

- 1 Inledning
- 2 Konststart eller industriell process
 - 2.1 Skapa något nytt
 - 2.2 Form och funktion
 - 2.3 Skeden i en designprocess
 - 2.4 Designprinciper
 - 2.5 Utmaningar i ett designprojekt
 - 2.6 Olika typer av design projekt
 - 2.7 Ett nytt sätt att designa
- 3 Design av produkter
 - 3.1 Helhet och detaljer
 - 3.2 Att tänka i funktioner
 - 3.3 En målbild
 - 3.4 Dokumentering av designprocessen
 - 3.5 Att hantera osäkerhet
 - 3.6 Stöd för användarna
 - 3.7 Designkvalitet
 - 3.8 En V&V process
 - 3.9 Ett ledningssystem
 - 3.10 Olika produktområden
 - 3.11 Vanliga problem i en designprocess
- 4 Design av system
 - 4.1 Allmänna principer
 - 4.2 Interaktion mellan människa och system
 - 4.3 Ett livstidsperspektiv
 - 4.4 System av system
 - 4.5 Socio-tekniska system
 - 4.6 Automation
 - 4.7 Design för säkerhet
- 5 Design av organisationer
 - 5.1 Organisationen som en källa för effektivitet
 - 5.2 Skillnaden mellan design och drift
 - 5.3 Om institutioner
 - 5.4 Kärnkraften som exempel
 - 5.5 Problem som har förekommit
 - 5.6 Design av digitala säkerhetssystem
 - 5.7 Stora projekt
 - 5.8 Balanser
- 6 Design i samhället
 - 6.1 Säkerhetsförbättringar
 - 6.2 Artificiell intelligens
 - 6.3 Designerns ansvar
 - 6.4 Effektiv myndighetstillsyn
 - 6.5 En global värld
- 7 Sammanfattning och rekommendationer
 - 7.1 Hur området har utvecklats
 - 7.2 Utmaningar
 - 7.3 Design i en global värld

Appendix

Förkortningar

Erkännanden

Referenser

Design; innovation, processer och produkter

Björn Wahlström

Sammanfattning: Föreliggande rapport behandlar design och konstruktion inom kärnkraftsområdet. En enkel jämförelse med hur anläggningarna byggdes i Finland och Sverige under 1970- och 1980-talen visar på att det man visste och gjorde då, kanske inte mera gäller. Vad som inom designområdet har skett sedan dess är att man börjat tala om designvetenskap, som innefattar allt mellan konsthantverk och industriell produktutveckling. Jag försöker här spegla vad som skrivits inom området, för att se på vilket sätt detta möjligen kunde användas när man talar om design och konstruktion i kärnkraftssammanhang. Problemen jag har sett, är att man både vid moderniseringar av nuvarande anläggningar och byggandet av helt nya anläggningar, dras med betydande överskridningar både i tidtabeller och i kostnader. Som exempel kan man se moderniseringarna av kontrollsystemen både i Ringhals i Sverige och Lovisa i Finland inte gick enligt planerna. På samma sätt har två systemanläggningar i Finland och Frankrike har dragits med betydande förseningar och kostnadsökningar. Jag gör här ett försök att analysera situationen, för att kunna se hur man möjligen kunde stöda design- och konstruktionsprocesserna med avseende på teorier, metoder, modeller och verktyg för att kunna erhålla en mindre osäkerhet i sina projekt när det gäller tidtabeller och kostnader.

Nyckelord: System av system, kravhantering, prestationsutvärderingar, projektplanering, myndighetstillsyn

1 Inledning

Denna rapport är en av de fem delrapporter, som mera utförligt beskriver delar av det som huvudrapporten "LearnSafe¹ projektet; ett återbesök" handlar om. Här ska redan från början påpekas att design inte togs upp i projektet, utan att texten nedanför baserar sig helt på nytt material som har tillkommit efter att projektet avslutades i juni 2004. Design har dock en klar och uppenbar påverkan hur driften av en kärnkraftsanläggning kommer att gestalta sig. Jag har i några sammanhang tidigare gjort jämförelsen mellan att designa en säker bil och att köra en bil säkert.

Design har att göra med artefakter, dvs. något människor har byggt. Att beskriva design handlar om att förstå hur något artificiellt skapas (Simon 1996). Roworth-Stokes (2011) ger i sin översikt av design som ett akademiskt forskningsområde en idé om hur synen på området har utvecklats över tid och vilka internationella journaler och vilka underområden man talar om. Krippendorff (2011) fortsätter från den artikeln med att beskriva hur design utvecklats från enkla produkter till att omfatta tjänster, system och stora projekt. Inom design har man talat mycket om en kombination av form och funktion (FoF) som alltid utgör två dimensioner i hur en design utvärderas. Esslinger (2011) bygger vidare på detta och ger i sin översikt en idé om design som en aktivitet som stöder innovation och utveckling mot samhällligt hållbara lösningar. När man talar om design² på svenska får man lov att vara uppmärksam på att betydelseerna i t.ex. finska (suunnittelu) och engelska (design) förmedlar olika skiftningar i ordet som det kan vara värda att uppmärksamma.

Denna uppsats bygger på dessa idéer och försöker utveckla dem för att förstå varför kärnkraften som lyckades utomordentligt i Finland och Sverige när anläggningarna byggdes under 1970- och 1980-talet, men inte sedan dess har kunnat nå likadana framgångar. När man talar om design, får man lov att på något sätt begränsa bilden. I det nästa avsnitt försöker jag ytterligheterna konstart och industriell produktion för att skapa något slag av gränsdragning. I det tredje avsnittet behandlar jag design av olika produkter, dvs. specifikt något som ska få avsättning på en marknad. Problemet här är att vad som kan kallas en produkt har med åren fått en betydligt vidare betydelse än vad som tidigare har varit fallet. I det fjärde avsnittet öppnar jag för design av system, vilket ofta betyder att man i stor utsträckning använder sig av redan existerande produkter, som man i

¹ Learning organisations for nuclear safety (FIKS-CT-2001-00162), <https://www.bewas.fi/learnsafe.html>.

² Med design menar jag här något som på svenska bäst innefattas av två ord "design och konstruktion".

en design- och konstruktionsprocess ser till att kan samverka på ett önskat sätt. I det femte avsnittet lyfter jag upp design av organisationer, som ett speciellt område att studera. Det är nämligen så att ett objekt som ska designas för det mesta är på något sätt unikt, vilket kan betyda att själva designprocessen måste anpassas till det som ska designas. I det sjätte avsnittet talar jag om design i samhället, vilket då specifikt handlar om mycket stora system som kan få en genomgripande förändring i mycket av det som händer i ett samhälle. Tills sist försöker jag ge något slag av sammanfattning och rekommendationer inför framtiden. I allt detta ser jag som en förutsättning att man redan i designprocessen bygger in kravet på säkerhet från första början. Om man inte gör det, utan i stället i efterhand försöker lägga till säkerhet, blir det ofta så att betydande problem kommer att uppstå långt innan nyttan av en ny anläggning kan erhållas.

