Optimization of recertification intervals for PSV based on major accident risk

Peter Okoh[a,*], Stein Haugen[b], Jan Erik Vinnem[b]

[a] *Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway*

[b] *Department of Marine Technology, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway*

Abstract

Overpressure is a major hazard in the process industry with the potential to lead to a major accident. Pressure Safety Valves (PSVs) are often used as the last layer of protection against such a hazard and require regular recertification in order to be dependable. The valve safely vents gas from a vessel when the pressure becomes excessive. It is often the practice in industry to apply one or two years as the normal recertification interval of PSV. However, experience from the Norwegian oil and gas industry is that the recertification process several times have caused leaks of gas. The process thus represents a certain risk in itself and the question is then whether the recertification intervals presently being used actually are optimal from a risk point of view? The objective of this paper is to look into this problem, applying typical data from an oil and gas installation. An optimal recertification interval will be calculated based on minimization of risk to personnel.

Keywords: PSV, Maintenance, Optimization, Process safety, Major accident, Risk

1. Introduction

The major accident risk in oil and gas industry may be defined as the risk associated with an unexpected event (e.g. a major leak/release, explosion, fire or structural failure), causing or having the potential to cause serious harm to humans, assets or the environment (Comlaw, 2007; EC, 2005; HSE, 1992; OGP, 2008; PSA, 2014; USEPA-OSHA, 1996). The causes of major accidents vary among the various types of accidents. In the case of major releases and explosions, one of the possible causes is overpressure, either caused by applying too high pressure to a vessel or due to increased temperature as a result of flames impinging on a vessel, section or pipe. This scenario is applicable to pressurized vessels and systems, e.g. separators.

To protect against this scenario, it is the usual practice to install Pressure Safety Valve (PSV) as a proactive barrier against overpressure. Since valves are subject to failure mechanisms such as blockage, corrosion and damage, regular recertification is required to ensure that they are able to fulfill the specified safety function. Recertification encompasses the removal of the PSV from the plant, testing/overhauling it in a workshop, putting it back in place and reporting. The problem with this is that the process of removing it and replacing it implies a certain possibility of a leak occurring (Vinnem et al., 2016; PSA, 2014).

* Corresponding author:
Email address: peter.okoh@ntnu.no (Peter Okoh)

The safety-critical failure modes associated with a PSV include fail-to-open and external leak (Darby, 2013; Hellemans, 2009; Rausand and Høyland, 2004; Rausand, 2014; Vinnem et al., 2016). Safety criticality defines the potential of the failure to pose serious risk to the workers, the environment or the installation. Fail-to-open will imply that overpressure in the vessel being protected by the PSV is not relieved (and may lead to explosion), whereas external leak implies a possibility of ignition and explosion. Other failure modes exist, which are not safety-critical (Hellemans, 2009; Rausand and Høyland, 2004; Rausand, 2014). However, some of these failure modes may affect quality in relation to the production process.

Considering how critical PSV is to safety, recertification is an important means to ensure acceptably low probability of failure on demand. However, since statistics show that leaks can occur in this process, the frequency of recertification becomes a matter of optimization. If the PSV fails to relieve overpressure when required, a serious release of gas/oil may occur and if this is ignited serious loss of life may occur. On the other hand, the recertification can lead to a leak which again may ignite and cause loss of life. This is a problem that is well suited for optimization, by finding the recertification interval that gives the lowest total risk of loss of life.

It is often the practice in industry to apply one or two years as the normal recertification interval of PSV. However, how can we be certain that this interval is optimal for a given case? Reliability-based (usually cost-related) and risk-based approaches exist for optimizing the interval at which an item should be maintained. However, the current practice is such that increased risk during recertification (e.g. in relation to leak) is often unaccounted for in the determination of recertification interval, whereas consideration is being given only to the reduced risk after recertification (Vinnem et al., 2016). In other words, existing optimization methods do not account for PSV-recertification-induced-leak, but only other failure modes (Chien et al., 2009; Maher et al., 1988).

In this paper, the main objective is to apply a method that directly optimizes with respect to risk to people, taking into account the safety-critical failure modes "fail-to-open" and "PSV-recertification-induced leak", thus accounting for the influence of recertification within the period after and during recertification.

This paper is delimited to focus on safety-critical failures of PSV, including its relationship with pressure vessels, in gas application in the hydrocarbon industry. It is also delimited to a situation whereby the plant is shutdown for PSV recertification. The rest of the paper is structured as follows. First, existing optimization methods will be reviewed. Second, further investigation on PSV recertification will be presented, including the situation in Norway and the effects of changing recertification interval. Third, a case study will be presented in relation to the selected optimization methodology. Fourth, there will be some discussion on the results. Finally, a conclusion will be drawn.

2. Review of existing methods for the optimization of maintenance interval

Optimization of maintenance interval with respect to maintenance costs while safety is kept as a constraint has been studied by many authors. The early methods focused on test interval optimization based on minimizing the time-average unavailability without considering cost (Jacobs, 1968; Hirsch, 1971; Signoret, 1976; Vaurio, 1991). This approach was later extended to optimization based on cost with safety primarily being a constraint (Vaurio, 1995; Vatn et al., 1996; Dekker, 1996; Vaurio, 1997; Vatn, 1997) and optimization based on equipment risk without consideration for risk to humans (Vaurio, 1995; Jo and Park, 2003; Khalaquzzaman et al., 2010, 2011; Kančev and Čepin, 2011a,b). Cost-based optimization is being widely applied in industrial engineering and features as a step in the RCM (Reliability Centered

Maintenance) process, where it is used to optimize the maintenance interval after a suitable maintenance task would have been selected with the RCM decision tree (Rausand and Vatn, 2008). In addition, cost-based optimization has also found application in the concept of maintenance grouping for setup cost-saving (Wildeman, 1996; Wildeman et al., 1997; Vatn, 2008; Nicolai and Dekker, 2008; Hameed and Vatn, 2012) and major accident risk management (Okoh, 2014, 2015).

