Rekommendation från
Sodahuskommittén
Allmänna villkor för användande av Sodahuskommitténs rekommendationer framgår av rekommendation A 3

Nr B 18
Utgåva 3, mars 2024
(Rev 2024-10-21)

Rekommendation för instrumenterade säkerhetssystem i Sodapannor, SIS (Safety Instrumented Systems)

Sodapannans säkerhetssystem, (SIS, Safety Instrumented System), är den del av pannans automatisering som när ordinarie processtyrsystem inte förmår att kontrollera situationen, skyddar pannan genom att försätta pannan i ett säkert tillstånd. Med farligt tillstånd avses driftsituation som kan orsaka skada på personal och utrustning. SIS inkluderar utrustning och installationer (till exempel logik, kablage, fält- och elektrisk utrustning) som behövs för uppbyggnad av säkerhetsfunktioner.

Rekommendation B18 är avsedd som vägledning vid planering, utformning, installation och användning av instrumenterade säkerhetssystem i sodapannor.
I rekommendation ges en översiktlig beskrivning av hur nyare säkerhetssystem för sodapannor skall vara utförda, med hänvisning till relevanta standarder.
Även ges generella rekommendationer om hur äldre säkerhetssystem för sodapannor skall vara utförda. Detta gäller hårdförtrådade system (reläsystem), omprogrammeringsbara system och icke omprogrammeringsbara system såväl som kombinationer av dessa systemtyper.

Rekommendationen ska inte ses som en komplett lista över de krav som ställs på sodapannors säkerhetssystem. Varje användare måste själv säkerställa genom egen riskanalys vilka ytterligare krav på sodapannors säkerhetssystem som finns.

I rekommendationen eftersträvas att för såväl definitionen av säkerhet, instrumentering, konstruktion, implementering, drift och underhåll, så långt som är tillämpligt följa branschstandarden SS-EN 61511eller den grundläggande standarden SS- EN 61508.

Befintliga säkerhetssystem, installerade före 2005, omfattas inte av SS-EN 61511, förrän deras säkerhetsfunktion, eller det de skyddar, förändras väsentligt.
Sodahuskommittén behåller därför delar av föregående utgåva av B18 som beskriver rekommendation för sodapannas säkerhetssystem av äldre modell.

Observera dock att Sodahuskommittén generellt rekommenderar att äldre säkerhetssystem byts ut eller moderniseras så att kraven i SS-EN 61511, SS-EN 50156 och SS-EN 12952 kan innehållas.

Eventuella lagar, förordningar och instruktioner och riktlinjer från behöriga myndigheter bör noteras och följas och är alltid överordnade rekommendationerna om diskrepans skulle föreligga.

Hänvisningar

Föreskrifter
AFS 2023:5 Tryckbärande anordningar

Standard
SS-EN 12952, Vattenrörspannor och hjälpinstallationer, del 7 - krav på pannas utrustning, del 1- krav på utrustning för vakter och säkerhetssystem för pannor och tillbehör

SS-EN 50156, Elutrustning för ugnar och pannor som eldas med fasta, flytande eller gasformiga bränslen

SS-EN 61511-1, -2, -3, Funktionssäkerhet – Säkerhetskritiska system för processindustrin

SS-EN 61508, Säkerhetsfordringar på elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska systems funktion

Rekommendationer

B 1, Sodapannans konstruktion och utrustning

B 8, Nödnedeldning och snabbtömning av sodapannor

B 12, Reservkraft

B13, Utrustning och säkerhetssystem för olje- och gaseldning i sodapannor (reviderad 2020).

B 14 Rekommendationer angående arrangemang av larm och indikeringar i manöverrum

Övrig information

SSG 2240 Säkerhetskritisk instrumentering enligt SS-EN 61511

SSG 2241 Användarhandledning säkerhetskritisk instrumentering enligt SS-EN 61511, *sammanfattar vilka krav som ställs på säkerhetssystem/ säkerhetsfunktioner inkl de komponenter som behövs för att realisera dessa funktioner och beskriver metodiken för att utforma säkerhetsfunktioner i enlighet med SS-EN 61511.*

SIL i praktiken (IPS, Intressentföreningen för processäkerhet),
en handledning utgiven av IPS (Intressentföreningen för processäkerhet) som ger detaljerade råd om hur man bygger upp en väl fungerande instrumentering för säkerhetskritiska funktioner i processindustrin. Handledningen utgår från SS-EN 61511, och till viss del även från SS-EN 61508.

Sodahuskommiten.se/Rapporter, Slutrapport Riskanalys Fas 3, Kiwa, Björn Lundgren

Innehåll

1 Inledning

1.1 Sodapannans säkerhetssystem

1.2 Allmänt

Krav på riskanalyser och riskhantering har formulerats i flera av Arbetsmiljöverkets föreskrifter. Initialt har det varit tillräckligt att efter en genomförd riskanalys konstatera att det finns skydd mot identifierade faror.

Numera har utarbetats standarder och metoder för att på ett systematiskt sätt visa att vidtagna skydd tillsammans är tillräckliga för att eliminera risken för skador till en godtagbar nivå. En sådan metod erbjuds genom SIL- nivåbestämning, vilket behandlas i det följande.

Under 2017 – 2023 har Sodahuskommittén i ett uppdrag till Kiwa genomfört en studie kring sodapannors säkerhetssystem med mål att utarbeta en rekommendation anpassad till moderna föreskrifter och standarder och med målsättning att:

- Samtliga krav på säkerhetsfunktioner finns listade
- För varje säkerhetsfunktion anges vart kravet härrör från
- För varje säkerhetsfunktion beskrivs den riskfyllda händelsen den ska skydda mot
- För varje säkerhetsfunktion anges ett lägsta SIL-krav som Sodahuskommittén rekommenderar

Resultaten av denna studie framgår på Sodahuskommitténs hemsida / Rapporter. Studien i rapporten hanterar en fiktiv panna och varje användare skall ta fram en egen riskanalys och utföra bedömning på den specifika pannan.

Ansvaret för implementering av sodapannans säkerhetssystem, SIS, åligger tillverkarna av utrustningen och de som implementerar sodapannas säkerhetssystem. Det är användarnas ansvar att tillse att SIS används och underhålls korrekt och med omsorg.

I rekommendation B13 beskrivs utrustning och krav på säkerhetssystem för oljeeldning.

I rekommendation B16, beskrivs Sodahuskommitténs rekommendationer för säkerhetssystem starka-/svaga gaser, metanol och terpentin.

Rekommendation B8, beskriver Sodahuskommitténs rekommendationer för säkerhetssystem för nödnedeldning och snabbtömning.

1.3 Förkortningar

Förkortningar som används i SS-EN 12952, se Bilaga 1.

1.4 Ordlista

Ordlista över vanligt förekommande termer och förkortningar se Bilaga 2.

1.5 Standarder

Sodapannan med alla dess hjälputrustningar skall vid nya installationer projekteras och tillverkas i överensstämmelse med EU direktiv 2014/68/EU. Direktivet har implementerats i svensk lagstiftning genom Arbetarskyddsstyrelsens föreskrift AFS 2016:1. Som ett sätt att uppfylla EU direktiv 2014/68/EU, vanligen kallat PED, har i fråga om ångpannors och sodapannors konstruktion och utrustning europastandardserien SS-EN 12952 utarbetats. Direktivet innehåller allmänna säkerhetskrav medan detaljerade säkerhetsanvisningar ges i standarder.

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.

Vissa standarder som SS-EN 12952 är harmoniserade mot tryckkärlsdirektivet vilket innebär att man förutsätts uppfylla direktivet om standarden åtföljs.

Beträffande instrumentering, elektrisk, elektronisk och elektronisk programmerbar utrustning hänvisar SS-EN 12952 vidare till SS-EN 50156 (som dessutom i vissa delar hänvisar till SS-EN 61508).
Serien SS-EN 61508, del 1-7, kan ses som grundläggande säkerhetsstandard för funktionssäkerhet hos ”elektriska, elektroniska och programmerbara elektroniska system”, oavsett tillämpning, d.v.s. utgör den centrala standarden för funktionssäkerheten hos styrsystem. Dock är inte SS-EN 61508 harmoniserad. Standarden införde begreppet SIL (Safety Integrity Level) och en metod för att använda dessa säkerhetsnivåer för att gradera riskerna och kraven på åtgärder för riskreducering.
SIL-nivåer, är diskreta nivåer för att definiera tillförlitlighet hos säkerhetsfunktioner som är elektriska, elektroniska eller programmerbar elektronisk utrustning. SIL-nivåerna är graderade i 4 steg från 1-4, varav 4 anger den högsta tillförlitligheten.

För att praktiskt tillämpa SS-EN 61508 inom olika branscher har sektorstandarder utvecklats. Standarden SS-EN 61511 är en sådan standard anpassad till processindustrin. Standarden består av 3 delar och är enklare att sätta sig in i. SS-EN 61511 tillämpar metoden med SIL på säkerhetskritiska system i processindustrin. Där införs begreppet Safety Instrumented System (SIS), för en kedja med utrustning som används för att implementera en säkerhetsfunktion.

Så länge man bygger sina funktioner av färdiga utrustningar och system på marknaden, enbart konfigurerar eller programmerar dessa med förenklade programspråk, d.v.s. integrerar färdiga utrustningar och system, täcker SS-EN 61511 tillämpningarna. Endast om man utvecklar egna utrustningar i sina säkerhetsapplikationer, eller vill använda sig av fri programmering i komplexa språk, behöver man tillämpa SS-EN 61508, något som följaktligen då gäller även leverantörer av instrumentutrustning,

Den första delen, SS-EN 61511-1 innehåller standardens krav. Del två och tre av SS-EN 61511 är informativa. Del två innehåller vägledning och exempel och del tre ger information om olika metoder för riskbedömning.

Standarden behandlar säkerhetssystemets hela livscykel, definierar krav för livscykelns olika faser från en ursprunglig riskanalys till design, installation, drift och slutligen skrotning av säkerhetssystemet.
Standarden ställer tydliga krav på organisation, ansvarsfördelning, kompetens och dokumentation.

Innan enskilda säkerhetsfunktioner specificeras ska generella säkerhetsstrategier i företaget säkerställas och en kvalitetssäkringsplan skall tas fram.