2 Konst eller industriell process

När man närmar sig begreppet design har man alltid en viss svårighet att på något vis begränsa det, samtidigt som man poängterar dess allmängiltighet (Buchanan, 2001). I vilken mån det har att göra med någonting helt nytt eller någonting man kan få till stånd genom att koppla ihop sådant som redan finns skiljer sig från fall till fall. Det område inom vilket en designer³ bildar dock en helhet där man alltid stöder sig på något som redan finns. Ett vanligt konstaterande i designlitteraturen påpekar att det rör sig om både funktion och form (FoF). Resultatet av en designprocess kan syfta till ett konstverk (form) eller till en industriell produkt som ska användas för något bestämt ändamål (funktion). När det är frågan om ett konstverk så är det kanske enastående eller ett exempel i en serie av andra liknande, som kommer till under en skapande period i en konstnärns liv. När det gäller en produkt är emellertid syftet att skapa något som kan mångfaldigas på ett effektivt sätt i en senare produktionsprocess. Man kan också skilja mellan två ytterligheter i en mindre helhet där konsthantverk associeras med manuella processer och industriell design med en produkt som tillverkas industriellt. När man i dagen värld söker exempel på produkter som kan skapas i en designprocess, kan man se att det knappast finns några begränsningar. Det kan vara en fysisk produkt, en produktionsprocess, ett datorprogram, ett system, en tjänst, men det kan också vara ett ledningssystem eller en organisation (Buchanan, 2008). I fortsättningen av denna uppsats begränsar jag mig dock till industriella designprocesser, som på ett sätt eller annat syftar till en produkt, som ett företag ämnar sälja till flera användare. Också i den meningen är en designprocess egentligen mera omfattande så att den vanligen också innefattar konstruktionsprocessen genom vilken designen visas fungera i praktiken.

2.1 Skapa något nytt

Ett klassiskt verk diskuterar vetenskapen om det artificiella (Simon, 1996). Simon diskuterar här bland annat begreppet funktion och det faktum att design ofta utgörs av ett sammankopplande av färdiga moduler som då kanske har konfigurerats för sitt syfte i den värdiga produkten.

Kidder (1981) ger en livfull beskrivning hur det kunde gå till när grunderna till ICT-revolutionen lades i början av 1980-talet. Motsvarande designprojekt skulle knappast idag kunna beskrivas i en bok på något över 250 sidor.

2.2 Form och funktion

I ett spektrum mellan konst och industriell design skiljer man ofta mellan form och funktion, där man menar att form har att göra med estetiska kvaliteter och funktion kvaliteter för ett bestämt ändamål. Form och funktion är dock intimt förknippade med varandra, vilket bl.a. framförs av (Hoegg, Alba, 2011).

2.3 Skeden i en designprocess

Horvath_2004, design mellan konst och produktutveckling, taxonomi för olika delar av ett designprojekt.

³ Här också i betydelsen konstruktör.

Ett designprojekt startas ofta av att någon ser ett behov, som inte är uppfyllt och då ser en möjlighet för ett hjälpmedel eller en produkt som kunde fylla detta behov.

2.4 Design principer

Att sätta samman något nytt av existerande delar, betyder ofta att det lönar sig att involvera slutanvändare i designprocessen

ofta gör man så att man egentligen designar en plattform, som kan användas för flera olika ändamål genom att slutanvändaren genom att definiera ett antal parametrar, egentligen tar över en del av designprocessen

Den kanske allra viktigaste principen när man modifierar en tidigare design, är att förvissa sig om att den faktiskt passar in i en ny omgivning. Problemet är här att man för att kunna göra en fungerande ändring, måste förstå de principer som tillämpades i den ursprungliga designen.

I artikeln (Hamraz et al. 2013) gör författarna i en litteraturstudie en kartläggning av olika ändringar som man kan göra, Artikeln ger en möjlighet att söka artiklar som beskriver något av de delområden de beskriver.

2.5 Utmaningar i ett designprojekt

Den största utmaningen i ett designprojekt är att förstå och se vad som behövs, för att man ska nå ett önskat slutresultat. Ett designprojekt består en kedja av på varandra beroende beslut, så att man ofta tvingas gå långt i kedjan, innan man faktiskt ser vad slutresultatet kommer att bli. Man kan här se en stor likhet med olika typer av pussel, där läggandet av en bit i början gör att man samtidigt väljer bort många senare alternativ man också kunde ha tagit på vägen mot en lösning.

En del författare talar om s.k. ondskefulla problem (wicked problems) som man söker en lösning på. Detta gäller i synnerhet för stora ändringar i samhällets infrastruktur, där man alltid ställs inför ett stort antal sinsemellan olika krav olika intressenter ställer på ett acceptabelt slutresultat. I sådana fall är problemet att designa ett system som består av både tekniska, organisatoriska och sociala delsystem, ofta kommer att vara ondskefulla i den meningen att det helt enkelt inte existerar någon lösning som är acceptabla för alla intressenter.

2.6 Olika typer av designprojekt

(Moreau, 2011) estetik eller funktionalitet, förgängliga eller varaktiga värden, offentlig eller privat sfär, projektarbetet görs i huvudsak av noviser eller experter

ett argument varför designprojekt misslyckas är att man sällan lyckas skapa en tillräcklig inlärningsprocess, utan de som varit med konstaterar "aldrig mera"

2.7 Ett nytt sätt att designa

Datorerna har sedan de blev allt vanligare erbjudit ett helt nytt sätt att designa genom att bygga program (Sheard 2018). Fördelen är att det går lätt att ändra och att man kan testa sin design i ett tidigt skede. Själva designprocessen kan dessutom stödas av olika datorbaserade system (CAD, VR, 3D modellering, osv.) så att man på en ganska godtycklig nivå kan testa sin design i en dator, utan att man behöver producera en fysikalisk prototyp. Detta har lett till att man åtminstone med avseende på programvara delvis har frångått den traditionella V-modellen för design (IAEA 2016, 11–12) och i stället argumenterar för en myckenhet av tidiga experiment med alternativa koncept (Goericke, 2020). Här kan man också använda sig av speciellt anpassade språk för att bygga modeller av objekt och interaktioner (Larman, 2005). I och med att man nu också kan använda 3D skrivare kan man dessutom föra sin design till fysiska komponenter för att testa dem på olika sätt. Vidare härifrån kan man också bygga upp en produktionsprocess, som också den i stor utsträckning kan vara

datorstödd (CAM). Allt detta betyder att man i en designprocess har mycket stora möjligheter att testa prototyper i olika skeden av processen.

3 Design av produkter

något som ska kunna tillverkas industriellt på ett ekonomiskt sätt för att kunna säljas tillräckligt billigt på en marknad

design betyder här alltid att man måste kombinera två krav, funktionalitet och pris

Luchs, Swan (2011) uppehåller sig länge i en diskussion av hur man definierar produktdesign i litteraturen. De baserar sina slutsatser på en litteraturstudie av 121 artiklar som publicerats i åtta journaler om design i perioden 1995–2008.

