety Evaluation and Reliability*, ISA Press, USA, 2010.

[2] IEC (International Electrotechnical Commission), *IEC61511-1: Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definition, System, Hardware and Software Requirements*, pp.32-37, 2003.

[3] T. Vollmer, K. Borcherding, G. Hellriegel, and R.-D. Penzhorn, "Process Control under Safety

Aspects", *Fusion Engineering and Design*, Vol.48, No.1-2, pp.57-61, 2000.

[4] W. M. Goble and H. Cheddie, *Safety Instrumented System Verification: Practical Probabilistic Calculations*, ISA Press, USA, 2005.

[5] A. Schimanski, "Application Experiences with Fieldbus Instruments", *ISA Transactions*, Vol.35, No.2, pp.137-145, 1996.

[6] S. Cavalieri, O. Mirabella, and S. Monforte, "Enhancing Reliability in IEC/ISA Fieldbus", *Computer Standards & Interfaces*, Vol.21, No.3, pp.217-240, 1999.

[7] R. Dettmer, "Self Validation in Process Control", *IEE Review*, Vo.46, No.4, pp.29-32, 2000.

[8] B. G. Liptak, *Instrument Engineers' Handbook: Process Control and Optimization*, CRC Press in Cooperation with ISA Press, USA, 2006.

[9] C. Diedrich, F. Russo, L. Winkel, and T. Blevins, "Function Block Applications in Control Systems Based on IEC61804", *ISA Transactions*, Vol.43, No.1, pp.123-131, 2004.

[10] ARC Advisory Group, "The Business Value Proposition of Control in the Field", *ARC White Paper*, pp.1-20, 2009.

[11] Fieldbus Foundation, *AG-181: Foundation Fieldbus System Engineering Guidelines*, Rev. 3.2.1, USA, 2012.

[12] J. Berge, *Fieldbuses for Process Control: Engineering, Operation and Maintenance*, ISA Press, USA, 2004.

[13] E. A. Mossin, R. P. Pantoni, and D. Brandao, "A Fieldbus Simulator for Training Purposes", *ISA Transactions*, Vol.43, No.1, pp.132-141, 2009.

[14] J. Chen, Z. Wang, and Y. X. Sun, "How to Improve Control System Performance Using FF Function Blocks", In: *Proc. of the IEEE International Conference on Control Applications*, Scotland, U.K., pp.1022-1026, 2002.

[15] P. Yimvuthipong, A. Rerkratn, T. Trisuwan-nawat, P. Julsereewong, and A. Julsereewong, "How to Fully Benefit from Function Blocks of Foundation Fieldbus for Digital Cascade Control with High System Safety", In: *Proc. of The International Conference on Industrial Application Engineering*, Kitakyushu, Japan, pp.124-131, 2015.

[16] Fieldbus Foundation, *FF-890-1.10: Foundation Specification-Function Block Application Process*, Part 1, USA, 2012.

[17] Fieldbus Foundation, *FF-891-1.10: Foundation Specification-Function Block Application Process*, Part 2, USA, 2012.

[18] A. Julsereewong, P. Julsereewong, and P. Harntujit, "Foundation Fieldbus Segment Scheduling for Fast Loop Controls", *ICIC Express Letters*, Vol.7, No.4, pp.1201-1207, 2013.

[19] T. Sangsuwan, S. Pongswatd, A. Julsereewong, Y. Morioka, and Y. Amano, "Communication Schedule Optimization of Cascade Control using Foundation Fieldbus", *ICIC Express Letters*, Vol.10, No.1, pp.197-204, 2016.

[20] H. L. Wade, *Basic and Advanced Regulatory Control: System Design and Application*, ISA Press, USA, 2004.