A Comparison of Hazards and Efficiencies of Conventional and Adaptive Control Algorithms Using Systems-Theoretic Process Analysis

Sveinung Johan Ohrem[1,*], HyungJu Kim[1], Mary Ann Lundteigen[1] and Christian Holden[1]

[1] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Norway

ABSTRACT

Control systems are an important and increasingly complex part of most industrial and non-industrial systems. As such, identifying and handling associated risks is increasingly important. Systems-Theoretic Process Analysis (STPA) is a relatively new hazard identification method developed to analyze modern, complex control systems. While traditional hazard analysis methods mainly focus on the failures of a system, STPA focuses on interactions among control commands and environmental conditions, so that potential non-failure problems, mainly caused by unsafe control actions, can be identified. Proportional-Integral-Derivative (PID) controllers are the most common conventional controllers (CCs) and are widely used in industry due to their simplicity. PID controllers are tuned for operation and based on the system behaviour, in a certain limited operating region. If the behavior and/or operating region of a system changes over time, the PID controller requires re-tuning to perform as desired and prevent loss of production, or accidents, due to inadequate control. Adaptive controllers (ACs) are able to self-adjust and adapt to changes in the system parameters and operating region, such that the overall control task is performed without the need for continuous re-tuning by an operator. The tuning of an AC is done once, at the time of implementation. This can be very helpful for both the efficiency and the safety of the control system. The interactions between the operator and the control system are reduced when the controller is able to self-adjust, potentially reducing the number of hazards. On the other hand, the complexity of ACs may introduce new kinds of hazards that do not exist when using CCs. In this paper, we compare CCs and ACs from both a control and a safety perspective using STPA. As a test case, we compare the efficiencies and hazards of a CC, and an AC applied to a pipeline-riser system subject to slug flow, a hazardous phenomenon occurring in mixed oil and gas pipes. This phenomenon is difficult to control since the behaviour changes drastically with different flow conditions.

Keywords: STPA; Adaptive Control; Oil and Gas.

1. INTRODUCTION

In the field of control theory and automatic control, the goal is to make a dynamic system behave in a predictable and desired way. There are many examples of dynamic systems: robots, cars, process plants, and economic and biological systems are some. Though quite different in behaviour and nature, all these systems undergo changes over time, and they are subject to changes in their environment. How each change over time occurs and how the systems react to changes in the environment is often possible to control. A dynamic system contains inputs, states and outputs, which are the quantities we can control. If we want the output or state of our system to stay at a certain value (reference) while under the influence of outside disturbances, we must

[*] Corresponding author: +47 93664407, sveinung.j.ohrem@ntnu.no

manipulate the input. This is where we introduce the controller. The controller receives a measurement of the output or state and compares it to the reference value. If there is a deviation, the controller applies an input such that the deviation reduces. This way of control is known as feedback control. The history of feedback control stretches back hundreds of years and is brilliantly summarized in Chapter 2 of Hackl (Hackl, 2012).

In most cases, dynamic systems can be mathematically described by systems of differential equations with different complexities. The numbers of states can differ from one or two to thousands. All dynamic systems are nonlinear and time-varying by nature, but if the nonlinearities are weak and the changes in parameters over time are very slow, we can linearize our system around a desired operating point and assume that our system is linear in this region. A linear controller can be designed for this assumed linear system. One example of a controller used in these cases is the Proportional-Integral-Derivative (PID) controller. The proportional part (P) corrects immediate deviations between the reference and the output, the integral part (I) corrects for past deviations, and the derivative part (D) counteracts predicted future deviations. PID controllers are widely used, and over 90% of all control loops use a PID controller. The derivative part (D), however, is rarely used (Åström & Hägglund, 2001). Thus we consider the PI controller as the conventional controller (CC) in this paper. The popularity of the PI(D) controller may be a result of its simplicity and ease of use. PI(D) controllers have fixed parameters, and the selection of these parameters is called tuning. Numerous tuning rules exist, giving the control designer guidelines as to how to choose the parameters based on the desired performance and response (O'Dwyer, 2009).

If the nonlinearities are strong or we want to operate at several points where the system parameters exhibit large differences, we cannot make the assumption of linear behaviour and thus, our controller needs to cope with the nonlinearities and changes in parameters. A PI(D) controller would have to be re-tuned for the new operating point, which would require some form of interaction (e.g. by an operator.) The nonlinear and time-varying behaviour of dynamic systems triggered the desire for more complex controllers. A controller that is able to learn and adjust to the environment it is currently operating in is called an adaptive controller (AC). This controller is tuned at the time of implementation and self-adjusts to changes as they occur.

Adaptive control was introduced in the 1950s, but due to lack of knowledge and tools to analyse the stability of nonlinear systems and inadequate hardware, the implementation of adaptive controllers in an aircraft led to an accident during a flight test. This caused research on adaptive control to enter a hiatus until the 1970s when the progress made in control theory during the 1960s led to an improved understanding of adaptive control (Åström, 1983). Today, mathematical proofs of stability for adaptive controllers applied to nonlinear systems exist and adaptive control is a broad field of research (Krstic, Kanellakopoulos, & Kokotovic, 1995).

PI(D) and adaptive controllers both have pros and cons related to them. As mentioned, PI(D) controllers are widely used, but their use, and the mathematical proofs for stability are limited to regions around an operating point. With adaptive control we can, at the cost of higher complexity, use the same controller for all operating points. From a control perspective, it is not trivial to decide which solution is better, as this depends on the dynamics of the system and the complexity of the controller. We can compare the deviations present with a PI(D) and an adaptive controller and, as such, get a numerical comparison, but the complexity of the controllers is difficult to put down in numbers. The experience of the control engineer also plays a role. This is why we introduce the safety perspective and the hazards when we evaluate our controllers.

A technique to evaluate the hazards present in the control system is the Systems-Theoretic Process Analysis (STPA) (Leveson & Thomas, 2018), a relatively new hazard identification method developed to analyse modern, complex control systems and based on the Systems-Theoretic Accident Model and Processes (STAMP). The latter was developed by Leveson (2012) and is an accident theory whose main idea is that major accidents in complex and software-intensive sociotechnical systems are not caused by a single failure of a physical component, but by complex interactions among various kinds of control actions, environmental conditions, and system components. Based on the STAMP theory, STPA was developed to analyse hazards of complex control systems with a special focus on control actions and feedbacks in system control architectures. Previous studies have shown that STPA can identify additional hazardous scenarios related to software, system design, the interaction of system components, and human behaviour, as well as the hazardous scenarios that can be identified by the traditional hazard analysis methods (Leveson & Thomas, 2013). Furthermore, STPA has been widely adopted and utilized in many domains and sectors, like aerospace (Ishimatsu et al., 2010; Nakao, Katahira, Miyamoto, & Leveson, 2011), aviation (Allison, Revell, Sears, & Stanton, 2017; Chen, Zhang, Lu, & Tang, 2015), cyber security (Schmittner, Ma, & Puschner, 2016; Young, 2014), subsea operations (Kim, Lundteigen, Hafver, Pedersen, & Skofteland, 2018; Hyungju Kim et al., 2018) and so on.

The purpose of this paper is to compare PI and adaptive controllers from both the control and the safety perspectives. STPA was preferred as the most appropriate method to identify the hazards of the conventional PI control system and the adaptive control system. From the control perspective, we will evaluate if the controller is able to bring the dynamic system to the desired value, and how well the controller tracks the changes in references. The safety perspective will also consider how well the controller tracks the reference since a deviation from the reference usually means a loss of production or ineffective operation. Furthermore, the safety perspective will consider the stability of the two controllers; an unstable controller can cause hazardous behaviour and lead to unsafe interactions between the operators and the control parameters. If the operator provides wrong tuning parameters, the controller may fail, or the performance may be worse than intended. By applying STPA to the control systems, we introduce a new tool for evaluation of control system efficiencies. We also show that the choice of controller affects the number of hazards present in a system. This implies that a hazard evaluation should consider the type of controller used. Furthermore, we show that STPA can be used for this purpose. To the best of the authors' knowledge, an analysis of adaptive and/or PI(D) controllers with STPA has not been carried out.

The paper is organized as follows: Chapter 2 provides a summary on control of pipeline-riser systems subject to slug flow, and it introduces the PI and $\mathcal{L}_1$ adaptive controller. Chapter 3 contains the results from the MATLAB simulations. Chapter 4 contains the STPA analysis while Chapter 5 and Chapter 6 contain the discussion and conclusions respectively.

