Säkerhetsklassificering för kritisk instrumentering inom processindustrin

Karin Johansson

Department of Fire Safety Engineering
Lund University, Sweden

Brandteknik
Lunds tekniska högskola
Lunds universitet

Report 5196, Lund 2006

Rapporten har finansierats av Hydro Polymers AB

Säkerhetsklassificering för kritisk instrumentering inom processindustrin

Karin Johansson

Lund 2006

Titel
Säkerhetsklassificering för kritisk instrumentering inom processindustrin

Title
Classification of safety instrumented systems in the process industry sector

Författare/Author
Karin Johansson

Report 5196
ISSN: 1402-3504
ISRN: LUTVDG/TVBB--5196--SE

Antal sidor/Number of pages: 67
Språk/Language: Svenska/Swedish
Illustrationer/Illustrations: Karin Johansson

Sökord
IEC 61511, klassificering, processindustri, risk, riskanalys, riskhantering, riskmatris, SIL

Keywords
classification, IEC 61511, process industry, risk, risk analysis, risk management, risk matrix SIL

Abstract
The base of the work is the standard IEC 61511 "Functional Safety – Safety Instrumented Systems for the Process Industry Sector". Developing a method for Hydro Polymers to decide a suitable Safety Integrity Level, SIL, for the safety instrumented system is the purpose of this thesis project. Assigning a SIL to the process is one way to handle the risk assessment and make the process adequately safe. The new method will be used for existing equipment and modifications as well as new projects. This report contains a description of theories on the subject such as: use of barriers, tolerable risk levels and types of errors in the systems. It also contains a summary of standard IEC 61511 and an overview of different methods of SIL assignment.

Brandteknik
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

brand@brand.lth.se
http://www.brand.lth.se

Telefon: 046 - 222 73 60
Telefax: 046 - 222 46 12

Department of Fire Safety Engineering
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

brand@brand.lth.se
http://www.brand.lth.se/english

Telephone: +46 46 222 73 60
Fax: +46 46 222 46 12

Sammanfattning

Säkerhetssystemen i processindustrin har annorlunda riskprofiler idag tack vare den tekniska utvecklingen som skett inom området. De nya systemen består ofta av elektroniska och programmerbara system medan de gamla oftast var baserade på reläer. I de gamla systemen var det främst hårdvarufel som påverkade driftsäkerheten av systemen medan i dagens system har mjukvarufelen nu fått en allt större betydelse. För att underlätta hanteringen av dessa nya typer av fel har nya standarder framkommit. Den standard som främst berör processindustrin är SS-EN 61511 ”Funktionssäkerhet – Säkerhetskritiska system för processindustrin”.

Standardens syfte är att ställa krav på de säkerhetskritiska systemen så att man kan lita på deras förmåga att behålla processen i eller föra den till ett säkert tillstånd. I standarden finns det krav för alla faser av systemets livscykel.

Syftet med detta projekt är att ta fram en metod som är anpassad till Hydro Polymers för att bestämma vilken säkerhetsnivå, SIL, som är lämplig på den säkerhetskritiska instrumenteringen. Att bestämma SIL är ett sätt att hantera riskerna i processen så att instrumenteringen blir tillräckligt säker. Metoden ska kunna användas för nya projekt, vid förändringar och på befintlig utrustning.

I rapporten finns en beskrivning av teorier om riskhantering i processindustrin så som t ex barriärer, tolererade risker och feltyper i säkerhetssystemen. Rapporten innehåller även en sammanfattning av innehållet i standarden och en genomgång av de metoder som finns för att bestämma SIL.

Metoden som utvecklats består av tre delar: grovanalys, utbyggd HAZOP och en detaljanalys. Grovanalysen används för att identifiera händelser med stora risker. De identifierade riskerna analyseras med den utbyggda HAZOP-analysen för att bestämma SIL. Är konsekvenserna av händelsen mycket allvarliga eller om resultatet från HAZOP-analysen är SIL 3 ska den detaljerade analysen genomföras.

För att utvärdera metoden har några riskområden inom företaget valts ut. De utvalda områdena är: generella risker i en ångpanna, läckage från en stor klorledning utomhus, övertryck i cellsalens klorsystem och skenande autoklav i PVC-fabriken.

Grovanalysen som inleder metoden är inte utvärderad inom ramen för detta arbete då det inte är en nyutvecklad metod utan en gammal beprövad teknik. Utvärderingen av den utbyggda HAZOP-analysen fokuserades på hur det går att klassificera resultaten i konsekvens- och sannolikhetsklasser samt hur den förenklade barriäranalysen fungerar. Den detaljerade analysen har testats i sin helhet då den är ny för företaget.

När de första testerna gjordes upplevdes det svårt att klassificera riskerna utan hänsyn till barriärerna. Efter några tester när analysgruppen vant sig vid tankesättet gick det lättare. Den detaljerade analysen var komplicerad, men på detta stadium kan inte några omfattande omarbetningar motiveras då den gav ett bra resultat. Den detaljerade analysen kommer inte att användas så ofta vilket gör det omotiverat att lägga mycket tid på att utveckla en enklare metod som fortfarande ger ett bra resultat.

Summary

Safety systems in the process industry have new risk profiles due to technical progress. Software failures are the most important risk factor in new electronic and programmable systems. In the old hardwired relay systems, however, hardware failures were most important. This technical progress and the resulting change in risk profiles has risen a need for safety standards. Most important to the process industry of the newly developed standards is IEC 61511 “Functional Safety – Safety Instrumented Systems for the Process Industry Sector”. Swedish law does not require the industry to follow the standard, it is hence optional.

The aim of the standard IEC 61511 is to yield a safety instrumented system that can be confidently entrusted to place and/or maintain the process in a safe state. The standard states requirements for the specification, design, installation, operation, and maintenance of the safety instrumented system.

Developing a method for Hydro Polymers to decide a suitable Safety Integrity Level, SIL, for the safety instrumented system is the purpose of this thesis project. Assigning a SIL to the process is one way to handle the risk assessment and make the process adequately safe. The new method will be used for existing equipment and modifications as well as new projects.

This report contains a description of theories on the subject such as: use of barriers, tolerable risk levels and types of errors in the systems. It also contains a summary of standard IEC 61511 and an overview of different methods of SIL assignment.

The developed method consists of three parts: screening analysis, an extended HAZOP analysis, and detailed analysis. Screening analysis is used to identify the scenarios with significant risks. Identified risks are analysed using the extended HAZOP to assign SIL. If consequences are severe or if the resulting SIL is 3, the detailed analysis is used.

Evaluation of the new method has been done by analysing parts of the existing plant at Hydro Polymers. General risks at the steam boiler, leakage from a large outdoor chlorine pipe, overpressure in the cell room chlorine system, and a run-away reaction scenario are chosen for evaluation.

As the screening analysis in the method is not new it has not been evaluated within this work. In the evaluation of the extended HAZOP focus was on the classifications of consequences and probability. The complete methodology of the detailed analysis has been evaluated, as it is completely new to the company.

During the first tests of the extended HAZOP the experience was that it was hard to classify the risks without considering the safety barriers already installed. After a few tests the analysis team got used with the way of thinking and it became easier. When tested, the detailed analysis was found complicated. No need for major changes is foreseen at this stage. The

analysis team not being familiar with the method is the most problematic aspect. As the detailed analysis is not expected to be frequently used, it is allowed to be more complex.

Förord

Denna rapport är ett examensarbete som ingår som avslutande moment i utbildningen till civilingenjör i riskhantering vid Lunds Tekniska Högskola. Examensarbetet omfattar 20 högskolepoäng vilket motsvarar 20 veckors arbete. Arbetet är utfört hos Hydro Polymers AB i Stenungsund.

Jag vill tacka mina handledare Anders Jacobsson på Brandteknik, LTH och Göran Stjern på Hydro Polymers för att all hjälp och inspiration. Ni fanns alltid till hands för att svara på alla mina frågor.

Ett stort tack till alla er som hjälpt och stöttat mig under skrivandet av detta arbete. Framförallt vill jag tack Inger, Matilda och Magnus för hjälpen med korrekturläsandet.

Slutligen vill jag tacka alla på Hydro Polymers för gemenskapen på morgonfika och bingopromenader. Jag kände mig som en i gänget.

Karin Johansson

Stenungsund, februari 2006

Innehållsförteckning

1 Inledning

Detta projekt är ett examensarbete som utförts på Hydro Polymers AB i Stenungsund. Examensarbetet har standarden SS-EN 61511 som utgångspunkt och målet är att skapa en metod för att avgöra erforderliga säkerhetsnivåer till processen.

1.1 Bakgrund

Moderna säkerhetssystem i processindustrin har en helt annorlunda riskprofil jämfört med äldre system (Weibull 2004). De nya systemen består av elektroniska och programmerbara system medan de gamla oftast var baserade på reläer. Från att mest ha handlat om hårdvarufel har mjukvarufelen nu fått allt större betydelse. För att underlätta hanteringen av dessa nya typer av fel har nya standarder framkommit. Den standard som främst berör processindustrin är SS-EN 61511 ”Funktionssäkerhet – Säkerhetskritiska system för processindustrin”.

Standarden ställer krav på den säkerhetskritiska instrumenteringen genom SIL, ”Safety Integrity Level”. Det finns fyra nivåer i SIL-systemet med olika krav på funktionssäkerheten hos instrumenten. En process med stora risker kräver högre SIL än en process med mindre risker.

1.1.1 Hydro Polymers

Norsk Hydro ASA är en börsnoterad norsk koncern med säte i Oslo. Hydro Polymers utgör en sektor inom koncernen som är Europas fjärde största PVC-producent. Anläggningar finns i Sverige, Norge och England. Hydro Polymers AB i Stenungsund började sin verksamhet 1967 och ingår sedan 1984 i Hydro-koncernen. Antalet anställda är 370. Produktionen är kontinuerlig med planerade underhållsstopp.

Att tillverka PVC är en flerstegsprocess. Hydro Polymers anläggning i Stenungsund består av tre produktionssteg:

- Klor
- Vinylkloridmonomer, VCM
- Polyvinylklorid, PVC

Råvaror till klorproduktionen är koksalt, natriumklorid, och elkraft. Saltet löses i vatten och passerar elekrolysceller. I cellen bildas klorgas vid anoden, +, av titan och natrium vid katoden, -, av kvicksilver. Natriumet tvättas ur kvicksilvret med hjälp av vatten. Vid denna process bildas vätgas och natronlut. Vätgasen används som bränsle i ångpannan och natronluten säljs till främst cellulosaindustrin. Klorgasen går vidare i produktionskedjan till VCM-fabriken.

VCM tillverkas av klorgas och eten. I en direktkloreringsprocess tillverkas mellanprodukten dikloretan, EDC, som är en förening av eten och klor.

EDC krackas sedan genom uppvärmning till cirka 500°C. Då slås EDC-molekylerna sönder till VCM-molekyler och saltsyra. Saltsyran går vidare till en oxikloreringsprocess där kloret får reagera med mer eten och syre. Denna process genererar ytterligare EDC som går till krackningen.

Det sista steget i tillverkningen av PVC är polymerisationsprocessen. Här blandas VCM med vatten och tillsatskemikalier. I reaktorn, autoklaven, sker polymerisationen vid högt tryck och noggrann temperaturkontroll. Vid reaktionen kopplas VCM-molekylerna ihop till långa kedjor PVC. När reaktionen är klar avskiljs vattnet och det vita PVC-pulvret torkas.

PVC har flera olika användningsområden då egenskaperna skiftar från mjukt till styvt och starkt. PVC används inom sjukvården till blodpåsar och dialysslangar och inom byggsektorn till bland annat rör, kablar, golv och fönster.

1.2 Syfte

Syftet är att ta fram en metod som är anpassad till Hydro Polymers för att bestämma vilken integritetsnivå, SIL, som är lämplig på den säkerhetskritiska instrumenteringen. Att bestämma SIL är ett sätt att hantera riskerna i processen så att instrumenteringen blir tillräckligt säker. Metoden ska kunna användas för nya projekt, vid förändringar och på befintlig utrustning. För Hydro Polymers är det viktigt att metoden blir lättanvänd.

1.3 Metod

Arbetet inleds med litteraturstudier. Litteraturstudierna ska ligga till grund för skapandet av metoden. När metoden är klar kommer den att testas på olika delar av Hydro Polymers anläggning. Efter testerna genomförs utvärdering och eventuella redigeringar i metoden.

1.4 Problemformulering

Projektet består av de två huvudfaserna metodutveckling samt test och utvärdering av metoden. Problemformulering med frågeställningarna till de båda huvudfaserna finns här nedan.

1.4.1 Utvecklingsfasen

För att kunna skapa en metod anpassad till Hydro Polymers studeras ett flertal generella riskanalysmetoder för bestämning av SIL. Följande frågor är centrala för denna fas i projektet:

- Hur bedöms SIL för ett riskobjekt?
- Vad blir det för skillnader i tillvägagångssättet för befintlig utrustning, vid ändringar och för nya projekt?

1.4.2 Test och utvärderingsfas

De två faserna kommer delvis att gå i varandra, mindre tester kommer att genomföras inom ramen för utvecklingsfasen. När metoden anses färdig för utvärdering bör följande frågeställningar beaktas:

- Är anvisningen lätt att följa?
- Är resultaten repeterbara? Blir resultatet detsamma oavsett vem som genomför analysen?

1.5 Avgränsningar

Den utvecklade företagsmetoden kommer endast att testas på en del av Hydro Polymers riskområden. Hela anläggningen kommer inte att ingå i projektet.

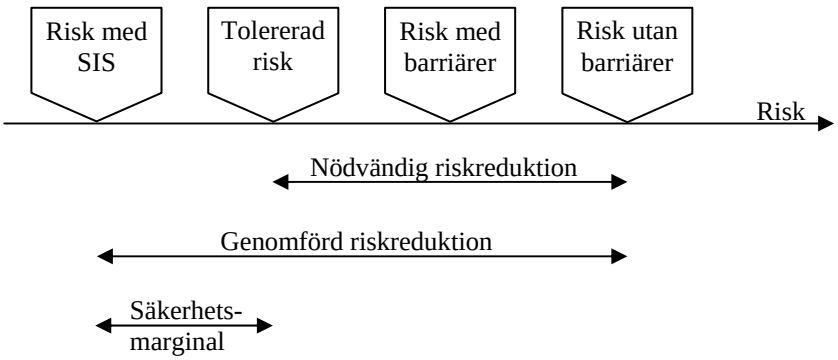
1.6 Rapportens disposition

Rapporten behandlar först generell riskhanteringsmetodik inom processindustrin och beskrivning av standarden. Därefter finns ett antal beskrivningar av olika metoder som finns för att bestämma SIL. Efter metodgenomgången följer utvecklingen av den nya metoden. Rapporten avslutas med ett kapitel om hur metoden testats och utvärderats. I slutet av rapporten finns en förteckning över de förkortningar som används i rapporten.