Tryckkärlsdirektivet förutsätter dock inte harmoniserade standarder för att en tillverkare skall kunna kvalificera sin personal och sina metoder. I avsaknad av harmoniserade standarder kan tillverkaren i stället behöva åberopa något tekniskt dokument som beskriver hur

metodkvalificeringen och kompetensprövningen skall utföras för att motsvara direktivets krav. Detta tekniska dokument kan tillverkaren själv ha upprättat.
Tillverkaren skall dock ”ha låtit tryckbärande anordningar genomgå ett förfarande för bedömning av överensstämmelse med de grundläggande säkerhetskraven”, (AFS 2016:1, 10§).
I motsats till vad som gäller vid tillämpning av SS-EN-standarden, måste därför i sådana fall konstruktion och tillverkning redovisas och vid behov godkännas av ett ”ackrediterat kontrollorgan” (”notified body”), kvalificerat att utföra kontroll av tryckbärande anordningar. När det gäller tänkbara avvikelser från SS-EN-standarden i en anläggning, bör även dessa tas upp till diskussion med ett för kontroll av tryckbärande anordningar ”ackrediterat organ”.

Det finns formellt endast en tillverkare av en tryckbärande anordning. Tillverkaren ansvarar under en 10-årsperiod för konstruktion och tillverkning av den tryckbärande anordningen. Det är viktigt att i ett tidigt skede klargöra vem som är tillverkare och därmed har ansvaret. Tillverkaren måste ha den kompetens som krävs enligt PED för att få åta sig tillverkarrollen och CE-märka anläggningen enligt PED.

Exempel på några som kan vara tillverkare är rörentreprenören, maskinleverantören, processleverantören eller användaren av anordningen.

1.6 Arbetsgång vid utformning av instrumenterade säkerhetssystem eller säkerhetsfunktioner

Arbetsgången för att specificera enskilda säkerhetssystem (SIS) eller säkerhetsfunktioner (SIF) beskrivs i SS-EN 61511 och sammanfattas i SSG 2240 som nedan:

- Genomföra riskbedömning
- Välja skyddsbarriärer
- Bestämma erforderlig integritetsnivå (SIL) för de skyddsbarriärer som är elektriska/elektroniska
- Göra en säkerhetskravspecifikation (SRS)
- Utforma en instrumentfunktion (SIF) som matchar den erforderliga integritetsnivån och säkerhetsspecifikationen
- Installera instrumentfunktionen och ta den i drift
- Kontinuerligt verifiera säkerhetsfunktionerna under hela livscykeln

Grundläggande för standarden är:

- **Livscykelperspektiv** – varje fas vid utformning av en säkerhetsfunktions (SIF), från dess tillkomst till dess skrotning beskrivs med de krav som gäller för varje fas
- **Ledningssystem** - krav på ledningssystem, kompetens för projektdeltagare plan för ansvar och aktiviteter under livscykelns olika faser

Alla personer som hanterar sodapannans säkerhetssystem, SIS, inklusive ledningsuppgifter, eller handläggning av säkerhetssystemets hårdvara, programvarusäkerhet under dess livscykel, bör ha lämplig utbildning, teknisk kunskap, erfarenhet och kompetens som är relaterade till deras specifika uppgifter.
Deltagare och deras ansvar i de olika faserna i SIS-projekt, måste definieras i början av projektet som en del i en säkerhetsplan. SIS's säkerhetsplan måste klargöra uppgifterna för de olika deltagarna, leveransbegränsningar (utrustning, dokument), deltagande i tester och idrifttagning.

Våra bruk har idag omfattande ledningssystem för kvalitet och miljö och det bör därför vara möjligt att integrera standardens krav på ledningssystem i dessa.

- **Kvalitetssäkring** – olika former av granskning, verifiering och revision under och efter de olika faserna i projektet
  - validering
  - hantering av ändringar, verifiering, provning och revision ingår, liksom uppföljning och avslutning av åtgärderna.

- **Dokumentation** – tydliga krav på dokumentation av olika faser i projektet.
  En väsentlig del av utformningen av SIS är att skapa dokumentation som möjliggör att kunna spåra systematisk verifiering och acceptans av SIL-krav.
  Verifiering måste tillämpas efter varje fas under projektarbetet och övergripande acceptans bör ske vid anläggningen före uppstart.

- **Riskanalys** – utformning av en SIF utgår från riskanalys och SIL- nivåbestämning.
  Hela den säkerhetskritiska funktionen från givare, logik manöverdon omfattas av SIF.

- **Säkerhetskravspecifikation (SRS) -** För varje SIF ska säkerhetskraven dokumenteras

- **Integritetsnivåer** – en SIF's förmåga till riskreduktion definieras i fyra SIL-nivåer

- **Tekniska krav –** specifika krav på val av utrustning, utformning av hård-och mjukvara.
  - provning av SIS-komponenter

1.7 Andra sektorstandarder för processindustrin

Det existerar även andra sektorstandarder för processindustrin.
En standard som ofta tillämpas mot maskindirektivets krav är SS-EN 62061. Denna standard är inte avsedd att tillämpas på trycksatta anordningar. SS-EN 62061 är utformad för säkerhetsfunktioner med hög anropsfrekvens något som ofta gäller för maskiners säkerhetsskydd. Anropsfrekvensen har betydelse för bland annat testning av säkerhetsfunktioner.

I sodahuset förekommer en hel del maskiner, som pumpar, fläktar, transportörer, mm.

- SS-EN 62061 är lämplig att tillämpas vid risker från maskiner direkt mot person.
- SS-EN 61511 tillämpas för skydd mot maskinens effekter i processen (tryck, temperatur).

2 Riskbedömning

Säkerhetskrav, angivna som SIL-nivå hos säkerhetsfunktioner, ska definieras baserat på riskanalys. Den mest utbredda metoden för definitionen av säkerhetsnivå är en riskgraf i enlighet med SS- EN 61508 och SS-EN 61511. Metoden bygger på riskbedömning, där konsekvenser och sannolikhet för exponering av faran bedöms när SIS inte används.

Inneboende faror eller riskkällor som förekommer i sodahusanläggningar är exempelvis inneslutna höga tryck och temperaturer, hantering av heta och frätande eller giftiga kemikalier, osv. Dessa faror ger upphov till risker för skador på människor och egendom. Risken (R) brukar definieras som produkten av sannolikhet (S) för skadans uppkomst och konsekvens (K) av skadan.

För att utvärdera riskers betydelse ska olika farosituationer och deras sannolikhet och konsekvens beaktas, samt avgöras vilken grad av risk som anses tolerabel.

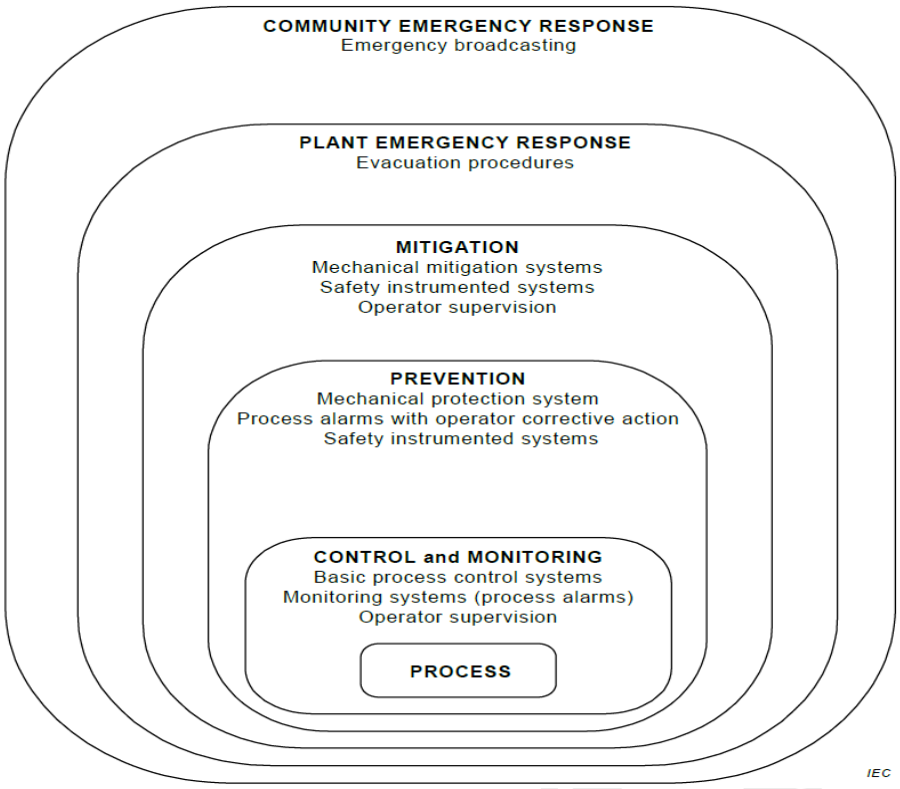
2.1 Riskhantering

Riskhantering syftar till att minska risken genom begränsning och kontroll av identifierade faror.
Nödvändig riskreduktion kan uppnås genom att:

- den grundläggande faran undanröjas, exempelvis genom att välja annan teknisk lösning, ersätta en farlig kemikalie mot en mindre farlig, osv

- minska sannolikhet för olyckshändelse genom att förebygga och förhindra faran att utvecklas till en olycka, exempelvis med olika mekaniska säkerhetsrelaterade system (SRS), som säkerhetsventiler, sprängbleck. SRS kan även inkludera instrumentella säkerhetssystem (SIS) för elektrisk, elektronisk eller programmerbar elektronik (E / E / PE). (Förkortningar hänvisar till standard SS-EN 61508 och SS-EN 61511).

- minska olyckans konsekvenser genom barriärer som begränsar och lindrar skadan, som brandskydd, skyddsutrustning, invallningar, utrymningsplaner, begränsade rörelseområden, instruktioner mm



Figur 1; Typiska skyddslager och riskbarriärer (se SS-EN 61511-1)

2.2 Riskreduktion

Vid bedömning av processens risk tar man även hänsyn till den riskreducering som det normala processtyrsystemet (BPCS) bidrar med. SS-EN 61511 begränsar nivån för processtyrsystemets bidrag till riskreducering (till en faktor 10).
Nödvändig riskreducering är den minsta riskreducering som måste åstadkommas för att uppnå tolererbar risk. Den nödvändiga riskreduceringen kan åstadkommas av en, eller av en kombination av sinsemellan oberoende riskreduceringsåtgärder.

Förmågan till riskreduktion hos en viss säkerhetskritisk instrumentfunktion anges av dess SIL-integritetsnivå. Standarden SS-EN 61511 definierar fyra SIL-nivåer, varav den lägsta nivån 1 ger er riskreduktion mellan 10 och100 och varje steg därutöver ökar riskreduktionen med en faktor 10.
Om flera barriärer finns fördelas riskreduktionen mellan dessa och den återstående risken bestämmer vilken SIL-nivå som instrumentfunktionen behöver svara för, dvs vilken SIL-nivå som krävs.