Reason (1997) highlights the effect of the amount of direct contact between people and the system. Such contacts constitutes the greatest human performance problem in most high-risk industries where frequency of contact can be seen as a greater error opportunity. The likelihood of error is further analyzed together with neglected maintenance to explain the risks they posed to the system. Besides, the safety-criticality of items is a key contributor to the motivation for high level of maintenance contact (which implies high level of exposure of personnel). As regards optimization to justify the rationale for preventive maintenance, Reason (1997) suggests a graphical approach (Cost vs. Level of maintenance plot) whereby the optimal level of preventive maintenance is determined by combining the cost of both preventive and corrective maintenance and then selecting the level that coincides with the lowest overall maintenance cost (Reason, 1997).

Optimization of maintenance interval with respect to risk has also been in existence. Apeland and Aven (2000) consider one of the main challenges to be the need for comparing options described through different system attributes, i.e. performance measures related to different categories, like fatality, environmental damage and economic loss. They mentioned the possibility of prioritizing these attributes via a weighting system (Apeland and Aven, 2000). Vaurio (1995) demonstrated risk-based maintenance optimization, considering risk to equipment only.

Some literature support the concept of risk-based optimization with consideration for risk to humans. According to Evans and Thakorlal (2004), following the Piper Alpha disaster in 1988, the issue of maintenance personnel exposure has resulted in a paradigm shift in the design of unmanned platforms. Post-Piper Alpha designs for such installations usually omit firefighting systems, e.g. fire pumps, based on the reason that the risk reduction benefit they offer to maintenance personnel is not commensurate with the frequency of visits of the personnel unlike in a manned facility (Evans and Thakorlal, 2004). In other words, fire pumps are considered to offer a negative risk contribution to an unmanned platform, due to increased need for visits by maintenance personnel.

A human-risk-related preventive maintenance problem has also been studied earlier in The Netherlands, where the focus is on scheduling maintenance to prevent fatalities due to unmanageable railway track maintenance workload at night (van Zante-de Fokkert et al., 2007).

Regarding direct focus on PSV, some existing literature have also been seen. Cost-based optimization in relation to reliability has been proposed (Maher et al., 1988). Furthermore, variations to reliability and risk-based approaches have been suggested, which include, the determination of recertification interval by considering a PSV's reliability/risk data as corresponding to one of some categories of reliability/risk-based inspection criteria and then suggesting a corresponding maintenance interval (Chien et al., 2009; Hellemans, 2009).

Concluding, existing approaches tend to focus on the least cost of doing recertification per unit time such that the existing risk acceptance criterion is satisfied (i.e. a reliability, cost-based approach) or the least frequency of doing recertification such that the equipment experiences the least possible risk of damage (i.e. an equipment, risk-based approach). In relation to the objective of this paper, the latter being more relevant to the objective of this paper, needs to be adapted to cover also human risk.

3. Further investigation on PSV recertification

3.1. PSVs in the Norwegian petroleum industry

PSVs are self-contained and self-actuating pressure relief devices. According to American Petroleum Institute (API), a pressure relief device is the general term for a device designed to prevent pressure or vacuum from exceeding a predetermined value in a pressure vessel by the transfer of fluid during emergency or abnormal pressure conditions. Pressure relief devices include reclosing relief devices (e.g. PSVs) and non-reclosing relief devices (e.g. rupture disc or buckling pin devices). PSVs must operate within the specified limits according to international codes and standards (e.g. EN/ISO 4126, API 527 etc) and this includes closing at a predetermined pressure when the system pressure has dropped to a safe level.

The primary purpose of a PSV in a process plant is the final protection of human, asset and the environment, through the controlled venting from an overpressurized vessel, of a specified amount of process fluid at a predetermined pressure. A PSV must respond reliably to the demand arising from the failure of other safety systems to sufficiently control process limits. It is statutory that when the external power sources (i.e. electric, hydraulic and pneumatic) to all safety systems fail, there remains an independent safety system powered only by the medium it protects (Hellemans, 2009). It is not the purpose of the PSV to influence the control/regulation of the vessel's pressure nor to assume the position of a control/regulating valve.

In other words, the PSV protects people and assets, by preventing overpressure from leading to explosion, release or fire whose blast, toxic or thermal effects could be seriously damaging. In the case of the environment, the PSV may be seen as preventing overpressure from leading to an explosion by which containment is lost, probably leading to dangerous pollution.

A look at the offshore petroleum industry in Norway, reveals the close attention being paid to PSVs, whereby the failure is monitored each year across all installations and reported annually in the RNNP (Risikonivå i Norsk Petroleumsvirksomhet) publication of the Petroleum Safety Authority (PSA) of Norway (PSA, 2014). In 2014, the mean percentage of PSV failures (i.e. the mean of the fraction of failed PSV tests over total number of tests) is 1.7%. According to Vinnem and Haugen (2015), the test intervals are unknown for PSVs on individual installations, thus making it difficult to establish possible correlation between test intervals and fraction of failures.

3.2. Effects of changing recertification interval of PSV

3.2.1. Exposure to existing risk

The first aspect to consider is the existing major hazards in the facility. Operations personnel are exposed to this risk part of the time, but when recertification work is performed, the number of persons exposed increases since maintenance personnel also are present. The risk is therefore higher during recertification periods than when recertification is not ongoing. The more recertification, the higher the risk, and vice versa. This can be illustrated as shown in Figure 1, where the risk (expressed as PLL) is plotted (principally) as a function of recertification interval (τ) – increasing recertification interval (less maintenance) implies reduced risk. PLL is the expected number of fatalities within a specified population (or within a specified area) per year (Rausand, 2011).