3.1 Helhet och detaljer

Simon, fördelen med modulära lösningar, anekdoten om två klockmakare

SoS tänkande betyder helheter, helheter kräver modeller av olika sort, men man behöver i alla fall semi-kvantitativa (i ordinal mening) jämförelser mellan alternativ. Hu et al. (2018) ger en idé om hur man kan närma sig problemet.

3.2 Att tänka i funktioner

När man definierar en produkt talar man om form och funktion. En viss funktion kan implementeras på många olika sätt, vilket betyder att man väljer en form av någon viss typ. När man talar om industriprodukter som definierades före andra världskriget så betydde den form man valde för en viss funktionalitet vanligtvis ett analogt system, dvs. man avbildade vissa funktionella parametrar genom att representera dem med fysikaliska storheter tex. längd, nivå, temperatur, spänning, ström, etc. Idag använder man sig med en stor preferens för digitala system, så att en viss funktionalitet bestäms av program i en dator.

Fiorineschi_etal_2016, påtalar brister i funktionstänkandet, något att analysera närmare, i detta fall kopplat till att man dokumenterar varför i en design för att efteråt kunna göra en bedömning av de problem man observerat senare, i kärnkraftssammanhang tillkommer C^3 kravet (completeness, consistency, correctness)

Eisenbart_etal_2017, liksom ovan något att fundera på, hur förstår man funktion, förstår alla deltagare i projektet på ett tillräckligt samstämmigt sätt, viktigt i varje fall för stora projekt med många komponenter.

Hur, var, när och varför använder man moduler (Bonvoisin et al. 2016).

3.3 En målbild

När man talar om ett nytt system har man vanligen något slag av målbild som man försöker uppfylla. Speciellt när man talar om design för kärnkraftsindustrin är denna målbild oftast ett kravsystem man måste anpassa sig till, fastän man mot en leverantör ställer upp ett antal önskade funktioner som man vill att produkten ska uppfylla. Formulerad i en beslutsmodell som sist och slutligen bestämmer som man vill att systemet ska uppfylla kan man se kraven som binära, antingen uppfyller systemet ett visst krav eller så gör det inte det. Här tillkommer då andra önskemål som kan uppfyllas mindre eller högre grad. Man kan tala om effektivitet för ett visst ändamål och man kan tala om priset man måste betala för systemet. När det gäller flera variabler får man då tala om ett optimeringsproblem där man balanserar mellan olika egenskaper hos det nya systemet.

I och med att man i betydligt större utsträckning än tidigare använder programmerbara komponenter i så gott som alla produkter, betyder detta att man har tillfört produkterna en högre komplexitet. Detta betyder att man

aldrig i praktiken kan tänka sig att genomföra något slag av ens tillnärmelsevis fullständig test av funktionen hos en produkt (jfr. Appendix).

(Fernandes et al., 2015) beskriver hur Rolls Royce hanterar sitt kravsystem, ändringar i kravbilden och hur man hanterar tillkommande krav under arbetets gång

olika typer av krav och kravsystem, målsättningen är vanligen att kraven inte ska vara alltför detaljerade

ett detaljerat kravsystem kan göra det göra det lätt att konstruera (fel kan undvikas, tidtabellsmässiga fördelar, arbetsmässiga fördelar) och göra drift och underhåll lätt att sköta (lätt att undvika fel, komponenterna är lätt åtkomliga, noggranna instruktioner), men det betyder i stället att man fråntar designarbetet friheter som kan betyda att mera fördelaktiga lösningar väljs bort i olika skeden av projektet

skador på person, arbetsbelastning, skador på miljön, ett implicit ekonomiskt krav, får inte kosta för mycket

C³ kravet

3.4 Dokumentering av designprocessen

Oberoende av vad som avses att bli designat är det viktigt att kraven man arbetar med och de lösningar man väljer blir tillräckligt noggrant dokumenterade. Det räcker inte bara med att dokumentera vad och hur, utan man borde alltid också på ett tillräckligt noggrant sätt dokumentera varför man valde en viss lösning. Detta för att senare när man vill ändra något av någon anledning. så borde man veta varför den existerande designen valdes framför andra möjliga. Om man inte har denna information går det lätt så att de ändringar som görs, på något sätt är i konflikt med den ursprungliga lösningen.

3.5 Att hantera osäkerhet

osäkerhet (epistemisk, aleatorisk), kunskap och konsekvenser, projekt (tid, kostnader)

osäkerhet i designprojektet, osäkerhet i den kommande driftperioden för systemet, vad måste man ta hänsyn till

en flexibilitet i designen, var binder man efterföljande beslut, kan man designa för återhämtningsförmåga när störningar uppträder

3.6 Stöd för användarna

användarna av objektet för design, stöd för designern i processen

Redan TMI olyckan gav en uppenbar lärdom för alla konstruktörer av kontrollrum att man måste beakta användarna. Olyckan ledde också till ett mycket stort intresse för att utveckla olika typer av riktlinjer man borde beakta när man designar ett kontrollrum. Härvid hade speciellt en rapport från Electric Power Research Institute i USA (EPRI, 1978) en mycket viktig position i arbetet. Också i Finland och Sverige gjordes ansträngningar att för att utveckla kunskapen (Ranta et al. 1981). Det kanske mest omfattande arbetet i den riktningen gjordes på Brookhaven National Laboratory i USA med dokumentet NUREG-0700 som nu finns som ett utkast till en tredje reviderad upplaga (USNRC 2020). Man kan visserligen fråga sig vad ett dokument på över 500 sidor kan ge för ett designprojekt som antingen syftar till att utveckla en plattform för kontrollsystem eller en specifik lösning för en ny anläggning. Det är uppenbart att man inte kan använda dokumentet som stöd i ett projekt, utan informationen måste på sätt eller annat redan ha anammats av de personer som deltar i projektet. De måste ha den nödvändiga inlevelseförmågan för att förstå operatörernas situation i olika upptänkliga driftsituationer. Hoc och Amalberti (2007) ger i sin artikel en inblick i vad en designer borde ta till sig och förstå, för att kunna ge operatörerna en tillräckligt rik och anpassad uppfattning om tillståndet hos det system de styr.

Nuvarande system som för det mesta innehåller datorer ger en betydligt större möjlighet att i designen bygga in olika typer av stöd för systemets användare. En enkel typ av stöd kan t.ex. utgöras av situationsberoende instruktioner. En mera avancerad form kan innehålla förklaringar, som gör det möjligt för nya användare att förstå varför man ska agera på ett visst sätt i en viss situation. Det att man numera använder sig av digitala system gör det möjligt att till och med använda olika tillämpningar av artificiell intelligens för att stöda användarna. Om sådana system dessutom förses med ett utökat antal givare som förmedlar en bättre översikt av de verkliga förhållandena i en situation och hur olika förebådande tecken småningom byggs upp, har man större möjligheter att försäkra sig om att användarna faktiskt förstår situationen i vilken systemet befinner sig. Nuvarande system har dessutom mycket goda möjligheter för 3-dimensionell modellering och presentation. Stöden för användarna kan också ge direkt input till databaser som beskriver systemets konstruktion i godtycklig detalj. Systemen har dessutom en möjlighet att byggas upp för olika typer av användare så att var och en får något som är relevant för de arbetsuppgifter han eller hon väntas utföra.