Ett annat sätt att ange förmågan till riskreduktion är att ange riskreduceringsfaktorn (RRF). Antag att en skyddsbarriär fungerar 999 ggr av 1000, dvs den reducerar risken till 1/1000. Riskreduceringsfaktorn, RRF, i detta exempel blir alltså 1000. Barriärens tillgänglighet avgör dess förmåga till riskreduktion.

2.3 Bestämning av integritetsnivå (SIL-nivåbestämning)

Det finns i princip tre olika typer av metoder för att bestämma integritetsnivå:

- Matrismetoder – kvalitativa metoder.
- Säkerhetsbarriäranalys (LOPA) – semikvantitativ metod.
- Felträd och händelseträd – kvantitativ metod (se EN 50156:2015 eller EN 61511).

Säkerhetsfunktioner (SIF) behandlas i SS-EN 61508 och SS-EN 615 11.
Standarden SS-EN 61511 är anpassad till processindustrin inom ramen för SS-EN 61508
Övriga tillämpliga standarder som behandlar säkerhetssystem, se SS-EN 764, SS-EN 50156.

I ett säkerhetskritiskt instrumentsystem (SIS), se avsnitt 3, ingår en eller flera säkerhetskritiska instrumentfunktioner (SIF), som ofta har någon gemensam del eller betjänar samma processavsnitt. Logikdelen och manöverdon kan vara gemensamma för flera SIF. Det är mer sällan som givare är gemensamma för flera SIF. Det är en fördel om man delar upp sina funktioner så att ett SIS omfattar alla SIF inom ett avgränsat processavsnitt.

Det ordinarie styr- och reglersystemet håller vid normal drift processen inom säkra gränser genom att mer eller mindre automatiskt styra processvariabler, såsom tryck, nivå, temperatur, flöde med mera. Processtyrsystemet kan inte användas för SIF med en riskreduktion mer än 10 ggr. Orsaken är att SIF ska vara oberoende från ordinarie processtyrning.

2.4 Konstruktion av den instrumenterade säkerhetsfunktionen

Efter utförd riskanalys, exempelvis med hjälp av riskgraf i enlighet med SS-EN 61511har erforderlig säkerhetsnivå, SIL-nivå bestämts för en instrumenterad säkerhetsfunktion.
Nästa steg blir för instrumentkonstruktören att realisera säkerhetsfunktionen med all utrustning som behövs för dess uppbyggnad (givare, kablage, fält- och elektrisk utrustning och logik). Den uppnådda säkerhetsnivån skall härvid verifieras.
Standarden SS-EN 61511 anger beräkningsmodeller för detta arbete. För enkla funktioner tillämpas formler ur sannolikhetsläran, medan för mer komplicerade sammansatta funktioner finns särskilda beräkningsprogram.
Begrepp som riskreduktionsfaktor, RRF, sannolikhet för farligt fel vid anrop PFD, otillförlitligheten,
PFH (felfrekvens/timme) är viktiga begrepp i dessa beräkningar liksom felsäkerhetskvot SFF.

Felsäkerhetskvot, SFF, är ett begrepp som beskriver hur felsäker utrustningen är.
Att man i säkerhetskritiska system eftersträvar val av certifierade och provade säkerhetsutrustningar (givare, reläer, PLC m.m.) är att få en hög grad av felsäkerhet.

3 Sodapannans säkerhetssystem

Sodapannans säkerhetssystem, (SIS, Safety Instrumented System), är, som inledningsvis konstaterats, den del av pannans automatisering som skyddar pannan från att komma i farligt tillstånd, eller som i farligt tillstånd kontrollerar och försätter pannan till ett säkert tillstånd. Med farligt tillstånd avses driftsituation som kan orsaka skada.
SIS (kan vara fler än ett system) ska omfatta alla nödvändiga instrumenterade säkerhetsfunktioner för att förhindra farliga tillstånd eller skador på person eller utrustning. SIS inkluderar utrustning och installationer (till exempel logik, kablage, fält- och elektrisk utrustning) som behövs för uppbyggnad av säkerhetsfunktioner.

En väsentlig del av utformningen av SIS är att skapa dokumentation som möjliggör att kunna spåra systematisk verifiering och acceptans av SIL-krav.

Beträffande säkerhetssystem ställs i SS-EN 12952, Part 7, avsnitt 4.5, krav på att tillämpa SS-EN 50156-1, (val och användning) och att bestämma en adekvat SIL-nivå för respektive säkerhetsfunktion. Det är behovet av riskreduktion som ska bedömas. Risk är produkten av skadans omfattning och dess sannolikhet. Dessa två parametrar behöver därför skattas.

Beträffande sodapannors säkerhetssystem av äldre modell, se avsnitt 5.

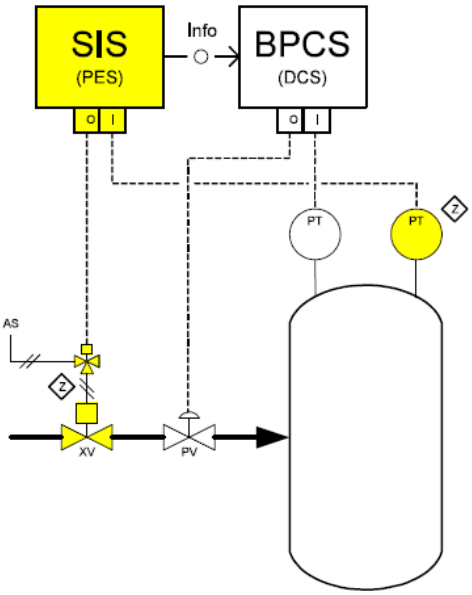
3.1 Säkerhetskritisk instrumentfunktion (SIF)

En säkerhetskritisk instrumentfunktion är en instrumentfunktion som är avsedd att uppnå eller upprätthålla processens säkra läge i förhållande till en specifik farlig händelse. En SIF ska vara oberoende av ordinarie processtyrning och realiseras i det säkerhetskritiska instrumentsystemet. En sådan funktion kan därför aldrig implementeras i det ordinarie processtyrsystemet, (BPSC), se avsnitt 3.4.

För att uppnå erforderlig integritetsnivå, kan en säkerhetsfunktion behöva kompletteras med ytterligare säkerhetsfunktioner. Detta innebär, till exempel för stopp av primärluftfläkten, att förutom säkerhetsfunktionen som stoppar fläktens motor, leder ytterligare en säkerhetsfunktion luftspjällen till ett stängt (säkert) läge.
Reglering och kontrollåtgärder som inte har säkerhetskrav implementeras i processtyrsystemet.

3.2 (SIS_1), hårdvara

Säkerhetssystemet måste vara oberoende av det ordinarie processtyrsystemet.
Processtyrsystemet kan anslutas till säkerhetssystemet för att ta emot information, genom till exempel bussanslutningar eller hårddisk. En separat SIS-enhet betyder en separat logik eller en (integrerad) logik som har byggts med separata styrsystemkomponenter och innehåller endast de åtgärder som är avsedda för säkerhetsfunktioner.
Givare med kretsar relaterade till SIS kopplas först till SIS_1, varifrån mätdata för indikering, rapportering, styrning leds till processtyrsystemet antingen direkt genom buss, genom en 1/1 transformator eller med ytterligare utgångar från SIS_1 .
SIS_I implementeras med den definierade högsta integrerade säkerhetsnivån baserad på riskanalysen.



3.3 SIS Mjukvara

Säkerhetssystemets mjukvara framtas och uppbyggs enligt beskrivning i SS- EN 61508 och SS-EN 61511.

3.4 Separation

En grundregel är att säkerhetskritiska instrumentfunktioner ska separeras från icke säkerhetskritiska, som övervakning, styrning och reglering.

- SIS eller SIF kan aldrig implementeras i ordinarie styrsystem (BPCS som inte har någon separat certifierad felsäker del).
- SIS eller SIF ska inte dela utrustningar som givare och ventiler med ordinarie styrsystem
- Säkerhetssystemet (SIS) ska enbart användas till säkerhetskritiska funktioner.
- Insignaler från givare och utsignaler till manöverdon ska överföras direkt till/från SIS inte hämtas eller först bearbetas via styr och reglersystem (BPCS).

3.5 Säkerhetssystemets fältutrustning

För fältutrustning allmänt, är det nödvändigt att uppmärksamma de krav på redundans och tillförlitlighet som krävs för funktion och upprätthållande av säkerhetsintegritetsnivåerna (SIL-nivå).
Vid specificering av fältutrustningen måste man också beakta möjligheten till periodiska tester under drift.
SIS´s säkerhet (sensorer - logik - ställdon) bör kontrolleras med hjälp av en beräkningsanalys, för att säkerställa att integritetsnivån som definieras med hjälp av riskanalysen uppnås, med valda utformningar av säkerhetsfunktioner (SIF), se SS-EN 61511 för detaljer.
Fältutrustning bör vara certifierad och avsedd för användning i säkerhetssystem.

3.5..1 Givare

Givare sensorer och vakter ska uppfylla kraven i SS-EN 12952-11.
De bör i första hand vara certifierade avsedda för användning i säkerhetssystem. Vid användning av vanliga givare bör mätningarna genomföras med hjälp av jämförelseprincipen 2/3 för att uppnå så hög tillgänglighet som möjligt.
Vid användning av givare med högkvalitativ självdiagnostik uppnås en högre integritetsnivå och användbarhet med hjälp av två givare och 1/2 -princip. Två separata signaler, mätsignal och diagnossignal, kan erhållas med säkerhetsgivare. Diagnossignalen ger information om givarens tillstånd. Det blir då inte nödvändigt att försätta anläggningen till ett säkert tillstånd på grund av ett givarfel, den uppgiften överförs till den andra givaren och operatören varnas för felstillståndet. Den felande givaren måste bytas ut inom en viss tidsperiod.

3.5..2 Tryckknappar och omkopplare

Tryckknappar för nödstopp (EMD) skall vara svampformade, röda i färg, utrustade med ett tillräckligt polantal. Knapparna måste låsas när de trycks in. Knapparna i fält måste vara markerade så att det är klart vilken effekt nödstoppsknappens användning kommer att ha. Knappen ska vara tydligt synlig från minst 10 meters avstånd. Den brytning som aktiverats av nödstoppsknapparna bekräftas med en separat kvitteringsknapp i kontrollrummet.

