

GKE ELEKTRONIK AB UTVECKLINGSMETODIK , HÅRDVARA OCH PROGRAMVARA

Detta dokument är avsett för internt bruk inom GKE Elektronik AB. Det kan dock lämnas till kund eller uppdragsgivare vid diskussioner kring ett projekt eller metodik. Dokumentet uppdateras fortlöpande.

Dokumentnamn: gkeutv970816. Ersätter gkeutv960512.

Tillkommande avsnitt är checklistan i avsnittet om riskanalys och taltyp fractional.

Inledning, varför behövs en metod?

Varje projekt har sin speciella karaktär och sina speciella krav. Gemensamt för all utveckling är dock att ett visst mål ska nås och att utvecklingen är avslutad då detta mål nås. GKE tillämpar en flexibel utvecklingsmodell - baserad på den så kallade V-modellen - för att styra utvecklingen så att den sker på ett överblickbart och strukturerat sätt. Målet är att dokumentera alla krav som ställs på systemet (sk inputs) och låta dessa krav utgöra grunden för uppdelningen av funktionerna i hårdvarulösningar och programvarukonstruktioner. Dessa dokumenterade krav används också för att generera detaljerade specifikationer för hårdvara och programvara. De används dessutom för att generera testspecifikationer för systemets olika delar och för det kompletta systemet. Genom att tillämpa en enhetlig metod - samma i samtliga projekt - når vi att dokumentationen blir likformig, lättare att producera, lättare att hitta i och fullständig. Det ger oss också en möjlighet att redan på offertstadiet bedöma dokumentationens omfattning och därmed ge en exaktare kostnadsuppskattning.

En alltmera viktig del av utvecklingen av ett system är att identifiera och eliminera de risker som användning av systemet kan innebära. Avsnittet om riskanalys har därför utökats med en checklista i syfte att tjäna som påminnelse så att uppenbara risker inte passerar utan att ägnas tillbörlig uppmärksamhet.

Fördelar med V-modellen, användning av andra metoder

V-modellen styr arbetet så att konstruktion sker "Top-Down" medan implementering sker "Bottom-Up". Genom att signalutbytet mellan olika enheter och nivåer specificeras på ett tidigt stadium i utvecklingen kan det arbetsintensiva implementeringsarbetet på de lägre nivåerna delas upp på flera av varandra oberoende grupper och/eller underentreprenörer. Validering av delsystem sker på respektive implementeringsnivå och systemintegrationen kan göras utgående från väl specificerade och testade delfunktioner. Andra metoder, som försöker greppa helheten och generera ett icke-hierarkiskt ("platt") system, kan vara försvarbara i utvecklingsarbete där antalet producerade enheter är stort (exempelvis konsumentelektronik) och det gäller att minimera kretskortsytta, kisel eller programminne. Vid sådana uppdrag bör lämplig utvecklingsmetodik diskuteras. Vid projekt av enskottscharaktär eller där många instanser är inblandade, dvs flertalet uppdrag, ska V-modellen alltid vara den utvecklingsmodell som i första hand ska väljas.

Begränsningar, alternativ till standardmodellen.