2. CONTROL OF PIPELINE-RISER SYSTEM SUBJECT TO SLUG FLOW

In multiphase flowlines, riser slug flow occurs if liquid blocks the gas from flowing into the riser. The gas will accumulate in the pipeline, and the pressure will increase until it overcomes that of the liquid column blocking the flow. The liquid column will blow out of the pipeline and into the receiving facility. Riser slugging can cause several problems, including exceeding the capacity of the topside receiving facility, production shut down and damage and stress on the equipment (Hill & Wood, 1994).

Slug catchers can be installed to handle the massive bursts of liquid caused by slug flow. The slug catchers, however, are very large and expensive installations, which are not practical on a platform with limited space. Another method to suppress the slugs is to reduce the opening of the topside choke valve. This solution is simple and inexpensive but causes higher back pressure and reduced flow through the production system leading to reduced production and economic losses (Godhavn, Fard, & Fuchs, 2005). In other words, to ensure the highest possible production, we want to open the topside choke valve as much as possible, but opening the choke valve is exactly what brings the system into slugging behaviour. Moreover, opening the choke valve reduces the overall controllability of the system due to complex dynamic relations between the choke valve opening and the riser bottom pressure.

With feedback control, we can control the topside choke valve opening and avoid slug flow, even when operating in conditions compatible with slugging. Automatic control of the topside choke valve to stabilize slug flow has been investigated in several research papers. Conventional PI control methods was used in Hedne and Linga (1990), Jahanshahi and Skogestad (2013) and in Godhavn et al. (2005), while more advanced controllers, such as nonlinear and adaptive controllers, have been investigated in Jahanshahi, Skogestad and Grøtli (2013), Di Meglio, Kaasa, Petit and Alstad (2010), de Oliveira, Jäschke and Skogestad (2015) and Ohrem, Holden, Jahanshahi and Skogestad

(2017). Anti-slug control solutions have also been implemented on production platforms. Havre, Stornes and Stray (2000) showed a feedback control solution that is able to tame the slug flow and which greatly improves the stability of the multiphase flow. Furthermore, Campos et al. (2015) implemented an advanced anti-slug control algorithm on three separate platforms leading to a massive decrease in compressor trips and gas flaring and hence increased operational stability and safety. This also led to an increase in income estimated at several million USD per year.

2.1. Pipeline-riser Model

The pipeline-riser model from Jahanshahi and Skogestad (2011) is used in this paper. The model is not presented in its entirety, as it is not the focus of this paper. The pipeline-riser system is nonlinear and the parameters of the model change when we move the operating point. The system is stable at choke valve openings up to 15%, but it becomes more and more unstable the more we open the topside choke valve. Opening the valve also reduces our ability to control the system, hence, controlling the pipeline-riser system becomes rather challenging.

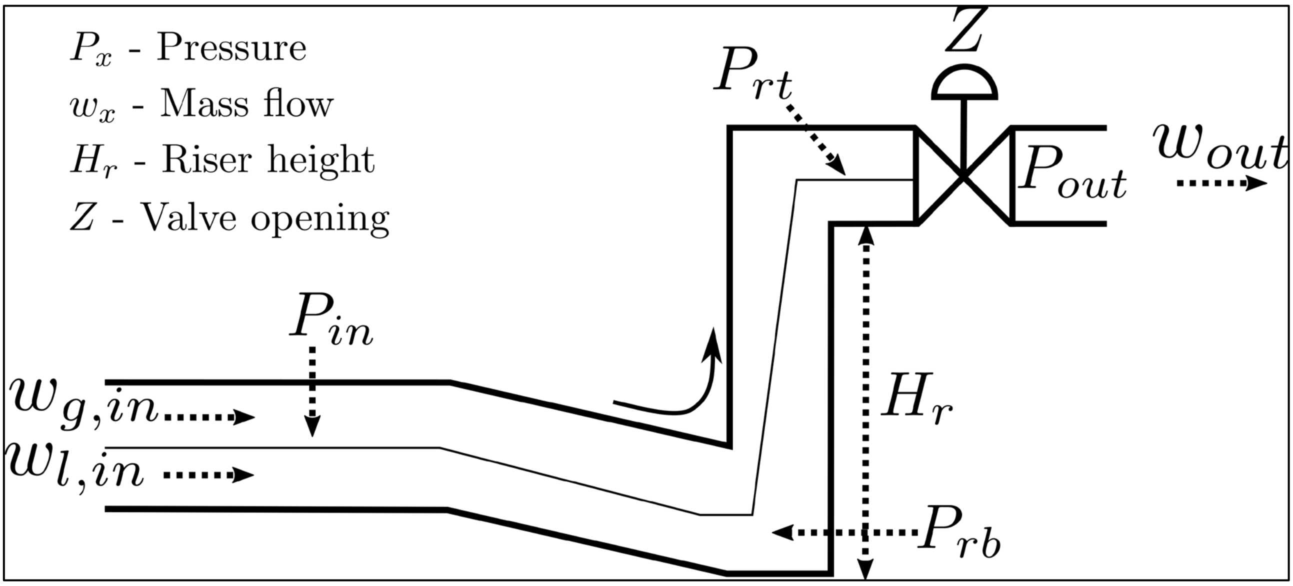

Figure 1: A schematic of a pipeline-riser system with a topside choke valve

2.2. PI Control

PI controllers are well suited for controlling linear systems with constant parameters. If the system is nonlinear, however, we must find a linear approximation of the system at the operating point and design our PI controller for operation in and close to this point. A PI controller has the form

$$u = -k_p\tilde{y} - \frac{k_p}{\tau_i}\int_0^t \tilde{y}\,dt \tag{1}$$

where $k_p > 0$ and $\tau_i > 0$ represents the proportional gain and the integration time for the proportional and integral part, respectively and $\tilde{y} = y - y_d$ is the deviation between the system output y and the reference (desired output) y_d. The goal of the PI controller is to ensure that $\tilde{y} \to 0 \Rightarrow y \to y_d$. A block diagram of a PI controller is shown in Figure 1.

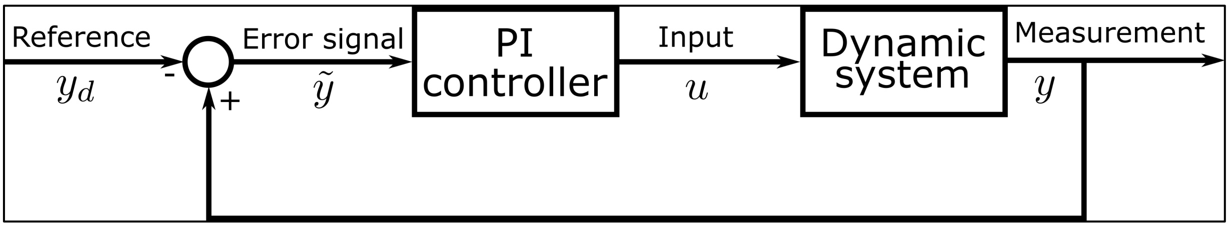

Figure 2: A block diagram of a system controlled by a PI controller

PI control of pipeline-riser systems has, as mentioned, been investigated in several research papers. In this paper, we will consider the control solution from Jahanshahi and Skogestad (2013) where the PI controller is derived by first designing an Internal Model Controller (IMC). The IMC method requires an estimate of the system model, and it can be argued that the design process is more complex than that of traditional PI controller tuning methods. Jahanshahi and Skogestad (2013) also mention that since the controller tuning is based on a linear model identified at a certain operating point, a controller working at one operating point may not work at other operating points. One solution to this is to use so-called gain-scheduling, where multiple controllers are designed for different operating points, and a switching algorithm is introduced to change between the controllers.

Two conventional PI controllers are presented in Jahanshahi and Skogestad (2013). The first is tuned based on a model derived at a valve opening of 20%, and the related tuning values are:

$$\begin{aligned} k_p &= 25.95 \\ \tau_i &= 107.38\,. \end{aligned} \tag{2}$$

The second controller tuning is based on a model derived with a valve opening of 30%, and the related tuning values are:

$$\begin{aligned} k_p &= 42.20 \\ \tau_i &= 53.53 \end{aligned} \tag{3}$$

which are quite different from the tuning based on a 20% opening, underlining the nonlinearities of the system.