3.5..3 Ventiler

Ventiler anslutna till SIS-kretsar måste vara utrustade med fjäderretur. Ställdonets körriktning måste väljas på ett sådant sätt att fjäderkraften leder ventilen till ett säkert tillstånd medan tryckluften lämnar ställdonet.
Omkoppling till säkert tillstånd initieras med en pilotventil (magnetventil), kopplad till ställdonet. Magnetventilen när den är frånslagen släpper ut trycket från ställdonet, och fjädern tvingar ventilen till ett säkert tillstånd. Det ska inte vara möjligt att manuellt styra magnetventilerna.
Ställdon med "Fjäder stänger" används som brandventiler och ESD-ventiler medan ställdon med funktion "fjäder öppnar" används som ventilations- / tryckventiler. Brandventiler och ESD-ventiler måste uppfylla kraven i mediet.
Avstängningsventiler för matarvatten, huvudångledning, startventil och snabbtömningsventiler är traditionellt elektriskt drivna och ska utrustas med en säkrad hjälpförsörjning.

3.5..4 Pumpar och fläktar

För manövrering av pumpar och fläktar används ofta motorkontaktorer, frekvensomformare eller effektbrytare***. De säkerhetshetsrelaterade utlösningskretsarna och de styrsystemrelaterade manöverkretsarna skall vara helt separerade och oberoende av varandra.***
Utlösningskretsarna skall vara felsäkra och konstrueras i enlighet med i riskbedömning erhållen SIL-nivå. De styrsystemrelaterade manöverkretsarna bör så långt som möjligt vara viloströmskopplade. Återföring av manöverdelarna och/eller motordrifternas erhållna lägen, position eller rotation bör återkopplas till styrsystemet så att dessa kan verifieras och övervakas.

3.5..5 Motorventiler

För manövrering av större ventiler för ånga, matarvatten, förbränningslufts- eller rökgassystem används ofta elektriska manöverdon bestående av ett elektriskt ställdon och

nödvändiga stödsystem såsom anslutning till ett UPS-system med tillhörande el-komponenter.
Grundprincipen är att manöverdonets säkerhetshetsrelaterade utlösningskretsar och de styrsystemrelaterade manöverkretsarna skall vara helt separerade och oberoende av varandra.
För att det elektriska ställdonet skall erhålla säkert läge då utlösningskretsarna aktiveras, krävs oftast anslutning till externt UPS-system med tillräcklig kapacitet för att möjliggöra manöver till säkert läge. Konstruktionen av manöverdonets säkerhetsfunktionalitet skall utföras i enlighet med i riskbedömning erhållen SIL-nivå och inkludera nödvändiga stödsystem. Återföring av manöverdonets verkliga läge, position, moment eller temperatur bör återkopplas till styrsystemet så att dessa kan verifieras och övervakas.

.

3.5..6 Säkerhetsbrytare

Både motorer och motorventiler ska utrustas med normala säkerhetsbrytare.

3.5..7 Spänningsförsörjning

Säkerhetssystem skall vara säkrat med avbrottsfri kraft, se rekommendation B 12. Där stipuleras att citat:
”Säkerhetssystem ska ha separat och avbrottsfri spänningsmatning för bibehållen funktion under minst 60 minuter.
I de fall programmerbara säkerhetssystem användes skall systemminnet vara beständigt, alternativt skall systemet vara försett med egen batterireserv för 7 dygns bevarande av minnet.

Huvudförsörjningen för säkerhetsrelaterade ställdon och motorventiler, samt övriga fältutrustning som givare mm måste vara anordnade med avbrottsfri reservkraft (t.ex. diesel och UPS).
UPS-säkert nätverk måste vara utformat på ett sådant sätt att det kan hålla systemet igång i 60 minuter.”

4 Instrumenterade säkerhetsfunktioner

Sodapannans säkerhetssystem, pannskyddet, består av flera säkerhetsfunktioner, SIF som är anpassade till olika tillstånd och driftlägen för pannan. SIF är baserade på definierade värden och tillstånd. När villkoren för pannans säkerhetsfunktioner är uppfyllda kan pannan startas och/eller förbränningen fortgå.

En detaljerad sammanställning av faror, risker och erforderliga SIL-integritetsnivåer framgår av den riskanalys för den fiktiva Sodapannan som utförts av Sodahuskommittén i samarbete med Kiwa Technical Consulting.
För detaljer om tillämpad metodik i denna studie samt för redovisning av resultat hänvisas till Rapporter på Sodahuskommitténs hemsida.

2016-1: Riskanalys Sodapanna Fas 1
2017-1: Riskanalys Sodapanna Fas 2 Bilaga 1 Checklista Excel-fil
2023-3: Riskanalys Sodapanna Fas 3, slutrapport

Nödvändiga säkerhetsfunktioner som anges i den harmoniserade standarden SS-EN12952, eller identifierats i riskanalys förtecknas i det följande. Avsnittshänvisningar inom parentes

avser hänvisning till standarden om inte annat anges.

4.1 Definierade Stopp-manövrar

I förteckningen över säkerhetsfunktioner (SIF) används ett antal begrepp för att beskriva ***sammansatta säkerhetsfunktioner*** (Stopp-manövrar) som består av flera enkla SIFs. Detta är framför allt aktuellt för olika typer av nödstopp och avbrott i eldningen.

Beskrivna Stoppfunktioner eller manövrar överensstämmer i huvudsak med och är hämtade från rapport KIWA Fas 3. (Inom parentes har angetts några benämningar som är vanligt förekommande vid våra bruk). Stoppfunktionernas säkerhetsfunktioner (SIFs)framgår av följande beskrivningar i avsnitt 4.2.

4.1..1 Nödnedeldning

Aktivering av pannans nödnedeldningssystem ska försätta pannan i säkert läge, samt säkerställa att pannan görs klar för snabbtömning. Nödnedeldning indelas i två steg, beskrivna i rekommendation B8.

4.1..1.1 Nödstopp

4.1..1.2 Förberedelse för snabbtömning

4.1..2 **Stopp Förbränning (”panntripp”)**
Stopp förbränning innebär att all förbränning av alla bränslen avbryts automatiskt, genom att tillförsel av bränslen och förbränningsluft avbryts.

4.1..3 **Stopp allt bränsle (”bränsletripp”)**
Eldning avbryts genom att all bränsletillförsel avbryts. Rundcirkulation av bränsle möjlig.

4.1..4 Stopp all destruktionseldning
Förbränning av stark-och svaggaser, metanol och terpentin avbryts

4.1..5 **Stopp Lut Bränsle**
Funktionen innebär snabbstängning av brännlut till eldstaden

4.1..6 Stopp Förbränningsluft

Tillförsel av all förbränningsluft avbryts

4.1..7 Stopp Lut Bränsle

Stopp lutbränsle innebär att förbränning av brännlut och destruktionseldning avbryts. Däremot kan, beroende på orsak till avbrottet, oljeeldning kunna fortgå. Ett sådant exempel är otillåtet låg luttorrhalt på brännlut som avbryter brännlutstillförsel och därmed destruktionseldning, men där oljeeldning fortfarande skulle kunna ske.
”Stopp Lut Bränsle” med rundcirkulation innebär Stängning av dubbla avstängningsventiler mellan ringledning och varje lutspruta.

4.1..8 Stopp lutcirkulation

I de fall inte rundcirkulation av brännlut tillåts kompletteras ”Stopp Lut Bränsle” med ”Stopp Lutcirkulation”, som innebär Stopp brännlutpump och stängning av avstängningsventil på brännlutledningens stam.

Man kan om det föredras alltid tillämpa ”Stopp Lut Bränsle” tillsammans med ”Stopp lutcirkulation” och välja att återstarta brännlutpump och rundcirkulation om startvillkoren för detta är uppfyllda.

4.1..9 Stopp Startolja Bränsle

Stopp med dubbla avstängningsventiler på varje startoljebrännare

4.1..10 Stopp Starkgasbrännare Bränsle

- Stopp dubbla avstängningsventiler Starkgas
- Stopp dubbla avstängningsventiler Metanol
- Stopp dubbla avstängningsventiler pilotbrännare

4.1..11 Stopp matarvatten

Innebär stopp av matarvattentillförsel till pannan.

4.1..12 Stopp utgående ånga

Stänger pannas utgående ångventil

4.2 Säkerhetsfunktioner med SIL-krav

För ett antal av de sammansatta säkerhetsfunktionerna (stopp manövrar) som definierats ges även förslag till förenklade SRS (Säkerhetskravspecifikation) för säkerhetskretsar, gjord enligt en enkel mall ”Sammanställning av SRS för SIF”.
I dessa SRS framgår dels orsak till anrop av viss SIF, dels vilken funktion/avsäkring som ska vidtas.
Erforderliga SIL-nivåer ska beräknas. För vissa SIF har viss SIL-nivå rekommenderats. För vissa säkerhetsfunktioner krävs en hög minsta nivå, för att säkerställa att även sammansatta SIF ska kunna uppnå tillräcklig SIL-nivå. I en fullständig SRS skall även anges vilka anläggningsspecifika instrument- och elkretsar som ska verkställa stopp.
Hänvisningar i det följande sker främst till SS-EN 12952-7,- 8, samt förkortat till Sodahuskommitténs rekommendationer med beteckning, exempelvis B1, B8, etc.

4.2..1 Nödnedeldning (SS-EN 12952-7, Annex A 3.1

Beträffande Nödnedeldning, se rekommendation B 8.

Aktivering av pannans nödnedeldningssystem ska försätta pannan i säkert läge, samt säkerställa att pannan görs klar för snabbtömning. Nödnedeldning skall aktivera

- Stopp förbränning

- Sopp allt bränsle
- Stopp förbränningsluft nedre del ugn
- Sopp matarvatten
- Stopp ångsotning
  Förberedelse för snabbtömning

För att möjliggöra SIL-verifiering av denna funktion har **Nödnedeldning**, se Slutrapport Kiwa, uppdelats i delmoment**, Nödstopp** och **Förberedelse för snabbtömning**

SIF Beteckning	**Nödnedeldning**
SIF Nr	1.
Hänvisning	SS-EN 12952-7, Appendix A, B8
Funktion/Vad avsäkras	➢ Nödstopp av pannan ➢ Förberedelse för snabbtömning
Orsak till anrop	○ Nödstopp (Aktivering av nödnedeldningsknappen) ○ Domnivån under lägsta tillåtna nivå ○ Eldstadstrycket över det fastställda högsta värdet
Andra oberoende skyddsbarriärer	Utrymning av pannhus. Manuella avstängningsventiler utanför sodahus Manuell kontroll och manövrering av funktioner
Säkert läge	Samtliga delfunktioner i säkert läge. Sodahuslarm aktiverat, ventiler och elkraft stängd
SIL för SIF	Rekommenderas SIL ≥2
Kommentar	Nödnedeldning skall nödstoppa pannan genom avbrott i förbränning samt ombesörja att pannan görs klar för snabbtömning. Reglerventiler får ej nyttjas för avstängning. Nödnedeldningens förlopp skall övervakas från särskild nödnedeldningspanel. I de fall automatisk avstängning fallerar skall samtliga funktioner kunna utföras manuellt utanför sodahuset antingen med snabbstängningsventiler eller särskilda avstängningsventiler. Dessa nödfunktioner innebär en skyddsbarriär vid bestämning av SIL-nivå

4.2..2 **Nödstopp** (SS-EN 12952-7,-8)

Nödstopp skall finnas för:

- Snabbstängning av pannan genom aktivering av nödnedeldningssystem, (12952-7, Annex A 3)
- Snabbstängning av tillförsel av brännlut, 12952-8, Annex A 2

- Snabbstängning av luktgaser inkl. metanol, terpentin, se 12952-8, Annex A 3.3.4

Utgör delmoment i Nödnedeldning och innebär att pannan nödstoppas. Med dessa åtgärder avbryts all eldning och det formella kravet på Nödstopp anses uppfyllt.