3.2.2. Introduction of new hazard or initiating event

The previous effect increased risk because the number of people exposed increased (i.e. the consequence increased). However, the performance of recertification work may also have other effects on the

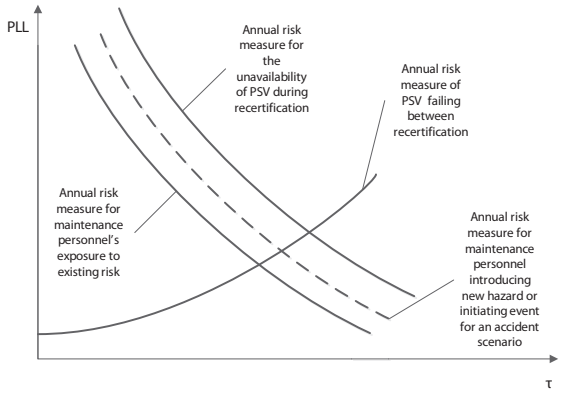

Figure 1: Effects of changing recertification interval of PSV

existing risk level. New hazards may be introduced (due to special equipment or special work operations), ignition probabilities may increase, consequences may increase (due to scaffolding or weather-cladding increasing explosion overpressures), etc (Okoh and Haugen, 2013a,b, 2014).

In this case, the new hazard that is considered is the additional leaks that can be caused by removing and replacing the PSV. This increases the exposure of all personnel present in the plant, during the period when recertification is being performed. Both operations personnel and maintenance personnel will be exposed to this. The magnitude of this effect will clearly be dependent on the type of recertification work to be performed, and in this case it is reasonable to assume that the increase in leak frequency will be proportional to the number of operations performed. This means that increasing number of recertification operations increases risk and vice versa. Plotted against the recertification interval, the risk will decrease with increasing recertification interval, as shown in Figure 1.

3.2.3. Unavailability of PSV due to failure between recertification

PSVs are operating only on demand. With a constant failure rate, the probability of the PSV not operating when required will increase with time. A primary purpose of recertification (including testing) of the PSV is therefore to verify that they are operating as intended and to repair the system if it is not working.

Increasing recertification intervals will thus increase the unavailability of the PSV. If we make the assumption that the risk to personnel is higher, if the PSV is not working compared to when the PSV is working, increased unavailability will also imply increased risk. This is illustrated in Figure 1. This is based on a constant failure rate and disregarding wear-out failures (i.e. the middle section of the bathtub).

3.2.4. Unavailability of PSV during recertification

In addition to unavailability of PSV due to failure, PSV may also be unavailable during recertification. This is relevant when PSV changeover is possible. Normal practice in the offshore industry is however to shutdown the system when you do not have redundant PSVs. This effect is therefore disregarded in the optimization.

3.2.5. Introduction of new failures/errors in the PSV being recertified

Even if the purpose of recertification is to improve the condition of a PSV, errors may be made which introduces failures/errors in the PSV. These may in turn cause the PSV to fail on demand (Okoh and

Haugen, 2013a).

These types of errors will usually go undetected until the next recertification operation takes place, or until there is a demand on the PSV. The effect is that the average unavailability of the PSV increases.

At the next recertification operation, it is likely that previous errors will be detected (effectively canceling out the earlier increase in risk), but at the same time, new errors may be introduced. If we assume that the rate of errors during recertification and the probability of detecting earlier errors is constant, the additional contribution to average unavailability will be constant and can be disregarded in the optimization.

3.2.6. Corrective maintenance

Decreasing recertification interval may increase the need for corrective maintenance on PSVs that have failed. For instance, PSV may become useless with ruptured bellows due to vigorous cycling of the PSV many times per second (i.e. fatigue-related failure). The failure may be detected by process fluid leaking through the bonnet vent, but this is not always detectable visually and other detection devices are not always highly reliable (Hellemans, 2009). Sometimes, personnel put whistles on the bonnet vent and blow it in order to reveal leakages (Hellemans, 2009). The effects on risk would be of a similar type as has been described above, so including the effect could be done by adding further elements to the optimization. For the purpose of this paper, we will assume that failures will not be detected until the next scheduled recertification (since the PSVs are in standby). The effect is then already covered by the PFD for the PSV,

4. Case study

4.1. Risk modelling

In this case study, the risk-based, nuclear-industry approach by Vaurio (1995) will be adapted to the process industry to cover personnel risk in relation to PSV. Optimization based on risk to equipment (e.g. the core damage frequency of a nuclear power plant) was performed earlier by Vaurio (1995) for a single component or a train of components in series, on standby or in normal operation. This involved the definition of a frequency function (i.e. the total average unavailability), R(τ), as equal to the product of the frequency of initiating event (f) and the product of unavailability states (basic events) of safety systems. For such a simple system (being used as an example), the frequency function is expressed mathematically as:

$$R(\tau) = f \bullet (\rho + \frac{d}{\tau} + \frac{\lambda\tau}{2} + \lambda\tau_r) \tag{1}$$

Where the terms in Equation 1 are defined as (Davoudian et al., 1994; Vaurio, 1995; Jo and Park, 2003; Zio, 2007; Verma et al., 2010; Cepin and Kančev, 2011):

- f - frequency of initiating event,
- ρ - human error contribution to unavailability of safety system (i.e. probability of failure due to testing/maintenance),
- τ - interval between tests of safety system,
- d - duration of test of safety system,
- λ - failure rate of safety system.

- d/τ - test contribution to unavailability of safety system (i.e. whereby the safety system is assumed to be overridden during testing).
- $\lambda\tau/2$ - contribution to unavailability of safety system from 'random failures' occurring between tests while the system is on standby.
- τ_r - average duration of corrective maintenance
- $\lambda\tau_r$ - contribution to unavailability of safety system from corrective maintenance
- $\rho + d/\tau + \lambda\tau/2 + \lambda\tau_r$ - the total average unavailability of the safety system.