2 Riskhantering

Den säkerhetskritiska instrumenteringen eller Safety Instrumented System, SIS, används för att reducera riskerna i processen. Ett SIS består av sensorer, logiklösare och manöverdon med uppgift att ta processen till ett säkert läge när en störning uppstår. Ett SIS kan vara uppbyggt av flera funktioner som kallas säkerhetskritiska instrumentfunktioner, SKIF. Att installera ett SIS är dock inte den första åtgärden för att reducera en risk. Den första åtgärden bör vara att, om möjligt, göra processen ”inherently safer”. Begreppet ”inherent safety” kan översättas med inneboende eller inbyggd säkerhet. Med detta menas att själva process-betingelserna ändras för att minska faran, till exempel sänkt tryck, minskad mängd eller ofarligare kemikalier. Om det inte går att göra processen ”inherently safer” är nästa åtgärd att införa skyddsbarriärer på olika nivåer, se figur 1. I figuren finns alla barriärer uppräknade i den ordning som de aktiveras, inte i den ordning som de installeras. Hade figuren varit uppbyggd i installationsordning hade den säkerhetskritiska instrumenteringen varit placerad längre ut då det är en av de sista utvägarna för att göra processen tillräckligt säker. Riskreduktionen illustreras i figur 2. Alla risker större än den tolererade kräver riskreducerande åtgärder. Att installera olika typer av barriärer räknas som riskreducerande åtgärder. (Weibull 2004)

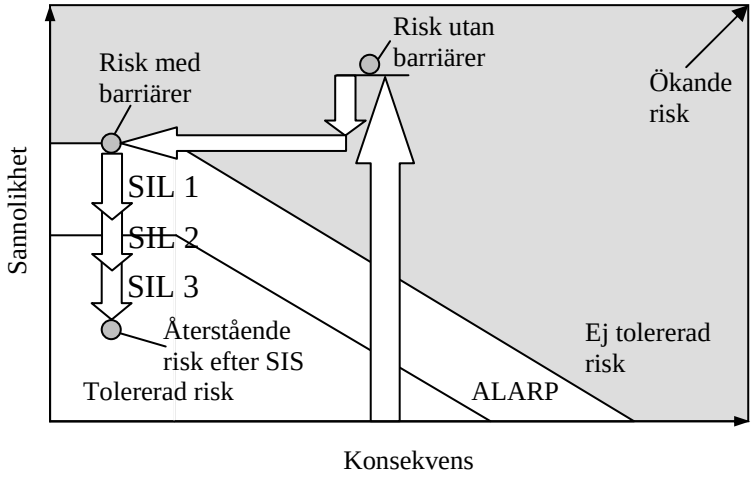
Figur 1 Översikt av barriärer till en process



Figur 2 Riskreduktion

Det går aldrig att helt eliminera en risk utan endast att reducera den. Risken beräknas genom att multiplicera sannolikheten med konsekvensen. De flesta riskreducerande åtgärderna sänker sannolikheten för att händelsen ska inträffa, medan en del går ut på att sänka konsekvensen istället. Figur 3

illustrerar hur de olika åtgärderna påverkar riskbilden. Exempel på åtgärder som reducerar sannolikheten är säkerhetsventiler och exempel på konsekvensreducerande åtgärder är invallningar och sprinklersystem. (Wiegerinck 2002)



Figur 3 Riskreducerandeåtgärders påverkan på riskbilden

Oftast begränsas riskanalyser till att endast innefatta konsekvenser för människor, både personal och allmänhet, ibland tas även miljökonsekvenser med. Konsekvenser för ekonomin såsom egendomsskador, produktionsbortfall och dåligt ryckte borde tas med enligt Marszal et al (1999) då det är större chans att välja ”rätt” SIL om de ekonomiska påverkningarna är med i analysen. White (2000) anser istället att fokus ska vara på säkerheten. Är en process säker för människor är den oftast säker för miljön resonerar White. Inte heller ekonomiaspekter ska tas med i analysen av säkerhetssystemet. Skydd mot ekonomisk skada ska ske genom det vanliga kontrollsystemet eller av ett eget system.

2.1 Tolererad risk

Då riskerna i praktiken inte går att eliminera helt reduceras de till en acceptabel eller tolerabel nivå. I absolut mening är inga risker acceptabla men man kan i realiteten nå en nivå som kan tolereras under en begränsad tid. Den tolerabla risknivån är beroende av flera faktorer: faktiska risken, upplevda risker, verksamhetens nytta, moraliska aspekter och från vems synpunkt risken bedöms, företagets, arbetsgivarens, arbetstagarens eller samhällets.(Kemikontoret 2001)

Alla risker går inte att reducera ner till den tolererade nivån men då nyttan av aktiviteten är stor väljer vi att ändå utsätta oss för riskerna (Wiegerinck 2002). Inom dessa områden används uttrycket ”As Low As Reasonably Practical”, ALARP. I ALARP-modellen delas riskerna i tre kategorier:

a) Risken är så stor att den inte kan tolereras.

b) Risken är, eller har gjorts, så liten att den är obetydlig.

c) Risken är någonstans mellan a) och b) har reducerats så långt det praktiskt är möjligt med tanke på nyttan den tillför.

Då en risk har reducerats enligt ALARP-modellen är den återstående risken den tolerabla risken för den specifika applikationen. Konceptet med ALARP går att använda både tillsammans med kvalitativa och kvantitativa nivåer. (SS-EN 61511-3 2005)

Den tolererade risken går att definiera på flera sätt. Risken kan gälla en process, en fabrik eller ett företag. Om den tolerabla risken väljs för en enskild process måste den bli lägre än om den väljs för ett företag. Då den tolerabla risknivån bestäms på processnivå kommer olika delar av en fabrik och ett företag att ha olika tolerabla risknivåer vilket kan leda till problem. Risknivån kan beskrivas med hjälp av skador på människor, dödsfall för personal eller allmänhet, skador på miljön eller påverkan på ekonomin. (Bhimavarapu & Stavrianidis 2000)

Koncernen Hydro rekommenderar att personer utanför fabriksområdet inte ska utsättas för en större risk att dö än 10^{-5} per år. Inom fabriksområdet finns två olika kriterier. Befinner man sig på ett kontor eller i kontrollrum ska inte risken vara större än 10^{-4} per år, medan risken får vara upp till 10^{-3} per år om man befinner sig på särskilt utsatta platser. (Hydro SARA)

2.2 Barriärer

Det finns flera olika typer av barriärer som brukar delas in i olika grupper. Passiva, aktiva, mekaniska samt mänskliga ingripanden är några av de indelningar som används. Passiva barriärer kräver ingen energi för att fungera. Exempel på passiva barriärer är invallningar och flamskydd, även konstruktionen av tryckkärl kan vara en passiv barriär. Aktiva barriärer kräver energi för att fungera. De mekaniska skydden är en undergrupp till de aktiva, de mekaniska har en inbyggd energikälla. Säkerhetsventiler och sprängbleck är exempel på mekaniska skydd. Exempel på aktiva barriärer med extern energikälla är förreglingssystem och styrsystem. Ingripande av operatörer är också en typ av barriärer. Hur effektiv denna barriär är beror på hur väl operatörerna är tränade på att genomföra ingripandet. (White 2000)

Om ”inherent safety” konceptet används när processen designas kan flera passiva barriärer byggas in. Dowell (1999) tar upp flera exempel på hur detta kan göras. En passiv barriär mot övertryck i en reaktor är att designa kärlet så att det klarar det högsta trycket som kan uppstå i det. En destillationskolonn kan ges en passiv barriär mot övertryck orsakat av fel i regleringen till återkokaren genom design. I designen ska kondensorn kunna kyla bort mer värme än vad återkokaren kan tillföra. Ett passivt överfyllnadsskydd kan vara att leda tillbaka överskottet till den tank det pumpats ifrån.

Vid bestämning av SIL är antalet oberoende barriärer ofta en viktig parameter. För att räknas som en oberoende säkerhetsbarriär måste följande krav uppfyllas:

- Måste vara oberoende d v s ett fel får inte kunna slå ut mer än en barriär.
- Ska reducera risken minst 100 gånger.
- Tillgängligheten måste vara minst 99%.
- Ska vara speciellt designad för att förhindra eller mildra konsekvenserna av en farlig händelse.
- Måste vara pålitlig att den gör det som var tänkt.
- Ska kunna revideras och granskas.

Om det vanliga styrsystemet, ofta kallat BPCS – basic process control system, ska räknas som en barriär gäller det att tänka genom det noga. Om den initierande händelsen är ett fel i BPCS kan inte BPCS samtidigt vara en barriär. Att tänka på när antalet oberoende barriärer beräknas är att om BPCS räknas som en barriär kan inte ett larm som har genererats av samma system var en barriär. Dessa är inte oberoende för om systemet havererar kommer inget larm att genereras. (Dowell 1998)

Ett exempel på när BPCS kan vara en barriär är en reaktor där högt tryck och hög temperatur hänger ihop. I BPCS finns en reglering av ångtillförseln som styrs av en temperaturgivare. Om temperaturen stiger stängs ångtillförseln vilket är ett sätt att förhindra högt tryck. BPCS är en barriär då det förhindrar det farliga tillståndet. (SS-EN 61511-3 2005)

2.3 Feltyper

Det finns flera olika typer av fel som kan inträffa på säkerhetskritisk instrumentering. En kort beskrivning av de olika benämningar som finns på feltyperna och vad man ska tänka på för att undvika dem följer nedan.

2.3.1 Slumpfel

Slumpfelen är fel i komponenter som beror på slumpvisa svagheter och åldrande. Felen är inte kopplade till någon speciell händelse eller betingelser utan kan uppstå när som helst. När tillverkare uppger felfrekvenser för utrustning är det oftast slumpfelen som avses. Sannolikheten för slumpfel kan minskas genom att installera redundanta system. (Weibull 2004)

2.3.2 Latenta fel

Om ett säkerhetssystem är drabbat av latenta fel eller oupptäckta fel kan det få svåra konsekvenser. Många system bygger på att de passivt väntar på att utföra en åtgärd när vissa betingelser uppstår. Man vet inte om systemet fungerar förrän det behövs. För vanliga instrumentsystem är oftast denna detektionstid kort men för säkerhetssystem kan den bli mycket lång. Detta

är viktigt att tänka på vid design av säkerhetssystem. För att undvika de latenta felen är det viktigt att regelbundet testa säkerhetssystemen. (Weibull 2004)

2.3.3 Systematiska fel

Systematiska fel kallas även dolda då är odetekterade, om ett systematiskt fel detekteras åtgärdas det och är inte längre något fel. De systematiska felen består av brister som byggs in i systemet under design, installation och drift. Felen gör att systemet inte fungerar som det är tänkt i vissa speciella situationer. Antalet systematiska fel ökar med systemets komplexitet. Med programmerade system har problemen med systematiska system ökat, dels eftersom systemen inbjuder till komplexitet och dels eftersom det är så lätt att ändra och lägga till nya funktioner. Redundanta system har ofta samma systematiska fel så det är oftast inte till någon hjälp att installera redundans, om systemen bygger på olika teknik kan vissa av de systematiska felen avhjälpas. (Weibull 2004)

2.3.4 Felsäkerhet

Felsäkerhet, eller på engelska ”fail safe”, definieras på följande sätt: *Felsäkerhet innebär att sannolikheten att komponenten felar i sitt säkra läge är mycket större än att den felar i osäkert läge.* Vilket som är komponentens säkra läge beror på konfigurationen. Vanliga felsäkra komponenter är fjäderbelastade ventiler, vid ett strömbortfall tar fjäderkraften ventilen till sitt säkra läge som kan vara öppen eller stängd. (Weibull 2004)

Traditionellt använda komponenter i processindustrin som ventiler och reläer är relativt felsäkra men det är inte elektroniska och programmerbara system. Ett traditionellt programmerbart system felar cirka hälften av gångerna i sitt säkra läge. Dessutom är de flesta felen odetekterbara. Det går att öka andelen säkra fel i dessa system men det kräver speciell utformning av kretsarna och mer avancerad diagnostik. (Weibull 2004)

2.3.5 Gemensam felkälla

Gemensam felkälla eller engelskans ”common cause” är de fel som drabbar gemensam utrustning och slår ut flera system. Exempel på gemensam utrustning kan vara ingångskort till styrsystemet, processanslutningar och processorer. Även olika kablar i samma kabelstråk kan drabbas av en gemensam felkälla.

När processtyrningsfunktionerna centraliseras ökar risken för fel från en gemensam felkälla. Vilka konsekvenser ett fel får är svårt att förutsäga, många system är sammankopplade och de gemensamma felkällorna är sällan helt utredda.

Även för redundanta system kan det finnas gemensamma felkällor. För att ange hur stor del av felen som inte är omfattade av redundansen i systemet

används β-faktor. Tillverkare av t ex redundanta PLC:er bör uppge β-faktorn för systemet. Om β-faktorn inte är känd bör 0,1 användas.

3 Standard SS-EN 61511

I detta kapitel finns en beskrivning av standardens historia, uppbyggnad, innehåll samt för- och nackdelar med standarden. Det finns även en beskrivning av olika typer av programspråk som kan användas för att programmera de system som berörs av standarden.