2.3. Adaptive Control

Several different adaptive control solutions exist. For the comparison in this paper, we have chosen the $\mathcal{L}_1$ adaptive controller suggested by Hovakimyan & Cao (Hovakimyan & Cao, 2010). This controller has fast adaptation and guaranteed robustness, which makes it very well suited for anti-slug control. The $\mathcal{L}_1$ adaptive controller is quite different from the PI controller. Firstly, it utilizes a prediction model to generate a trajectory that the output should track. The prediction model has the form

$$\dot{\hat{y}} = a_m\hat{y} + b_m(\hat{\omega}u + \hat{\theta}\hat{y} + \hat{\sigma}) \tag{4}$$

where $\hat{y}$ is the predicted output, a_m < 0 is the prediction model time constant, b_m is the prediction model gain, $\hat{\omega}$ is the estimated system gain, $\hat{\theta}$ is the estimated system time constant and $\hat{\sigma}$ is the estimated unknown disturbance. Secondly, the input generated by the $\mathcal{L}_1$ adaptive controller is

$$u = -kD(s)(\hat{\eta} - k_g y_d) \tag{5}$$

where $k > 0$ is the feedback gain, $D(s) = \frac{1}{s}$ is an integrator, $\hat{\eta} = \hat{\omega}u + \hat{\theta}y + \hat{\sigma}$ and $k_g = -\frac{1}{a_m^{-1}b_m} = -1$ ensures that the correct steady state value is reached. The estimated parameters are updated using the adaptation laws:

$$\dot{\hat{\omega}} = \gamma Proj(\hat{\omega}, -\tilde{y}pbu) \quad (6)$$

$$\dot{\hat{\theta}} = \gamma Proj(\hat{\theta}, -\tilde{y}pby) \quad (7)$$

$$\dot{\hat{\sigma}} = \gamma Proj(\hat{\sigma}, -\tilde{y}pb) \quad (8)$$

where $\gamma > 0$ are the adaptation gains, $\tilde{y} = \hat{y} - y$ is the deviation between the prediction model output and the actual system output, p is the solution to the Lyapunov equation $a_m p + p a_m = -q$ for arbitrary $q > 0$ (we have chosen $q = 1$ in this paper) and $Proj$ is the projection operator which ensures that the adapted parameters are bounded.

The goal of the $\mathcal{L}_1$ adaptive controller is to ensure that $y \to y_d$. The tuning parameters for the $\mathcal{L}_1$ adaptive controller in this case are the adaptation gains γ and the feedback gain k. Furthermore, the prediction model gain and time constants must be chosen appropriately (i.e. the dynamics should not be faster than what the system is able to follow). A block diagram showing the $\mathcal{L}_1$ adaptive controller is shown in Figure 2. Since the $\mathcal{L}_1$ adaptive controller parameters are updated automatically, it is not required that we find a set of tuning parameters for different valve openings.

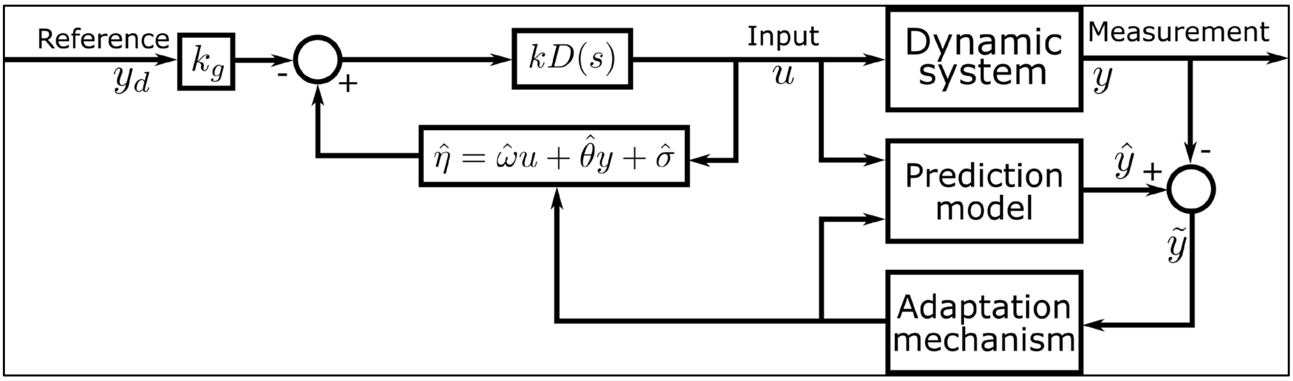

Figure 3: A block diagram of the $\mathcal{L}_1$ adaptive controller

3. SIMULATION RESULTS

The pipeline-riser model from Jahanshahi and Skogestad (2011) was implemented in MATLAB 2018b (The MathWorks Inc., 2018). The model equations are solved using MATLAB's ODE15s solver while the adapted parameters and the prediction model dynamics of the $\mathcal{L}_1$ adaptive controller are discretized and solved using first-order Euler integration with a step length of 0.1 seconds. The choice of step length and Euler integration is based on an implementation done in a small-scale laboratory (Ohrem et al., 2017). We simulate with the PI controller derived for a 20% valve opening and a 30% valve opening, and with the $\mathcal{L}_1$ adaptive controller.

The system is initialized with a valve opening of 20%, which corresponds to an initial pressure of 26.5 kPa and is well into the unstable region. In all simulations, we introduce 3 negative steps in the pressure reference signal to bring the system further into the unstable region. The first two steps are unit steps, while the last step is slightly larger (-1.4 kPa) to really push the controllers. When using the PI controllers, the reference steps are passed through a first-order low pass filter with a time constant of 50 seconds to smooth out the signal. This is the same time constant used in the prediction model for the $\mathcal{L}_1$ adaptive controller. The controller parameters used in the simulations are listed in Table 1.

Table 1 Controller parameters

k_p	25.95, 42.20
τ_i	107.38, 53.53
γ	30
k	2
a_m	-1/50
b_m	1/50
q	1
p	1

As can be seen in Figure 4, the PI controller tuned for a valve opening of 20% is able to control the system during the first two reference step changes. It performs very well initially and during the first two steps, but the final step brings the system too far away from the linearized region and slugging occurs (visible as extreme oscillations in pressure). The PI controller tuned for a valve opening of 30% is shown in Figure 5. This controller is able to keep the system stable for a while longer than the previous PI controller is, but eventually, it also fails. The performance during the first two steps, however, is very good. In Figure 6, we see the performance when using the $\mathcal{L}_1$ adaptive controller. This controller is able to stabilize the system after the third step, and the performance during all steps is very good. The adapted parameters are shown in Figure 7. We note that during each step, the parameters update automatically to counteract the increased instability of the system.

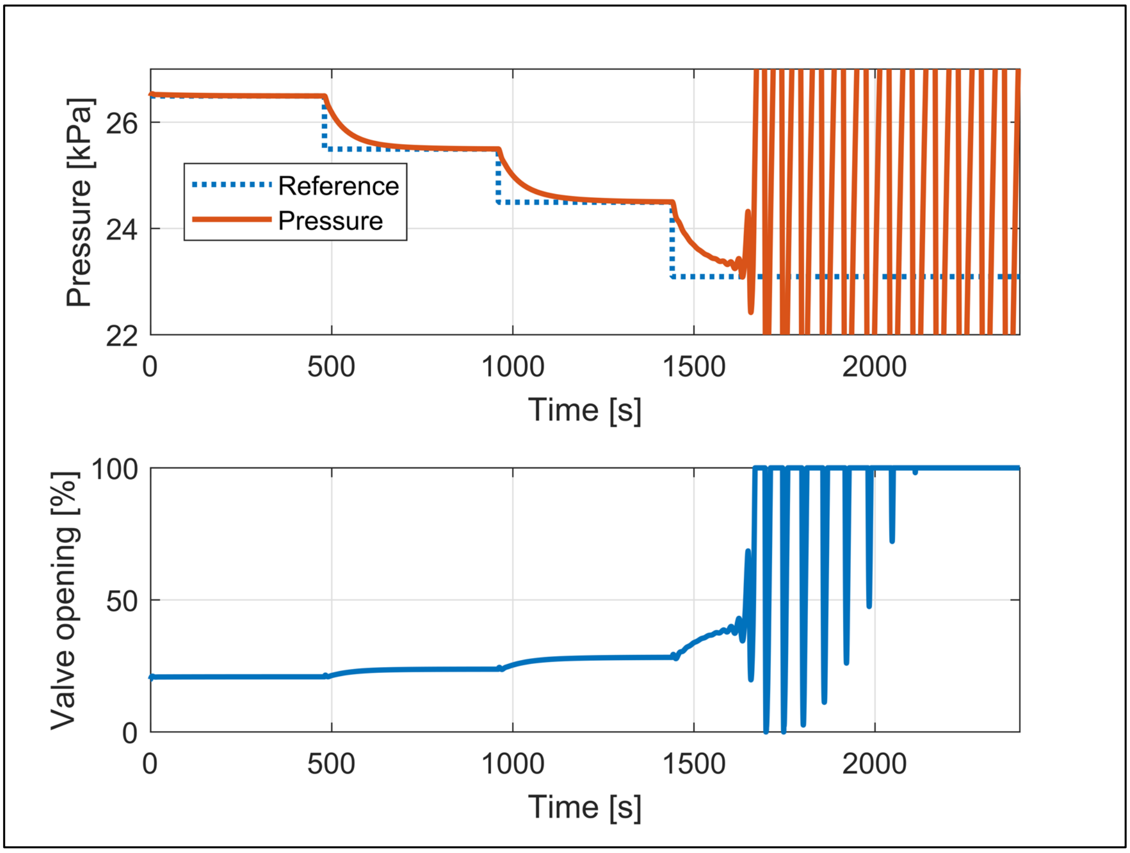

Figure 4: Simulation using a PI controller with tuning based on a model derived with 20% valve opening