By setting the derivative $dR/d\tau$ of Equation 1 to zero, the optimal maintenance interval, τ^* is given as:

$$\tau^* = \sqrt{\frac{2d}{\lambda}} \tag{2}$$

However, in this paper, the aforementioned approach (Davoudian et al., 1994; Vaurio, 1995; Jo and Park, 2003; Zio, 2007; Verma et al., 2010; Cepin and Kančev, 2011) will be adapted in relation to the effects of changing PSV recertification interval. Furthermore, event trees will be drawn to illustrate these effects in relation to PSV (See Figures 2 and 3) and frequency functions will be derived from the event trees and used as a basis for the optimization. Meanwhile, the following assumptions, limitations and key definitions have been considered.

- The recertification of PSV encompasses the PSV being isolated, blinded off, depressurized, dismounted, tested/overhauled and reinstalled.
- There is no redundant PSV. The system is shutdown during recertification. This implies that the d/τ term will disappear in further analysis. This is because, the dismounted PSV does not add risk to the operation by being taken down, since the operation will not go on without it.
- If recertification is ongoing, then there are personnel present. The likelihood of undetected gas leak and undetected fire is then 0.0.
- The maintenance personnel are those involved in the performance of recertification. They are assumed to be present part of the time.
- The operations personnel are those involved in production, isolation and depressurization. They are also assumed to be present part of the time.
- The number of people exposed (N) is a combination of both maintenance and production personnel.
- Risk is expressed in terms of potential loss of life (PLL) in this paper. PLL is the expected number of fatalities within a specified population (or within a specified area) per year (Rausand, 2011).
- The recertification optimization formulation assumes $\lambda\tau \ll 1$ and $d \ll \tau$.
- The failure rate of a PSV is assumed to be constant.

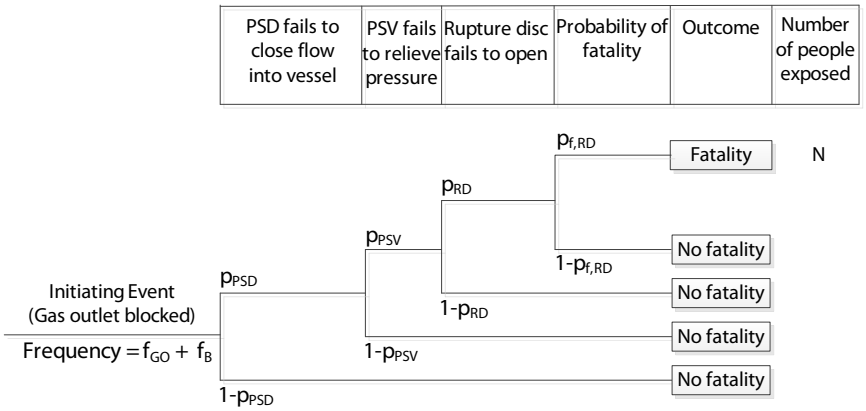

Figure 2: An event tree analysis for the failure mode "PSV fail to close"

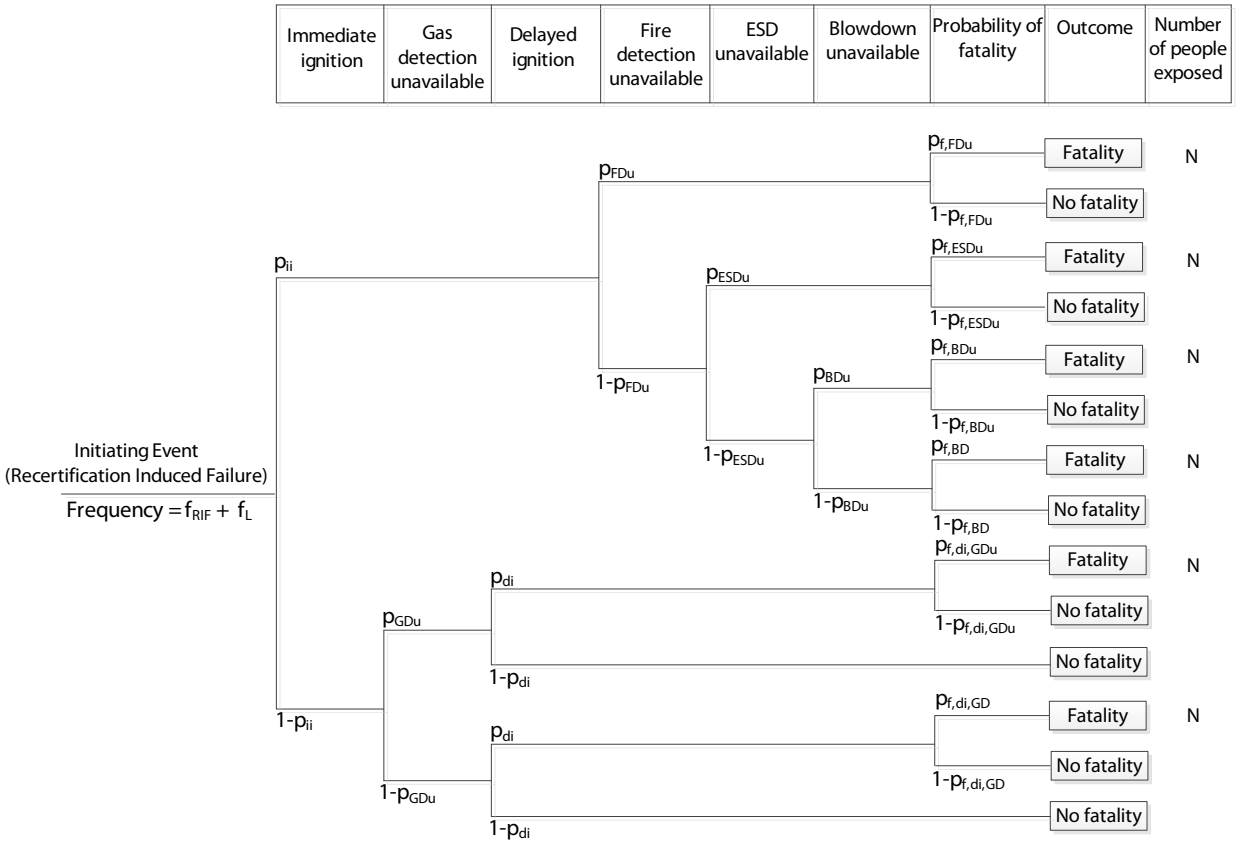

Figure 3: An event tree analysis for the failure mode "PSV recertification induced leak"