SIF Beteckning	**Nödstopp**
SIF Nr	2.
Hänvisning	SS-EN 12952-7, Appendix A, B8
Funktion/Vad avsäkras	➢ Aktivering sodahuslarm ➢ Stopp förbränning o Stopp allt bränsle o Stopp lutcirkulation o Stopp oljecirkulation o Stopp förbränningsluft ➢ Stopp matarvatten ➢ Stopp sotånga
Orsak till anrop	o Nödstopp (Aktivering av nödnedeldningsknappen) o Domnivån under den lägsta tillåtna nivån (rekommendation B 6) o Eldstadstrycket över det fastställda högsta värdet
Andra oberoende skyddsbarriärer	Utrymning av pannhus. Manuella avstängningsventiler utanför sodahus Manuell kontroll och manövrering av funktioner
Säkert läge	Samtliga delfunktioner i säkert läge. Sodahuslarm aktiverat, ventiler och elkraft stängd
SIL för SIF	Rekommenderad SIL ≥2
Kommentar	Nödstopp skall avbryta all förbränning och försätta pannan i säkert läge

4.2..3 Förberedelse för snabbtömning

Delmoment 2 i nödnedeldning. Dessa åtgärder är vid SIL-verifiering att anse som processrelaterade manövrar som syftar till förberedelse för snabbtömning av pannan. Genom att programmera dessa manövrar i säkerhetssystemet, SIS, erhålls rimlig säkerhetsnivå.

SIF Beteckning	**Förberedelse för snabbtömning**
SIF Nr	3.
Hänvisning	SS-EN 12952-7, Appendix A, B8
Funktion/Vad avsäkras	➢ Elfiltren görs spänningslösa ➢ Elfiltrens mekaniska drifter stoppas ➢ Asktransportör till sulfatblandartank stoppas ➢ Täckningskemikalier till sulfatblandartank stoppas o Ventil stängs o Pump stoppas ➢ Sodapannans huvudångventil stängs ➢ Ventiler för utblåsning eller dränering av pannan stängs (kontinuerlig och diskontinuerlig utblåsning, bottenblåsning). ➢ Sotningssystemets huvudångledning stängs ➢ Stängning av vatten till ångkylare av insprutningstyp
Orsak till anrop	o Aktivering av nödnedeldning
Andra oberoende skyddsbarriärer	Utrymning av pannhus. Manuella avstängningsventiler utanför sodahus Manuell kontroll och manövrering av funktioner
Säkert läge	Samtliga delfunktioner i säkert läge. Sodahuslarm aktiverat, ventiler och elkraft stängd
SIL för SIF	Rekommenderad SIL≥2
	Aktivering av Nödnedeldning ska jämte ”Nödstopp” aktivera manöver ”Förberedelse för snabbtömning”

Stopp Förbränning
Stopp förbränning innebär att all förbränning av alla bränslen avbryts automatiskt, genom att tillförsel av bränslen och rundcirkulation av bränslen, samt förbränningsluft avbryts.
Vädring ska ske med tertiär- och kvartärluft. Eftersom explosiva gaser avgår från bädden skall spänning till elektrofiltren halveras, (SS-EN 12759), alternativt brytas för undvikande av gasexplosion eller brand i elektrofiltren.

SIF Beteckning	**Stopp förbränning**
SIF Nr	4.
Hänvisning	SS-EN 12952-7, Appendix A, C1, B1
Funktion/Vad avsäkras	➢ Stopp förbränning ○ Stopp allt bränsle ▪ Snabbstängning brännlut ▪ Stopp oljeeldning ○ Stopp rundcirkulation brännlut ○ Stopp rundcirkulation olja ○ Stopp destruktionseldning ○ Stopp förbränningsluft ○ Vädring med kvartär o tertiärluft ○ Halvering eller brytning av elfilterspänning (Rek. C1)
Orsak till anrop	Förbränning ska avbrytas automatiskt vid ○ Nödstopp (Aktivering av nödnedeldningsknappen) ○ Kraftavbrott ○ Stopp samtliga rökgasfläktar ○ Rökgasväg blockerad av spjäll ○ Bortfall av lufttillförsel under lutsprutenivå ○ Elavbrott på säkerhetssystemet ○ Snabbstängningsventiler manövrerade ○ Störningar i lösaren som kräver att smältaflödet avbryts (stopp omrörare, hög densitet, låg nivå i lösartank)
Andra oberoende skyddsbarriärer	Manuella avstängningsventiler utanför sodahus Manuell kontroll och manövrering av funktioner
Säkert läge	Samtliga delfunktioner i säkert läge.
SIL för SIF	Rekommenderad SIL ≥2
Kommentar	

4.2..4 Stopp allt bränsle

Stopp allt bränsle innebär att eldning avbryts genom att bränsletillförsel avbryts.
Rundcirkulation av bränsle i ringledningar kan pågå. Luftfläktar i drift för vädring av

eldstaden. Kan anropas när *inte* vatteninträngning eller läckage i brännlutledningar eller brand/explosion befaras. **(**Exempelvis kan denna stoppmanöver tillämpas vid låg luttorrhalt)

SIF Beteckning	**Stopp allt bränsle**
SIF Nr	5.
Hänvisning	SS-EN 12952-7, Appendix A, B1
Funktion/Vad avsäkras	○ Stopp allt bränsle ▪ Snabbstängning brännlut ▪ Stopp oljeeldning ○ Stopp destruktionseldning
Orsak till anrop	Bränsletillförsel ska avbrytas automatiskt vid ○ Nödstopp (Aktivering av nödnedeldningsknappen) ○ Elavbrott på säkerhetssystemet ○ Låg luttorrhalt ○ Bortfall primärluft ○ Bortfall sekundärluft ○ Villkor för ”Stabil luteldning” ej uppfyllt och eldning utan olja 5 min
Andra oberoende skyddsbarriärer	Manuella avstängningsventiler utanför sodahus Manuell kontroll och manövrering av funktioner
Säkert läge	Samtliga delfunktioner i säkert läge.
SIL för SIF	Rekommenderad SIL ≥2
Kommentar	Nödstopp skall avbryta all förbränning och försätta pannan i säkert läge

4.2..5 Stopp brännlut

Funktionen innebär Snabbstängning/nödstopp för brännlut och ingår i ”Stopp förbränning” och ”Stopp allt bränsle”.
Vid lutsprutorna ska finnas ventiler för avstängning av lutflödet manuellt från manöverrum och/eller från sodapannans säkerhetssystem. (Annex A 2.4).
Sodahuskommittén rekommenderar dubba automatiska avstängningsventiler mellan lutledning och varje lutspruta. Finns inte dubbla ventiler måste ”Stopp brännlut” kompletteras med ”Stopp lutcirkulation”.

SIF Beteckning	**Stopp Lut Bränsle (**med rundcirkulation av brännlut**)**
SIF Nr	6.
Hänvisning	SS-EN 12952-7, SS-EN 12952-8, B 1
Funktion/Vad avsäkras	Automatisk avstängning av brännlut innebär o *Vid såväl öppet som trycksatt system (Figur 5 resp. Figur 6)* o De dubbla avstängningsventilerna i avgreningar från stamledning till lutsprutorna stängs, (pos.2). o Om rundcirkulation av säkerhetsskäl måste avbrytas, stoppas insprutningspump och stängs ventil på stamledningen (pos.3). Dräneringen av brännluten skall ske till en trycklös cistern, som är placerad på en lägre nivå än lutsprutorna. o *Vid öppet system (B1,**Fel! Hittar inte referenskälla.**)dessutom* o ventilerna i ledningarna till lutsprutorna stängas, (pos.2). o ventil i ledningen till dumptanken öppnas (pos. 4), alternativt öppnar reglerventil (pos.9) i returledningen, samt ventil i returledningen till sulfatblandartanken (pos.5). o pumpar och avstängningsventiler för tillsatskemikalier till sulfatblandartank stängs o askredler till sulfatblandartank stannas o (stopp förbränningsluft tillkommer i bränsletripp och eldningsavbrott)

	○ *I trycksatt system (**Fel! Hittar inte referenskälla.**) dessutom* ○ ventilerna i ledningarna till lutsprutorna stängas, (pos.2). ○ ventilen i ledningen till dumptanken ska öppna (pos.4), ○ samt ska ventilerna i returledningen till den trycksatta cisternen stänga (pos.5) ○ samtidigt som mellanliggande avluftning skall öppna (pos.8).
Orsak till anrop	Stopp Lut Bränsle aktiveras vid ○ Låg luttorrhalt ○ Bortfall av primärluft ○ Nödstopp
Andra oberoende skyddsbarriärer	Manuella avstängningsventiler
Säkert läge	Gränslägen för ventiler, spjäll och motorström
SIL för SIF	Rekommenderad SIL ≥2
Kommentar	Funktionen ingår i Stopp förbränning

4.2..6 Stopp lutcirkulation

Kombineras med stopp brännlut när läckage i brännlutledningar eller brand/explosion, vatteninträngning befaras, samt i anläggningar där dubbla automatiska avstängningsventiler saknas mellan ringledning och lutspruta.