3.1 Historia

Ett första steg mot ett annorlunda synsätt på säkerhetssystemen i processindustrin togs den 24 februari 1992. Då lagstiftades det i USA att både processen och de tillhörande säkerhetssystemen skulle ingå i en omfattande ”Process hazard analysis”, PHA. I PHA ingår att identifiera och utvärdera riskerna i processen samt att införa säkerhetssystem som minskar dessa risker. Designen av säkerhetssystemet skulle följa ”good engineering practice”. Ett av problemen var att det inte fanns en standard som definierade vad som var ”good engineering practice”, vilket ledde till subjektiva bedömningar. 1996 antogs i USA en standard ANSI/ISA S84.01 där implementeringen av processäkerhetssystem definierades. Standarden kan beskrivas som en samling av ”best practice” bland användare av SIS. Det var i denna standard som ”Safety integrity level”, SIL infördes för att definiera kraven på säkerheten. I standarden definieras nivåerna i SIL-systemet enligt tabell 1. De europeiska standarderna IEC 61508 och 61511 motsvarar den amerikanska ANSI/ISA S84.01. (Beckman 1998)

Tabell 1 Definitionen av nivåerna i SIL-systemet

SIL	Sannolikhet för fel vid anrop	Riskreduktion
4	10^{-4}-10^{-5}	10 000 – 100 000
3	10^{-3}-10^{-4}	1 000 – 10 000
2	10^{-2}-10^{-3}	100 – 1 000
1	10^{-1}-10^{-2}	10 – 100
-	$>10^{-1}$	<10

Enligt Weibull (2005) var Storbritannien pådrivande för utvecklingen av standarder i Europa. IEC 61508 var den första av de europeiska standarderna inom området. Standarden publicerades i december 1998. I oktober 2002 publicerades den som svensk standard under namnet SS-EN 61508 ”Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska system”. IEC 61511 är en sektorstandard för processindustrin som i september 2005 fick sitt svenska namn SS-EN 61511 ”Funktionssäkerhet – Säkerhetskritiska system för processindustrin”. Den första delen av IEC 61511 publicerades i januari 2003. (SIS 2005)

I Sverige finns inga lagkrav på att man ska följa dessa standarder utan de är frivilliga, men myndigheterna kommer att utgå från standarden vid

revisioner och föreskrifter. Om man inte jobbar efter standarderna ska man kunna motivera det väl. (Weibull 2005)

De nya standarderna gör det möjligt att utveckla ny teknologi för säkerhetsfunktionerna. Detta beroende på att standarderna inte föreskriver exakt hur man ska gå till väga utan endast vilka mål som ska uppnås. Nu är det möjligt att komma fram med alternativ till de traditionella reläsystemen (Piggin 2004). Ytterligare en följd av de nya standarderna är att det nu är tillåtet att använda gemensam utrustning för kontroll- och säkerhetsfunktioner, speciellt gäller det logiklösare. Detta är inte rekommenderat men tillåtet om logiklösaren är klassad enligt SIL. Goble (2005) beskriver det som ”ett gatlopp” att lyckas designa ett kombinerat system för kontroll och säkerhet, speciellt om det krävs hög SIL på systemet. Goble är nöjd med formuleringarna i standarden som inte förbjuder en gemensam lösning men manar till stor försiktighet om en kombination görs. Weibull (2005) nämner standardens absoluta krav på separation av kontroll- och säkerhetsfunktioner då felet både orsakar och utlöser händelsen. Ett exempel på ett sådant fall är överfyllnadsskydd till en tank. Om nivåmätaren slutar fungera och inte registrerar hög nivå kommer mer vätska att pumpas in och tanken kommer överfyllas. I detta fall krävs en separat nivågivare till säkerhetssystemet.

3.2 Uppbyggnad och innehåll

Standard SS-EN 61511 är uppdelad i tre delar:

Del 1: *”Allmänt, definitioner samt fordringar på system, maskinvara och programvara*” innehåller en beskrivning av standardens krav.

Del 2: *”Vägledning vid tillämpning av IEC 61511”* innehåller råd för tillämpningen av standarden.

Del 3: *”Vägledning vid bestämning av erforderliga säkerhetsnivåer (SIL)”* innehåller råd för bestämning av erforderlig SIL.

I standardens första del (SS-EN 61511-1 2005) framgår att standarden riktar sig till elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska instrumentsystem. Är systemets logik baserad på en annan teknik gäller de grundläggande principerna från standarden ändå. Standarden innefattar sensorer och manöverdon oavsett teknik.

I standarden är de två koncepten ”safety lifecycle” och ”safety integrity level” fundamentala för tillämpningen. ”Safety lifecycle” betyder att alla faser från idé, design, implementering, drift och underhåll till skrotning av det säkerhetskritiska systemet innefattas av standarden. (SS-EN 61511-1 2005)

Syftet med standarden är att ställa krav på de säkerhetskritiska systemen så att man kan lita på deras förmåga att behålla processen i eller föra den till ett

säkert tillstånd. Det finns krav för alla faser i livscykeln. (SS-EN 61511-1 2005)

I standarden definieras en säkerhetsfunktion som *”function to be implemented by a SIS, other technology safety-related system or external risk, reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event”*. (SS-EN 61511-1 2005)

Innehållet i standarden kan kort sammanfattas i följande punkter:

- specifikation av krav för att uppnå funktionssäkerhet men inga regler för vem som är ansvarig för att implementera kraven.
- gäller när utrustning som uppfyller kraven i IEC 61508 är integrerade i system i processindustrin. Standarden gäller inte när en tillverkare vill visa att utrustning är lämplig för säkerhetssystem.
- gäller när mjukvara är utvecklad med begränsat programspråk eller konfigurering men inte för mjukvara utvecklad med högnivåspråk.
- redogör för sambanden mellan säkerhetsfunktioner och övriga instrumentfunktioner.
- resulterar i identifikation av säkerhetsfunktioner och krav på dess SIL med hänsyn till den riskreduktion som sker på andra sätt.
- specifikation av krav på systemens arkitektur och hårdvarans konfiguration samt applikation av mjukvara.
- kraven på mjukvara innefattar följande:
    - kontroll i hela livscykeln på att fel inte byggs in och kontroll på de fel som uppstår
    - information om hur systemet valideras måste ges till organisationen som integrerar systemet
    - förberedande av information och procedurer för drift, underhåll och modifieringar i systemet.
- gäller när säkerhetskritiska funktioner används för att uppnå funktionssäkerhet för personal, allmänhet och miljön. Kan även användas för icke-säkerhetsfunktioner som skyddar egendom.
- kräver att riskanalyser görs för att definiera kraven på funktionssäkerhet och SIL för varje kritisk instrumentfunktion.
- fastställer numeriska mål för medelsannolikheten för fel vid anrop och frekvensen av farliga fel per timma för olika SIL.
- definierar den högsta prestanda (SIL 4) som kan uppnås på säkerhetskritiska instrumentfunktioner genom att följa denna standard.

- definierar vilken som är den lägsta prestanda (SIL 1) som säkerhetskritiska instrumentfunktioner måste ha för att standarden ska gälla.
- tillhandahåller ett ramverk för hur SIL fastställs men fastställer inga värden för specifika applikationer.
- fastställer krav på alla delar i ett säkerhetssystem, från sensor till manöverdon.
- kräver att hänsyn tas till mänskliga fel vid design av säkerhets-kritiska instrumentfunktioner.
- ställer inga direkta krav på individer bland operatörer och underhållspersonal.

I standardens tredje del (SS-EN 61511-3 2005) presenteras en översikt av ett antal metoder. Det är metoder av olika typer som presenteras. En del kräver stor arbetsinsats, semikvantitativ, andra metoder kräver en mindre arbetsinsats, kvalitativa. De metoder som kräver stor arbetsinsats är bland annat en barriärsanalys, LOPA. Bland de som kräver mindre arbete finns metoder som bygger på grafer och matriser. Dessa och fler metoder finns mer utförligt beskrivna i kapitel 4. I standarden finns inga krav på att det är dessa metoder som ska användas. Det är tillåtet att utveckla egna metoder eller modifiera de presenterade så att de bättre passar företaget.

3.3 För- och nackdelar

Timms (2003) anser att genom att följa standarden kan besparingar göras i flera led. Främst kan besparingar göras vid design av nya system, då standarden ger vilka krav som ska ställas, behöver inte onödigt dyr utrustning köpas in. Besparingar kan också göras genom livscykel-perspektivet med underhåll och testningsintervall. Om ingen i organisationen känner ansvar för livscykeltänkandet är det svårt att hitta en optimal balans mellan design- och användningskostnader.

Weibull (2004) ser följande fördelar med att tillämpa standarden

- Användare av komponenter och system kan verifiera att produkterna har tillräcklig tillgänglighet och är tillräckligt felsäkra.
- Instrumentfunktioner kan utformas så att de ger den tillgänglighet som krävs i det enskilda fallet.
- Risken för förödande systematiska fel i en SKIF bör minska.
- Standardens metoder leder till mer ordning och reda.

Självklart finns det även nackdelar med att använda standarden

- Standardens krav kan leda till en onödig byråkratisering och eventuellt dyrare komponenter.

- Det krävs en investering i att utveckla egna metoder och utbilda personal.
- Den eventuella vinsten i form av enklare instrumentfunktioner och/eller högre säkerhet äts delvis upp av kostnader för riskvärdering, dokumentation och skräddarsydd design.

3.4 Programmeringsspråk

Tre olika typer av programmeringsspråk används för SIS: Konfigurering, begränsade programspråk och högnivåspråk. Konfigurering innebär att användaren endast kan göra mindre förändringar till exempel ändra området för en transmitter. Med ett begränsat programspråk finns färdig-programmerade funktioner som användaren kan kombinera för att uppnå det som funktionen ska göra. Begränsat programspråk används bland annat i PLC:er. Högnivåspråk är det som används för att programmera datorer, till exempel C++, Pascal och Java. IEC 61511 rekommenderar användning av konfigurering eller begränsade programspråk. Om högnivåspråk används, vilket inte är förbjudet enligt standarden, ska applikationen vara utvecklad enligt IEC 61508. (Summers 2002)

Trots att de mjukvarubaserade säkerhetssystemen nu är utvecklade enligt IEC 61508 anses de fortfarande mer opålitliga än de traditionella ”hardwired” systemen. Orsaken till detta anser Halang & Zalewski (2003) är att inga ny programmeringsspråk, eller ens modifieringar av redan existerande, har utvecklats för säkerhetsapplikationer.

Mjukvaran blir inte för gammal men när den teknologiska utvecklingen går framåt kan det bli svårt att hantera den. SIS programmen måste gå att komma åt. Kontrollen att programmet stämmer överens med säkerhets-kraven genomförs i tre steg: förståelse för designens syfte, genomgång av programmet av oberoende person samt verifikation av programmets verkställande. Verifikationen sker genom tester. Testerna är mycket viktiga, Summers (2002) anser att det inte går att testa för mycket. Om programmet innehåller fel kommer inte SIS att kunna fungera. Att göra ändringar i programmet bör behandlas på samma sätt som modifieringar i processen. Det är även viktigt att kontrollera att ändringarna inte påverkar några andra funktioner.

4 Översikt av metoder

Det finns ett flertal olika metoder för att bestämma vilken SIL som krävs på instrumenteringen till ett riskobjekt. Metoderna kan delas upp i kvalitativa, semikvantitativa och kvantitativa metoder. Eftersom det är resurskrävande att bestämma SIL är det viktigt att de händelser som identifieras verkligen behöver en SIL-analys. Det finns händelser som inte går att åtgärda med SIS och händelser med mycket liten risk är inte lönt att analysera med avseende på SIL (Bhimavarapu & Stavrianidis 2000). Summers (1998) rekommenderar följande frågeställningar för att besluta vilken metod som ska användas:

- Vilken metod används idag för riskanalyser?
- Hur komplex är processen?
- Är processen välförstådd?
- Hur är erfarenheterna och kunskapen om processens dynamik?
- Kommer den grupp som gör SIL bedömningarna att vara densamma från projekt till projekt?

I standarden (SS-EN 61511-3 2005) väljs metod med hjälp av följande faktorer:

- Komplexiteten av processen.
- Riktlinjer från myndigheter.
- Vilken typ av risk det är och den krävda riskreduktionen.
- Erfarenhet och kunskap hos personalen som ska göra arbetet.
- Tillgänglig information om parametrar som är relevanta för risken.

Enligt standarden är det ibland lämpligt att använda flera olika metoder till en och samma process. Weibull (2004) föreslår användning av kvalitativa metoder för screening och för säkerhetssystem upp till SIL 2. Semikvantitativa metoder kan användas för SIL 3. För komplexa säkerhetssystem och händelser med stora konsekvenser rekommenderas att kvantitativa metoder används.

De flesta metoderna utgår från en skadehändelse för att bedöma riskerna i processen. Vad som menas med en skadehändelse måste definieras klart. Följande definitioner används:

- Initierande händelse, t ex orsak som leder till att säkerhetsventil öppnas
- Själva olyckan, t ex brand, giftigt utsläpp
- Förlusterna till följd av olyckan, t ex antal döda

Vilken av definitionerna som används har stor betydelse för sannolikheten att händelsen ska inträffa. Det gäller också att komma ihåg att ha samma

definition vid beskrivning av konsekvensen för en händelse. När risken bedöms kan inte sannolikheten att en säkerhetsventil öppnas jämföras med konsekvenserna för en brand. För att branden ska uppstå krävs fler händelser, det måste bland annat finnas en tändkälla. (Bhimavarapu & Stavrianidis 2000)

4.1 Kvalitativa metoder

De kvalitativa metoderna är de som kräver den minsta arbetsinsatsen, men är också de som ger de mest översiktliga resultaten. Dessa metoder passar bra till äldre processer där det finns stor erfarenhet om hur de beter sig i olika situationer.

De stora fördelarna med kvalitativa metoder är enkelheten och den begränsade resursåtgången. Bhimavarapu & Stavrianidis (2000) anser att de fyra stora nackdelarna med metoderna är:

- Inkonsekventa resultat då de är mycket beroende på experternas erfarenheter och åsikter.
- Svårigheter att dokumentera hur arbetet leder till resultaten.
- Ger inte något handlingsprogram för ändringar som krävs med avseende på standardens livscykelperspektiv.
- Svårt att använda för komplexa processer.

Summer (1998) anser att det svåraste att analysera är sannolikheten så det är bra om analysgruppen har en uppfattning om med vilken frekvens olika händelser inträffar i processen.

4.1.1 Enhetlig SIL

Den allra enklaste metoden för att bestämma SIL är enligt Summer (1998) att göra bedömningen ”ett säkerhetssystem är ett säkerhetssystem och ska därför vara SIL 3”. Det vill säga överallt där ett SIS behövs används SIL 3. Denna metod används främst av små företag som inte har tid att lägga mycket energi på att bestämma vilken SIL det skall vara. Metoden sparar tid då en hel del frågor kan lämnas utan beaktande.

4.1.2 Enbart konsekvensanalys

Vid användning av denna metod tas ingen hänsyn till sannolikheten, endast konsekvensen bestämmer SIL. Exempel på beslutsunderlag, från Summer (1998), till metoden finns i tabell 2.

Tabell 2 Beslutstabell för enbart konsekvensanalys

SIL	Konsekvens
4	Flera dödade i samhället
3	Flera döda
2	Flera svårt skadade eller en dödad
1	Lindriga skador

Fördelen, enligt Dowell (1998), är att med denna metod slipper uppskattningar av sannolikheten göras, vilket oftast är de svåraste. Metoden är alltså tidsbesparande. Nackdelen är att det inte alltid blir ”rätt” SIL. Om en händelse är mycket osannolik kommer den eventuellt att bli för högt klassad medan en mycket sannolik händelse kan bli för lågt klassad. Är en händelse mycket sannolik bör andra åtgärder än endast hög SIL på befintligt SIS övervägas.