4.2. Meaning of notations

The notations on the event trees in Figures 2 and 3 are defined in Table 1 and they can be determined from different sources. The frequency of the initiating event "Gas outlet blocked" (f_{GO}) is associated with outlet block valve failure, loss of power to operate the valve, actuator failure or a process upset in

the control loops (Hellemans, 2009). The term "f_B" is the contribution to this frequency due to human error in relation to the block valve.

Furthermore, the frequency of the initiating event "Recertification induced failure" is associated also with several unacceptable actions such as allowing foreign particles in PSV before reinstallation, subjecting PSV to shock (especially during handling and transportation), putting lift lever in wrong position or tension, damage to outlet piping support, etc. These will lead to internal damage, misalignment and valve seat leak (Hellemans, 2009). Besides, damage/dirt on flange surface, replacement with unrecommended gasket and incorrect attachment of gasket will also lead to leak from the flanged joint. The term "f_L" is the contribution of the associated leak to the aforementioned frequency.

4.3. Relationship between failures and the effects of changing recertification interval of PSV

The failures mentioned in the event trees in Figures 2 and 3 can be matched with corresponding categories of the effects of changing recertification interval of PSV as shown in Table 2.

4.4. The risk-based optimization

We have chosen to express risk in terms of PLL, Potential Loss of Life, which means that it is only the end events with "Fatalities" as outcome that are relevant to include. The total PLL is then calculated from the event trees in Figures 2 and 3 as follows:

$$R(\tau) = R_1(\tau) + R_2(\tau) = PLL_1 + PLL_2 \tag{3}$$

$$R(\tau) = \left(f_{GO} + \frac{f_B}{\tau}\right)\left(\rho + \frac{\lambda_{PSV}\tau}{2}\right) \bullet C_1 + \left(f_{RIF} + \frac{f_L}{\tau}\right) \bullet C_2 \tag{4}$$

Where,

$$C_1 = p_{PSD} \bullet p_{RD} \bullet p_{f,RD} \bullet N \tag{5}$$

and

$$C_2 = N \bullet \sum_{i=1}^{6} p_i \tag{6}$$

Where p_i is probability of ith end event with fatality outcome, which includes the following:

1. $p_1 = p_{ii} \bullet p_{FDu} \bullet p_{f,FDu}$
2. $p_2 = p_{ii} \bullet (1 - p_{FDu}) \bullet p_{ESDu} \bullet p_{f,ESDu}$
3. $p_3 = p_{ii} \bullet (1 - p_{FDu}) \bullet (1 - p_{ESDu}) \bullet p_{BDu} \bullet p_{f,BDu}$
4. $p_4 = p_{ii} \bullet (1 - p_{FDu}) \bullet (1 - p_{ESDu}) \bullet (1 - p_{BDu}) \bullet p_{f,BD}$
5. $p_5 = (1 - p_{ii}) \bullet p_{GDu} \bullet p_{di,GDu} \bullet p_{f,di,GDu}$
6. $p_6 = (1 - p_{ii}) \bullet (1 - p_{GDu}) \bullet p_{di,GD} \bullet p_{f,di,GD}$

Table 1: Failure data from Installation X in Norway

Parameter	Meaning	Value	Source
f_{GO}	Frequency of initiating event "Gas outlet blocked"	0.5	Assumed, probability that the protection system (PSD, PSV, RD) needs to be used per year per vessel
p_{PSD}	PFD(PSD not closing), i.e. probability of failure on demand for the process shutdown (PSD) system to close flow into the vessel	0.0035	Based on RNNP 2015 (average 2012-2015)
p_{PSV}	PFD(PSV not opening), i.e. probability of failure on demand for the process safety valve (PSV) to open	Defined in terms of failure rate	-
p_{RD}	PFD(Rupture disc not opening), i.e. probability of failure on demand for the rupture disc to open	0.0001	(Cadwallader, 1998)
$p_{f,RD}$	Probability of fatality given rupture disc does not open	0.3	Based on QRA for an installation (anonymous)
N	number of maintenance and operation personnel exposed	5	Assumed, based on QRA
f_{RIF}	Frequency of recertification induced failure (RIF)	0.0003	???
p_{ii}	Probability of immediate ignition of gas	0.001	Based on QRA for an installation (anonymous)
p_{GDu}	PFD(Gas detection unavailable), i.e. probability of failure on demand for gas detection system to detect leak	0.008	Based on RNNP 2015 (average 2012-2015)
$p_{di,GDu}$	Probability of delayed ignition given gas detection unavailability	0.016	Based on QRA for an installation (anonymous)
$p_{di,GD}$	Probability of delayed ignition given gas detection availability	0.004	Based on QRA for an installation (anonymous)
p_{FDu}	PFD(FD unavailable), i.e. probability of failure on demand for fire detection system to detect fire	0.004	Based on RNNP 2015 (average 2012-2015)
p_{ESDu}	PFD(ESD unavailable), i.e. probability of failure on demand for emergency shutdown system (ESD) to function in emergency situation	0.09	Based on QRA for an installation (anonymous)
p_{BDu}	PFD(BD unavailable), i.e. probability of failure on demand for blowdown system to depressurize	0.022	Based on RNNP 2015 (average 2012-2015)
$p_{f,FDu}$	Probability of fatality given fire detection unavailability	0.06	Based on QRA for an installation (anonymous)
$p_{f,ESDu}$	Probability of fatality given emergency shutdown system (ESD) unavailability	0.15	Based on QRA for an installation (anonymous)
$p_{f,BDu}$	Probability of fatality given blowdown unavailability	0.08	Based on QRA for an installation (anonymous)
$p_{f,BD}$	Probability of fatality given blowdown availability	0.03	Based on QRA for an installation (anonymous)
$p_{f,di,GDu}$	Probability of fatality given delayed ignition and gas detection unavailability	0.2	Based on QRA for an installation (anonymous)
$p_{f,di,GD}$	Probability of fatality given delayed ignition and gas detection availability	0.21	Based on QRA for an installation (anonymous)
f_L	Frequency of leak per recertification	0.001	Assumed, based on leak statistics and assumed number of recertifications of HC PSVs
f_B	Frequency of block valve manual closure/misalignment per recertification	0.001	(Maher et al., 1988)
ρ	Constant contribution of human error in PSV during recertification	0.01	(Maher et al., 1988)
λ_{PSV}	Failure rate for PSV	0.025	Based on RNNP 2015 (average 2012-2015) (assumed recertification interval of 2 years)