SIF Beteckning	**Stopp lutcirkulation**
SIF Nr	7.
Hänvisning	SS-EN 12952-8, A 2.4, B 1
Funktion/Vad avsäkras	Rundcirkulation av brännlut avbryts
Orsak till anrop	○ Nödnedeldning ○ Nödstopp
Andra oberoende skyddsbarriärer	Handventiler
Säkert läge	○ Stopp brännlutpump ○ Stäng avstängningsventil brännluten stam ○ Öppna avluftning och dränering av returledning för brännlut. ○ Säkert läge indikeras med Ventilgränslägen, motorström
SIL för SIF	Rekommendation SIL≥2
Kommentar	○ Funktionen ingår i Stopp förbränning

4.2..7 Stopp Startolja Bränsle

SIF Beteckning	**Stopp Startolja**
SIF Nr	8.
Hänvisning	SS-EN 12952-8, B13
Funktion/Vad avsäkras	Tillförsel av olja till eldstad ○ Stopp dubbla avstängningsventiler på varje startoljebrännare
Orsak till anrop	○ Nödstopp ○ Flamvaktsbortfall
Andra oberoende skyddsbarriärer	
Säkert läge	○ Stopp dubbla avstängningsventiler på varje startoljebrännare
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	

4.2..8 Stopp Starkgasbrännare Bränsle

- ○ Stopp dubbla avstängningsventiler Starkgas
- ○ Stopp dubbla avstängningsventiler Metanol, Terpentin

SIF Beteckning	**Stopp Starkgasbrännare**
SIF Nr	9.
Hänvisning	SS-EN 12952-7, C1
Funktion/Vad avsäkras	○ Stopp destruktionseldning
Orsak till anrop	○ Nödstopp ○ Ej Stabil luteldning
Andra oberoende skyddsbarriärer	Manuella ventiler utanför pannhus
Säkert läge	○ Stopp dubbla avstängningsventiler på ledningar
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	

4.2..9 Stopp förbränningsluft

SIF Beteckning	**Stopp förbränningsluft**
SIF Nr	10.
Hänvisning	SS-EN 12952-7, B1
Funktion/Vad avsäkras	○ Lufttillförsel till eldstad avbryts
Orsak till anrop	○ Nödstopp (aktiverad nödnedeldningsknapp) ○ Stopp förbränning
Andra oberoende skyddsbarriärer	
Säkert läge	○ Stopp primärluftfläkt ○ Stopp sekundärluftfläkt ○ Stäng luftspjäll primärluft ○ Stäng luftspjäll sekundärluft ○ Stopp luftfläkt starkgas
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	

4.2..10 Stopp matarvatten

SIF Beteckning	**Stopp matarvatten**
SIF Nr	11.
Hänvisning	SS-EN 12952-7
Funktion/Vad avsäkras	○ Matarvatten till pannan
Orsak till anrop	○ Nödnedeldning ○ Nödstopp ○ Domnivå HWL över högsta tillåtna
Andra oberoende skyddsbarriärer	
Säkert läge	○ Stopp matarvattenpump ○ Stopp reservmatarvattenpump ○ Stängd stamventil mava
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	

4.2..11 **Stopp utgående ånga**

Avstängning huvudångledning.

Huvudångledning ska vara försedd med motoriserad avstängningsventil med manöver från manöverrum. Beträffande reservkraft se rekommendation B12.

SIF Beteckning	**Avstängning ångledning**
SIF Nr	12.
Hänvisning	SS-EN 12952-7, B8
Funktion/Vad avsäkras	○ Stängning av utgående ångventil
Orsak till anrop	○ Förberedelse för snabbtömning

Andra oberoende skyddsbarriärer	
Säkert läge	○ Stängd ventil, gränsläge
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	Ingår i nödstopp

4.2..12 Låg Domnivå

Vid lägsta tillåtna domnivå (LWL), skall eldning avbrytas, se även rekommendation B6 Sodahuskommittén rekommenderar dessutom nödnedeldning, se rekommendation B 8, eftersom nivå under lägsta tillåtna kan indikera vattenläckage.

SIF Beteckning	**Låg domnivå**
SIF Nr	13.
Hänvisning	SS-EN 12952-7, B6, B8
Funktion/Vad avsäkras	○ Vattennivå i pannan
Orsak till anrop	○ Låg-låg nivåvakt
Andra oberoende skyddsbarriärer	
Säkert läge	○ Nödnedeldning, ○ Eldningsavbrott,
SIL för SIF	Rekommenderad SIL 3
Kommentar	Kan indikera vattenläckage

4.2..13 Hög nivå i ångdom

När högsta tillåtna domnivå (HWL) överskrids
rekommenderar Sodahuskommittén efter riskanalys, att eldning avbrytas med Stopp förbränning, se även B6.

SIF Beteckning	**Hög nivå i ångdom**
SIF Nr	14.
Hänvisning	B6
Funktion/Vad avsäkras	○ Vattennivå i pannan
Orsak till anrop	○ Vakt för högsta tillåtna vattennivå (LWL)
Andra oberoende skyddsbarriärer	
Säkert läge	○ Stopp förbränning
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	Hög nivå kan orsaka vattenslag, sprängning av överhettare, vatteninsprutning via sotapparater samt turbinhaveri

4.2..14 Sotångledningar

Sotångledningar ska vara försedda med säker dränering för avledning av kondensat. Sodahuskommittén rekommenderar temperaturövervakning av dräneringen med automatisk förbigångsventil vid låg temperatur. Om ej temperatur återgår till normalt värde inom förutbestämd tid, skall huvudångventil till sotånga samt eventuellt vatten för ångkylning stängas med automatik.

SIF Beteckning	**Dränering sotångledning**

SIF Nr	15.
Hänvisning	SS-EN 12952-7 Annex 2.11, B9
Funktion/Vad avsäkras	○ Kondensat i ångledning
Orsak till anrop	○ temperaturvakt
Andra oberoende skyddsbarriärer	
Säkert läge	○ temp över fastställt värde ○ automatisk ventilöppning vid låg temp ○ stängd ventil sotånga efter tidsfördröjning
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	

4.2..15 Snabbtömning

Sodapannan skall vara försedd med snabbtömningssystem.

- Motorventiler för dränering skall vara motorstyrda. (Annex A 3.2)
- Snabbtömningsventiler ska kunna provas på ett säkert sätt under drift (Annex A 3.5)
- Övrigt se rekommendation B8

SIF Beteckning	**Snabbtömning**
SIF Nr	16.
Hänvisning	SS-EN 12952-7, Appendix A 3.2 och 3.5, B8
Funktion/Vad avsäkras	Snabbtömning av pannan Startvillkor ○ Manöverställare ”Larm” i läge Larm ○ Manöverställare ”Nödnedeldning” i läge Nödnedeldning ○ Eldningsavbrott enligt SIF 3 ○ Ventil 2, snabbtömningsventil manövreras enligt rekommendation B 8 ○ Ventil 3, snabbtömningsventil manövreras enligt rekommendation B 8
Orsak till anrop	Aktivering av snabbtömning från särskild tablå
Andra oberoende skyddsbarriärer	Sodahuslarm och utrymt pannhus
Säkert läge	○ Pannan tömd ○ Väntetid innan tillträde
SIL för SIF	SIL-bestämning
Kommentar	Tidigare rekommendation om förbikoppling av startvillkor med nyckel utgår. (Förreglade startvillkor skulle med särskild nyckel i snabbtömningspanelen, kunna förbikopplas av ansvarig sodahusoperatör, i huvudsak när det är uppenbart att startvillkoren faktiskt är uppfyllda men snabbtömningen inte kan ske pga signalfel el. dyl.)

4.2..16 Reservkraft (SS-EN 12952-7)

Nödnedeldnings- och snabbtömningssystem samt sodapannans säkerhetssystem ska vara anslutna till reservkraft.
Beträffande spänningsförsörjning till säkerhetskretsarnas komponenter se krav i denna rekommendation, B 18, avsnitt 3.5.7, samt rekommendation B 12.

SIF Beteckning	**Reservkraft**
SIF Nr	17.
Hänvisning	SS-EN 12952-7 Annex 3.7, B12
Funktion/Vad avsäkras	Strömförsörjning Säkerhetssystem ○ separat och avbrottsfri spänningsmatning för bibehållen funktion under minst 60 minuter. ○ systemminnet beständigt, alternativt skall systemet vara försett med egen batterireserv för 7 dygns bevarande av minnet Huvudförsörjningen för säkerhetsrelaterade ställdon och motorventiler, fältutrustning, givare mm ○ anordnade med avbrottsfri reservkraft (t.ex. diesel och UPS). UPS-säkert nätverk måste vara utformat på ett sådant sätt att det kan hålla systemet igång i 60 minuter.”
Orsak till anrop	○ Spänningsbortfall till säkerhetssystem ○ Spänningsbortfall för fältutrustning
Andra oberoende skyddsbarriärer	

4.2..17 Vädring eldstad och rökgasvägar

- Före start av eldning ska rökgasvägar vara effektivt vädrade, se 6.5ff i standarden
- Före start av eldning ska elektrofiltrens spänning minskas under 50% av normal spänning
- Efter eldningsavbrott skall vädring ske före återstart
- Efter vädring skall tändning påbörjas inom 10 min. Om luftmängd om minst 20% av total förbränningsluftmängd uppehålls kan tändningstid utsträckas till 30 min, se 6.5.7.

SIF Beteckning	**Vädring eldstad**
SIF Nr	18.
Hänvisning	SS-EN 12952- 8, B13
Funktion/Vad avsäkras	Risk för explosion av oförbrända gaser
Orsak till anrop	○ Startvillkor för oljeeldning ○ Startvillkor för återstart eldning
Andra oberoende skyddsbarriärer	
Säkert läge	○ Fastställda luftmängder, flödesmätning ○ Fastställd vädringstid, timer ○ Lastreducering elfilter, spänningsmätning ○ Tändning inom fastställd tid efter vädring, ○ Timer ○ Luftflödesmätning ○ Signal vädringsbehov avlägsnad
SIL för SIF	⇨ 2
Kommentar	

4.3 Övriga säkerhetsfunktioner

Ett flertal säkerhetsfunktioner SIF, förekommer i Standarden där ovanstående Stopp-manövrar anropas. För vissa övervakningsfunktioner kan man efter godkännande av kontrollorganet förlägga funktionen i DC systemet om man kan visa att det finns andra SIF som oberoende försätter pannan i säkert läge.