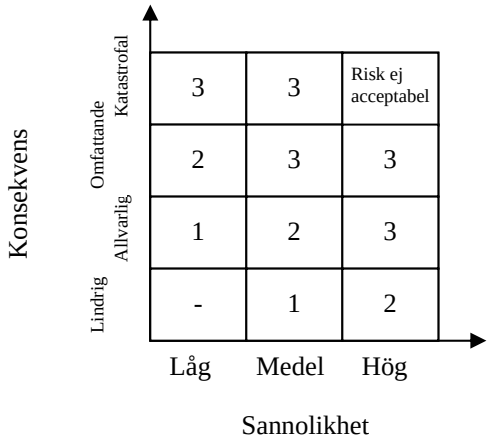
4.1.3 Modifierad HAZOP

Metoden utgår från en vanlig HAZOP-analys. HAZOP är en förkortning av ”HAZard and Operability” och analysen är mycket vanlig för riskanalyser i processindustrin. För att använda metoden för SIL bestämning har den modifierats. De händelser som identifierats i matrisen jämför medlemmarna i ett team med sina erfarenheter vad gäller konsekvens och frekvens för liknande händelser. Utifrån denna jämförelse väljs SIL vilket gör att metoden enligt Dowell (1998) är mycket beroende av medlemmarnas erfarenheter. För att metoden ska fungera krävs enligt Summers (1998) att medlemmarna i teamet har en stor förståelse för processen och riskerna. Det är viktigt att teamet har ungefär samma sammansättning för alla bedömningar inom ett företag då det annars blir mycket svårt att få jämförbara resultat.

4.1.4 Riskmatris

Riskmatriser tillhör de vanligaste metoderna för att bestämma SIL. Det finns ett flertal olika matrismetoder, matriserna kan vara två- eller tre-dimensionella. Alla metoderna går ut på att uppskatta några olika parametrar och sedan läsa av SIL i en matris. Alla händelser utvärderas var för sig och den högsta SIL som erhålls är den som krävs för systemet. Med en matrismetod beräknas aldrig risken för en händelse utan endast uppskattningar av sannolikheten och konsekvensen görs (White 2000).

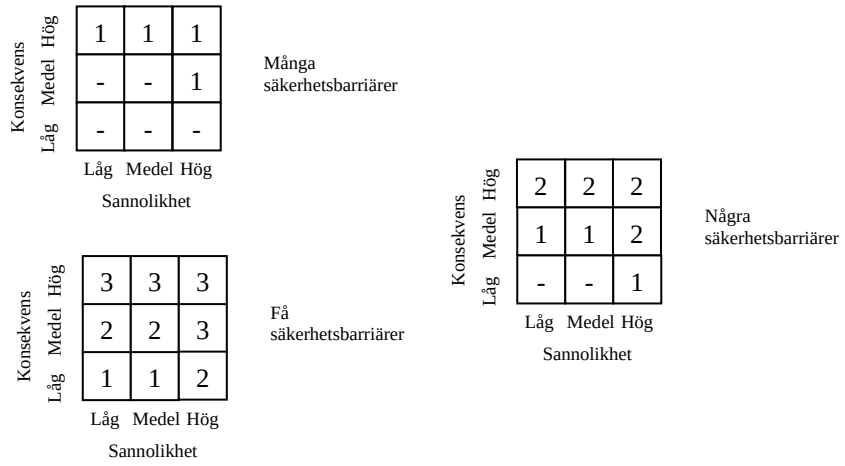
I de tvådimensionella matriserna bestäms sannolikheten och konsekvensen för en händelse med hänsyn till de säkerhetsbarriärer som finns. En tvådimensionell riskmatris för bestämning av SIL kan se ut enligt figur 4. (Summers 1998)



Figur 4 Tvådimensionell riskmatris

Vid användning av de tre-dimensionella riskmatriserna görs analysen utan hänsyn till säkerhetsbarriärerna. Beroende på antalet barriärer väljs vilken matris resultatet ska avläsas i. På detta sätt

är det lätt att få en överblick av hur antalet barriärer påverkar SIL. Ett exempel på tredimensionell riskmatris finns i figur 5. (Summers 1998)



Figur 5 Tredimensionell riskmatris

Weibull (2004) beskriver en annan typ av tredimensionell riskmatris. I denna modell är de tre dimensionerna: Anropsfrekvensen, konsekvensklass samt sannolikhet för eskalering. Här har dimensionen sannolikheten delats upp i två. En för hur ofta händelsen inträffar och en för hur bra befintliga barriärer är på att minska konsekvenserna av händelsen. Denna uppdelning gör det enligt Weibull (2005) lättare att uppskatta sannolikheten.

Dowell (1998) föreslår att riskmatriserna ska kalibreras för att passa det egna företaget. I denna kalibrering bör klargöras vad företaget anser vara låg, medel och hög sannolikhet. Är detta klart preciserat blir resultaten från olika analyser mer lika varandra.

4.1.5 Riskgraf

Riskgrafen har stora likheter med riskmatriserna vad gäller tillvägagångssättet. Båda metoderna kräver kalibrering till det egna företaget samt att den händelse som ger högst SIL blir dimensionerande för systemet. Riskgrafen blir mer överskådlig än riskmatriserna då fler faktorer tas hänsyn till. Vanligast är att följande fyra analyseras: Konsekvens (C), frekvens och exponeringstid (F), möjlighet att undvika faran (P) och sannolikheten för händelsen (W).

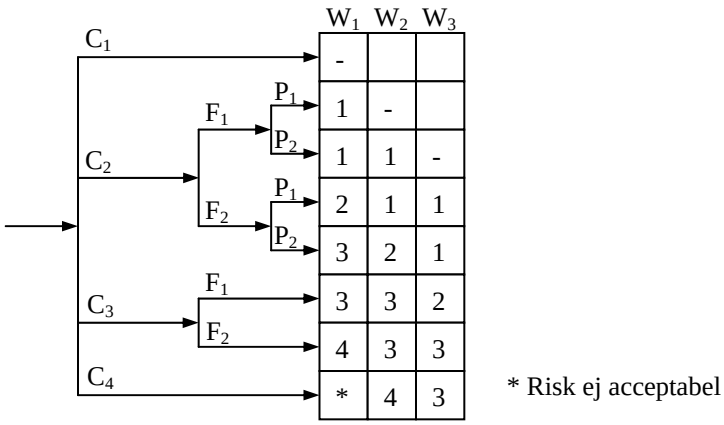
Metoden fokuserar på att utvärdera individrisk för en teoretisk person som befinner sig i händelseområdet. I analysen tas hänsyn till säkerhetsbarriärerna d v s man räknar med att de fungerar.

Till de fyra faktorerna som ska analyseras skapas ett antal nivåer. I Summers (1998) exempel har konsekvensen fyra nivåer, frekvensen två, möjligheten att fly två samt tre nivåer för sannolikheten. Dessa nivåer måste bestämmas med stor eftertanke för att passa företaget. Beskrivning av de olika nivåerna finns i tabell 3.

Tabell 3 Beskrivning av nivåer i riskgrafen

Nivå	Beskrivning
C_1	Mindre skador
C_2	Allvarliga permanenta skador för en eller flera personer
C_3	Flera personer dödade
C_4	Många personer dödade
F_1	Personer närvarande sällan eller ibland
F_2	Personer konstant eller nästan alltid närvarande
P_1	Möjligt att under vissa omständigheter fly
P_2	Nästan omöjligt att fly
W_1	Låg sannolikhet
W_2	Medel sannolikhet
W_3	Hög sannolikhet

Analys av en händelse inleds med att bestämma konsekvensnivån. Nästa faktor att ta ställning till är frekvensen på närvaron och sedan möjligheterna att kunna fly. Den sista faktorn att ta ställning till är sannolikheten. När alla faktorer är bestämda kan SIL för händelsen läsas av i riskgrafen, se figur 6. Beroende på vilken nivå det blir på de olika faktorerna behövs inte alltid tas ställning till alla faktorer.



Figur 6 Riskgraf

Enligt Timms (2003) är en välkalibrerad riskgraf en lika bra analysmetod som en semikvantitativ metod, till exempel säkerhetsbarriäranalys.

4.2 Semikvantitativa metoder

De semikvantitativa metoderna är enligt Stavrianidis & Bhimavarapu (1998) mer systematiska än de kvalitativa. Metoderna har nästan alla fördelar som de kvalitativa metoderna har, men utan dokumentationsproblemet.

En riskmatris kan vara antingen kvalitativ eller semikvantitativ beroende på mängden information den ger. Stavrianidis & Bhimavarapu (1998) presenterar en riskmatris som de anser är semikvantitativ. Denna matris har fyra klasser av konsekvenser och sannolikheter.

Felträdsanalyser är oftast kvantitativa men Hauptmanns (2004) presenterar en felträdsmetod som är semikvantitativ. Metoden kan beskrivas i tre steg:

- skapa ett felträd
- välja indata
- utvärdering av felträdet

Indata väljs från klasser av frekvenser. Det är dessa klasser som gör metoden semikvantitativ.

4.2.1 Säkerhetsbarriäranalys

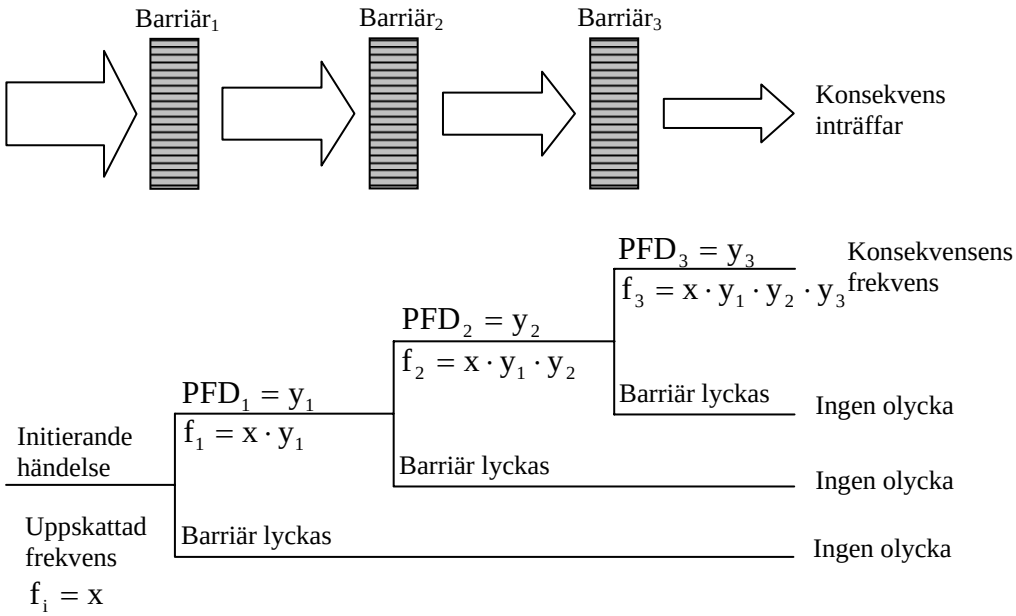
Säkerhetsbarriäranalys benämns ofta med den engelska förkortningen LOPA, Layer of Protection Analysis. Metoden använder semikvantitativa värden på konsekvensen, numerisk uppskattning av sannolikheten för händelsen och numeriska värden på sannolikheten för fel vid anrop, PFD, för varje säkerhetsbarriär. PFD kommer från engelskans Probability of Failure on Demand. Med LOPA läggs mer energi på att bestämma sannolikhet för en händelse än att utvärdera konsekvensen av den. (Marszal et al 1999)

Arbetsgången med metoden är att fylla i en tabell motsvarande tabell 4. Arbetet inleds med att identifiera skadehändelser, initierande orsaker och barriärerna. För att bestämma SIL genomförs beräkningar. Multiplicera sannolikheten för händelsen, kolumn 3 i tabell 4, med PFD för varje barriär, kolumn 4 och 5. Resultatet blir sannolikheten för händelsen med hänsyn till barriärerna, kolumn 7. Är denna risk högre än den av företaget accepterade behövs ett säkerhetssystem, SIS. Gör om beräkningen med säkerhetssystemet som en extra barriär. Finns redan ett säkerhetssystem, ge systemet en högre SIL-klass. SIL skall vara så hög att sannolikheten för händelsen med hänsyn till alla barriärer blir lägre än den av företaget accepterade.

Tabell 4 Översikt av LOPA

1	2	3	4	5	6	7
Skade-händelse och konsekvens-klass	Initierande orsaker	Sannolikhet för händelse	Oberoende säkerhets-barriärers PFD T ex processdesign, reglersystem, larm mm och SIS	Övriga säkerhets systems PFD T ex säkerhets ventiler	Antal barriärer	Sannolik-het för händelsen med barriärer

Metoden kan också illustreras enligt figur 7. Konsekvensens frekvens går endast att beräkna på detta sätt om barriärerna är helt oberoende av varandra.



Figur 7 Översikt av LOPA

LOPA passar bra att använda efter en HAZOP för att bestämma SIL eftersom alla skadehändelser och de initierande orsaker redan är identifierade i HAZOP:en. Metoden kräver inte så mycket mer än de kvalitativa metoderna men ger ett resultat där förutsättningarna och resonemangen kring beslutad SIL tydligt visas. Är inte resultatet från LOPA tillfredsställande är det passande att utöka analysen till en kvantitativ analys genom att använda felträd, FTA. (Dowell 1998)

4.3 Kvantitativa metoder

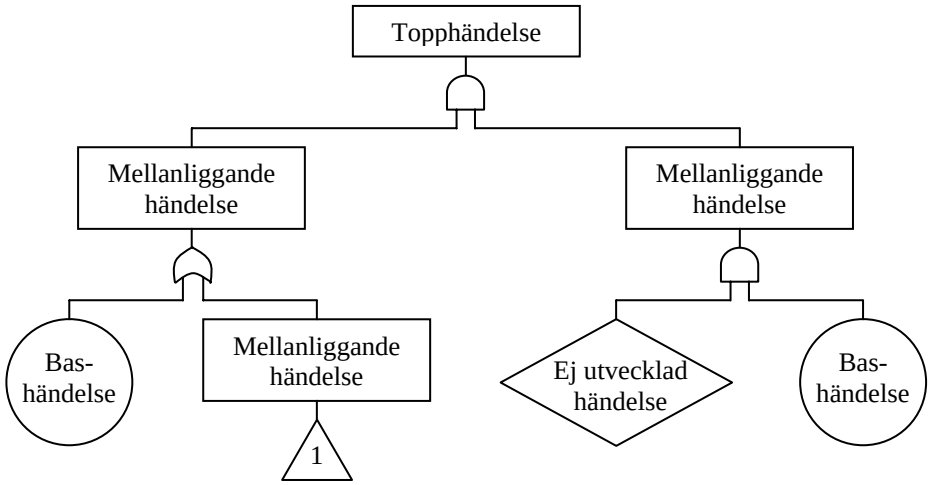
De kvantitativa metoderna är de mest omfattande och tidskrävande. De används främst då tillgången på historisk information om processen är begränsad eller om processen är komplex. Metoderna kan ge mer objektiva resultat än de kvalitativa och semikvantitativa metoderna men fortfarande ingår en del subjektiva bedömningar. Felträd och händelseträd är vanligast bland de kvantitativa metoderna.