Table 2: Failures Vs. Effect of changing recertification interval of PSV

Failure indicated on event tree	**Effect of changing recertification interval**
Gas outlet blocked (probably due to human error)	Introduction of new failure/error
PSV does not relieve pressure	(1) Unavailability of PSV due to failure between recertification, or (2) Introduction of new failure/error
Leak due to PSV recertification	Introduction of new hazard or initiating event
Failure of PSD, rupture disc, gas detection system, fire detection system, isolation system and blowdown system	Exposure to existing risk

By differentiating R(τ) with respect to τ, setting this to zero and solving the equation with respect to τ, we get the following expression for the optimal interval:

$$\tau^* = \sqrt{\frac{(f_B \bullet \rho \bullet C_1 + f_L \bullet C_2) \bullet 2}{f_{GO} \bullet \lambda_{PSV} \bullet C_1}} \tag{7}$$

By applying the data given in Table 1 to Equation 7, the optimal recertification interval is determined as being equal to 37 years. Compared to the typical intervals applied today of 1-2 years, this is vastly different. If this interval was to be followed, the result for many plants would be that recertification should not be performed at all.

Based on a simple sensitivity analysis, where all input values are marginally changed one by one to see the effect on the final results, we find that only the following parameters have any significant influence on the result (all the others have no or very marginal effect on the interval):

- f_{GO} - Frequency of gas outlet blockage
- p_{PSD} - Probability of PSD not closing
- p_{RD} - Probability of rupture disc failing
- $p_{f,RD}$ - Probability of fatality given rupture disc failing
- $p_{di,GD}$ - Probability of delayed ignition given gas detection available
- $p_{f,di,GD}$ - Probability of fatality given delayed ignition, given gas detection available
- f_L - Frequency of leak per recertification
- f_B - Frequency of block valve manual closure/misalignment per recertification
- λ_{PSV} - Failure rate for PSV

In summary the effects are as follows:

1. If we increase f_{GO}, p_{PSD}, p_{RD}, $P_{f,RD}$ or λ_{PSV}, the interval will decrease. This is because increasing these values will increase the risk associated with gas outlet blocked, implying that it is more important to have a functioning PSV.

2. If we increase $p_{di,GD}$, $p_{f,di,GD}$, f_B or f_L, the interval will increase because the risk associated with the recertification itself increases.

It may be worthwhile to look into some of the key input parameters in more detail and see how modifying these values changes the recertification interval:

- A key factor is obviously how likely it is that a recertification will give a leak, f_L. The value that has been applied in the calculation, 0.001 or a leak from 1 in 1000 recertifications, is estimated from statistics but is quite uncertain. Reducing this value by a factor 10, to 0.0001, reduces the recertification interval to 11.7 years. Even a reduction of two orders of magnitude, to 0.00001, gives a recertification considerably longer than what is commonly used today, at 3.7 years.

- Another important factor is the frequency of gas outlet blocked, f_{GO}. This is in effect the demand rate for the PSV and has also been estimated based on fairly uncertain information. Increasing this value will decrease the recertification interval, but even increasing this from 0.5 per year to 5 per year (i.e. the PSV needs to relieve pressure 5 times per year) gives a recertification interval of 11.7 years.

In broad terms, we can say that changing the values of any of the parameters listed above as having a significant effect on the interval by one order of magnitude will change the recertification interval by approximately a factor of 3. In other words, even taking into account that uncertainties in some of these values can be quite large, we still arrive at the conclusion that the current practice with regard to recertification increases risk to personnel.

5. Discussion and conclusion

This paper has described a case study for optimization of the recertification interval for PSVs, based on risk to personnel working at the plant or performing maintenance. The method relies on input from quantitative risk assessment (QRA) and other data sources to describe the risk to people. It takes into account the different effects that the maintenance interval will have on the safety system availability and also potential risk-increasing effects of maintenance.

Based on typical data from QRAs for offshore installations in Norway and data from the public domain, an optimal recertification interval of 37 years was found. Clearly, a recertification interval this long is not realistic to implement. If we calculate the average PFD for the PSV based on a recertification interval of 37 years (assuming no other tests are performed), we get a value of 0.45, i.e. more or less a fifty-fifty chance that the PSV will work. It may be argued that there will be minimum requirements for the availability of safety systems that should be met and that these will be the governing requirements, not allowing for increase of the maintenance intervals as much as this method indicates. If the purpose of these availability requirements is to protect people, this paper however shows that there are strong arguments for relaxing these requirements, since they may actually have a negative total impact on personnel risk.