3.7 Designkvalitet

funktionalitet, enkelhet

dålig design (viktiga krav har inte tagits om hand, ett system är svårt att förstå/hantera, användarna fångas av sina misstag, felaktigheter i namn och/eller beskrivningar)

Design kvalitet kanske i första rummet har att göra med att undvika fel. Det mest allvarliga fel man kan göra är att man inte har beaktat ett viktigt krav, så att man i mitten av designprocessen försöker ta med också detta. Viktigt då är att man backar tillräckligt mycket så att man kan integrera det nya kravet i den design som utgår från denna punkt. En annan sak är om man på något annat sätt upptäcker att något av designbesluten har gjorts med felaktiga premisser, då får man på samma sätt backa själva processen så att man återgår till en punkt där ett riktigt beslut har tagits. Från detta får man då göra om all design som beror av det förnyade designbeslutet.

Ett annat sätt att se på designkvalitet är att medge att så gott som allt kan göras på flera sätt så att önskade krav är uppfyllda. Man kan då i mängden av användbara designlösningar föra in andra godhetskriterier, såsom enkelhet, förståelighet, ändamålsenlighet, osv. I de försök man har gjort att jämföra noviser och experter i vilken typ av lösningar de föreslår, har man tydligt kunnat visa att experterna presterar betydligt bättre lösningar än noviser (Sun_etal_2014). Detta leder osökt till några intressanta frågor enligt:

- hur definierar man designkvalitet,
- hur skiljer man noviser från experter (utbildning, erfarenhet, etc.),
- hur borde man utbilda personer som ämnar göra en insats inom design i sin yrkesverksamhet?

En designprocess genomförs ofta av två eller flera personer på grund av att den arbetsmässigt blir för stor för en enda person. Den färdiga produkten kommer då att bestå av flera helt eller delvis sammankopplade delar som ska fungera som en helhet. När designgrupp består av ett litet antal personer, har man den fördelen att de kan göra besluten tillsammans och så att risken för dåliga beslut blir mindre. De flesta designprocesser med en industriell relevans har dock sällan denna fördel, utan man får se till att man har något slag av ledningssystem som gör det möjligt för alla att passa in sitt arbete i en gemensam ram. Trots detta råkar man ofta ut för direkta fel i designen och det att en dålig design väljs framför en annan som hade varit bättre.

Olika typer av fel

- ett viktigt krav som borde ha beaktats har fallit bort,
- sena ändringar i kravbild
- missförstånd i interfacen mellan två och flera av de ansvariga personerna
- dålig utbildning eller kunskap
- hur utbilda personer för design, sätt dem i en omöjlig situation, om man kastar folk i sjön lär de sig att simma
- projektplanering, tidtabell och kostnader har överskridits

(Taylor, 2007; Kinnersley, Roelen, 2007) designfel orsaken i mer än 50% av störningarna under driften

3.8 En V&V process

En viktig del i varje designprocess är att man under processens gång verifierar att vald design uppfyller de krav som ställs. På samma sätt måste man göra en helhetsbedömning av en slutförd design, så att man på lämpligt sätt förvissar sig om (validerar) att den färdiga produkten uppfyller förväntningar som har ställts. För enklare produkter kanske endast detta sista steg räcker på så sätt att man utsätter en prototyp av produkten för ett antal sluttester.

Wynn_Clarkson_2018, många olika modeller, vilka ska man använda och när, VPohjola_2003, Morten Lind massa/energiflöden, simuleringsmodeller APROS, en modell av processen, hur man gör det är det fel att pressa in för mycket, modellen ohanterlig, inte naturlig

kan man modellera för vad man vill ha, modeller är alltid begränsade avbildningar av en verklighet
en virtuell verklighet

3.9 Ett ledningssystem

finns, förstått, använt (ansvar, befogenheter, arbetsprinciper)

design principer med vilka man försäkrar sig om en lyckad design, principerna integrerade i ett ledningssystem

3.10 Olika produktområden

Kannengiesser_Gero_2015, tre olika områden, hur är de lika, hur skiljer de sig, kan man skapa en modell av processen

3.11 Vanliga problem i en designprocess

se hur ett beslut i processen påverkar slutresultatet (intractable problems, wicked problems)

När projektet är i gång, finns det inte mera tid för teoretiserande, man kör med det man har, dock bör man beakta att göra projektet framtungt, se till att man förutser de problem som kan uppstå, se till att man förstår varandra i kontaktytorna mellan delprojekten

varför har användare vanligtvis uppfattningen att designern av en produkt aldrig själv behöver använda den

4 Design av system

I design av system är en första åtskillnad om det är frågan om ett enskilt system för ett visst ändamål eller om man i stället bör tala om att man vill skapa ett system av system (SoS, system of systems). I det första fallet talar man om ett väl avgränsat system där visserligen flera olika komponenter kan ingå. Man kan dock i detta fall anta att komponenterna är välkända och inte behöver mera än en begränsad anpassning för att de ska kunna användas. I det senare fallet talar man om ett betydligt större system där man egentligen kommer att kräva att de ingående delsystemen behöver sina egna delprojekt, för att de ska kunna fungera på ett ändamålsenligt sätt i den större helheten.

utmaningar för en design av industriella anläggningar, alternativ och lösningar (hur jämföra)

- platser
- teknologier
- typer av projekt (nyckelfärdigt, architect engineer, själv koordinerat om man köper insatser från olika leverantörer)
- leverantörer (förmåga, tillförlitlighet, pris, tidtabell)

4.1 Allmänna principer

När det gäller design av system utgår man ofta från att en stor del av den färdiga produkten baserar sig på existerande lösningar. Man får visserligen lov att noga granska de delar man tar in i systemet, så att de faktiskt kommer att fungera i sin nya omgivning. Idag kan man visserligen konstatera att problemet är större än bara ett system. Man måste samtidigt tänka på hur det nya systemet ska produceras, konfigureras, användas och underhållas. Detta betyder att man sällan designar och konstruerar ett system, utan att man i stället efterfrågar ett system av system. I praktiken betyder detta att man har en betydligt större palett av lösningar som på något sätt måste passas in i en större helhet. Om detta går att göra i en övergripande designansträngning där man således skapar en arkitektur av en helhet innan man går till de enskilda sammankopplade systemen är en annan fråga. I varje fall är kanske detta man borde göra (Batkovskiy_etal_2019) för att få en tillräcklig välfungerande helhet utan att göra alltför många prototyper som utvecklas under en längre tid.