En kvantitativ analys bidrar till bättre förståelse för processen, processens riskbild och säkerhetssystemens bidrag till riskreduktionen. Utvecklingen av de kvantitativa metoderna började på 1980-talet, innan dess användes främst kvalitativa metoder. (Bhimavarapu & Stavrianidis 2000)

4.3.1 Felträd

Felträdsanalys, FTA, är en analysmetod baserat på ett logiskt diagram. Diagrammet, felträdet, fokuserar på en allvarlig händelse. Vid uppbyggnaden av felträdet blir denna allvarliga händelse topphändelsen. Trädet grenas ut för att identifiera topphändelsens primära orsaker, bashändelserna. I figur 8 visas hur felträdet byggs upp. För att topphändelsen ska ske krävs att båda de översta mellanliggande händelserna sker, de är sammankopplade med topphändelsen via en OCH-grind. På nästa nivå beskrivs vad som ska

inträffa för att dessa mellanliggande händelser ska ske. I den vänstra grenen är det en bashändelse eller en ny mellanliggande händelse som orsakar händelsen. De är sammankopplade med en ELLER-grind till nivån ovanför. Trianglar som den med en etta i används när felträden blir stora och behöver delas upp på flera sidor. Trianglarna är då markeringar för hur de olika delarna hänger ihop. En händelse som inte är utvecklad har lämnats outvecklad för att den faller utanför det avgränsade systemet. (Karlsson 1997)



Figur 8 Felträd för beräkning av kravet från processen

När trädets byggts upp görs en tabell över de felkombinationer, cut sets, som leder till topphändelsen. De felkombinationer som kallas minimal cut sets, MCS, anger det minsta antalet bashändelser som leder till topphändelsen. (Karlsson 1997)

För att metoden ska bli kvantitativ måste alla bashändelser tilldelas en sannolikhet eller en frekvens. Det går då att räkna ut sannolikheten för topphändelsen. Beräkningarna börjar längst ner i trädet. Är två bashändelser förbundna med en OCH-grind multipliceras deras sannolikheter och sannolikheten för händelsen på nivån ovanför erhålls. Är två bashändelser förbundna med en ELLER-grind adderas deras sannolikheter och sannolikheten för händelsen på nivån ovanför erhålls. På detta vis fås till slut sannolikheten för topphändelsen. (Karlsson 1997)

Med felträdsanalys kan både mänskliga fel och utrustningsfel analyseras tillsammans. Metoden är bra på att redovisa skillnader med olika riskreducerande åtgärder, det blir lätt att avgöra vilken åtgärd som ger störst effekt. (Kemikontoret 2001)

En fördel med metoden är att det är lätt att modellera flera konsekvenser av samma händelse. En nackdel är att det är svårt att arbeta i team med metoden. Detta medför att det blir svårare att utnyttja flera kompetensområden. (Weibull 2004)

Bestämning av SIL görs med hjälp av ekvation 1. Sannolikhet för fel vid anrop motsvarar en SIL i tabell 1. Krav från processen är detsamma som

sannolikheten för topphändelsen. Varje gång topphändelsen kan ske görs ett anrop från processen, som ställer ett krav på funktion från säkerhetssystemet. Kravet från processen räknas ut i felträdet, figur 8. (Summers 1998)

$$\text{Sannolikhet för fel vid anrop} = \frac{\text{Tolerabel risk}}{\text{Krav från processen}}$$

Ekvation 1 Bestämning av SIL med FTA

4.3.2 Finansiell riskanalys

Den finansiella riskanalysen, FRA, är mycket omfattande. Både sannolikheten och konsekvensen av en händelse bestäms kvantitativt för flera områden. Dessa områden är påverkan på människor, egendom, miljö samt produktion och förtjänst. När beräkningarna är gjorda för alla områden räknas resultatet om till ett gemensamt jämförelsetal. Nu görs en konstnads-nyttaanalys för att se om vald SIL kan motiveras. FRA är den metod som används minst eftersom mycket detaljerad information krävs vilket är mycket resurskrävande. (Marszal et al 1999)

4.4 Tillförlitlighetsanalys

En tillförlitlighetsanalys kan göras efter en kvalitativ, semikvantitativ eller kvantitativ analys. Oftast görs det efter en kvantitativ analys, FTA, då det endast är då som alla beräkningar kan utföras. För att göra en kvantitativ analys går det åt stora resurser och marginalinsatsen för att utföra tillförlitlighetsanalysen liten. Tillförlitlighetsanalysen görs för att hitta vilken del av systemet som ska modifieras för att öka tillförlitligheten, höja SIL. (Jin et al 2003)

Tillförlitlighetsanalysen består av sju steg:

Steg 1: Beskriv systemet.

Steg 2: Utvärdera säkerheten i systemet.

Steg 3: Bestäm SIL för systemet med valfri metod, helst en kvantitativ. Om SIL är tillräckligt för att uppfylla den tolererade risken gå till steg sju.

Steg 4: Identifiera de bashändelser som kan modifieras för att höja säkerheten med hjälp av parametrarna: viktighet, riskökande faktor, riskminskande faktor och känslighetsanalys.

Steg 5: Välj metod för att öka säkerheten: Byt ut delar i systemet för att nå den tolererade risken, lägg till kritisk instrumentering eller modifiera produktions- eller underhållsrutiner.

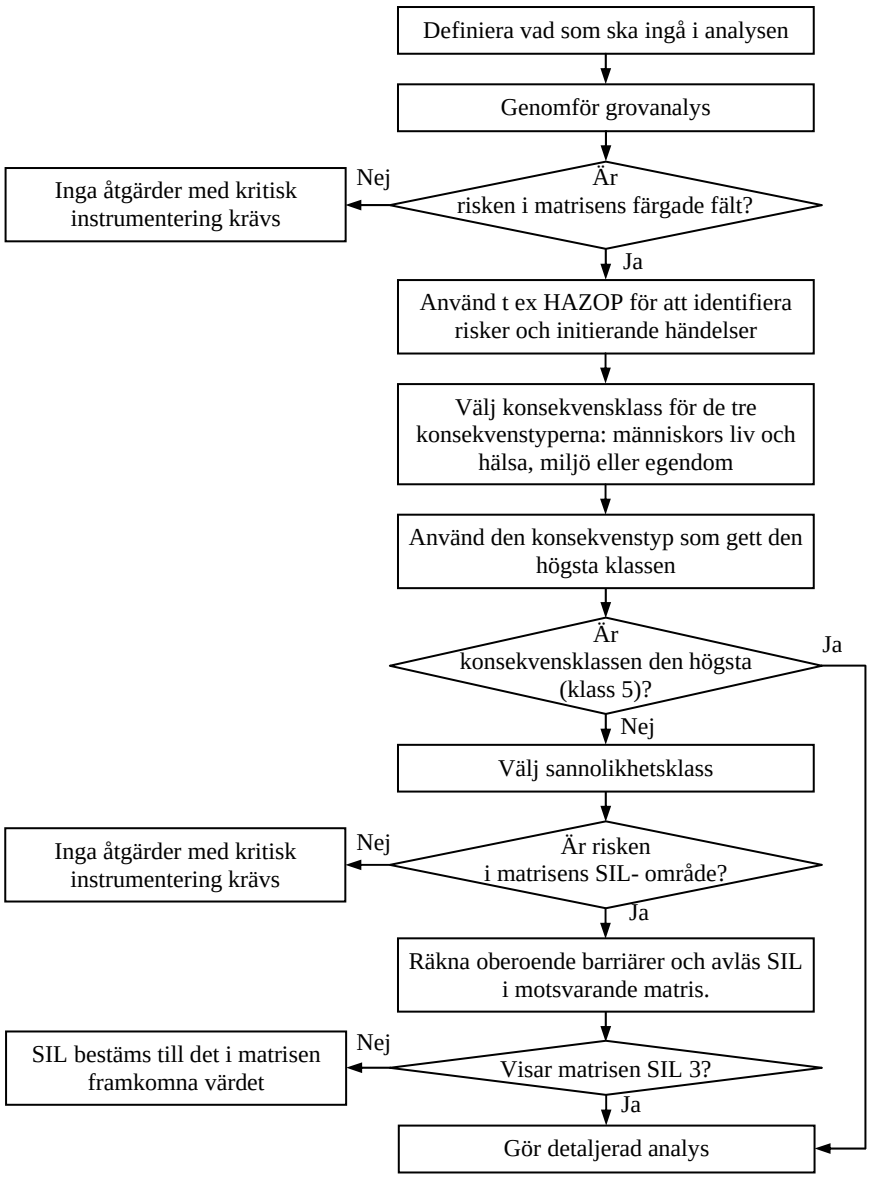
Steg 6: Gå tillbaka till steg tre.

Steg 7: Analysen klar, dokumentera.

5 Utveckling av metod

Huvudidéen är att använda en grovanalys med tillhörande matris för screening och analysera identifierade faror mer ingående. När de identifierade riskerna värderas ska inte skyddsbarriärerna räknas med, d v s värdera riskerna som om barriärerna inte finns. Då det från Hydro Polymers sida är önskvärt att metoden blir lättanvänd har deras tidigare rutiner för riskanalyser studerats och legat till grund för utvecklingen. Även om metoden är utvecklad åt Hydro Polymers kan andra företag inom processindustrin använda den.

Metoden finns översiktligt beskriven i figur 9 och beskrivs mer ingående i de följande underrubrikerna.



Figur 9 Översikt av metoden

5.1 Grovanalys

Metoden inleds med en grovanalys. I grovanalysen görs en översiktlig bedömning av de risker som finns i processen. De händelser som identifierats indelas i klasser med avseende på konsekvens och sannolikhet. Är risken i medel- eller högriskområdet i matrisen går man vidare med ytterligare analyser. Händelser i lågriskområdet kräver inga åtgärder med kritisk instrumentering och analysarbetet kan avslutas.

5.1.1 Konsekvensklasser

Konsekvensklasser är skapade för tre olika typer av konsekvenser från en skadehändelse. Konsekvenser för människors liv och hälsa, yttre miljö samt egendom finns indelade i klasser enligt tabell 5, 6 och 7. Beskrivningen av klasserna är en kombination av koncernens rekommendationer och de på företaget tidigare använda beskrivningarna.

Tabell 5 Konsekvensklasser för människors liv och hälsa

Klass	Beskrivning
1	Obetydliga personskador, första hjälpen
2	Lost time injury, LTI, medicinsk behandling
3	Enstaka svårt skadade, längre sjukhusvistelse och bestående men
4	En död eller flera svårt skadade
5	Flera döda eller 10-tals svårt skadade

Tabell 6 Konsekvensklasser för miljö

Klass	Beskrivning
1	Inga egentliga skador.
2	Kortvariga skador, liten utbredning. Ingen eller enkel sanering.
3	Långvariga skador (<2 år), liten till stor utbredning. Enkel sanering.
4	Långvariga skador (2-5 år), liten utbredning. Svår eller omöjlig sanering
5	Mycket långvariga skador (>5 år), stor utbredning. Svår eller omöjlig sanering.

Tabell 7 Konsekvensklasser för egendom

Klass	Beskrivning
1	Liten skada på fabriken. Liten påverkan på produktionen.
2	Mindre skador på fabriken. Mindre påverkan på produktionen.
3	Betydande skador på fabriken. Betydande påverkan på produktionen.
4	Allvarliga skador på fabriken. Långt produktionsstopp.
5	Fabriken eller huvuddelar av fabriken förstörd. Mycket långt produktionsstopp.

Vid bedömning av konsekvenserna för miljön vägs även frågor av PR-mässig karaktär in enligt följande: (Jacobsson 2003)

Klass 1: Ingen uppmärksamhet i massmedia.

Klass 2: Uppmärksamhet i form av notiser.

Klass 3: Stor uppmärksamhet i massmedia.

Klass 4: Mycket stor uppmärksamhet i massmedia.

Klass 5: Mycket stor uppmärksamhet i massmedia, anläggningens framtid är hotad.

Konsekvensklasserna för egendom är uppbyggda som beskrivningar av skadorna och produktionsbortfallet. Tidigare har företaget använt konsekvensklasser uppbyggda av kostnader. Dessa kostnader har varit kostnader för att ersätta förstörd utrustning medan förluster på grund av produktionsbortfall har lämnats utan beaktande. Genom dessa nya klasser tas hänsyn till störningar i produktionen, medan någon uppskattning i direkta kostnader inte behöver göras.

5.1.2 Sannolikhetsklasser

De sannolikhetsklasser som valts är de som vanligen används på företaget vid riskanalyser, se tabell 8. Inom koncernen rekommenderas en uppdelning i sex klasser där den minst sannolika är mindre än en gång på 10 000 år. Anledningen till att denna rekommendation frångås är att personalen är van vid de valda klasserna och att det är mycket svårt att ha en uppfattning om någon kan hända inom 1 000 eller 10 000 år. Det blir en stor osäkerhet i uppdelningen och dessutom ger det inte så mycket mer för resultatet om det händer inom 1 000 eller 10 000 år.

Tabell 8 Sannolikhetsklasser

Klass	Frekvens
1	Mindre än 1 gång per 1000 år
2	1 gång per 100-1000 år
3	1 gång per 10-100 år
4	1 gång per 1-10 år
5	Mer än 1 gång per år

Vid analys kan de olika klasserna realiseras på följande sätt:

Klass 1: Mycket osannolikt att det skulle hända under anläggningens livstid.

Klass 2: Det kan hända under anläggningens livstid.

Klass 3: Det är troligt att det inträffar under anläggningens livstid.