One reason why optimization purely with respect to risk is usually not very interesting is because there will be other aspects that also determine the optimal interval, in particular cost of failure and cost of performing the maintenance. The optimization has only considered loss of life (PLL) and not failure modes for the PSVs that can influence production. Optimizing with respect to loss of production may tip the scales in favor of more frequent recertification, although it is noted that the practice today is to shut down the system during recertification, i.e. a loss of production in itself.

It is also noted that the assumption in this paper is that no other testing of PSVs is performed than recertification. If the PSVs can be tested in other ways, the PFD will decrease and the risk reduction achieved by recertification becomes even smaller. This will then increase the optimal interval again.

For safety systems, it can be argued that risk should be the primary factor, since the systems are put in place to reduce risk. The benefits obtained by having the system, therefore should be balanced against the disadvantages. This is particularly relevant when we see that the intervals actually are increased (in some cases significantly) and the cost can thus be reduced at the same time as optimizing risk.

The PSV will also have an effect in reducing risk to assets; by limiting damage to equipment should an accident occur. This has not been taken into account in the present method. To do that, it would be necessary to assign a cost to the personnel risk. This is possible to do (using e.g. the principles applied in cost-benefit analysis of risk reducing measures), but we have chosen not to pursue this further in this paper. The method can however in principle be extended to cover also this aspect. The effect of this is however uncertain since asset risk also will increase by the increased leak frequencies. Without having done the calculations, our view is that taking this into account would not change the intervals dramatically.

The case study has focused on major accident risk and risk associated with occupational accidents has not been explicitly discussed. However, the method can also relatively easily be extended to cover this. This would increase the negative impact of maintenance even more, increasing the maintenance intervals further.

In conclusion, the calculations performed show that the risk related to the maintenance work itself in some cases can be significant and should be considered when maintenance intervals are determined. We are not advocating an approach where this should be the sole criterion, but being aware of this effect and taking that into account in the decision-making should be done.

Acknowledgement

This paper is related to work performed in the MIRMAP project and the authors wish to acknowledge the Norwegian Research Council for their financial support to the MIRMAP project, no 228237/E30, funded by PETROMAKS2.

References

Apeland, S., Aven, T., 2000. Risk based maintenance optimization: Foundational issues. Reliability Engineering and System Safety 67 (3), 285–292.

Cadwallader, L. C., 1998. Selected Component Failure Rate Values from Fusion Safety Assessment Tasks, INEEL/EXT-98-00892. Tech. rep., Idaho National Engineering and Environmental Laboratory, Idaho.

Cepin, M., Kančev, D., 2011. Evaluation of risk and cost using an age-dependent unavailability modelling of test and maintenance for standby components. Journal of Loss Prevention in the Process Industries 24, 146–155.

Chien, C. H., Chen, C. H., Chao, Y. J., 2009. A strategy for the risk-based inspection of pressure safety valves. Reliability Engineering and System Safety 94 (4), 810–818.

Comlaw, 2007. Occupational Health and Safety (Safety Standards) Regulations 1994. Commonwealth of Australia, Canberra. (http://www.comlaw.gov.au/Details/F2007C00737).

Darby, R., 2013. The dynamic response of pressure relief valves in vapor or gas service, part I: Mathematical model. Journal of Loss Prevention in the Process Industries 26 (6), 1262–1268.

Davoudian, K., Wu, J.-s., Apostolakis, G., 1994. Incorporating organizational factors into risk assessment through the analysis of work processes. Reliability Engineering and System Safety 45, 85–105.

Dekker, R., 1996. Applications of maintenance optimization models: a review and analysis. Reliability Engineering & System Safety 51 (3), 229–240.

EC, 2005. Guidance on the Preparation of a Safety Report to meet the Requirements of Directive 96/82/EC as amended by Directive 2003/105/EC (Seveso II), Report EUR 22113 EN. Tech. rep., European Commission.

Evans, J., Thakorlal, G., 2004. Total Loss Prevention - Developing Identification and Assessment Methods for Business Risks. In: 11th International Symposium on Loss Prevention and Safety Promotion in the Process Industries. WP Loss Prevention, Prague, pp. 1207–1214.

Hameed, Z., Vatn, J., 2012. Role of grouping in the development of an overall maintenance optimization framework for offshore wind turbines. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 226 (6), 584–601.

Hellemans, M., 2009. The Safety Relief Valve Handbook: Design and Use of Process Safety Valves to ASME and International Codes and Standards. Butterworth Heinemann, Oxford.

Hirsch, H., 1971. Setting test intervals and allowable bypass times as a function of protection system goals. IEEE Trans. Nuclear Science N-18, 488–494.

HSE, 1992. A guide to the Offshore Installations (Safety Case) Regulations 1992. Health and Safety Executive, London.

Jacobs, I., 1968. Reliability of engineered safety features as a function of testing frequency. Nuclear Safety 9, 303–312.

Jo, Y.-d., Park, K.-s., 2003. Dynamic management of human error to reduce total risk. Journal of Loss Prevention in the Process Industries 16, 313–321.

Kančev, D., Čepin, M., 2011a. Evaluation of risk and cost using an age-dependent unavailability modelling of test and maintenance for standby components. Journal of Loss Prevention in the Process Industries 24 (2), 146–155.

Kančev, D., Čepin, M., 2011b. The price of risk reduction: Optimization of test and maintenance integrating risk and cost. Nuclear Engineering and Design 241 (4), 1119–1125.

Khalaquzzaman, M., Gook, H., Cheol, M., Hyun, P., 2011. Optimization of periodic testing frequency of a reactor protection system based on a risk-cost model and public risk perception. Nuclear Engineering and Design 241 (5), 1538–1547.