Tidig planering

- platsförberedelser, logistik, lokala leverantörer,
- rekrytering för designprojektet,
- infrastruktur på platsen, teknologier, projektet och dess delar, val av leverantörer,
- projekt metoder och verktyg,
- designprocessen har styrts av ett ledningssystem.

principer för god projekthantering, ett ledningssystem för projektet

4.2 Interaktion mellan människa och system

människans roller (Newman, 1999)

- a. Människa/System roller, definition av funktion och interaktion (HF);
- b. Människa /System Interface/Design och implementering av samspel (HE);
- c. Urval, utbildning och träning;

användare, operatör, underhållare/ändringar, tränare, utvecklare, kund, planering för en integrerad drift, layout av enskilda arbetsplatser

MTO-system

gränssytorna måste förstås från båda sidor, förutsätter kommunikation och överenskommelser

anpassa systemet till dess operatörer (riktlinjer för interfacedesign, Ranta et al. 1981, NUREG-0700 first version 1981, John O'Hara, Brookhaven National Laboratory)

- kontrollrummet
- expertroller
 - underhåll
 - konfigurera kontrollsystemen
 - planera och genomföra revisioner

faser i en anläggning, från färdig konstruktion till återställd plats

- idrifttagning
- provdrift
- kommersiell drift
 - start och avstängning
 - normal drift
 - störningar och nödsituationer
- anläggningsändringar
- avställning
- återställning av platsen

en arbetsfördelning mellan automation och operatör, olika lösningar (Sheridan 2014)

Flach_etal_2017, för vissa svåra områden kan man med speciella lösningar försöka komma åt hur användare förstår en display, design för att skapa omedelbar förståelse, gärna så att lösningen är skalningsbar

hur validera valda lösningar (mockupp, simulatorer, anläggningsanalyser)

4.3 Ett livstidsperspektiv

Varje system har en viss tänkt livstid under vilken man förutsätter att det fungerar som det är tänkt. Redan vilken dator som helst behöver under sin livstid en hel del uppdateringar t.ex. då man upptäcker fel i den ursprungliga designen. Det betyder då att det företag som designat datorn får lov att samtidigt i designprocessen, bygga ett system som tar till vara drifterfarenhet och ett annat system som gör ändringar i den ursprungliga designen och förmedlar dem till alla användare som har köpt produkten.

Livstidsaspekten betyder att man på sätt och vis i en värdering av den ekonomiska nyttan för ett system kan särskilja mellan kostnaderna för designprojektet och kostnaderna för att sköta uppdateringarna

val av plats, design, konstruktion, idrifttagning, drift, ändringar, avställning, återföring av platsen för andra användningar (restore to green field)

4.4 System av system

Man får också lov att skilja mellan design av enskilda system och av system av system (SoS).

Man kan särskilja på system av systemberoende på sättet de erhåller sin gemensamma styrning och man kan då tala om

- toppstyrda SoS (ett ledningssystem styr de samverkande systemen)
- hierarkiska SoS (systemen styrs centralt genom ett system av interna mål och medel)
- polycentriska SoS (ingen central styrning finns, utan varje system har sina egna rutiner, men har frivilligt underkastat sig vissa regler för koordinering)
- virtuella SoS (styrning, koordinering och samarbete sker uteslutande genom datorer och nätverk)

4.5 Socio-tekniska system

I varje system har man på sätt och vis funktionalitet som går utöver det som vanligen menas när man talar om interaktionen mellan användare och systemet. Redan det faktum att man måste underhålla ett system kanske genom att uppdatera det med jämna mellanrum eller att byta ut någon del som har gått sönder, betyder att systemet har ett interface till ett större system som ser till att det fungerar under sin planerade livstid.

(Aven, Ylönen, 2018)

felhandlande och systemfel, taxonomi

4.6 Automation

Design för säkerhet har alltid involverat automation i någon form. Utvecklingen inom informationsteknologi (hårdvara, programvara, robotik, artificiell intelligens) har gett betydligt större möjligheter att automatisera än det ena och än det andra. Idag har vi även tillgång till avancerad displayteknik (3-D, virtuell verklighet), som har gjort att man kan bygga nya koncept för en interaktion mellan människor och automation. Jag kan visserligen anta att denna möjlighet leder samma väg som Bainbridge påtalade för nästan fyrtio år sedan Bainbridge (1983), dvs. ingenjörerna automatiserar det som går lätt att automatisera, men samtidigt ger användarna en hopplöst spretig bild av uppgifter. Man kan visserligen hoppas att dagens insikt om att anpassa systemet till människan och inte tvärtom ska möjliggöra en mera ändamålsenlig utvecklingsväg. Visserligen tycks samma gamla problem uppträda att den lilla grupp som ansvarar för säkerheten i ett skarpt läge, inte

förstår vad alla signaler betyder och således inte förmår hantera situationen på ett ändamålsenligt sätt (Oliver et al. 2017). Jag kan således än en gång verifiera påståendet att samma förebyggande åtgärder kan leda till både säkerhet och olyckor.

automation i objektet för design, automation i designprocessen

4.7 Design för säkerhet

hot, aktioner för att återvinna säkerhet efter en händelse (är händelsen behandlad i riskanalysen eller inte), är aktionerna effektiva eller inte,

vad borde man göra före, under och efter händelsen, klassisk riskanalys

resiliens, säkerhet II, exploatera/utnyttja, utforska/undersöka, två sätt att förhålla sig, känd teknik och innovationer, allt nytt är inte nödvändigtvis bra

design principer (DiD, graded approach to goals, redundancy, diversity, separation, grace rule)

design av ett ledningssystem

design för en intervention (Karanikas_etal_2022). Författarna har gjort en genomgång av litteratur som beskriver interventioner som gjorts för en bättre säkerhet. Av totalt 73 beskrivna studier som de valde beskrev 26 sådana som faktiskt hade gjorts medan resten var sådana som var planerade eller hade genomförts i en mindre skala. Deras artikel argumenterar för att man bör starta med en beskrivning på en abstrakt nivå som man sedan för mot en mera fullständig beskrivning av vad man tänker göra och vilka resultat man förväntar sig att nå.

5 Design av organisationer

En iakttagelse när det gäller design och konstruktion av något helt nytt är att man då ofta får lov att designa en ny organisation för ändamålet (Yoo et al. 2006)

(Bevan_etal_2007) organisationsförändring UK

att sätta upp en projektorganisation, struktur, organisatoriska enheter (design moduler, kontaktytor), myndigheter, ansvar, rapportering, prestationsindikatorer

5.1 Organisationen som en källa för effektivitet

arbetsfördelning, chef – medarbetare, behov att koordinera aktiviteter, kommunikation, bakgrund/utbildning, chef/medarbetare problematiken, språket för att överbygga kunskapsområden, generalist/specialist

skillnad mellan att vara chef och att vara ledare, betydelsen av karisma

5.2 Skillnaden mellan design och drift

kunskap och förståelse för att designa en säker bil och för att köra bilen säkert

varaktigheten för en designorganisation är oftast kort, i synnerhet om den skapats för att genomföra ett enskilt projekt

5.3 Om institutioner

En institution är en organisation som man hoppas kan bli varaktig. Man kan också se att institutioner ofta bildar av sig själv bildar en institution antingen som en egen organisation eller en del av den ursprungliga organisationen (emergens).