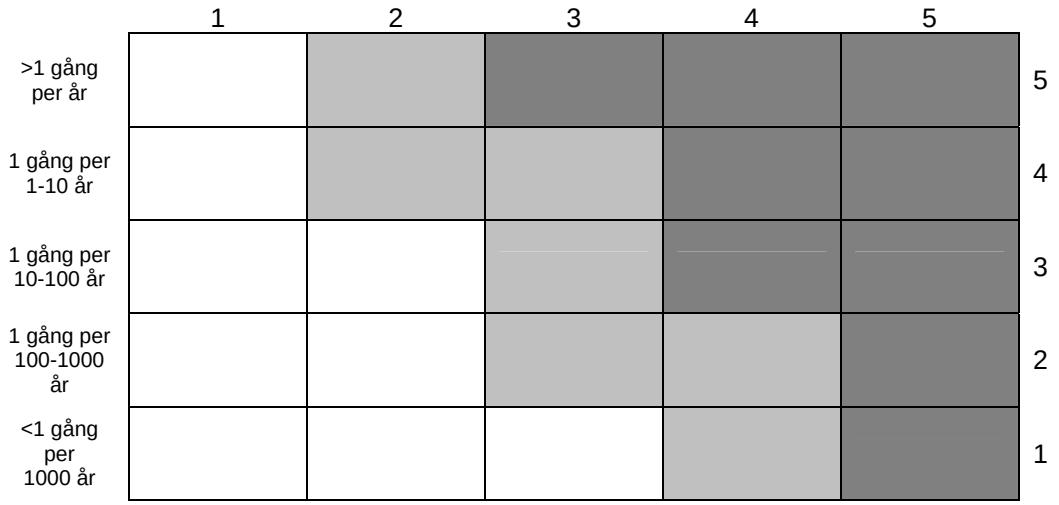
Klass 4: Det har hänt här på företaget.

Klass 5: Det brukar inträffa varje år.

5.1.3 Matrisen

När sannolikhetsklass och konsekvensklass valts placeras händelsen i riskmatrisen, se figur 10. Om händelsen placerats i något av de färgade

fälten krävs ytterligare analys. Placeras däremot händelsen i det vita området är risken liten och inga åtgärder krävs.



HÄLSA	Obetydliga personskador, första hjälpen	Lost time injury, LTI, medicinsk behandling	Enstaka svårt skadade, längre sjukhus-vistelse och bestående men	En död eller flera svårt skadade	Flera döda eller 10-tals svårt skadade
MILJÖ	Inga egentliga skador.	Kortvariga skador, liten utbredning. Ingen eller enkel sanering.	Långvariga skador (<2 år), liten till stor utbredning. Enkel sanering.	Långvariga skador (2-5 år), liten utbredning. Svår eller omöjlig sanering.	Mycket långvariga skador (>5 år), stor utbredning. Svår eller omöjlig sanering.
EGENDOM	Liten skada på fabriken. Liten påverkan på produktionen.	Mindre skador på fabriken. Mindre påverkan på produktionen.	Betydande skador på fabriken. Betydande påverkan på produktionen.	Allvarliga skador på fabriken. Långt produktions-stopp.	Fabriken eller huvuddelar av fabriken förstörd. Mycket långt produktions-stopp.

Figur 10 Riskmatris

5.2 Utbyggd HAZOP

SIL-analysen fortsätter med en utbyggd HAZOP som är uppbyggd som en kvalitativ matrismetod och kommer att användas för att identifiera de delar av processen som är så riskfyllda att säkerhetskritisk instrumentering krävs.

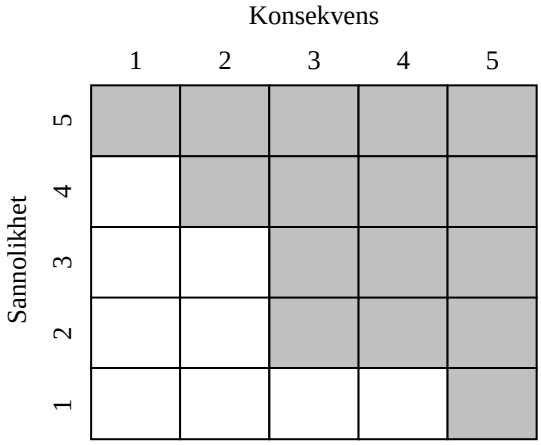
5.2.1 Identifiering av risker

För att identifiera de risker som ska värderas med avseende på SIL kan en redan gjord HAZOP-analys ligga till grund för arbetet. Identifierade risker skrivs in i analysprotokollet som sedan fylls på med fler uppgifter allt eftersom arbetet fortsätter. Protokollet kan se ut enligt bilaga 1. De identifierade riskerna klassificeras med samma konsekvens- och sannolikhetsklasser som i grovanalysen. Matrisen som används är däremot annorlunda.

Om sannolikheten bedöms till klass 5 bör det ses över om en ändring i det vanliga styrsystemet kan göra händelsen mindre sannolik.

5.2.2 Matrisen

När sannolikhetsklass och konsekvensklass valts placeras händelsen i riskmatrisen, se figur 11. Om händelsen placerats i SIL-området, det gråmarkerade, krävs ytterligare analys. Placeras däremot händelsen i det vita området är risken liten och inga åtgärder krävs.



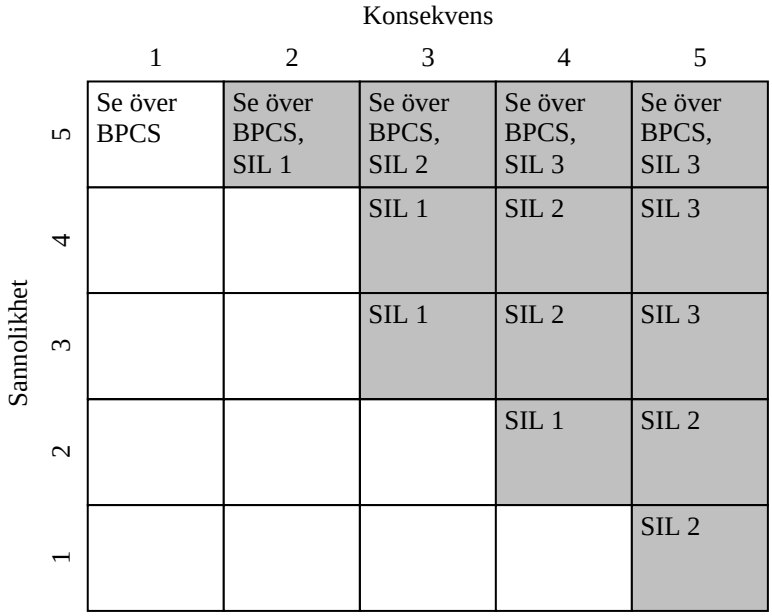
Figur 11 Riskmatris med SIL-området gråmarkerat.

För händelser i det gråmarkerade SIL-området görs först en enkel barriäranalys. Denna enkla barriäranalys går ut på att räkna hur många oberoende barriärer det finns som skyddar mot aktuell händelse. För varje barriär som finns att tillgå minskar kravet på SIL, d v s då antalet barriärer ökar blir det vita fältet i matrisen större. När antalet barriärer är bestämt läses SIL av i motsvarande matris, se figur 12, 13 och 14.

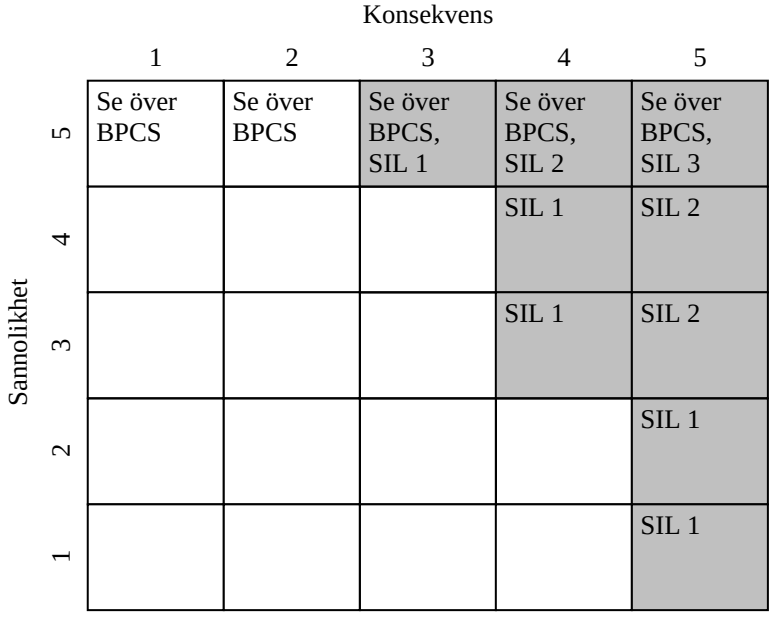
Konsekvens

Sannolikhet	1	2	3	4	5
5	Se över BPCS, SIL 1	Se över BPCS, SIL 2	Se över BPCS, SIL 3	Se över BPCS, fler barriär krävs	Se över BPCS, fler barriär krävs
4		SIL 1	SIL 2	Fler barriär krävs	Fler barriär krävs
3			SIL 2	Fler barriär krävs	Fler barriär krävs
2			SIL 1	SIL 2	Fler barriär krävs
1					Fler barriär krävs

Figur 12 Riskmatris för avläsning av SIL. Gäller då inga barriärer finns.



Figur 13 Riskmatris för avläsning av SIL. Gäller då en oberoende barriär finns.



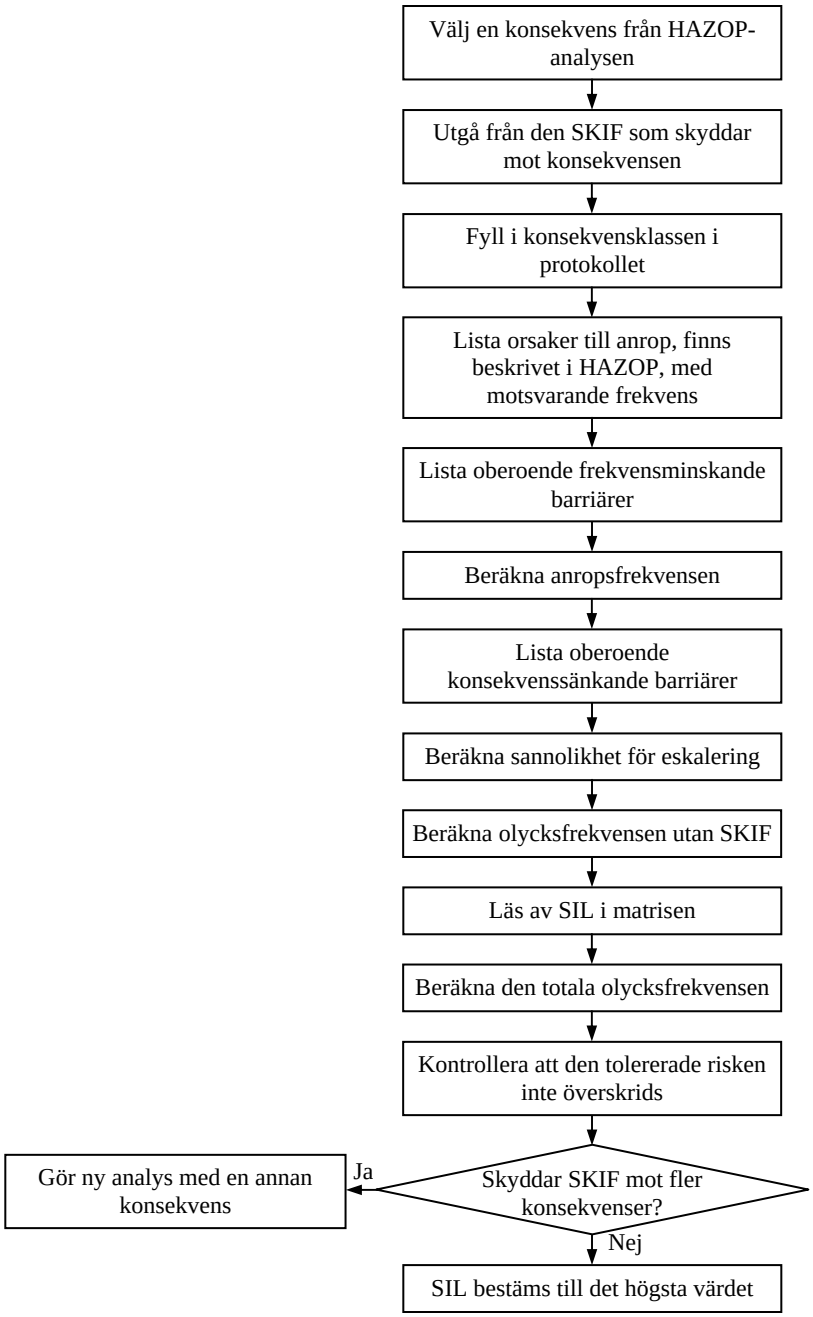
Figur 14 Riskmatris för avläsning av SIL. Gäller då två oberoende barriärer finns.

Händelser som i den utbyggda HAZOP-analysen får den högsta konsekvensklassen eller SIL 3 bör genomgå detaljerad analys.

5.3 Detaljerad analys

De händelser som i den utbyggda HAZOP-analysen idetifierats för mer detaljerad analys bör analyseras med barriäranalys, LOPA, på det vis som Weibull (2004) föreslagit. I barriäranalysen är det sannolikheten för händelsen som utreds noggrannare. Konsekvensen har kvar sin

klassbeskrivning från den utbyggda HAZOP-analysen. En översikt av metoden finns i figur 15.



Figur 15 Översikt av detaljerad analys

I HAZOP-analysen har risker som kräver riskreduktion identifierats. När ett förslag på riskreducerande SKIF framkommit analyseras vilken SIL som krävs med hjälp av barriäranalysen. I barriäranalysen beräknas anrops-frekvens och sannolikheten för eskalering. Med hjälp av dessa två parametrar avläses SIL i en matris, se figur 16. En kontrollberäkning görs för att kontrollera att tillräckligt högt SIL valts, den tolererade risken får inte överskridas.