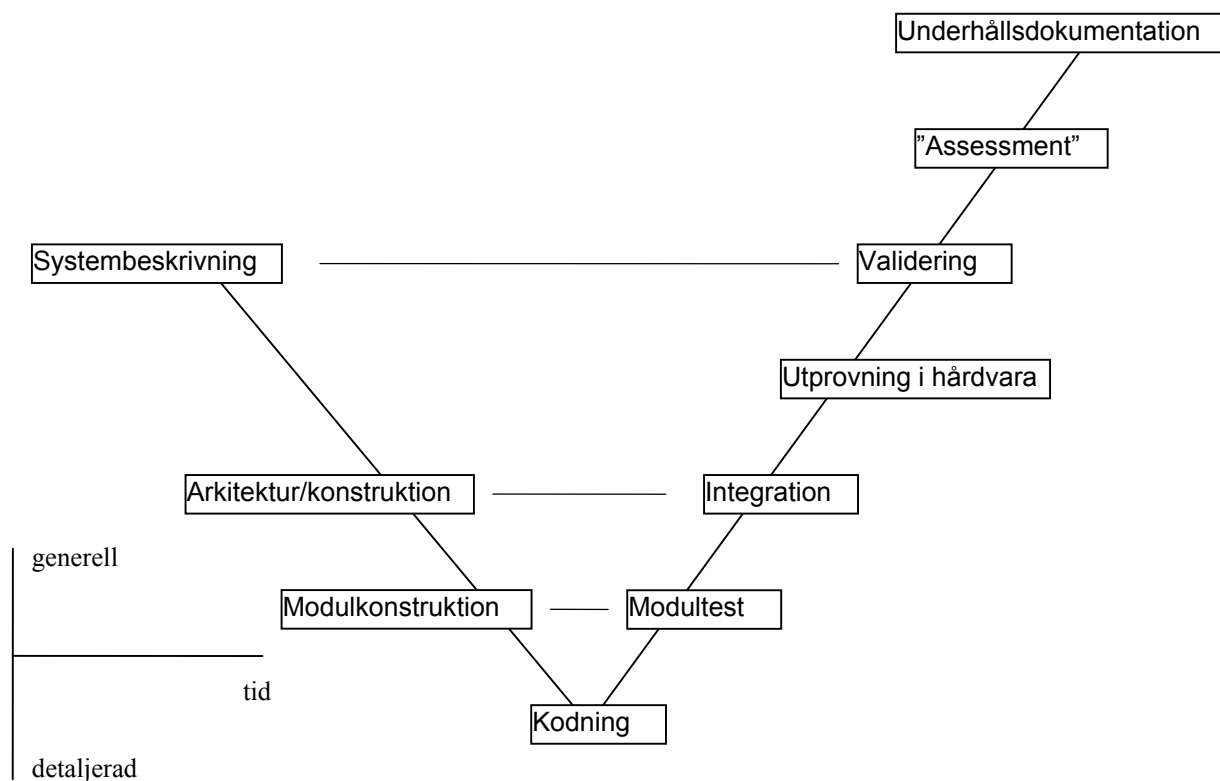
V-modellen bygger på en idealiserad bild av förhållandet beställare/leverantör. Beställaren förutsätts ha kompetent personal som kan sin process och vet vad det beställda systemet ska göra. Kravspecifikationen förutsätts vara författad av beställaren eller dennes konsult. I dagens slimmade organisationer saknas ofta den kompetens som detta kräver. V-modellen kan då bli ett hinder för ett effektivt arbete. GKE bör då överväga tre utvägar:

- ta över rollen som systembeskrivare
- låta systemet växa fram organiskt och beskriva systemet i samband med att varje deletapp färdigställs
- avböja att ta uppdraget.

Var ska V-modellen inte användas?

Mycket små uppdrag där målet är att snabbt lösa en speciell uppgift i samband med exempelvis kvalitetsproblem i en pappersmaskin eller där mätutrustning för några timmars studium av ett förlopp ska tas fram karakteriseras av begränsad budget och - framför allt - mycket snäva tidsramar. I sådana fall kan arbetet genomföras mera intuitivt, baserat på rutin och specifikt processkunnande. Flertalet uppdrag av servicekaraktär är sådana att V-modellen inte blir aktuell.

V-modellen



Bilden visar V-modellen så som den används vid programvarukonstruktion. Vid hårdvarukonstruktion och/eller en kombination av båda tillämpas V-modellen på

motsvarande sätt. Arkitektur/konstruktion motsvaras av uppdelning i funktionsenheter medan Modulkonstruktion motsvaras av kretskonstruktion. Kodning har ingen egentlig motsvarighet i rena hårdvarusystem men där PLD förekommer är det förstås detsamma som syntes av logikfunktioner i VHDL, PALASM eller liknande.

Software Integrity Levels, hur långt ska GKE gå?

I kritiska projekt, exempelvis system för flyg och signalsystem för järnvägstransporter, gäller speciella krav på programvarans och hårdvarans utförande så att ett visst mått av "okränkbarhet" (integrity) uppehålls även vid onormala eller ej förutsedda situationer. Som exempel kan nämnas EN 30128:Railway Applications, Software for Railway Control and Protection Systems. Där läggs bland annat kraven på olika SoftWare Integrity Levels (SWSIL 0 - 4) fast. För andra kritiska system, exempelvis inom medicinska tillämpningar finns motsvarande normer. Beroende på vilken grad av SWSIL man vill uppnå är olika grad av dokumentation och testning nödvändig. Att bygga system för högre SWSIL är ett jobb för stora organisationer. GKE ska därför inte befatta sig med SWSIL högre än 0 eller 1. GKE kan däremot ingå i större team vid projekt som syftar till SWSIL 2 eller högre.