Institutioner har ett sätt att arbeta, ett sätt att vara, sina egna regler för hur man fungerar

5.4 Kärnkraften som exempel

Ibland gäller designen av ett nytt system något mera än vad man tidigare har producerat. Man brukar do ofta tala om design av det första systemet av vad man hoppas ska kunna bli en ny serie av produkter som kan produceras och säljas under en längre tid. Några exempel av detta från kärnkraftvärlden är design och konstruktion av Oskarshamn 1, som lade grunden för en serie av totalt nio reaktorer som byggdes av Asea Atom. Ett liknande exempel är konceptet AP-600 som lanserades av Westinghouse, men som inte omedelbart lyckades lika bra. Från dessa exempel vill jag dock föra fram idén att sådana stora design- och konstruktionsprojekt egentligen förutsätter inte endast design av den nya produkten, utan ett samtidigt skapande av en infrastruktur som ska betjäna design och konstruktion av en serie av system av samma slag. Detta betyder att man initialt måste designa en helt ny organisation, som på ett sätt förstår detta faktum och kan beakta det i en tillräcklig grad för att infrastrukturen ska kunna skapas. Ett exempel på detta ges av Yoo et al. (2006), som visserligen inte helt passar in, men i alla fall för fram problemet med vad som på engelska brukar kallas FOAKE (first-of-a-kind-engineering), som för det mesta för med sig att uppskattningar av varken kostnader eller projekttid kommer att hålla.

kärnkraftens utveckling, en lösning till PWR och BWR teknologi (Pool 1997), jfr. QWERTY-keyboarden (Brian Arthur)

I vilken grad denna bild passar in på några av de problem jag har sett inom kärnkraften först i samband med moderniseringar av kontrollsystem och scenarier i samband med nya anläggningar är en annan sak, men uppenbart är i alla fall att design och konstruktion inte har lyckats anpassa sig till den nya teknologin eller till ändrade företagsstrukturer. Med utgångspunkt från de problem man sett bara i Finland (Fortum, TVO, Fennovoima), kan man säga att Arevas insatser för moderniseringen av anläggningarna i Lovisa och konstruktionen av Olkiluoto 3 samt Rosatoms insatser för Hanhikivi 1 har lidit av att leverantören⁴ av projekten inte har kunnat anpassa sin organisation för det faktiska behovet. Vad detta i sin tur beror på är svårt att hitta argument för i detta sammanhang.

5.5 Problem som har förekommit

På 1980-talet kunde man föra byggandet av en ny kärnkraftsanläggning till ett lyckat slut på en kalendertid av 5–7 år enligt erfarenheter från Finland och Sverige. När man försöker göra samma sak idag verkar man stöta på oöverstigligena problem. Något måste alltså ha ändrat och man kan fråga vad. En lista på möjligheter kunde vara följande

- kompetensen hos leverantörerna har försvunnit,
- nyttillkomna krav har gjort kravsystemen svårare att hantera,
- systemen har blivit mera komplexa, man måste helt enkelt göra mera arbete

den första versionen av ett system blir alltid dyrare och tar längre tid att få färdigt, FOAKE (first of a kind engineering), för senare system har man nytta av en inlärningsprocess (referenser?)

Hur ska man kombinera kunskap i en designorganisation, se till att man har både bredd och djup, en förmåga att förstå och kommunicera?

5.6 Design av digitala säkerhetssystem

kravsystem, arkitektur, konceptuell design, detaljerad design, integration, verifiering och validering (V&V), FAT och SAT (factory and site acceptance tests), idrifttagning

⁴ Nu gick det så att Rysslands oprovocerade anfall på Ukraina i februari 2022 ledde till att projektet blev ohållbart.

funktioner (säkerhet, driftstörning, skydd, sekvensautomatik), arkitektur, delsystem, programmering med tillhjälp av funktionsblock, plattform, detaljer, simulering

5.7 Stora projekt

Infrastrukturliknande, många olika aktörer (Matinheikki, 2019)

5.8 Balanser

Jag har i andra sammanhang argumenterat för nödvändigheten att en organisation kan anpassa sin verksamhet med avseende på ett antal balanser. Detta gäller med säkerhet också för organisationer som sysslar med design och konstruktion. När det då gäller s.k. FOAKE-projekt så finns det egentligen ingen tidigare information om vad som kommer att bli kritiskt för den organisation som måste skapas. När det gäller kärnkraftsprojekt kan man i varje fall identifiera några faktorer som man uppenbart måste ta hänsyn till och man kan då exempelvis ge följande lista:

- placeringen av anläggningen (vilka bestämmelser och vilken praxis gäller i landet i fråga),
- tänkta ägarförhållanden (finansiering, nationell infrastruktur),
- projekttyp (centraliserat, distribuerat, beställarens roll).

När det gäller landet där anläggningen kommer att placeras är den största frågan om det finns tidigare nukleära anläggningar i landet eller om den tänkta anläggningen är den första. Viktigt att veta är också vilken normal industriell praxis gäller, dvs. om man kan anse att landet är industrialiserat eller ett utvecklingsland. De tänkta ägarförhållandena har betydelsen för finansieringen, är t.ex. den eller de tänkta ägarna inom den offentliga eller den privata sektorn. Inom den privata sektorn kan man även särskilja mellan kraftproducenter och användare av elkraft. I många fall är det även så att man inte har en entydig ägare i vanlig mening utan ägarföretaget ägs i sin tur av flera olika ägare. När det gäller projekttyp kan man utan vidare säga att här har skett en ändring under de senaste trettio åren. Idag gäller så gott som uteslutande en distribuerad projekttyp, där visserligen en huvudleverantör ges en viss typ av helhetsansvar, vilket dock betyder att underleverantörer kan engageras så gott som obegränsat och också så att djupet av kedjade kontrakt kan vara stort.

samarbete / konkurrens (0-summe spel eller win-win möjligheter)

6 Design i samhället

det finns många olika faktorer man måste vara uppmärksam på, i synnerhet gäller detta då man har att göra med designprojekt som avser att skapa ett nytt system av system

Initiativ för säkerhetsförbättringar i ett samhälle kanaliseras vanligen genom att ansvariga myndigheter ges i uppgift att effektivisera tillsynen så att en bättre säkerhet kan nås. Ofta är det också att sådana initiativ för med sig ett slag av obalans mellan olika teknikområden, så att det mera allmänna målet om att kravsystem borde byggas i stort på samma detaljnivå.

stora system i samhället

- många intressenter
- många olika krav att ta hänsyn till

samspel med myndigheten

- miljökonsekvensbeskrivning (när, hur detaljerad)
- riskanalyser (normal drift, störningar, nödsituationer)
- säkerhetsargumentering

6.1 Säkerhetsförbättringar

Med ny teknologi kan man ofta föra in säkerhetsförbättringar antingen genom automatiska system eller genom att ge operatörerna bättre stödfunktioner. Nu är det tyvärr så att systemförbättringar ofta underlåter att ge de säkerhetsförbättringar man väntar sig, eftersom man i stället använder sig av möjligheten att förbättra systemets produktionsförmåga. Gerald Wilde (1994) har kallat fenomenet för risk homeostasis.