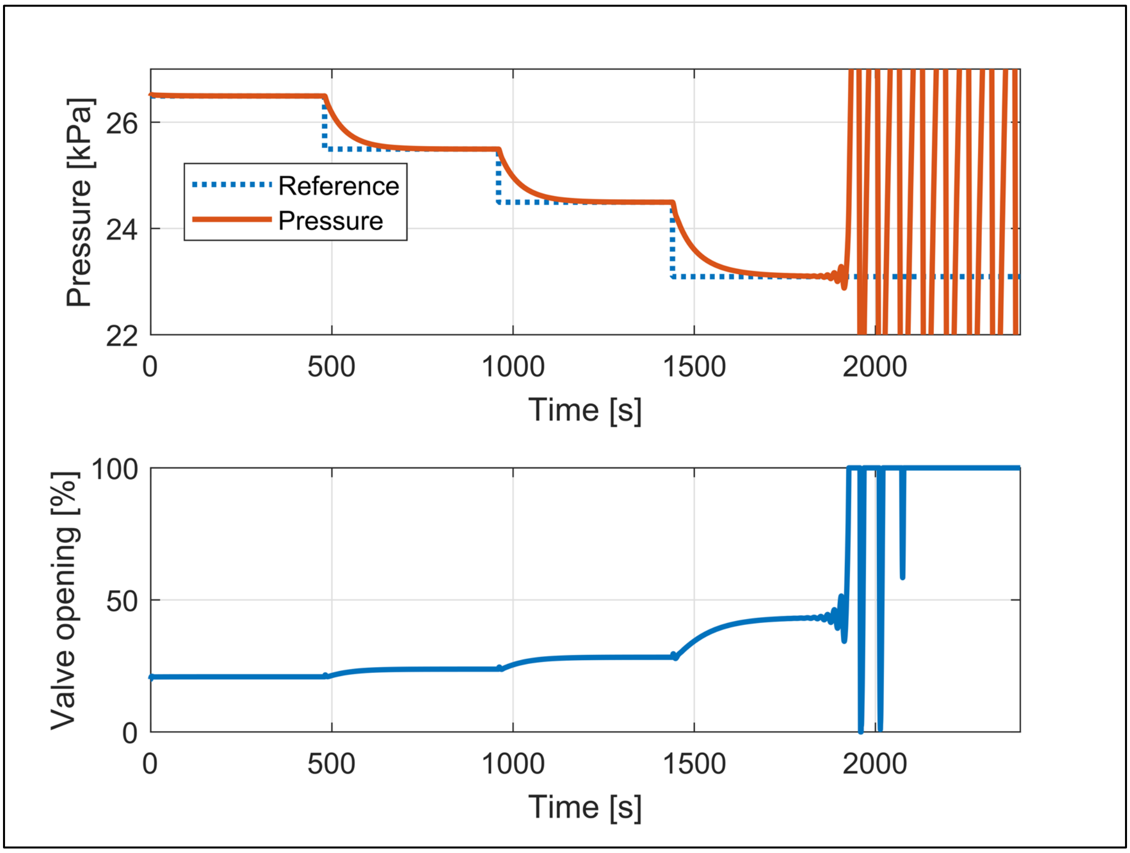

Figure 5: Simulation using a PI controller with tuning based on a model derived with 30% valve opening