SIL		Konsekvenser														
		1			2			3			4			5		
Anropsfrekvens	5			1		1	2	1	2	3	2	3	*	*	*	*
	4						1		1	2	1	2	*	3	*	*
	3								1	2	1	2	*	2	3	*
	2									1		1	2	1	2	*
	1														1	*
Sannolikhet för eskalering %		1	10	100	1	10	100	1	10	100	1	10	100	1	10	100

* = mer än en barriär krävs

Figur 16 SIL-matris för detaljanalysen

Blankett för genomförande av barriäranalys finns i tabell 9. I beskrivningen av hur beräkningen går till används bokstäver som återfinns i tabellen. För att bestämma erforderlig SIL görs följande:

- Anropsfrekvensen, A, beräknas genom att frekvenser, B, adderas och sannolikheter, C, multipliceras.
- Sannolikheten för eskalering, D, beräknas genom att multiplicera de olika sannolikheterna, E.
- Olycksfrekvens utan SKIF, F, beräknas genom att multiplicera anropsfrekvensen, A, med sannolikheten för eskalering, D.
- Med hjälp av konsekvensklassen, G, anropsfrekvensen, A, och sannolikheten för eskalering, D, avläses i matrisen, figur 16, erforderlig SIL.
- Den totala olycksfrekvensen, H, beräknas genom att multiplicera olycksfrekvensen utan SKIF, F, med frekvensen för fel i SKIF. Felfrekvensen är beroende av SIL enligt tabell 1. Konservativt räknat är frekvensen10^{-SIL}, d v s är SIL 2 är felfrekvensen 10^{-2}.
- Kontrollera att den totala olycksfrekvensen inte överskrider den tolerabla risken. Om den tolerabla risken överskrids höj SIL ett steg eller inför fler barriärer.

Tabell 9 Blankett för beräkning av SIL med barriäranalys

Fabrik	**Enhet**	**Utrustning**	**Skade-händelse (nr)**	**Datum**	**Signatur**

Säkerhetskritisk instrumentfunktion (SKIF)	**Konsekvensbeskrivning**	**Klass**
		G

	Beskrivning	**Sannolikhet**	**Frekvens (per år)**
1 Orsaker till anrop			B
2			B
3			B
4			B
5			B
Förutsättning för anrop		C	
Oberoende barriärer som reducerar anropsfrekvensen			
Styr- och reglersystem		C	
Mänskligt ingrepp		C	
Andra oberoende barriärer		C	
Anropsfrekvens på SKIF			A=(B+B)*C
Konsekvensbegränsande barriärer och faktorer			
Avsäkring		E	
Andra oberoende barriärer		E	
Antändning		E	
Sannolikhet för personal i området		E	
Sannolikhet för skada		E	
Sannolikhet för eskalering		D=E*E	
Andra säkerhetsåtgärder (inte oberoende barriärer)			
Olycksfrekvens utan SKIF			F=A*D
SIL (avläst i matris)		**Total olycksfrekvens**	H
Tolerabel risk för konsekvensen		Tolerabel risk nådd?	
Erforderliga åtgärder			
Noteringar			

5.4 Befintlig utrustning, ändringar och nya projekt

Så som metoden beskrivits är den anpassad för att analysera befintlig utrustning. Vid ändringar och nya projekt som kräver nya installationer behöver metoden modifieras något för att passa.

5.4.1 Ändringar

Vid ändringar behöver inte hela analysen göras om utan endast uppdateringar av de delar i analysen som berörs.

5.4.2 Nya projekt

En av de största skillnaderna mellan befintlig utrustning och nya projekt är att vid nya projekt finns inga gamla HAZOP-analyser att titta på utan allt analysarbete måste göras från grunden. Det är viktigt att riskanalyser genomförs på ett tidigt stadium, då det är på idéstadiet som riskbilden kan påverkas bland annat genom ”inherent safety”. När detaljplaneringen av projektet är färdig kan SIL-analyserna göras. Vid konstruktionen av säkerhetssystemen är det viktigt att de inte görs för komplexa utan att enkelhet eftersträvas. Komplexa system är mycket svåra att överblicka, det blir svårt att avgöra om säkerhetskraven är uppfyllda.

6 Utvärdering

För att utvärdera metoden har några riskområden inom företaget valts ut. De utvalda områdena är:

- generella risker i en ångpanna
- läckage från en stor klorledning utomhus
- övertryck i cellsalens klorsystem
- skenande autoklav i PVC-fabriken.

Grovanalysen som inleder metoden är inte utvärderad inom ramen för detta arbete då det inte är en nyutvecklad metod utan en gammal beprövad teknik. Vid utvärderingen av den utbyggda HAZOP-analysen har fokus varit på hur det går att klassificera resultaten från HAZOP-analysen i konsekvens- och sannolikhetsklasser samt hur den förenklade barriäranalysen fungerar. Även test av den detaljerade analysen kommer att utföras.

Vid utvärderingen av metoden är det viktigt att kontrollera att metoden uppfyller de mål som sattes. Har metoden blivit lättanvänd?

6.1 Ångpannan

Testningen av metoden inleds med riskerna i ångpannan. Testet av ångpannan har i huvudsak bestått av jämförelser med en redan gjord SIL-analys för att se om metoden ger resultat som är jämförbara med andra metoder för SIL-analys. Till jämförelsen gjordes inte något nytt analysarbete utan endast resultat från föregående analys användes.

En konsultfirma har analyserat ångpannan med avseende på SIL. I denna analys gjordes först en riskanalys med SWIFT, Strukturerad What-If Teknik, och sedan SIL-värdering med hjälp av en riskgraf. I analysen framkom att SIL 1 var passande men om fler personer hade vistats i området hade det krävts SIL 2. (DNV 2003)

Vid jämförelsen har de bedömda riskerna i SWIFT-analysen använts som utgångspunkt för SIL-värderingen med den nyutvecklade metoden. Värderingen med den nya metoden ger att SIL 2 behövs eller eventuellt SIL 3. Denna skillnad beror till stor del på att SWIFT-analysen inte identifierat några barriärer. Den SIL-värdering som gjorts med hjälp av riskgrafen har endast tagit hänsyn till konsekvenser för människors liv och hälsa medan den nya metoden även analyserar konsekvenser med avseende på miljö och egendom. Vid den nya värderingen är det på flera punkter miljö- eller egendomskonsekvenserna som blir dimensionerande för SIL.

För att kunna göra en bra SIL-värdering med den nya metoden är det viktigt att befintliga barriärer identifieras i HAZOP-delen av analysen. Om barriärerna inte identifieras kommer onödigt höga SIL att implementeras i systemen vilket leder till onödigt stora kostnader.

6.2 Klorledningen

Testet på klorledningen genomfördes med hjälp av driftingenjören från klorfabriken och HMS-chefen.

6.2.1 Första mötet

Från en sedan tidigare gjord grovanalys över hela klorfabriken valdes en händelse ut för SIL-analys. Den utvalda händelsen är *läckage på klorledning utomhus ansl 50,* se bilaga 2. För att gå vidare gjordes en avgränsning av ett system kring ledningen. Detta system analyserades med HAZOP. Resultatet av HAZOP-analysen finns i bilaga 3. För detta system var det uteslutande konsekvenserna för människors liv och hälsa som blev dimensionerande. Vid analysen framkom att SIL 2 eller eventuellt SIL 3 krävs. För att utreda detta bör en detaljerad analys genomföras.

De moment som identifierats som svåra under analysen var främst att klassificera konsekvenser och sannolikheter utan att ta hänsyn till barriärerna. Den enkla barriäranalysen var också orsak till vissa frågetecken. Med barriäranalysen var problemen att avgöra vad som kan räknas som barriär och vilken barriär den identifierade SIL tillhör.

6.2.2 Andra mötet

Det andra mötet inleddes med att göra en detaljanalys av den händelse som gav SIL 3 i HAZOP-analysen. Händelsen är nr 4 i bilaga 3, *omvänd riktning av flödet*. När detaljanalysen gjordes inkluderades även fall 7 och 9 då de har samma konsekvens som fall 4 och är en orsak till anrop på sektioneringssystemet som ska SIL-klassas. Resultatet av analysen finns i bilaga 4. Även i den detaljerade analysen framkom att det är SIL 3 som krävs. Analysgruppen kände inte att detta var ett rimligt resultat för denna del av processen. Orsaken till det höga värdet är att frekvensen av händelsen *omvänd riktning av flödet* är så hög som flera gånger per år. Det är inte troligt att det omvända flödet genererar ett så högt tryck i ledningen att den skulle kunna gå läck. Med anledning av denna insikt modifierades HAZOP-analysen enligt bilaga 5. I denna modifierade analys är högsta identifierade SIL 2 så någon ny detaljerad analys behöver inte göras.

Den detaljerade analysen kändes svår att använda. Det var krångligt att förstå vad som skulle stå på vilken rad. Det gällde även att inte förväxla sannolikheter och frekvenser vid beräkningarna. Analysen var ändå bra då det blev lättare att identifiera orsakerna till det höga SIL-värdet. Trots att analysen upplevdes krånglig kommer inga stora förändringar ske eftersom det blir lättare med lite vana. Då den detaljerade analysen inte kommer att användas så ofta är det omotiverat att lägga mycket tid på att utveckla analysen så att den blir enklare när den ändå ger ett bra resultat. För att underlätta arbetet kommer ett tydligt exempel på hur den detaljerade analysen ska göras ska bifogas instruktionen till Hydro Polymers.

6.3 Klorupparbetning

Från den sedan tidigare gjorda grovanalysen över klorfabriken valdes ytterligare en händelse ut för SIL-analys. Den utvalda händelsen är *övertryck i Cl_2-systemet i cellsalen samt upparbetningen*, se bilaga 6. En HAZOP-analys gjordes och resultatet finns i bilaga 7.

Detta test gick bra vilket antagligen beror på att analysgruppen nu börjar bli van vid tankesättet i analysen.

6.4 PVC-autoklav

Testet genomfördes med hjälp av en processingenjör och driftchefen från PVC-fabriken, projektingenjör för instrument och HMS-chefen.

Hela PVC-fabriken har sedan tidigare analyserats med en grovanalys. Från denna analys valdes en händelse ut för SIL-analys. Den utvalda händelsen är *skenande autoklav*, se bilaga 8. För att gå vidare påbörjades en analys med HAZOP. På grund av tidsbrist gjordes ingen fullständig analys. Resultatet av HAZOP-analysen finns i bilaga 9. Även vid detta test var det konsekvenserna för människors liv och hälsa som blev dimensionerande. Vid analysen framkom att SIL 2 krävs.

Under testet uppkom diskussioner om instruktionens utformning, speciellt om när SIL-analys ska genomföras. Instruktionen behöver här omarbetas för att bli användbar. Förtydliganden krävs på ytterligare några stycken för att göra instruktionen mer lättanvänd. Vid testet fördes diskussioner om:

- Hur stort är ett system?
- Vilka delar är det som omfattas av den identifierade SIL?

Med barriäranalysen var problemen att veta hur man ska ta hänsyn till riskreducerande system som inte är tillräckligt säkra för att kunna räknas som en barriär. De finns och gör ett jobb, någonstans måste detta räknas.

Mer tid behöver läggas på analysarbetet, än vad som gjordes vid testet, för att metoden ska fungera bra och funktioner klassade enligt SIL ska identifieras. I fallet med autoklaven måste alla orsaker, exempelvis hög nivå, utredas ordentligt. Alla orsaker går inte att åtgärda med ett instrumentsystem. Ett exempel är fel initiator, däremot går fel mängd initiator att kontrollera med ett SIL-klassat instrumentsystem.

7 Slutsats

Examensarbetet har tillkommit för att Hydro Polymers ska kunna tackla de nya krav som ställs i standarden SS-EN 61511. Standarden har utvecklats för att förenkla hanteringen av instrumentsystemens förändrade riskprofil. Vilken metod som ska användas för att bestämma SIL är inte preciserat i standarden utan upp till företaget att välja själv.

I rapporten har en tredelad metod föreslagits. De två första delarna av metoden är kvalitativa och den avslutande tredje delen är semikvantitativ. Metoden är framtagen år Hydro Polymers men även andra företag inom processindustrin kan använda den.

Under arbetets gång har frågorna från problemformuleringen delvis fått svar:

- För att bedöma SIL för ett riskobjekt görs någon typ av riskanalys. Utifrån den bedömda risken tilldelas objektet lämplig SIL.
- Det blir små skillnader i tillvägagångssättet för befintlig utrustning, nya projekt och vid ändringar. Skillnaden ligger i omfattningen på analysen.
- Anvisningen är lätt att följa fram till den detaljerade analysen. För att förenkla kommer ett tydligt exempel att bifogas anvisningen.
- Repeterbarheten hos metoden har inte utretts. Detta beror dels på tidsbrist och dels på att för de olika fabriksdelarna har olika personer varit inblandade. Metoden har inte testats på två personer från samma fabriksdel vilket skulle krävts för att kolla repeterbarheten.

Vid utvärderingen har en jämförelse med en annan metod gjorts och resultatet blev liknande. Skillnaden kan bero på att det saknades viss information för användning av min metod i de tidigare resultaten.

Den viktigaste erfarenheten från testerna var att det är viktigt att ha med någon som är kunnig på instrumentsystemen vid analysen, det räcker inte med personer väl insatta i processen.