Erforderliga dokument (SW)

Antalet dokument kan bli överväldigande stort. Vid SWSIL 4 fordras exempelvis ca 80 olika dokumenttyper. Lägre SWSIL nöjer sig med avsevärt mycket mindre antal dokument. För normala projekt är de väsentliga dokumenten: Systembeskrivning, Systemarkitektur, Modulbeskrivningar, Kvalitetssäkringsplan, Konfigureringsplan, Verifieringsplan, Integrationsplan, Modultestplan, Systemtestplan, Modultestrapport, Systemtestrapport, Källkod (kommenterad), Hårdvarudokumentation, Valideringsplan, Valideringsrapport, Underhållsdokumentation, Ändringsdokumentation. Till detta kommer ofta testvektorer och dokumenterade utdata. Appendix A innehåller en sammanställning över de dokument som kan finnas i dokumentationen.

Många av dokumenten kan sammanfattas i ett dokument. Genom att exempelvis utföra modulbeskrivningen som en kommenterad Finite State Maskin grafisk "bubbelplan" har man full dokumentation över arkitektur, I/O och funktion. Den grafiska redovisningen kan också tjänstgöra som testplan och testrapport genom att uppnådda testresultat förs in direkt i schemat. Samma metodik används för övrigt sedan länge inom hårdvarukonstruktion och test.

En kategori dokument är särskilt viktig: underhållsdokumentationen. Dokumentera allt som har relevans:

- Använda systemkomponenter, version, datum
- Ingående program och datafiler, version, datum
- Operativsystem, version
- Inifiler etc ska utöver magnetmedia/CD finnas på papper
- Utvecklingshjälpmedel (assembler/kompilator, tillverkare, version etc)
- Använda batchfiler ska utöver magnetmedia/CD finnas på papper
- Konfigurering och start från scratch
- Adress och telefonnummer (personnamn) till samtliga systemkomponentleverantörer

Programmeringsanvisningar

Style Guides

Olika programmeringsmetoder kräver olika programmeringsstilar. Generellt gäller dock att textbaserade metoder (programlistningar) ska utformas så att programmets funktion kan följas av andra än programmeraren. Även programmeraren kan ha svårigheter att följa sina egna tankegångar om programmet inte är dokumenterat på ett bra sätt. Appendix B innehåller "guidelines" för assemblerprogrammering, C-programmering och programmering i Basic/Visual Basic. Gemensamt för dessa guidelines är att variabler och konstanter ska ha namn som säger vilken funktion de har. Kommentarer ska finnas både i form av sammanfattande beskrivning av varje programmodul och löpande på de programrader där processen behöver förtydligas.

För grafiska system med direkt grafisk inmatning (HP VEE, Visual Basic, HiDraw etc) gäller att de är snabba och säkra att programmera och testa men svåra att underhålla om inte funktionsbeskrivning i textuell form kompletterar dem. I vissa system kan kommentarer och förklaringar läggas in direkt i den grafiska miljön. Man bör då eftersträva att beskriva funktionerna på input/output-form så att kommentarernas volym hålls nere (så kallade strategiska kommentarer) och undvika att kommentera varje delfunktion (taktiska kommentarer). Symbolerna får här tala för sig själva.

I de system som inte tillåter kommentarer i programbeskrivningen (Visual Designer t. ex.) ska motsvarande beskrivande text finnas som ett kompletterande dokument.

Editorer

Källkod ska skrivas i ASCII-editor eller speciella editorer för respektive programmeringsystem. Undvik specialeditorer som kräver konfiguration för varje speciellt tillfälle. De skapar fler problem än de anses lösa.

Talsystem, enheter

I *flyttalsystem* används alltid *tekniska enheter* (engineering units, e.u.) endast i undantagsfall ska normerade enheter (p.u.) användas. Använd SI-enheter i programmet och konvertera vid behov till praktiska enheter som °C, pounds per linear inch etc.

I *heltalsystem* måste man försöka hitta en enhet som ger tillräcklig upplösning samtidigt som den valda ordlängdens värdeområde inte överskrids. Vid ett mätsystem med upplösningen 0,01 mm och totalt mätområde +/- 10 mm är valet enkelt; en μm ger en tiondel av upplösningskravet och 16 bitars ord ger värdeområdet +/- 32767 μm dvs +/- 32,7 mm. I andra fall kan det vara mycket svårt att hitta ett bra sätt att representera data. Det kan då vara en lösning att arbeta med dubbel ordlängd i de delar av programmet där kravet på upplösning/dynamik är stort i stället för att gå över till en processor med större intern ordlängd. I vissa fall kan kompression (log/exp) ge önskat resultat men där absolut noggrannhet krävs över hela värdeområdet är det ingen lösning.