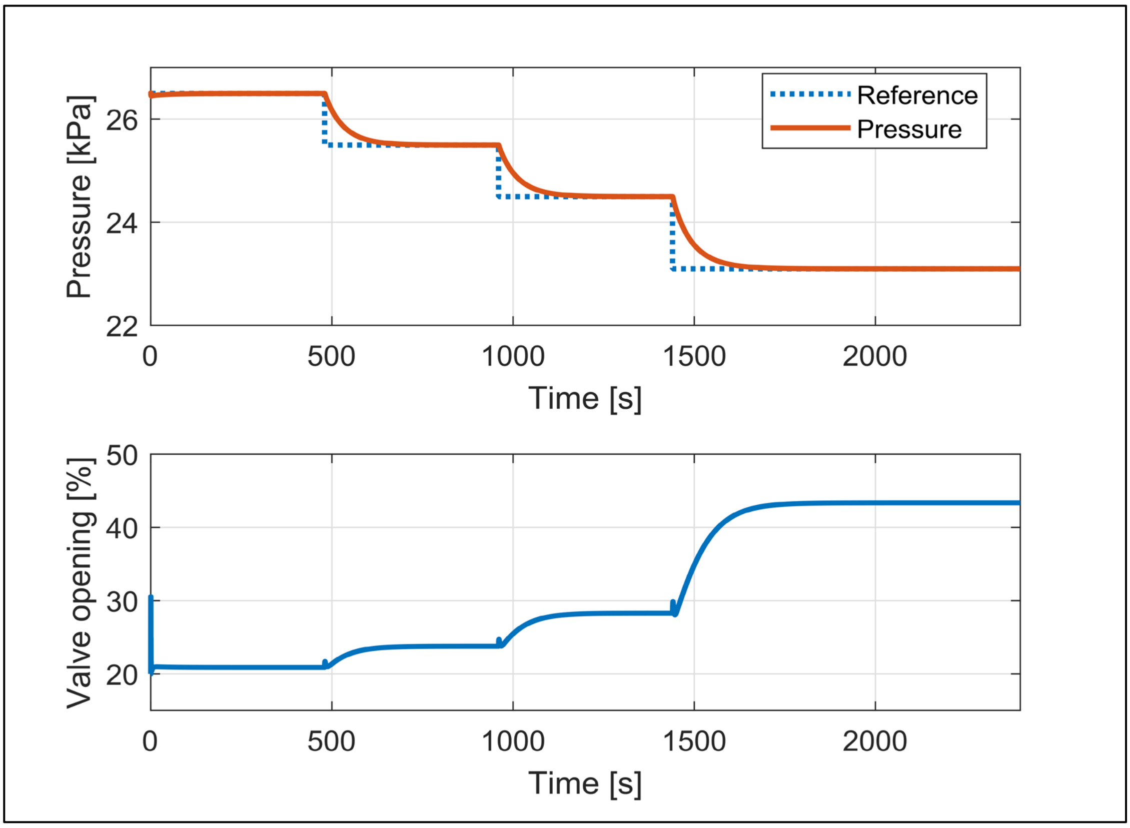

Figure 6: Simulation using the $\mathcal{L}_1$ adaptive controller

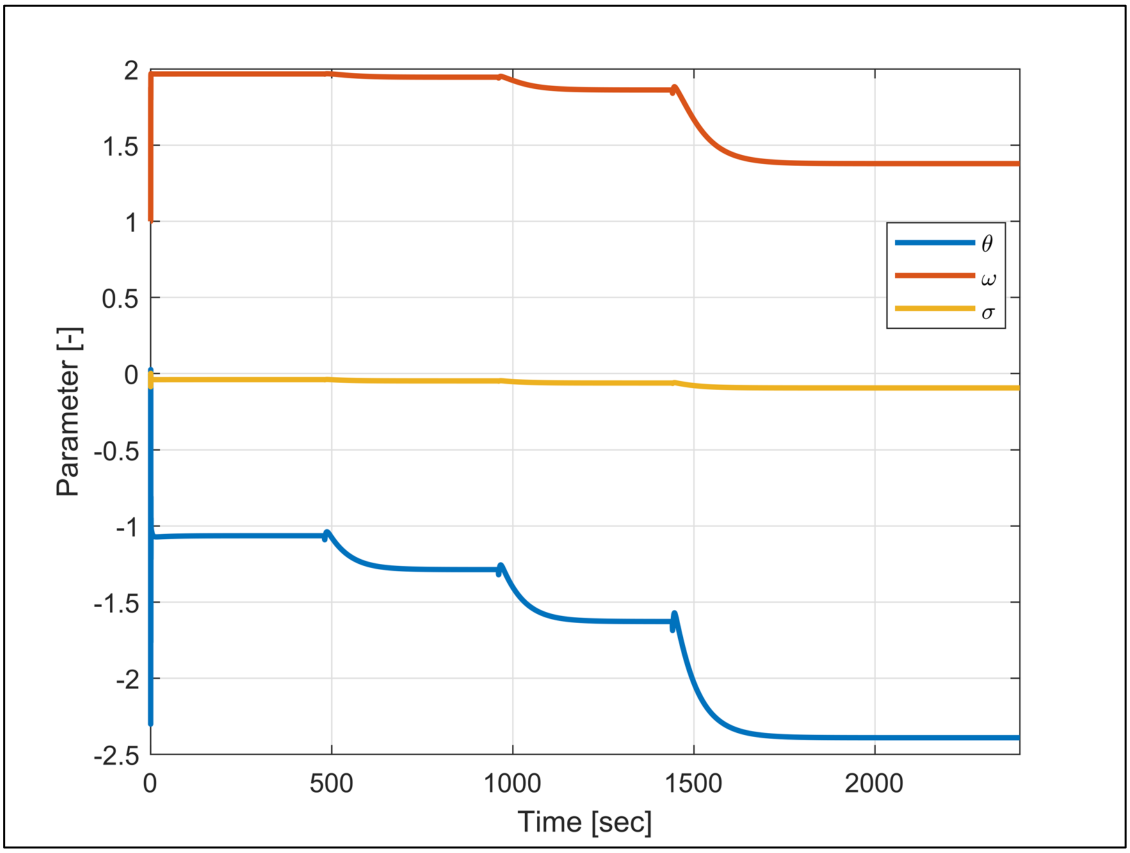

Figure 7: The adapted parameters in the $\mathcal{L}_1$ adaptive controller

4. STPA RESULTS

4.1. STPA Procedure

The STPA procedure consists of four main steps (Leveson & Thomas, 2018). The first step is to define the purpose of the analysis, which has four sub-steps: (1) identify losses, (2) identify system-level hazards, (3) identify system-level safety constraints, and (4) refine hazards (optional). The loss involves something that is unacceptable to the stakeholders, such as loss of human life, environmental pollution, loss of mission and property damage. In STPA, the hazard is defined as a system state or set of conditions that can lead to a loss, together with a particular set of worst-case environmental conditions.

The second step is to define a control structure that models the system as a set of feedback control loops and captures functional relationships and interactions among the system components. The control structure is a hierarchical system model that is composed of feedback control loops, which can enforce constraints on the behaviour of the overall system. The third step is to identify unsafe control actions (UCAs). A UCA is defined as a control action that will lead to a hazard in a particular context and worst-case environment. In this step, we examine control actions in the control structure to identify how the control actions may lead to the hazards and consequently result in the losses defined in the first step. The fourth step is to identify loss scenarios, where we can identify the reasons why the UCAs, identified in the third step, might occur in the system, respectively why the control actions might be improperly executed or not executed. The reader can refer to the STPA handbook (Leveson & Thomas, 2018) for further details on the STPA procedure. In the following two sections, we apply STPA to the choke valve controlled pipeline-riser system and evaluate the hazards present when using PI control and adaptive control.

4.2. Choke Valve-Controlled System with PI Controller

Regardless of whether the system is controlled by a PI controller or by an adaptive controller, the same losses, system-level hazards and system-level constraints are present; see Table 2.

Table 2 Losses, system-level hazards and constraints of choke valve-controlled system

System	Losses	System-Level Hazards	System-Level Constraints
Choke valve controlled system	L-1: Shutdown of oil/gas production	H-1: Slugging occurs in riser [L-1]	SC-1: Occurrence of slugging should be prevented [H-1]
	L-2: Damage to subsea production systems	H-2: Pressure exceeds upper or lower limit [L-2]	SC-2: Pressure should be maintained between upper and lower limit [H-2]
	L-3: Reduced oil/gas production	H-3: Pipeline-riser pressure is not optimal [L-3]	SC-3: Pipeline-riser pressure should be optimal [H-3]

The system consists of five main parts: human operator, PI controlled system, valve actuator, choke valve, and pressure sensor. The responsibilities of the human operator is to set the desired pressure and tune the parameters of the PI controller. Based on these inputs from the human operator, the valve opening calculator calculates required valve opening, and the valve position controller adjusts valve position to meet the required valve opening. The valve actuator generates physical force to adjust the valve opening in accordance with the commands from the PI control system. The new pressure is measured by the pressure sensor and updated to the PI control system. The deviation between the actual and desired pressure is then provided to the human operator via the control system. The control structure of this control system and the responsibilities of each controller are given in Figure 88 and Table 3, respectively.

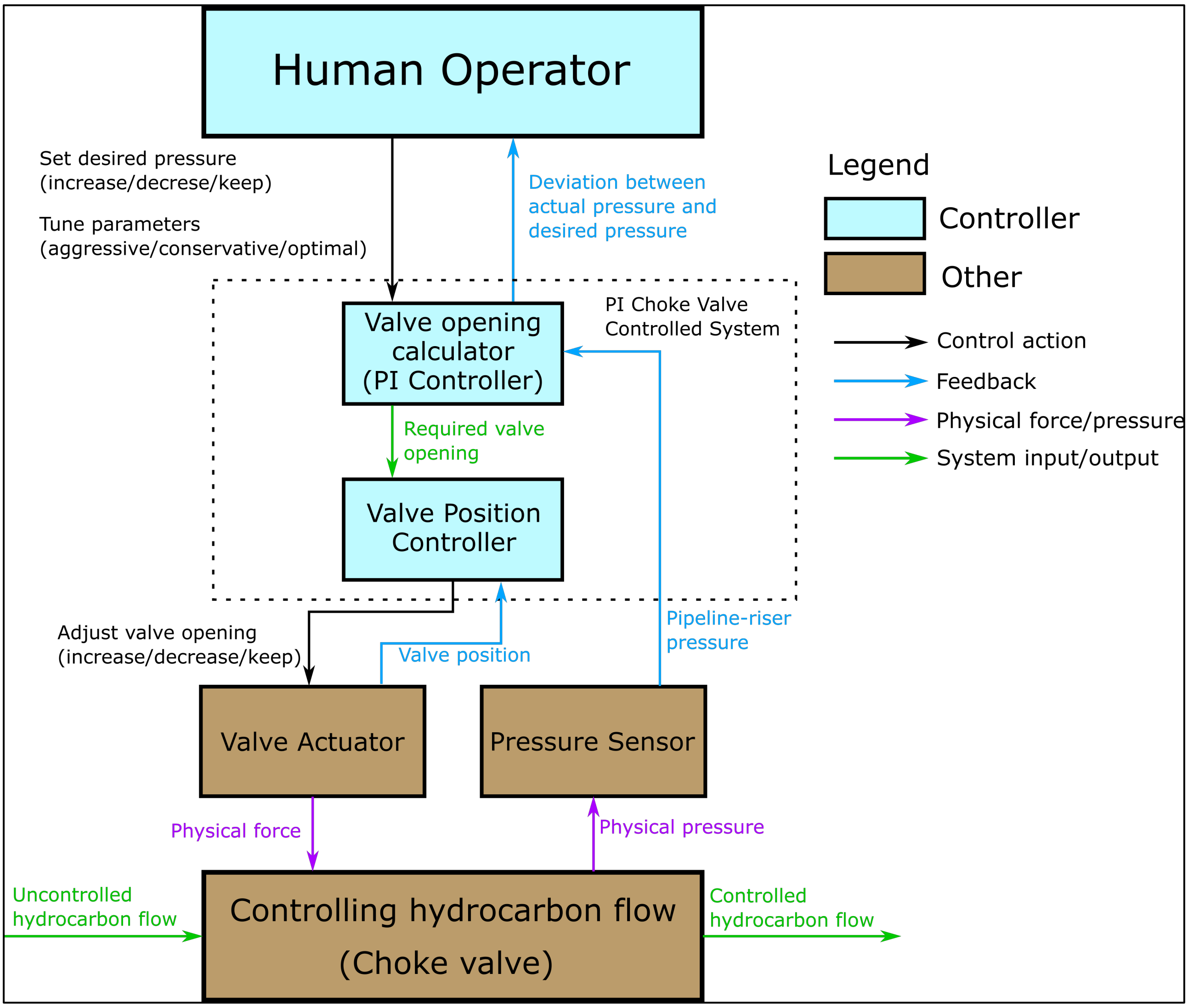
Human Operator
Set desired pressure (increase/decrese/keep)
Tune parameters (aggressive/conservative/optimal)
Deviation between actual pressure and desired pressure
Legend
Controller
Other
Control action
Feedback
Physical force/pressure
System input/output
PI Choke Valve Controlled System
Valve opening calculator (PI Controller)
Required valve opening
Valve Position Controller
Adjust valve opening (increase/decrease/keep)
Valve position
Pipeline-riser pressure
Valve Actuator
Pressure Sensor
Physical force
Physical pressure
Uncontrolled hydrocarbon flow
Controlling hydrocarbon flow (Choke valve)
Controlled hydrocarbon flow