8 Förkortningar

ALARP	As Low As Reasonably Possible
BPCS	Basic Process Control System, vanliga styrsystemet.
HAZOP	Hazard and Operability study
FTA	Felträdsanalys
LOPA	Layer of Protection Analysis, säkerhetsbarriäranalys
MCS	Minimal Cut Sets
PFD	Probability to Fail on Demand, sannolikhet för fel vid anrop
PVC	Polyvinylklorid
SIL	Safety Integrity Level, integritetsnivå
SIS	Safety Instrumented System, säkerhetskritiskt system
SKIF	Säkerhetskritisk instrumentfunktion
SWIFT	Strukturerad What-If Teknik

9 Referenser

Beckman L. (1998) *Determining the required safety integrity level for your process,* ISA Transactions, 37, 105-111

Bhimavarapu, K. & Stavrianidis, P. (2000) *Safety Integrity Level Analysis for Processes: Issues and Methodologies,* Process Safety Progress, vol.19 nr.1, 19-24

DNV (2003) Hydro *Polymers AB – SIL-värdering av en ombyggnad av en ångpanna*

Dowell III, A. M. (1998) *Layer of protection analysis for determining safety integrity level,* ISA Transactions, 37, 155-165

Dowell III, A. M. (1999) *Layer of Protection Analysis and Inherently Safer Processes,* Process Safety Progress, vol.18 nr.4, 214-220

Goble, W.M. (2005) *Separation between control and safety*, Hydrocarbon Processing, Jan 2005, 1

Halang, W.A & Zalewski, J. (2003) *Programming languages for use in safety-related applications,* Annual Reviews in Control, 27, 39-45

Hauptmanns, U. (2004) *Semi-quantitative fault tree analysis for process plant safety using frequency and probability ranges,* Journal of Loss Prevention in the Process Industries, 17, 339-345

Hydro SARA *Corporate Handbook of Safety Risk Assessment (SARA)*

Jacobsson, A. (2003) *Handledning för rationell riskanalys i processindustrin,* IPS Guide

Jin, S.H., Yeo, Y-K., Moon, I., Chung, Y., Kim, I-W. (2003) *Evaluation of Safety Instrumented Systems Using Reliability Analysis*, Process Safety Progress, vol.22 nr.3, 169-173

Karlsson, H.T (1997) *Riskanalysmetoder,* avdelningen för kemisk teknologi, Lunds Universitet

Kemikontoret (2001) *Riskhantering 3-Tekniska riskanalysmetoder*

Marszal, E.M., Fuller B.A. & Shah, J.N. (1999) *Comparison of Safety Integrity Level Selection Methods and Utilization of Risk Based Approaches,* Process Safety Progress, vol.18 nr.4, 189-194

Piggin, R. (2004) *Shifting expectations: automation and safety networking,* Assembly Automation, vol.24 nr.4, 344-351

SIS (2005) Information från www.sis.se 2005-12-15

SS-EN 61511-1 (2005) *Funktionssäkerhet – Säkerhetskritiska system för processindustrin – Del 1: Allmänt, definitioner samt fordringar på system, maskinvara och programvara*

SS-EN 61511-3 (2005) *Funktionssäkerhet – Säkerhetskritiska system för* processindustrin – *Del 3: Vägledning vid bestämning av säkerhetsnivåer (SIL)*

Stavrianidis, P. & Bhimavarapu, K. (1998) *Safety instrumented functions and safety* integrity *levels (SIL),* ISA Transactions, 37, 337-351

Summers, A. E. (1998) *Techniques for assigning a target safety integrity level*, ISA Transactions, 37, 95-104

Summers, A. E. (2002) *Software-Implemented Safety Logic*, Process Safety Progress, vol.21 nr.2, 161-163

Timms, C. R. (2003) *IEC 61508/61511 – Pain or Gain?,* Process Safety Progress, vol.22 nr.2, 105-108

Weibull, B. (2004) *Säkerhetskritisk instrumentering Vad innebär IEC 61511 för processindustrin,* IPS Guide

Weibull, B. (2005) *Säkerhetskritisk instrumentering*, Föreläsning under IPS kursvecka 11/10 2005

White, R.S (2000) *Easily Determine Safety Integrity Level*, Chemical Engineering Progress, 96, 3, 51-54

Wiegerinck, J. A. M. (2002) *Introduction to the Risk based design of Safety Instrumented Systems for the process industry*, Proceedings of the 7th International Conference on Control, Automation, Robotics and Vision (ICARCV'02), 1383-139

Bilaga 1

ARBETSSCHEMA FÖR SIL-ANALYS METOD: UTBYGGD HAZOP

	Fabrik		Enhet	Utrustning	Granskningsunderlag (t ex P&I)			Datum			Signatur
Nr	Avvikelse		Orsaker	Konsekvenser	Kommentarer Vidtagna åtgärder, skydd	Riskvärdering K S H, M, E		Antal barriärer	SIL avläst i matris	Rekommenderade åtgärder	Ansvar - Tid
	Variabel	Nyckelord									

Bilaga 2

ARBETSSCHEMA FÖR SÄKERETSGRANSKNING **METOD: GROVANALYS**

	Fabrik	Enhet	Utrustning	Granskningsunderlag (t ex P&I)			Datum	Signatur
	Klorfabriken	Klorlager		426-00-28			05-10-18	
Nr	Skadehändelse	Möjliga orsaker	Konsekvenser	Kommentarer Vidtagna åtgärder	Riskvärdering K H, M, E	S	Rekommenderade åtgärder	Ansvar - Tid
4	Läckage på klorledning utomhus ansl 50	Korrosion pga vattenläcka från förgasare	Klorutsläpp utomhus (kraftigt)	– Detektorer – Snabb-avstängnings systemet	4,3,2	1		

HYDRO

Bilaga 3

ARBETSSCHEMA FÖR SIL-ANALYS METOD: UTBYGGD HAZOP

	Fabrik	Enhet	Utrustning	Granskningsunderlag (t ex P&I)	Datum	Signatur
	Klor	Klorlager	Klorledning 50Cl-12	426-00-28	05-12-07	KJ

Nr	Avvikelse		Orsaker	Konsekvenser	Riskvärdering		Skydd	Antal barriärer	SIL avläst i matris	Rekommenderade åtgärder	Ansvar - Tid
	Variabel	Nyckelord			K H, M, E	S					
1	Flöde	Högt	Reglering PC-0089 stängd	Marginellt högre tryck	-	-					
2			Brott på ledning	Stort klorutsläpp	5,3,2	1	Rörbrottsventil	1	2	Systemet med klordetektorer och sektioneringsventiler ska vara SIL 2	
3		Lågt	Stängda ventiler	Termisk expansion leder till sprängt rör	3,1,1	3	Sprängbleck	1	1		
4		Omvänd riktning	Högt tryck i Cl_2-förgasare i VCM när HTC trippar	Högt tryck som kan leda till ledningsbrott	5,3,2	5	– Mekanisk överströmning – Sprängbleck – (Designen av rör)	2 (3)	3	Se fall 2, men eventuellt SIL 3	
5	Tryck	Högt									
6		Lågt									
7	Temp	Hög	Yttre brand	Klorutsläpp	5,3,2	2	Rörbrottsventil	1	2	Se fall 2	
8		Låg	Ej relevant								
9	Sammansättning, vatten i systemet		Förgasaren läck	Korrosion, utsläpp	5,3,2	3	– Lägre tryck på vattensidan – Rörbrotts-ventil	2	2	Se fall 2	

Fabrik	**Enhet**	**Utrustning**	**Skade-händelse (nr)**	**Datum**	**Signatur**
Klor	Klorlager	Klorledning	4,7 och 9	060103	KJ, GS

Säkerhetskritisk instrumentfunktion (SKIF)	**Konsekvensbeskrivning**	**Klass**
Sektioneringssystemet	Brott på ledning – stort klorutsläpp	5

	Beskrivning	**Sannolikhet**	**Frekvens (per år)**
1 Orsaker till anrop	Högt tryck i Cl_2-förgasare när HTC trippar		6
2	Yttre brand		0,005
3	Vatten i systemet – förgasaren läck		0,013
4			
5			
Förutsättning för anrop			
Oberoende barriärer som reducerar anropsfrekvensen			
Styr- och reglersystem			
Mänskligt ingrepp			
Andra oberoende barriärer	Överströmningsventil	0,1	
Anropsfrekvens på SKIF	(6*0,1)+0,005+0,013		0,618
Konsekvensbegränsande barriärer och faktorer			
Avsäkring	Sprängbleck	0,005	
Andra oberoende barriärer	Rörbrottsventil	0,005	
Antändning			
Sannolikhet för personal i området	Ibland på dagtid	0,33	
Sannolikhet för skada	Gasmasker, flera flyktvägar	0,5	
Sannolikhet för eskalering	0,005*0,005*0,33*0,5	$4{,}125*10^{-6}$	
Andra säkerhetsåtgärder (inte oberoende barriärer)			
Olycksfrekvens utan SKIF	$0{,}618*4{,}125*10^{-6}$		$2{,}55*10^{-6}$

SIL (avläst i matris)	3	**Total olycksfrekvens**	$2{,}55*10^{-6}*10^{-3}$	$2{,}55*10^{-9}$
Tolerabel risk för konsekvensen		Tolerabel risk nådd?	Ja	
Erforderliga åtgärder				
Noteringar				

SIL	Konsekvenser														
	1			2			3			4			5		
Anropsfrekvens 5			1		1	2	1	2	3	2	3	*	*	*	*
Anropsfrekvens 4						1		1	2	1	2	*	3	*	*
Anropsfrekvens 3								1	2	1	2	*	2	3	*
Anropsfrekvens 2									1		1	2	1	2	*
Anropsfrekvens 1														1	*
Sannolikhet för eskalering %	1	10	100	1	10	100	1	10	100	1	10	100	1	10	100

* = mer än en barriär krävs

HYDRO

Bilaga 5

ARBETSSCHEMA FÖR SIL-ANALYS **METOD: UTBYGGD HAZOP**

	Fabrik	Enhet	Utrustning	Granskningsunderlag (t ex P&I)			Datum			Signatur
	Klor	Klorlager	Klorledning 50Cl-12	426-00-28			06-01-03			KJ

Nr	Avvikelse		Orsaker	Konsekvenser	Riskvärdering K H, M, E	Riskvärdering S	Skydd	Antal barriärer	SIL avläst i matris	Rekommenderade åtgärder	Ansvar - Tid
	Variabel	Nyckelord									
1	Flöde	Högt	Reglering PC-0089 stängd	Marginellt högre tryck	-	-					
2			Brott på ledning	Stort klorutsläpp	5,3,2	1	Rörbrottsventil	1	2	Systemet med klordetektorer och sektione-ringsventiler ska vara SIL 2	
3		Lågt	Stängda ventiler	Termisk expansion leder till sprängt rör	3,1,1	3	Sprängbleck	1	1		
4		Omvänd riktning	Högt tryck i Cl_2-förgasare i VCM när HTC trippar	Marginellt högre tryck		5					
4.1				Högt tryck som kan leda till ledningsbrott	5,3,2	2	– Mekanisk överströmning – Sprängbleck	2	-		
5	Tryck	Högt									
6		Lågt									
7	Temp	Hög	Yttre brand	Klorutsläpp	5,3,2	2	Rörbrottsventil	1	2	Se fall 2	
8		Låg	Ej relevant								
9	Sammansättning, vatten i systemet		Förgasaren läck	Korrosion, utsläpp	5,3,2	3	– Lägre tryck på vattensidan – Rörbrotts-ventil	2	2	Se fall 2	

HYDRO

Bilaga 6

ARBETSSCHEMA FÖR SÄKERETSGRANSKNING METOD: GROVANALYS

	Fabrik	Enhet	Utrustning	Granskningsunderlag (t ex P&I)			Datum	Signatur
	Klor	Klorupparbetning		706-00-07			05-10-18	GS
Nr	Skadehändelse	Möjliga orsaker	Konsekvenser	Kommentarer Vidtagna åtgärder	Riskvärdering S	 K H, M, E	Rekommenderade åtgärder	Ansvar - Tid
18	Övertryck i Cl_2 systemet i cellsal samt upparbetningen	Stopp på klorfläkt samt att ej PIC 728-645 ej öppnar	Klorutsläpp i cellsal	Manuell neddragning av produktionen	3	3,2,1		

HYDRO

Bilaga 7

ARBETSSCHEMA FÖR SIL-ANALYS **METOD: UTBYGGD HAZOP**

	Fabrik		Enhet	Utrustning	Granskningsunderlag (t ex P&I)			Datum			Signatur
	Klor		Klorupparbetning		707-00-07			06-01-03			KJ, GS
Nr	Avvikelse		Orsaker	Konsekvenser	Riskvärdering K H, M, E	S	Skydd	Antal barriärer	SIL avläst i matris	Rekommenderade åtgärder	Ansvar - Tid
	Variabel	Nyckelord									
1	Flöde	Högt	Ej relevant								
2		Lågt	Klorfläkt stopp	Högt tryck i celler	3,2,1	4	Manuell neddragning	1	1	SIL 1 på övertrycks-skydd	
3			Igensättning i klortork	Fläkten orkar inte, mindre allvarligt än stopp på fläkten							
4			Klorkompressor stopp	Högt tryck i celler	4,2,1	4	Manuell neddragning	1	2	3 oberoende system finns	
4		Omvänd riktning	Ej relevant								
5	Nivå	Hög/ låg	Ej relevant								
6	Temp	Hög	Förhöjd spänning i en cell	Cellen blir varm, kokar. Eventuellt explosion	1,1,1	5		Inga	1	2 (eller 3) oberoende system finns	
7		Låg	Ej relevant								
8	Sammansättning, fel pH-värde		Lågt pH-värde i saltlösningen pga för mycket syra	Explosioner av celler pga hög halt H_2	3,2,3	2		Inga	1		

ARBETSSCHEMA FÖR SÄKERETSGRANSKNING METOD: GROVANALYS

	Fabrik	Enhet	Utrustning	Granskningsunderlag (t ex P&I)			Datum	Signatur
	PVC-fabrik	Autoklav					05-10-06	
Nr	Skadehändelse	Möjliga orsaker	Konsekvenser	Kommentarer Vidtagna åtgärder	Riskvärdering K H, M, E	S	Rekommenderade åtgärder	Ansvar - Tid
2	Skenande autoklav	– Fel mängd initiator – Kylvatten-bortfall	Svagaste punkten brister på autoklaven, kan bli följd scenario med brand	– Nöd-avblåsning – Tömning till annat kärl – Satsning av moderator – Satsning av killer – Katastrof-ventilation	4,2,4	2	– Beräkna säkerhetsventilernas kapacitet. – Undersök vilket ställe på autoklaven som är bäst att köra in killer på.	

HYDRO

Bilaga 9

ARBETSSCHEMA FÖR SIL-ANALYS **METOD: UTBYGGD HAZOP**

	Fabrik		Enhet	Utrustning	Granskningsunderlag (t ex P&I)			Datum			Signatur
	PVC		Autoklav					05-12-13			KJ
Nr	Avvikelse		Orsaker	Konsekvenser	Riskvärdering K H, M, E	S	Skydd	Antal barriärer	SIL avläst i matris	Rekommenderade åtgärder	Ansvar - Tid
	Variabel	Nyckelord									
1	Nivå	Hög	Ej tömd vid start	När värmning startar stiger trycket. Kommer troligen läcka vid en fläns och trycket sjunker.	2,1,2	5	Säkerhetsventil	1	1		
2			Fel på flödesmätare	Se fall 1	2,1,2						
3			Fel i recept	Se fall 1	2,1,2						
4			Termisk expansion	Se fall 1	2,1,2						
5		Låg	Ej relevant								
6	Tryck	Högt	Se fall 1	Killer utlöses. Om det ej hjälper sker bristning vid svagaste punkten eller eventuell	4,2,4						
7			Fel initiator	Se fall 6	4,2,4						
8			Fel mängd initiator	Se fall 6	4,2,4						
9			Kylvattenbortfall	Se fall 6	4,2,4	3	Säkerhetsventil	1	2		
10			Stopp på omrörare	Se fall 6	4,2,4						
11			Fel temperatur	Se fall 6	4,2,4						