Vid val av intern representation bör man försöka tillgodogöra sig de fördelar som multiplikation/division med 2-exponenter ger. Framför allt är 16 och 256 lämpliga skalfaktorer.

BCD-aritmetik med flera dekader kan ofta vara en bra lösning, speciellt när kommunikationen med operatören sker via enkla knappsatser/tumhjul och numeriska displayer. Man bör överväga denna lösning även om den aktuella processorn inte förfogar över BCD-operationer.

I DSP-tillämpningar med *flyttalsprocessorer* är problemen med talrepresentation inte så stora. Man kan i allmänhet använda sig av tekniska enheter. Inga generella anvisningar ges

här eftersom dessa uppdrag oftast avvecklas i tätt samarbete med beställaren och dennes uppfattning om talrepresentation får vara bestämmande.

DSP-tillämpningar med heltalsprocessorer ger samma problem som heltalsprocessorer i allmänhet. Försök att styra mot processorer som har talrepresentation *fractional*. Gärna med saturation mode och dubbellängdsackumulator med overflowarea. Motorola DSP5630x är ett extremt bra val i sådana fall. Dess 24 bitars ordlängd ger mer än tillräcklig upplösning i tekniska sammanhang.

Risakanalys

Även det enklaste och mest okritiska system kan ha oönskade drifttillstånd. En fläktstyrning som inte startar då den ska starta eller - vilket ofta är sämre - inte stannar när den ska stanna är ett exempel på en oönskad funktion hos en styrning. Den oönskade funktionen utgör i sig ingen risk, det är först när den kan medföra en farlig situation som den utgör en risk.

Om fläkten har till uppgift att evakuera farlig gas så är det en uppenbar risk med att den inte startar när den ska. Om den har till uppgift att tillföra friskluft och den inte stannar när frysskyddet larmar så är risken för förstörda rörledningar också uppenbar. Om dessa i sin tur innehåller giftiga eller frätande ämnen så är katastrofen ett faktum.

Risk och hasard

Felfunktion hos ett system innebär i sig inte en risk. Det är först när felfunktionen kan ge upphov till farlig situation som en risk föreligger. Engelsmännen använder uttrycket HAZARD om ett sådant tillstånd. Något bra svenskt uttryck är svårt att hitta. Vi kommer därför att använda ordet hasard om ett tillstånd som ligger utanför normalt beteende och, om det kombineras med farliga förutsättningar, kan leda till personella eller materiella skador.

Metoder

Ett otal metoder för mer eller mindre automatisk risakanalys har utvecklats. I normala projekt har risakanalysen inom GKE hittills (våren 1996) utgjorts av bedömningar av sådana risker som utebliven bromsförmåga, risk för kortslutning, risk för okontrollerat utsläpp, risk för felaktiga mätvärden etc. Motmedlen har varit felsäkra konstruktioner, redundans, checksumma etc. Dessa tekniker är fortfarande fullt gångbara men de måste i vissa kritiska tillämpningar kompletteras med övervakningsfunktioner i form av monitorer som i sig själva är utförda på ett felsäkert sätt och som självtestas vid varje start.

Exempel på en sådan monitor är övervakning av ankarströmmen i en likströmsmotor till en lyftanordning. Risakanalysen visar att det finns risk för att tändpulser till tyristorbryggan uteblir. Missade tändpulser ger oren ankarström, vilket i sin tur leder till att kollektor och borstar förstörs. Vid snabbstopp blir kraven på borstar och kollektor mycket höga (hög ström krävs). Om dessa komponenter är skadade kan man i stället för effektiv bromsning få så kallat rundslag, vilket leder till utlösning och bromseffekt noll. Genom att övervaka ankarströmmens övertonsinnehåll och larma när andelen 50 eller 100 Hz blir för stor kan man upptäcka det potentiellt farliga feltilståndet innan kollektor och borstar skadats.

Denna typ av monitorering blir allt mer aktuell ju mer man drar in på personal på underhållsavdelningarna och ju mer av arbetet som sker via bildskärmar i stället för att operatörerna vistas ute i anläggningen. Risakanalysens uppgift är att kartlägga vilka risker som finns och hur de kan hanteras.