Khalaquzzaman, M., Kang, H. G., Kim, M. C., Seong, P. H., 2010. Quantification of unavailability caused by random failures and maintenance human errors in nuclear power plants. Nuclear Engineering and Design 240 (6), 1606–1613.

Maher, S. T., Rodibaugh, R. K., Sharp, D. R., DeSaedeleer, G., 1988. Relief Valve Testing Interval Optimization Program for the Cost-effective Control of Major Hazards. In: Second Symposium on Preventing Major Chemical Accidents: IChemE Symposium Series 110. Institution of Chemical Engineers, Oslo.
URL http://www.icheme.org/communities/subject{_}groups/safetyandlossprevention/resources/hazardsarchive/{~}/media/Documents/SubjectGroups/Safety{_}Loss{_}Prevention/HazardsArchive/S110-PreventingAccidents/S110-13.pdf

Nicolai, R. P., Dekker, R., 2008. Optimal Maintenance of Multi-component Systems : A Review. In: Kobbacy, K., Murthy, D. (Eds.), Complex System Maintenance Handbook. No. 1991. Springer, London, Ch. 11, pp. 263–268.

OGP, 2008. Asset integrity - the key to managing major incident risks. Tech. Rep. 415, International Association of Oil and Gas Producers, London.

Okoh, P., 2014. Optimizing maintenance to manage the major accident risk. In: Institution of Chemical Engineers Symposium Series 159, Hazards 24. Institution of Chemical Engineers, Edinburgh.

Okoh, P., 2015. Maintenance grouping optimization for the management of risk in offshore riser system. Process Safety and Environmental Protection 98 (0), 33–39.

Okoh, P., Haugen, S., 2013a. Maintenance-related major accidents: Classification of causes and case study. Journal of Loss Prevention in the Process Industries 26, 1060–1070.

Okoh, P., Haugen, S., 2013b. The Influence of Maintenance on Some Selected Major Accidents. Chemical Engineering Transactions 31, 493–498.

Okoh, P., Haugen, S., 2014. Application of Inherent Safety to Maintenance-related Major Accident Prevention on Offshore Installations. Chemical Engineering Transactions 36, 175–180.

PSA, 2014. Trends in risk level in the petroleum activity. Tech. rep., Petroleum Safety Authority, Stavanger, Norway.

Rausand, M., 2011. Risk Assessment: Theory, Methods, and Applications, 1st Edition. John Wiley & Sons, New Jersey.

Rausand, M., 2014. Reliability of Safety-Critical Systems: Theory and Applications. John Wiley & Sons, New Jersey.

Rausand, M., Høyland, A., 2004. System Reliability Theory: Models, Statistical Methods, and Applications, 2nd Edition. John Wiley & Sons, New Jersey.

Rausand, M., Vatn, J., 2008. Reliability Centred Maintenance. In: Kobbacy, K., Murthy, D. (Eds.), Complex system maintenance handbook. Springer, London, Ch. 4, pp. 79–108.

Reason, J., 1997. Managing the risks of organisational accidents. Ashgate, Aldershot, UK.

Signoret, J., 1976. Availability of a periodically tested standby system, NUREG/TR-0027. Tech. rep., Nuclear Regulatory Commission, Washington, DC.

USEPA-OSHA, 1996. MOU Between The United States Environmental Protection Agency, Office of Solid Waste and Emergency Response, Office of Enforcement and Compliance Assurance and The United States Department of Labor, Occupational

Safety and Health Administration. USA.
URL http://www.osha.gov/pls/oshaweb/owadisp.show{_}document?p{_}table=MOU{\&}P{_}id=246
van Zante-de Fokkert, J., den Hertog, D., van den Berg, F., Verhoeven, J., 2007. The Netherlands Schedules Track Maintenance to Improve Track Workers' Safety. Interfaces 37, 133–142.
Vatn, J., nov 1997. Maintenance optimisation from a decision theoretical point of view. Reliability Engineering & System Safety 58 (2), 119–126.
URL http://linkinghub.elsevier.com/retrieve/pii/S0951832097000252
Vatn, J., 2008. Maintenance in Railway Industry. In: Kobbacy, K., Murthy, D. (Eds.), Complex System Maintenance Handbook. Springer, London, Ch. 21, pp. 509–534.
Vatn, J., Hokstad, P., Bodsberg, L., mar 1996. An overall model for maintenance optimization. Reliability Engineering & System Safety 51 (3), 241–257.
Vaurio, J., jul 1991. Comments on system availability analysis and optimal test intervals. Nuclear Engineering and Design 128, 401–402.
Vaurio, J., 1995. Optimization of test and maintenance intervals based on risk and cost. Reliability Engineering & System Safety 49 (1), 23–36.
Vaurio, J., apr 1997. On time-dependent availability and maintenance optimization of standby units under various maintenance policies. Reliability Engineering & System Safety 56 (1), 79–89.
Verma, A. K., Ajit, S., Karanki, D. R., 2010. Reliability and Safety Engineering, 2nd Edition. Springer-Verlag, London.
Vinnem, J. E., Haugen, S., Okoh, P., 2016. Maintenance of petroleum process plant systems as a source of major accidents ? Journal of Loss Prevention in the Process Industries 40, 348–356.
URL http://dx.doi.org/10.1016/j.jlp.2016.01.021
Wildeman, R., Dekker, R., Smit, A., jun 1997. A dynamic policy for grouping maintenance activities. European Journal of Operational Research 99 (3), 530–551.
Wildeman, R. E., 1996. The Art of Grouping Maintenance. Doctoral, Erasmus University Rotterdam.
Zio, E., 2007. An Introduction to the Basics of Reliability and Risk Analysis. World Scientific Publishing Co. Pte. Ltd., Singapore.