Figure 8: Control structure of choke valve-controlled system with PI controller

Table 3 Responsibilities, process models and feedbacks

Controller	Responsibility	Process Model	Feedback
Human Operator	Adjust desired pressure to maximize oil/gas production	Production rate • Optimal • Not optimal	Pipeline-riser pressure
	Update parameters to properly control Choke valve opening	Parameters • Optimal • Aggressive • Conservative	Indirectly by pipeline-riser pressure
PI Controller	Adjust Choke valve opening to meet the desired pressure, using fixed or irregularly updated parameters	Actual pressure • High than desired pressure • Same with desired pressure • Lower than desired pressure	Deviation between actual pressure and desired pressure

From the control structure, we identified 120 UCAs that can lead to the losses defined in Table 2. Eight UCAs are related to *H-1: Slugging occurs in riser*, 18 UCAs with *H-2: Pressure exceeds upper or lower limit*, and 94 UCAs with *H-3: Pipeline-riser pressure is not optimal*. The eight UCAs that can lead to the occurrence of slugging are listed in Table 4. Aggressive and conservative tuning relates to a short or long integral time, respectively. Short integral time may cause overshoots, wind-up issues, which can render the control system unresponsive, and other undesirable behaviours.

Table 4 UCAs of choke valve-controlled system with PI controller

No.	UCA
UCA.HO.011	Human operator provides “Decrease desired pressure” command when pressure is close to slugging [H-1]
UCA.HO.021	Human operator provides “Tune to aggressive parameters” command when parameters are optimal, pressure is close to slugging, and disturbance occurs [H-1]
UCA.HO.036	Human operator provides “Tune to aggressive parameters” command when parameters are conservative, pressure is close to slugging, and disturbance occurs [H-1]
UCA.HO.050	Human operator does not provide “Tune to conservative parameters” command when parameters are aggressive, pressure is close to slugging, and disturbance occurs [H-1]
UCA.HO.079	Human operator does not provide “Tune to optimal parameters” command when parameters are aggressive, pressure is close to slugging, and disturbance occurs [H-1]
UCA.HO.081	Human operator provides “Tune to optimal parameters” command too late when parameters are aggressive, pressure is close to slugging, and disturbance occurs [H-1]
UCA.HO.102	Human operator provides “Tune to optimal parameters” command too early when parameters are conservative, pressure is close to slugging, and disturbance occurs [H-1]
UCA.VP.011	Valve Position Controller provides “Decrease valve opening” command when pressure is close to slugging [H-1]

From the eight UCAs, we identified 42 high-level loss scenarios that could be classified into five categories: human error (15 scenarios), technical system failure (19 scenarios), design requirement (6 scenarios), software flaw (1 scenario), and others (1 scenario). Some examples of the loss scenarios are

LSC.HO.036.02 (human error)
The riser pressure is close to slugging and a disturbance occurs, but the human operator provides “Tune to aggressive parameters” command [UCA.HO.036], because the human operator wrongly interprets the feedback and incorrectly believes that the riser pressure is not close to slugging. This flawed process model can occur if the human operator is under excessive stress or not properly trained. As a result, slugging occurs in the riser [H-1].

LSC.HO.079.05 (technical system failure)
The parameters are aggressive, riser pressure is close to slugging, and a disturbance occurs. The human operator, therefore, provides “Tune to optimal parameters” command, but the control system does not respond to this command [UCA.HO.079]. This flawed process can occur if the controller fails or if power is not supplied to the control system. As a result, slugging occurs in the riser [H-1].

LSC.HO.079.07 (inadequate design requirement)
The parameters are aggressive, riser pressure is close to slugging, and a disturbance occurs, but the human operator does not provide “Tune to optimal parameters” command [UCA.HO.079], because the human operator is not aware of this situation. This flawed process model occurs because there is no direct feedback that indicates whether the parameters are aggressive or optimal. As a result, slugging occurs in the riser [H-1].

LSC.VP.011.01 (software flaw)
The riser pressure is close to slugging, but the valve position controller provides “Decrease valve opening” command [UCA.VP.011], because the valve position controller wrongly interpret the feedback. This flawed process can occur due to inadequate control algorithm inside the valve position controller. As a result, slugging occurs in the riser [H-1].

LSC.VP.011.04 (other reason)
The riser pressure is close to slugging, but the valve position controller provides “Decrease valve opening” command [UCA.VP.011], due to inadequate parameters. This flawed process can occur when UCA.HO.021, UCA.HO.036, UCA.HO.050, UCA.HO.079, UCA.HO.081, UCA.HO.102 occur. As a result, slugging occurs in the riser [H-1].

4.3. Choke Valve-Controlled System with Adaptive Controller

The configuration of the adaptive control system is similar to that of the conventional PI controller, but there is a significant difference. There are additional elements inside the adaptive choke valve-controlled system, namely the prediction model and the adaption mechanism. The parameters are continuously self-adjusted by the adaption mechanism, without human intervention; hence, the adaptive mechanism is responsible for tuning the parameters in this system. The feedback from the pressure sensor is provided to the human operator for the desired pressure setting and to the adaptive mechanism for self-adjusting the parameters. The control structure of this control system and the responsibilities of each controller are given in Figure 99 and Table 5, respectively.

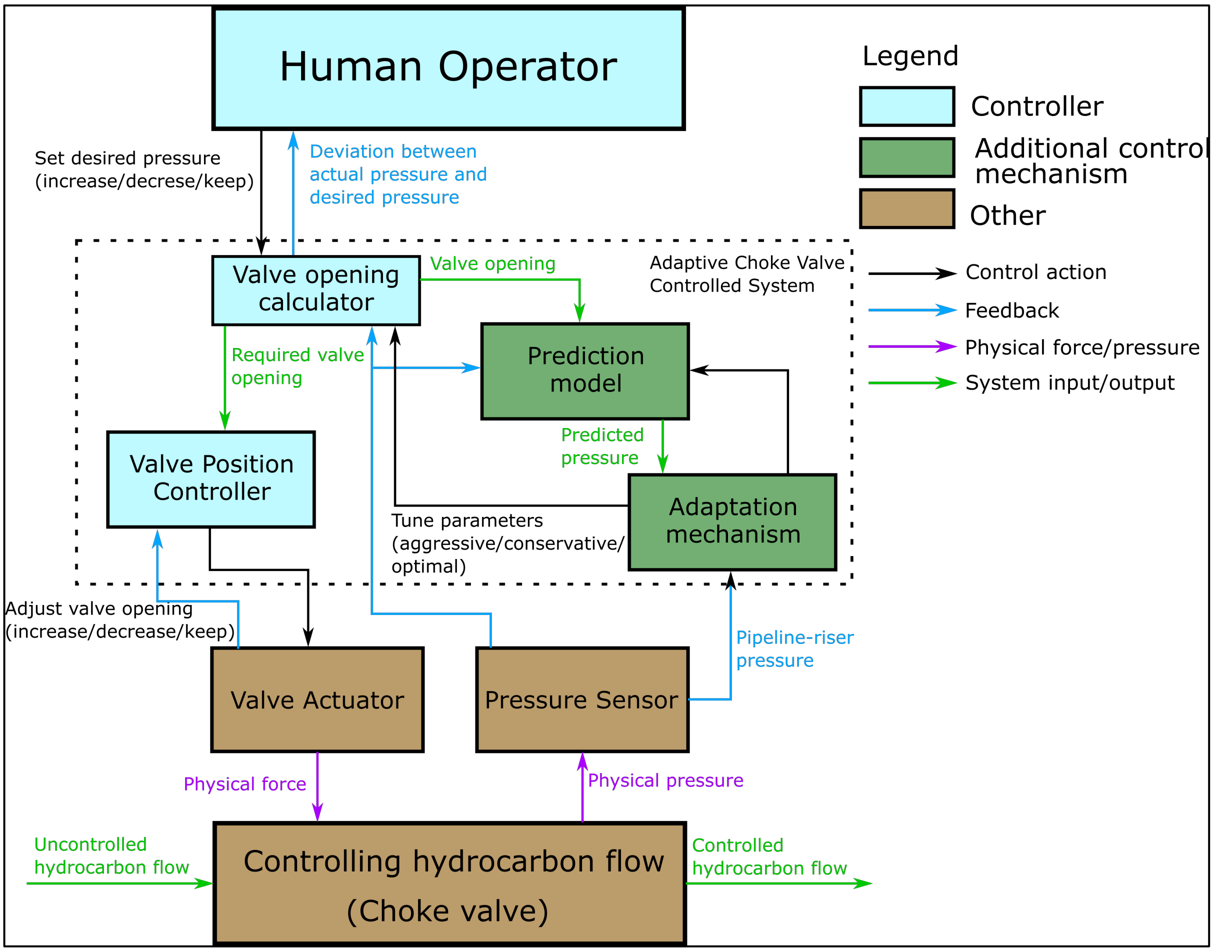
Human Operator
Legend
Controller
Additional control mechanism
Other
Set desired pressure (increase/decrease/keep)
Deviation between actual pressure and desired pressure
Valve opening calculator
Valve opening
Adaptive Choke Valve Controlled System
Control action
Feedback
Physical force/pressure
System input/output
Required valve opening
Prediction model
Predicted pressure
Valve Position Controller
Adaptation mechanism
Tune parameters (aggressive/conservative/ optimal)
Adjust valve opening (increase/decrease/keep)
Pipeline-riser pressure
Valve Actuator
Pressure Sensor
Physical force
Physical pressure
Uncontrolled hydrocarbon flow
Controlling hydrocarbon flow (Choke valve)
Controlled hydrocarbon flow