6.2 Artificiell intelligens

på senaste tid har olika typer av design stöd växt fram, man motser också en tilltagande användning av artificiell intelligens i systemen, designstöd för att göra det lättare att beakta alla krav som ställs på systemen som designas

system som innehåller artificiella komponenter som kan ge dess användare ett stöd

symbios mellan maskiner och människor i grupper (Malone, 2018)

6.3 Designerns ansvar

En fråga när det gäller design och konstruktion är vilket ansvar de har för att resultatet av deras arbete är rimligt säkert. Frågan blir ännu mera komplicerad om de råkar ut för påtryckningar från högre ort att titta om brister i design eller konstruktion eller om de i sitt yrke förutsätts komma fram med lösningar som kan anses strida mot internationella lagar eller normer. Tjernobyl som med goda argument kan kallas för en reaktor med två huvudfunktioner, dvs. den ena att producera elektricitet och den andra att producera plutonium för bomber kan enligt min uppfattning anses som en konstruktion som inte borde ha fått föras fram som en standard-konstruktion.

Många har argumenterat för att design håller på att förändras så att man alltmer kommer att integrera framtida systemanvändare i designprocessen (Sanders, Stappers, 2008). Det finns mycket som tyder på att detta faktiskt händer, vilket åtminstone ger en förhoppning om att kommande system ska vara lättare att använda.

vem får skulden om dålig design förorsakar dödsfall (fallet Maria i Sverige, Ödegård 2006)

6.4 Effektiv myndighetstillsyn

Myndighetstillsyn syftar till att ta tillvara samhällets intresse gentemot stora aktörer, stoppa dåliga system, skydda enskilda konsumenter

6.5 En global värld

en global klimatförändring, styra in marknader och samhällen mot hållbara alternativ

7 Sammanfattning och rekommendationer

designtänkandet, designteori

7.1 Hur området har utvecklats

stora förändringar har skett under de senaste 50 åren i hur man designar och bygger stora industriella system

- från en huvudleverantör till ett lapptäcke av dellerleverantörer
- från att bygga allt på en vald plats till att sätta samman allt större moduler i en fabrik
- från lokala till globala leverantörer
- kravet att hantera många olika gränssnitt
 - språk

- företag
- teknologier
- roller

design nu ett eget område, egen forskning, egna tidningar

digitala tvillingar, datoriserade system (kravhantering, dokumentering, instruktioner, ...)

7.2 Utmaningar

(Eppinger, 2011) snabba förändringar, digitala processer, flexibla plattformar, hantering av komplexitet management, outsourcing och offshoring, involvering av kunden, nätverk av innovationer, hållbarhet

återcirkulerade och jungfruliga material, icke giftiga material, förnyelsebar energi, mindre fotavtryck

ondskefulla problem, design i samhället (risker, politiska processer, demokratins svagheter)

7.3 Design i en global värld

BAT (best available technology), architect engineer, systemleverantörer, kravsystem, ackreditering och certifiering, normer

Appendix

När man ställer krav på en produkt brukar man ofta ha en implicit förhoppning om att man ska kunna visa att kraven för det första är konsistenta, dvs. inga krav i kravsystemet är i konflikt med varandra (en egenskap krävs samtidigt som dess motsats också krävs). För det andra brukar man nära en förhoppning om att de krav som krävs skulle vara fullständiga i den meningen att de täcker in de funktionella beteenden som produkten ska uppvisa. Ett sista önskemål brukar vara att produkten ska vara så enkel och lättförståelig som möjligt, trots att man har tagit hänsyn till att olika felfunktioner av produkten tagits om hand, så att den inte i någon situation som helst kan fungera fel på ett sätt som på något vis kan hota produktens användare. Detta är nämligen omöjligt annat än i produkter med en mycket begränsad funktionalitet, dvs. C³ (consistency, completeness, correctness) är inte möjligt att säkerställa annat än i mycket begränsade fall.

Förkortningar

Jag har här valt att endast använda förkortningar som ofta används i engelskspråkig litteratur. Följande förkortningar har använts

3D	tredimensionell
AI	artificiell intelligens
AR	augmented reality (visningar i anläggningen genom speciella glasögon)
C ³	completeness, consistency, correctness (fullständighet, konsistens, riktighet)
CAD	computer aided design
CAM	computer aided manufacturing
CAT	computer aided testing
DiD	defence in depth (djupförsvar)
FAT	factory acceptance tests
PSA	probabilistic safety analysis
SAT	site acceptance tests
SoS	systems of systems (system av system)
VR	virtuell verklighet (virtual reality)
V&V	verifiera och validera

Erkännanden

Texten ovan består fortfarande till största delen av korta platsreservationer för längre tillägg. Det kommer antagligen att behövas en större insats för att få en färdig text. Så här långt har jag fått ett betydande stöd av de mina medförfattare till texten i (Schöbel et al., 2022). Om Du är en läsare av denna text och samtidigt har eget intresse av processerna som syftar till nya anläggningar, så är Du mycket välkommen att kontakta mig för att diskutera möjligheterna till en gemensam skivarsats.

Referenser

Terje Aven, Marja Ylönen (2018). A risk interpretation of sociotechnical safety perspectives, *Reliability Engineering and System Safety*, 175, 13–18.

Lisanne Bainbridge (1983). Ironies of Automation, *Automatica*, Vol. 19, No. 6. pp. 775-779.

Aleksandr M. Batkovskiy, Aleksandr V. Leonov, Aleksey Yu. Pronin, Elena G. Semenova, Alena V. Fomina, Victor M. Balashov (2019). Sustainable development of industry 4.0: The case of high-tech products system design, *Entrepreneurship and Sustainability Issues*, Volume 6, Number 4 (June).

Helen Bevan, Glenn Robert, Paul Bate, Lynne Maher, Julie Wells (2007). Using a Design Approach to Assist Large-Scale Organizational Change; "10 High Impact Changes" to Improve the National Health Service in England, *The Journal of Applied Behavioral Science*, Vol. 43 No. 1, March 135-152

Jérémy Bonvoisin, Friedrich Halstenberg, Tom Buchert & Rainer Stark (2016) A systematic literature review on modular product design, *Journal of Engineering Design*, 27:7, 488-514.