4.3..1 Fel på matarvattenpump

Larm ska ges vid fel på matarvattenpump (SS_EN 12952-7, p 5.1.2f)

SIF Beteckning	**Fel på matarvattenpump**
SIF Nr	19.
Hänvisning	SS-EN 12952-7
Funktion/Vad avsäkras	○ Matarvattentillförsel
Orsak till anrop	○ Matarvattentryck ○ Varvtal matarvattenpump ○ Matarvattenflöde 2oo3
Andra oberoende skyddsbarriärer	○ Reservmatarvattenpump
Säkert läge	Panna med 1 matarvattenpump Kraftavbrott till mavapump ska dels ○ avbryta eldning, Panntripp ○ dels ge larm (5.1.1.1, 5.1.2.2f) Panna med minst 2 oberoende kraftmatade matarvattenpumpar ○ Automatisk lastminskning så att villkor 4.2.3 uppfylls (max 400°C innan pannvattnet sjunkit till 50mm över värmeytans högsta punkt) ○ I annat fall Panntripp (5.1.1.2) ○ Larm
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	

4.3..2 Hög ångtemperatur

Larm ska avges om utgående ångtemperatur överstiger tillåtet designvärde (SS-EN 12952-7, p 5.7.3).
Sodakommittén rekommenderar efter riskanalys, automatisk lastminskning, eller efter förvald tidsfördröjning att eldningen skall avbrytas.

SIF Beteckning	**Hög ångtemperatur**
SIF Nr	20.
Hänvisning	SS-EN 12952-7, Rek B1
Funktion/Vad avsäkras	○ Materialskador på överhettare

Orsak till anrop	○ Temperaturvakt
Andra oberoende skyddsbarriärer	
Säkert läge	○ Larm ska avges om utgående ångtemperatur överstiger tillåtet designvärde (p 5.7.3 i standarden) ○ Automatisk lastminskning ○ Panntripp se SIF 1, efter tidsfördröjning
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	Hög temp kan orsaka överhettarskador

4.3..3 Luftfläktar och luft/bränsleförhållande (SS-EN 12952-8, Annex A 2.3)

Övervakning skall ske av

- förbränningsluftsfläktar enligt moment 5.1
- samt av luft/bränsleförhållande enligt 5.2

SIF Beteckning	**Stopp förbränningsluft**
SIF Nr	21.
Hänvisning	SS-EN 12952-8, Annex A2.3
Funktion/Vad avsäkras	○ Luftöverskott
Orsak till anrop	○ Nödstopp (aktiverad nödnedeldningsknapp) ○ Stopp allt bränsle (Bränsletripp)
Andra oberoende skyddsbarriärer	
Säkert läge	○ Bränsletripp
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	

4.3..4 Avbrott primärluft

Vid bortfall av primärluft (under tillåten gräns) skall eldning avbrytas genom automatiskt snabbstopp av bränsletillförsel.

SIF Beteckning	**Avbrott primärluft**
SIF Nr	22.
Hänvisning	SS-EN 12952-8 Annex A 2.3
Funktion/Vad avsäkras	○ Bortfall av Förbränningsluft
Orsak till anrop	○ Fläktmotor (kontaktor) ○ Lägesgivare luftspjäll ○ Flödesmätning primärluft 2oo3
Andra oberoende skyddsbarriärer	
Säkert läge	○ Stopp allt bränsle
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	

4.3..5 Avbrott sekundärluft

Vid bortfall av sekundärluft (under tillåten gräns) skall eldning avbrytas genom automatiskt snabbstopp av bränsletillförsel.

SIF Beteckning	**Avbrott sekundärluft**
SIF Nr	23.
Hänvisning	SS-EN 12952-8 Annex A 2.3 och 2.7
Funktion/Vad avsäkras	○ Förbränningsluft
Orsak till anrop	○ Stopp primärluftfläkt ○ Stängt luftspjäll ○ Flödesmätning Utvärdering 2oo3
Andra oberoende skyddsbarriärer	
Säkert läge	○ Stopp allt bränsle
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	Anropas även som start och driftvillkor för olje-och luteldning

4.3..6 Luft/bränslekvot

Om luft/bränslekvot understiger tillåtet värde skall eldning stoppas genom att bränsletillförsel avbrytas, se p 5.2 i standarden

SIF Beteckning	**Luft bränslekvot**
SIF Nr	24.
Hänvisning	SS-EN 12952-8 p 5.2
Funktion/Vad avsäkras	○ Skydd mot explosion av oförbrända gaser
Orsak till anrop	Kvot flöde luft/Bränsle under fastställd gräns
Andra oberoende skyddsbarriärer	
Säkert läge	○ Stopp allt bränsle (Bränsletripp)
SIL för SIF	
Kommentar	

Rökgasfläktar, drag, öppen rökgasväg

Rökgasfläktar och drag i eldstad ska övervakas enligt p 5.2, p 5.3 (Annex A 2.3)

SIF Beteckning	**Öppen rökgasväg**
SIF Nr	25.
Hänvisning	SS-EN 12952-8, p 5.2 ,5.3 och Annex 2.3
Funktion/Vad avsäkras	○ Öppen rökgasväg
Orsak till anrop	○ Spjäll gränsläge ○ Fläktmotor, motorström
Andra oberoende skyddsbarriärer	
Säkert läge	○ Rökgasspjäll, gränsläge öppna

	○ Rökgasfläkt i drift, varvtal ○ Eldstadstryck inom fastställda värden
SIL för SIF	
Kommentar	Anropas som start och driftvillkor för olje-och luteldning

4.3..7 Rökgasflöde

Vid stängt rökgasutlopp skall eldning avbrytas med automatiskt, Stopp Förbränning.

SIF Beteckning	**Rökgasflöde**
SIF Nr	26.
Hänvisning	SS-EN 12952-8, A 2.3
Funktion/Vad avsäkras	○ Öppen rökgasväg
Orsak till anrop	○ Start och driftvillkor för olje- och luteldning ○ Gränslägen spjäll ○ Högt tryck eldstad
Andra oberoende skyddsbarriärer	
Säkert läge	○ Stopp Förbränning ○ Rökgasspjäll öppna ○ Rökgasfläkt i drift ○ Eldstadstryck inom fastställda värden Utvärdering 2oo3
SIL för SIF	⇨ SIL ≥ 2 rekommenderas
Kommentar	Anropas som start och driftvillkor för olje-och luteldning

4.3..8 Avbrott rökgasfläkt

Vid stopp på rökgasfläkt skall eldning avbrytas med automatisk, Stopp Förbränning (Annex A 2.3)

SIF Beteckning	**Avbrott rökgasfläkt**
SIF Nr	27.
Hänvisning	SS-EN 12952-8 Annex 2.3
Funktion/Vad avsäkras	○ Rökgasflöde
Orsak till anrop	○ Fläktmotor, motorström ○ Fläktvarvtal Utvärdering 1oo2
Andra oberoende skyddsbarriärer	
Säkert läge	○ Erforderligt drag i eldstad ○ Rökgasspjäll öppna ○ Rökgasfläkt i drift
SIL för SIF	⇨ SIL ≥ 2 rekommenderas

Kommentar	Anropas som start och driftvillkor för olje-och luteldning

4.3..9 Eldstadstryck

Vid otillåtet högt eldstadstryck skall eldning avbrytas genom, automatiskt snabbstopp av bränsletillförsel. (Annex A 2.3, A 2,7).

SIF Beteckning	**Högt tryck i eldstad**
SIF Nr	28.
Hänvisning	SS-EN 12952-8 Annex 2.3 och 2.7
Funktion/Vad avsäkras	Eldstadstryck
Orsak till anrop	○ Dragmätning, 3 givare Utvärdering 2oo3
Andra oberoende skyddsbarriärer	
Säkert läge	○ Nödnedeldning
SIL för SIF	⇨ ≥ 2 rekommenderas
Kommentar	Kan vara tecken på vatteninträngning i ugnen

4.4 Start och driftförreglingar

Förutom standardhänvisningar se rekommendation B1.

Start och driftförregling för olja (SS-EN 12952-8)

Återstartsfördröjning för oljebrännare 30 s även vid stabil luteldning, definition se C1.

Övriga villkor enligt SS-EN 12952-8, avsnitt 3-8, samt Annex A 3.2. Se även rekommendation B 13

.

Startvillkor för luteldning (SS-EN 12952-8)

Innan luteldning påbörjas skall startvillkor för luteldning enligt Annex A 2.5 och A 2.7 vara uppfyllda.

Driftvillkor för luteldning (SS-EN 12952-8)

Eldning ska avbrytas genom automatiskt snabbstopp av bränsletillförsel om driftvillkor ej är uppfyllda enligt Annex A 2.7

Start och driftförregling för luktgaser (metanol och terpentin)

Tillförsel av luktgaser eller gasblandningar får inte ske om pannans last understiger 50% (Annex A 3.3.1). Rekommenderad tillämpning se rekommendation B16.

Start-och driftförregling för utspädda icke kondenserbara gaser (DNCG), (SS-EN 12952-8)

Villkor för eldning av DNCG ej uppfyllt

- matarventilerna för DNCG stängs av
- DNCG ledes till en skorsten eller till en extra förbränningsstation

Start-och driftförregling för koncentrerade icke kondenserbara gaser (CNCG), (SS-EN 12952-8)

Villkor för eldning av CNCG ej uppfyllt

- matarventilerna för CNCG stängs av
- CNCG leder till en skorsten eller till en extra förbränningsstation
- matarventilerna för hjälpbränslet på CNCG stängs av

4.5 Ytterligare säkerhetsfunktioner från utökad riskanalys

Nedan följer förteckning över övriga instrumenterade säkerhetsfunktioner som efter riskanalys och beprövad erfarenhet rekommenderas av Sodahuskommittén utan att det direkt föreskrivs i standard.

Sotning Stopp / Utdraget läge

Ej säkerhetskritiskt, men vid nödnedeldning eller panntripp bör utdrag av sotlansar ske för att undvika skador på lansar.

Lösartank

Start och driftvillkor för sodapannan enligt rekommendation B 4

- Vid stopp på all omrörning avbryts tillförsel av brännlut omedelbart.
- Vid stopp på 1 omrörare av 2 (eller fler) avbryts tillförsel av brännlut efter kort tidsfördröjning för försök till återstart (förutbestämd tid i riskanalysen).
  - Om lösartankens normala uppehållstid väsentligt understiger 1 timme enligt avsnitt 1.2 bör dock luteldning avbrytas omedelbart.
- Vid bortfall av svaglutflöde till lösaren skall reservspädning med varmvatten >40C aktiveras automatiskt. (Kallvatten ökar risken för kristallisation). Dessutom skall finnas möjlighet till manuell inkoppling av brandvatten om vattentillförsel skulle fallera.
- Otillåtet hög densitet i lösaren avbryter tillförsel av brännlut.
- Bottentömningsventil bör vara manuell. Stängd fjärrmanövrerad bottentömningsventil är start- samt driftvillkor för eldning.