Figure 9: Control structure of choke valve controlled system with an adaptive controller

Table 5 Responsibilities, process models and feedbacks

Controller	Responsibility	Process Model	Feedback
Human operator	Adjust desired pressure to maximize oil/gas production	Production rate • Optimal • Not optimal	Measured pipeline-riser pressure
Adaptive controller	Update parameters to properly control choke valve opening	Parameters • Optimal • Aggressive • Conservative	Predicted pipeline-riser pressure
	Adjust choke valve opening to meet the desired pressure, with continuous, self-adjusting parameters	Actual pressure • High than desired pressure • Same with desired pressure • Lower than desired pressure	Deviation between actual pressure and desired pressure

From the above control structure, we identified 120 UCAs that can lead to the losses defined in Table 2. Eight UCAs are related to *H-1: Slugging occurs in riser*, 18 UCAs with *H-2: Pressure exceeds upper or lower limit*, and 94 UCAs with *H-3: Pipeline-riser pressure is not optimal*. The eight UCAs that can lead to the occurrence of slugging are listed in Table 6.

Table 6 UCAs of choke valve control system with adaptive controller

No.	UCA
UCA.HO.011	Human operator provides "Decrease desired pressure" command when pressure is close to slugging [H-1]
UCA.AM.008	Adaptive mechanism provides "Tune to aggressive parameters" command when parameters are optimal, pressure is close to slugging, and disturbance occurs [H-1]
UCA.AM.023	Adaptive mechanism provides "Tune to aggressive parameters" command when parameters are conservative, pressure is close to slugging, and disturbance occurs [H-1]
UCA.AM.037	Adaptive mechanism does not provide "Tune to conservative parameters" command when parameters are aggressive, pressure is close to slugging, and disturbance occurs [H-1]
UCA.AM.066	Adaptive mechanism does not provide "Tune to optimal parameters" command when parameters are aggressive, pressure is close to slugging, and disturbance occurs [H-1]
UCA.AM.068	Adaptive mechanism provides "Tune to optimal parameters" command too late when parameters are aggressive, pressure is close to slugging, and disturbance occurs [H-1]
UCA.AM.089	Adaptive mechanism provides "Tune to optimal parameters" command too early when parameters are conservative, pressure is close to slugging, and disturbance occurs [H-1]
UCA.VP.011	Adaptive valve position controller provides "Decrease valve opening" command when pressure is close to slugging [H-1]

From the eight UCAs, we identified 30 high-level loss scenarios that could be classified into four categories: human error (2 scenarios), technical system failures (20 scenarios), software flaw (7 scenario), and others (1 scenarios). Some examples of the loss scenarios are:

LSC.HO.011.02 (human error)

The riser pressure is close to slugging, but the valve position controller provides "Decrease desired pressure" command [UCA.HO.011], because the human operator wrongly interprets the feedback and incorrectly believes that the riser pressure is not close to slugging. This flawed process model can occur if the human operator is under excessive stress or not properly trained. As a result, slugging occurs in the riser [H-1].

LSC.AM.066.05 (technical failure)
The parameters are aggressive, riser pressure is close to slugging, and a disturbance occurs. The adaptive mechanism, therefore, provides “Tune to optimal parameters” command, but the control system does not respond to this command [UCA.AM.066]. This flawed process can occur if the controller fails or if power is not supplied to the control system. As a result, slugging occurs in the riser [H-1].

LSC.AM.066.01 (software flaw)
The parameters are aggressive, riser pressure is close to slugging, and a disturbance occurs, but the adaptive mechanism does not provide “Tune to optimal parameters” command [UCA.AM.066], because the adaptive mechanism wrongly interprets the feedback. This flawed process can occur due to inadequate control algorithm inside the adaptive mechanism. As a result, slugging occurs in the riser [H-1].

LSC.VP.011.04 (other reason)
The riser pressure is close to slugging, but the valve position controller provides “Decrease valve opening” command [UCA.VP.011], due to inadequate parameters. This flawed process can occur when UCA.AM.008, UCA.AM.023, UCA.AM.037, UCA.AM.066, UCA.AM.068, UCA.AM.089 occur. As a result, slugging occurs in the riser [H-1].

4.4. Comparison of the Results

The number of UCAs and loss scenarios of a conventional PI control system and an adaptive control system are summarized in Table 7. The UCAs identified from the PI control system and the adaptive control system were almost identical. The only difference was who provides UCAs. This difference is caused by the different responsibilities of the human operator and the control system. In the PI control system, the human operator tunes parameters manually, while the adaptive mechanism automatically tunes parameters in the adaptive control system. An example of this difference is shown in the below UCAs. The two UCAs have the same control command and the same conditions, but the controllers are different.

UCA.HO.053 (from PI control system)
Human Operator provides “Tune to conservative parameters” command when parameters are optimal, the pressure is higher than optimal, and disturbance occurs.

UCA.AM.037 (from adaptive control system)
Adaptive Mechanism provides “Tune to conservative parameters” command when parameters are optimal, the pressure is higher than optimal, and disturbance occurs.

Table 7 Number of UCAs and scenarios of the two systems

	Choke Valve-Controlled System with PI Controller	**Choke Valve-Controlled System with Adaptive Controller**
Number of UCAs	120	120
UCAs related to H-1	8	8
UCAs related to H-2	18	18
UCAs related to H-3	94	94
Number of scenarios related to H-1	42	30
Scenarios caused by human error	15	2
Scenarios caused by technical failure	19	20

	Choke Valve-Controlled System with PI Controller	**Choke Valve-Controlled System with Adaptive Controller**
Scenarios caused by design requirement	6	0
Scenarios caused by software flaw	1	7
Scenarios caused by other reasons	1	1

Unlike with the UCAs, we could identify considerable differences between the loss scenarios identified from the PI-controlled system and the adaptively controlled system. One of the differences is the number of scenarios related to human error and software flaws, as shown in Table 7. The parameters are automatically updated in the adaptive control system; hence, a larger number of scenarios caused by software flaws were identified than with the conventional PI control system. For the same reason, the number of scenarios caused by human error was smaller in the adaptive control system than in the PI control system.

Another difference is the scenarios caused by the inherent design requirement. In the PI control system, the human operator has no direct feedback that indicates whether the parameters are optimal or not. When tuning is required, the human operator can only realize the situation by observing the variation of pipeline-riser pressure. It would be too late to tune the parameters after observing large pressure variations. LSC.HO.079.07, provided in Section 4.1 above, is an example of this scenario. In contrast with the PI control system, the parameters are continuously updated by the adaptive mechanism with the support from the prediction model in the adaptive control system. The parameters can, therefore, be properly tuned before we experience a large amount of pressure variation inside the riser. These differences are summarized in Table 8.

Table 8 Summary of differences between the two systems

	Choke Valve-Controlled System with PI Controller	**Choke Valve-Controlled System with Adaptive Controller**
Parameters	Fixed or irregularly updated by human operator	Continuously self-adjusted by adaptive mechanism and prediction model
UCAs related to parameter tuning	Provided by human operator	Provided by adaptive mechanism
Main cause of loss scenarios related to parameter tuning	Human error (15 scenarios) and technical failure (19 scenarios)	Technical failure (20 scenarios) and software flaw (7 scenarios)
Direct feedback of parameters	Non-existent	By prediction model
Loss scenarios caused by absence of parameter feedback	Six scenarios	None

5. DISCUSSION

The simulations show that both the PI and the adaptive control solutions are able to prevent riser slugging. The adaptive solution, however, is able to control the system at operating points where the PI controller fails. Another significant difference is that the PI control solution requires manual updates of the tuning parameters, while the adaptive control solution includes automatic updates of the controller parameters. As mentioned in the introduction, the PI controller is widely used in the industry. Compared to the adaptive controller, it is easier to understand and implement, but the STPA analysis showed that the amounts of hazards caused by human errors were larger when using the PI controller. This, along with the improved stability of the system, can be used as arguments for implementing an adaptive control solution. The slight increase in complexity of the adaptive compared to the PI controller will not negate the benefits of the adaptive controller, nor significantly increase the likelihood of implementation errors over the traditional controller.