Richard Buchanan (2001). Design Research and the New Learning, *Design Issues: Vol.17, No.4, Autumn*.

Richard Buchanan (2008). Introduction: Design and Organizational Change, *Design Issues: Vol.24, No.1, Winter*.

Marta B. Calás (1993). Deconstructing charismatic leadership: rereading Weber from the darker side, *Leadership Quarterly*, 4(3/4), 305-328.

Peter Checkland (1999). *Systems thinking, systems practice*, Wiley.

Thomas Donaldson, James P. Walsh. Toward a theory of business, *Research in Organizational Behavior* 35 (2015) 181-207.

Steven Eppinger (2011). The Fundamental Challenge of Product Design, *The Journal of product innovation management*; 28: 399-400.

Hartmut Esslinger (2011). Sustainable Design: Beyond the Innovation-Driven Business Model, *The Journal of product innovation management*; 28: 401-404.

Lorenzo Fiorineschi, Federico Rotini & Paolo Rissone (2016) A new conceptual design approach for overcoming the flaws of functional decomposition and morphology, *Journal of Engineering Design*, 27:7, 438-468,

Stephan Goericke (ed.) (2020). *The Future of Software Quality Assurance*, Springer Open.

Bahram Hamraz, Nicholas H. M. Caldwell, P. John Clarkson (2013). A Holistic Categorization Framework for Literature on Engineering Change Management, *Systems Engineering* Vol. 16, No. 4, 473-505.

J. M. Hoc, R. Amalberti (2007). Cognitive Control Dynamics for Reaching a Satisficing Performance in Complex Dynamic Situations, *Journal of Cognitive Engineering and Decision Making*, Vol. 1, No 1, pp. 22-55.

JoAndrea Hoegg, Joseph W. Alba (2011). Seeing Is Believing (Too Much): The Influence of Product Form on Perceptions of Functional Performance, *The Journal of product innovation management*; 28:346-359.

- Jiexiang Hu, Yang Yang, Qi Zhou, Ping Jiang, Xinyu Shao, Leshi Shu & Yahui Zhang (2018) Comparative studies of error metrics in variable fidelity model uncertainty quantification, *Journal of Engineering Design*, 29:8-9, 512-538.
- IAEA (2016). Design of instrumentation and control systems for nuclear power plants, *Specific Safety Guide*, SSG-39.
- Scott Jackson, Timothy L. J. Ferris (2013). Resilience Principles for Engineered Systems, *Systems Engineering* Vol. 16, No. 2, 2013.
- Nektarios Karanikas, Shanchita R. Khan, Philip R.A. Baker, Colin Pilbeam (2022). Designing safety interventions for specific contexts: Results from a literature review, *Safety Science*, 156, 105906.
- Tracy Kidder (1981). *The soul of a new machine*, Penguin Books.
- Kinnersley, S., Roelen, A., 2007. The contribution of design to accidents. *Saf. Sci.* 45, 31–60.
- Klaus Krippendorff (2011). Principles of Design and a Trajectory of Artificiality, *The Journal of product innovation management*; 28: 411–418.
- Craig Larman (2005). *Applying UML and patterns; an introduction to object-oriented analysis and design and iterative development*, Prentice Hall.
- Michael Luchs and K. Scott Swan (2011). Perspective: The Emergence of Product Design as a Field of Marketing Inquiry, *J Prod Innov Manag*;28:327–345.
- Thomas W. Malone (2018). *Superminds; the surprising power of people and computers thinking together*, Oneworld.
- Juri Matinheikki, Kirsi Aaltonen, Derek Walker (2019). Politics, public servants, and profits: Institutional complexity and temporary hybridization in a public infrastructure alliance project, *International Journal of Project Management*, 37, 298– 317.
- C. Page Moreau (2011). Inviting the Amateurs into the Studio: Understanding How Consumer Engagement in Product Design Creates Value, *The Journal of product innovation management*; 28: 409–410.
- Richard A. Newman (1999). Issues in Defining Human Roles and Interactions in Systems, *Syst Eng* 3: 143-155.
- Nick Oliver, Thomas Calvard, Kristina Potočnik (2017). Cognition, Technology, and Organizational Limits: Lessons from the Air France 447 Disaster. *Organization Science* 28(4):729-743.
- Robert Pool (1997). *Beyond engineering ; how society shapes technology*, Oxford University Press.
- Ranta Jukka, Wahlström Björn, Westesson Rolf (1981). Guidelines for man-machine interface design, *VTT Tutkimuksia* 23.
- Seymour Roworth-Stokes (2011). The Design Research Society and Emerging Themes in Design Research, *The Journal of product innovation management*; 28:419–424.
- Elizabeth B.-N. Sanders & Pieter Jan Stappers (2008). Co-creation and the new landscapes of design, *Co-Design*, 4:1, 5-18.
- Markus Schöbel, Inmaculada Silla, Anna-Maria Teperi, Robin Gustafsson, Antti Piirto, Carl Rollenhagen, Björn Wahlström (2022). Human and organizational factors in European nuclear safety: A fifty-year perspective on insights, implementations, and ways forward, *Energy Research & Social Science*, 85, 102378.
- Sarah A. Sheard (2018). Evolution of systems engineering scholarship from 2000 to 2015, with particular emphasis on software, *Systems Engineering*, 21:152–171.

Herbert Simon (1996). The sciences of the artificial, 3rd edition, The MIT Press.

Ganyun Sun, Shengji Yao, Juan A. Carretero (2014). Comparing Cognitive Efficiency of Experienced and Inexperienced Designers in Conceptual Design Processes, Journal of Cognitive Engineering and Decision Making, Vol. 8, No. 4, pp. 330–351.

Taylor, J.R., 2007. Statistics of design errors in the process industries. Saf. Sci. 45, 61–73.

USNRC (2020). Human-System Interface Design Review Guidelines, Draft NUREG-0700, Rev. 3, läst 220621 på adressen <https://www.nrc.gov/docs/ML1815/ML18158A333.pdf>.

Gerald J.S. Wilde (1994). Target Risk, PDE Publications.

David D. Woods (2015). Four concepts for resilience and the implications for the future of resilience engineering, Reliability Engineering & System Safety, DOI: 10.1016/j.ress.2015.03.018.

David D. Woods (2018). The Theory of Graceful Extensibility: Basic rules that govern adaptive systems, Environment Systems and Decisions, DOI: 10.1007/s10669-018-9708-3.

David D. Woods (2019). 4 Essentials of resilience, revisited, Handbook on resilience of socio-technical systems, 2019 - elgaronline.com.

David C. Wynn, P. John Clarkson (2018). Process models in design and development, Res Eng Design, 29:161–202.

Youngjin Yoo, Richard J. Boland, Jr., Kalle Lyytinen (2006). From Organization Design to Organization Designing, Organization Science 17(2):215-229.

Synnöve Ödegård (2006). Säker Vård; patientskador, rapportering och prevention, NHV – Nordiska högskolan för folkhälsovetenskap.