- Om imångkanalen är ansluten till pannans luftsystem, skall tvättvatten till imångkanalen vara förreglat mot vattensensor och stängt spjäll mot pannan så att vatteninförsel till pannan förhindras.

Gas från lösartank

När villkor för eldning ej är uppfyllt skall

- Lösartankens gasspjäll mot pannan stängas
- Lösartankens gasspjäll till skorstenen öppnas, gränslägen med 2/3 val

Vattentvätt imkanal

Vid vattentvättning av imkanal krävs att

- kanalen före tvätt avblindas och låses mot pannan.
- Vidare rekommenderas att kanalen förses med larm för vatten i kanalen.
- Fast anslutning av tvättvatten bör undvikas och måste om det installeras förreglas mot kanalens avblindning, samt mot larm för vatten i kanalen.

Vattentvätt brännlut och tjocklutledningar

Anslutningar för tvättning av brännlutsystemet skall utformas och användas så att tvättvätskan aldrig kan komma in i eldstaden, se rekommendation B1.
Nedanstående funktioner bör säkerställas med signaler från gränslägen och förregling av vattenpådrag.

Före tvättning skall

- Lutsprutor demonteras
- Skyddsanordning (exempelvis giljotinspjäll) mot ofrivillig vatteninsprutning i eldstaden anbringas.
- Anslutning av tvättvätska till brännlutledning kan utföras med demonterbara mellanstycken. Larm skall ges när tvättvätskan är ansluten till brännlutledningen,

  (eller med svängbara rörböjar, enligt B1, Figur 9. Vid ett arrangemang med en sammanbyggd svängbar rördel, enligt Figur 9 behövs inte någon larmfunktion).
- Ventillägen, demontering av lutsprutor och applicering av giljotinspjäll för lutspruteöppningar kan även säkerställas med interlocksystem.

5 Sodapannors säkerhetssystem, äldre modell

Som nämnts inledningsvis omfattas inte befintliga säkerhetssystem, installerade före 2005, av SS-EN 61511 förrän deras säkerhetsfunktion, eller det de skyddar, förändras väsentligt.

Även för äldre säkerhetssystem gäller dock följande:

5.1 Säkerhetssystem, allmänna principer

- Säkerhetssystem skall agera självständigt från övriga till sodapannan hörande system såsom larm-, instrument- och styrsystem etc.

- Ett säkerhetssystem skall vara dedikerat för endast en panna.

- Den elektriska strömförsörjningen till säkerhetssystem skall härröra från två oberoende kraftkällor varav minst en skall vara UPS-matad för bibehållande av funktion under minst en timme vid avbrott i ordinarie kraftförsörjning.

- Val av i säkerhetssystem ingående komponenter samt kapsling och placering av dessa, skall göras med stor noggrannhet. Vid val av fältplacerade komponenter skall speciell hänsyn tas till besvärlig omgivningsatmosfär med risk för att komponenterna utsätts för skadlig påverkan, t.ex. fukt, damm, olja, lut och korrosiva gaser. Även temperaturförhållanden, brandrisk och vibrationer skall beaktas.

- Tiden från det att ett drifttillstånd faller (säkerhetssystemet aktiveras) till dess att reservsystem aktiveras skall vara maximalt 2 sekunder så att önskat händelseförlopp i fält initieras via reservsystemen inom 10 sekunder.

- Signalöverföring av förreglingssignaler mellan olika system skall vara redundant.

5.2 Programmerbara säkerhetssystem

Säkerhetsutrustning skall uppfylla kraven i AFS 2016:1, Tryckbärande anordningar.

- Den skall vara konstruerad och tillverkad så, att den är tillförlitlig och anpassad för sin avsedda användning och så, att behovet av underhåll och provning har beaktats.

- Den skall vara oberoende av andra funktioner utom då utrustningens säkerhetsfunktion inte kan påverkas av andra funktioner.

- Den skall följa lämpliga konstruktionsprinciper som säkerställer ett ändamålsenligt och tillförlitligt skydd. Dessa principer innefattar i synnerhet felsäkerhet, redundans, diversifiering och självövervakning.

Vid användning av ett programmerbart processorbaserat säkerhetssystem kan kraven ovan exemplifieras som beskrivet i avsnitt 5.3.

5.3 Användning av ett programmerbart, processorbaserat säkerhetssystem

Vid användning av ett programmerbart processorbaserat säkerhetssystem kan kraven i AFS 2005:2 exemplifieras som nedan beskrivet:

- Systemet skall självövervakas så att vid fel i systemet, den enhet i vilket felet uppstått går till ett säkert förutbestämt tillstånd (påverkan på utgångar från enheten elimineras) och operatören skall automatiskt göras uppmärksam på det inträffade.

- Varje eventuell programändring skall dokumenteras och signeras gällande anledning,

funktion och uttestning.

- Obehörig omprogrammering skall förhindras genom behörighetskontroll.

- Säkring av systemminne och reservkraft se rekommendation B12

- På ett tillförlitligt sätt skall för kritiska signaler säkerställas att återkoppling sker så att aktivering av begärt tillstånd verifieras. Vid avvikelse skall åtgärd i enlighet med moment 1 ovan automatiskt utlösas.

- Moderna styrsystemsarkitekturer tillåter att information skickas mellan säkerhetssystemen och övriga styrsystem. Vikt skall dock läggas vid att säkerställa att 5.1 punkt a) i rekommendationen uppfylls ”Säkerhetssystem skall agera självständigt från övriga till sodapannan hörande system såsom larm-, instrument och styrsystem etc.”

Underhållsrutiner för datorbaserade säkerhetssystem

För att nå en hög tillförlitlighet på anläggningen krävs fortlöpande inspektioner av de olika delar som ingår i ett säkerhetssystem. Dessa rutiner skall samordnas med övriga rutiner för Funktionskontroll av nödnedeldnings- och snabbtömningssystemen, vilka finns i Rekommendation B 8**.**

Tidsintervallen nedan bör ses som minimum och utförda kontroller skall journalföras.

- Utrymmet där datorn med utrustning är placerad bör kontrolleras minst två gånger per år med avseende på miljön. Minst en av kontrollerna bör inträffa under sommarmånad.

- Kontroll av spänningsmatning, redundans, larmnivåer, rippel, kylfläktar och eventuell batteri-backup av minne bör utföras två gånger per år.

- Det skall finnas backup och återställningsrutiner för systemkritiska delar. Rutinernas funktion skall verifieras vid revisionsstopp för att säkerställa att de är i funktion.

- Självdiagnostik i form av larm och händelselistor samt övriga automatiska systemövervakningsfunktioner skall kontinuerligt följas upp.

6 Bilagor

6.1 Bilaga 1, Förkortningar i SS-EN 61511-1

Förkortningar som används I SS-EN 61511-1, avsnitt 3.3 framgår av nedanstående tabell.

Abbreviation	Full expression
AC/DC	Alternating current/direct current
AIChE	American Institute of Chemical Engineers
ALARP	As low as reasonably practicable
ANSI	American National Standards Institute
AP	Application program
BPCS	Basic process control system
CCPS	Centre for Chemical Process Safety (AIChE)
DC	Diagnostic coverage
E/E/PE	Electrical/electronic/programmable electronic
EMC	Electro-magnetic compatibility
FAT	Factory acceptance test
FPL	Fixed program language
FSA	Functional safety assessment
FSMS	Functional safety management system
FTA	Fault tree analysis
FVL	Full variability language
HFT	Hardware fault tolerance
H&RA	Hazard & risk assessment
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization

LVL	Limited variability language
MooN	“M” out of “N” channel architecture
MPRT	Maximum permitted repair time
MRT	Mean repair time
MTTR	Mean time to restoration
NFPA	National Fire Protection Association(US)
NP	Non-programmable
OEM	Original Equipment Manufacturer
PE	Programmable electronics
PES	Programmable electronic system
PFD	Probability of dangerous failure on demand
PFDavg	Average probability of dangerous failure on demand
PFH	Probability (average frequency of dangerous failures) of failure per hour
pl	Plural
PLC	Programmable logic controller
SAT	Site acceptance test
SC	Systematic capability
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification

6.2 Bilaga 2, Ordlista

BMS (Burner Management System)
Säkerhetssystem (förreglingssystem) för brännare.

***Busskommunikation* (*Buss*)**
Datorbaserat kommunikationssystem för samtidig, kollektiv överföring av ett stort antal signaler mellan två datorbaserade system.

BPCS,"Basic Process Control System", normal processtyrning
Det system som hanterar normal processtyrning.

DCS (Distributed Control System)
Datorbaserat styrsystem, innehållande reglerfunktioner, operatörsgränssnitt, larmhanteringssystem och lagringssystem för driftdata med trendvisualisering m.m.

Hårdförtrådning
Teknik för signalöverföring där förreglande givares kontaktfunktion(er) via tråd är direkt kopplad(e) till spänningsmatningskretsen för den förreglade komponenten.

I/O
Signalöverföring till (*I* står för *Input* eller *Ingång*) respektive från (*O* står för *Output* eller *Utgång*) ett datorbaserat system. Överföringen sker via en för varje signal individuell *in*-eller *utgång*.

Processorbaserat säkerhetssystem
Datorbaserat säkerhetssystem i vilket en inprogrammerad logik via utgångar påverkar de förreglade komponenterna.

Redundans
Användandet av två likadana system för en och samma uppgift. Systemen fungerar inbördes oberoende av varandra. Deras status jämförs; detta för att säkerställa funktionen.

SIF, "Safety Instrumented Function", säkerhetskritisk instrumentfunktion
Instrumentfunktion (ofta förregling) som behövs för att skydda mot en specifik fara, och som tilldelats en SIL-nivå. Finns fler risker hanteras de av olika SIF.

SIS, "Safety Instrumented System", Säkerhetskritiskt instrumentsystem
En grupp av flera SIF. Det kan exempelvis avse alla SIF som skyddar ett processavsnitt, eller alla SIF som implementerats i en viss säkerhets-PLC. Det finns inga begränsningar i hur många SIF man kan ha under en SIS.

SIL, "Safety Integrity Level", integritetsnivå
Nivån av säkerhetsklass på säkerhetsfunktionen (SIF). Motsvarar den riskreduktion som funktionen erbjuder. SIL1 innebär att säkerhetsfunktionen minskar risken till en tiondel, SIL2 minskar risken till en hundradel.

SRS "Safety requirement specification" Säkerhetskravspecifikation
Specifikation av de säkerhetskrav som ett skyddssystem skall uppfylla.

UPS (Uninterruptible Power Supply)
System för att tillhandahålla avbrottsfri kraft under en begränsad tid. Vanligen batterimatad.