The STPA also identified that the conventional PI control system has an inherently vulnerable point because there is no direct feedback of the optimality of the controller parameters to the human operator. In contrast, the adaptive control system can update the parameters properly via the prediction model and the adaptive mechanism. We can, therefore, eliminate many loss scenarios related to human errors and design problems related to the tuning of the parameters when we apply adaptive control. On the other hand, new loss scenarios related to software errors were identified in the adaptive control system, which indicates that we need additional measures to demonstrate and test the software integrity of the prediction model and the adaptive mechanism when we apply the adaptive control system.

We could also observe a couple of interesting issues when we applied STPA to the PI and adaptive control systems. One is that some scenarios are directly linked to other UCAs, which are classified as "Other reasons" in Table 7. These scenarios occur due to the occurrence of specific UCAs, and this generates a hierarchy of UCAs and loss scenarios. Investigating this hierarchy in other systems and their impacts on the safety of the system would be interesting future work. The other is that some scenarios can occur more frequently than other scenarios. It is difficult to assign accurate likelihood to the scenarios, and several studies argued that assigning poorly founded likelihood to loss scenarios can dangerously mislead us (Abrecht et al., 2016; Leveson & Thomas, 2013, 2018). However, at least in this case study, it is obvious that there are some scenarios that might occur far more frequently than others. It might be impossible to allocate accurate likelihood of the two scenarios, but it is obvious that if there is an inherent flaw in the design, this can lead to the loss more frequently than a single physical component failure. A post-process to evaluate the likelihood and/or criticality of loss scenarios would be helpful when we utilize STPA to compare the safety of different solutions.

6. CONCLUDING REMARKS

In this study, we have compared a PI and an $\mathcal{L}_1$ adaptive controller from a control and safety perspective. The control perspective informs us whether the controllers are able to perform the required task, i.e., bring the dynamic system to the desired value. It does not evaluate the complexity of the control system or the number of hazards the controller introduces to our system. To evaluate the hazards, we applied STPA and introduced a new tool for evaluation of control systems. The STPA showed that, amongst other things, the adaptive controller is less sensitive to human errors and more sensitive to technical errors such as software flaws.

Furthermore, we identified a key difference between PI control and adaptive control, i.e., the feedback of control parameters. An adaptive controller continuously monitors and automatically updates its controller parameters whereas a PI controller is dependent on a human operator to do the same. It can be difficult for a human operator to perform this evaluation of control parameters. The STPA provided different results for the different controllers. This indicates that it is important to consider the type of controller when performing a hazard analysis and not consider the controller as a generic device.

ACKNOWLEDGEMENTS

This work was carried out as a part of SUBPRO, a Research-based Innovation Centre within Subsea Production and Processing. The authors gratefully acknowledge the financial support from SUBPRO, which is financed by the Research Council of Norway, major industry partners, and NTNU.

REFERENCES

Abrecht, B., Arterburn, D., Horney, D., Schneider, J., Abel, B., & Leveson, N. (2016). *A New Approach to Hazard Analysis for Rotorcraft.* Paper presented at the Proceedings of the 2016 American Helicopter Society Technical Meeting, Huntsville, AL.

Allison, C. K., Revell, K. M., Sears, R., & Stanton, N. A. (2017). Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. *Safety science, 98*, 159-166.

Campos, M., Takahashi, T., Ashikawa, F., Simões, S., Stender, A., & Meien, O. (2015). Advanced anti-slug control for offshore production plants. *IFAC-PapersOnLine, 48*(6), 83-88.

Chen, J., Zhang, S., Lu, Y., & Tang, P. (2015). *STPA-based hazard analysis of a complex UAV system in take-off.* Paper presented at the International Conference on Transportation Information and Safety (ICTIS).

de Oliveira, V., Jäschke, J., & Skogestad, S. (2015). An autonomous approach for driving systems towards their limit: an intelligent adaptive anti-slug control system for production maximization. *IFAC-PapersOnLine, 48*(6), 104-111.

Di Meglio, F., Kaasa, G.-O., Petit, N., & Alstad, V. (2010). *Model-based control of slugging flow: an experimental case study.* Paper presented at the American Control Conference (ACC), 2010.

Godhavn, J.-M., Fard, M. P., & Fuchs, P. H. (2005). New slug control strategies, tuning rules and experimental results. *Journal of process control, 15*(5), 547-557.

Hackl, C. (2012). Non-identifier based adaptive control in mechatronics.

Havre, K., Stornes, K. O., & Stray, H. (2000). Taming slug flow in pipelines. *ABB review, 4*, 55-63.

Hedne, P., & Linga, H. (1990). Suppression of terrain slugging with automatic and manual riser choking. *Advances in Gas-Liquid Flows, 155*(19), 453-460.

Hill, T., & Wood, D. (1994). *Slug flow: Occurrence, consequences, and prediction.* Paper presented at the University of Tulsa Centennial Petroleum Engineering Symposium.

Hovakimyan, N., & Cao, C. (2010). *L1 adaptive control theory: guaranteed robustness with fast adaptation* (Vol. 21): SIAM-Society for Industrial and Applied Mathematics.

Ishimatsu, T., Leveson, N. G., Thomas, J., Katahira, M., Miyamoto, Y., & Nakao, H. (2010). *Modeling and hazard analysis using STPA*. Paper presented at the 4th IAASS Conference, Huntsville, Alabama.

Jahanshahi, E., & Skogestad, S. (2011). Simplified dynamical models for control of severe slugging in multiphase risers. *IFAC Proceedings Volumes, 44*(1), 1634-1639.

Jahanshahi, E., & Skogestad, S. (2013). Closed-loop model identification and pid/pi tuning for robust anti-slug control. *IFAC Proceedings Volumes, 46*(32), 233-240.

Jahanshahi, E., Skogestad, S., & Grøtli, E. I. (2013). Nonlinear model-based control of two-phase flow in risers by feedback linearization.

Kim, H., Lundteigen, M., Hafver, A., Pedersen, F., & Skofteland, G. (2018). *Application of System-Theoretic Process Analysis to the Isolation of Subsea Wells: Opportunities and Challenges of Applying STPA to Subsea Operations.* Paper presented at the Offshore Technology Conference.

Kim, H., Lundteigen, M. A., Hafver, A., Pedersen, F. B., Skofteland, G., Holden, C., & Ohrem, S. J. (2018). *Application of Systems-Theoretic Process Analysis to a Subsea Gas Compression System*. Paper presented at the European Safety and Reliability Conference (ESREL 2018), Trondheim, Norway.

Krstic, M., Kanellakopoulos, I., & Kokotovic, P. V. (1995). *Nonlinear and adaptive control design* (Vol. 222): Wiley New York.

Leveson, N. (2012). *Engineering a safer world: Systems thinking applied to safety*: MIT press.

Leveson, N., & Thomas, J. (2013). *An STPA primer*. Retrieved from Cambridge, MA:

Leveson, N., & Thomas, J. (2018). *STPA Handbook*. Retrieved from Boston, MA, USA:

Nakao, H., Katahira, M., Miyamoto, Y., & Leveson, N. (2011). *Safety guided design of crew return vehicle in concept design phase using STAMP/STPA.* Paper presented at the Proc. of the 5: th IAASS Conference.

O'Dwyer, A. (2009). *Handbook of PI and PID controller tuning rules*: Imperial College Press.

Ohrem, S. J., Holden, C., Jahanshahi, E., & Skogestad, S. (2017). *$\mathcal{L}$1 adaptive anti-slug control.* Paper presented at the American Control Conference (ACC), 2017.

Schmittner, C., Ma, Z., & Puschner, P. (2016). *Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis.* Paper presented at the International Conference on Computer Safety, Reliability, and Security, 22 Sep. 2015, Delft, Netherlands.

The MathWorks Inc., N., Massachusetts, United States. (2018). MATLAB 2018b (Version 2018b).

Young, W. E. (2014). STPA-SEC for cyber security mission assurance. *Eng Syst. Div. Syst. Eng. Res. Lab*.

Åström, K. J. (1983). Theory and applications of adaptive control- A survey. *Automatica, 19*(5), 471-486.

Åström, K. J., & Hägglund, T. (2001). The future of PID control. *Control engineering practice, 9*(11), 1163-1175.