Risakanalys, alltid tillsammans med beställaren

GKE ska inte genomföra risakanalys utan beställarens medverkan. Men, GKE ska se till att en risakanalys genomförs, även om beställaren anser att det är onödigt. GKE ska därvid bidra

med det kunnande vi har inom kraftelektronik och industriell elektronik medan beställaren ska bidra med kunnande om processen. I de fall där GKE har kunskap från tidigare arbeten på likartade anläggningar ska GKE dra nytta av dessa erfarenheter och påpeka de risker som vi bedömer existera. I vissa fall kan det innebära ett visst mått av tåtrampning. Se till att ha relevanta lagrum och föreskrifter helt aktuella innan du tar upp en diskussion i sådana sammanhang. Tänk på att det också finns praxis och traditioner inom olika branscher och att det kan vara mycket svårt att införa "nymodigheter" i vissa branscher. Använd tidningsartiklar, om sådana finns, eller ta med beställaren på en kurs i ämnet. Det är ofta en bra "eye-opener".

Det finns en stor risk med risker och det är att den personal som dagligen hanterar risken slutligen blir så medveten om risken att man inte tänker på att meddela andra att risken finns. Man måste vara medveten om detta och prata med många olika människor som hanterar den process som man ska in i med nyutrustning eller med nya system. Ofta finns det någon äldre person, som inte har med den direkta driften att göra, som har perspektiv nog på verksamheten och kan plocka fram sådant som de mera aktiva int tänker på. Att snabbstoppa en pump som matar ut avloppsvatten i en lång rörledning är till exempel självklart för en operatör på ett reningsverk men sällan något som man får med i specifikationerna - just för att det anses självklart att alla vet det.

Checklista

Metoder för riskanalys sträcker sig från den enkla intuitiva bedömningen av ett systems "farlighet" till en omfattande, strängt formaliserad felträdskonstruktion. GKE har sedan 1977 arbetat med industriella system, ofta i samband med höga effekter och energiansamlingar i stålverk, pappersbruk och verkstäder. Riskanalysen har därför alltid intagit en central plats men tyngdpunkten har legat på att bedöma risk för produktionsstörningar, kortslutningar, lastfall och sådana situationer där lagrad kinetisk eller statisk energi kan leda till skada. I och med att nya krav ställs på systemen (ISO 9001 etc) måste vi även bedöma - och konstruera - systemen med tanke även på andra risker. Följande checklista kan vara till hjälp vid identifieringen av tänkbara risker. Använd den inte rakt av! Gör först en egen preliminär analys av de osäkerhetsmoment som kan finnas i systemet (en preliminär hasardlogg). Kolla sedan mot listan om det kan finnas något som ytterligare ska vara med.

Energirisiker

El: kortslutning, laddning, induktiv kick-back, ljusbåge, ESD, EMI

Statisk: trycksatta kärl och ledningar, spända fjädrar, hängande last

Dynamisk: roterande massor, linjära rörelser, vätskor i rörelse

Kemisk: explosiva gasblandningar, explosiva ämnen, antändning av brännbara ämnen

Termisk: åldring, kolning, antändning

Giftrisker

All hantering av giftiga ämnen är förenad med risk. Branschspecifika rekommendationer ska följas. Arbetarskyddsstyrelsen, Giftinformationscentralen.

Gas, ånga, tryckluft

Kombination av förgiftningsrisk, explosionsrisk, miljörisk och trycksatta kärl. Egensäkra kretsar. Konsultera SA vid tvekan. De ska i allmänhet besiktiga. Läckage är inte bara en hälsorisk eller miljörisk, det ger också ekonomiska förluster. Säkerhet kan alltså ofta räknas hem utan redan innan riskanalysen görs.

Vatten

Främst översvämning. Även vacuum (kollaps) vid tömning av kärl och "vattenslag" vid snabb stängning av ventiler. Observera även frysrisk! Dubbla nivåvakter i kritiska installationer.

Upplag, rasrisk

Främst i transportanläggningar och automatiska godshanteringsutrustningar. Rasrisk ofta förbisedd, kommer överraskande.

Stick, kross- och skärskada

Inga kommentarer. Har aldrig varit aktuellt. Kan förekomma i vissa arbetsmaskiner och transportanordningar.

Joniserande strålning

Syns ej, hörs ej, luktar ej. Omfattande säkerhetssystem krävs. Högsta varsamhet. Kundens expertis nödvändig.

Obefogat tillträde eller manöver

Lås, spärrar, lösenord.

Mätvärdesintegritet

Stor risk på grund av att mätvärden oftast har ett värde men varken kvalitetsstämpel eller ID-kort. Kvaliteten på mätvärdet måste säkerställas genom att mätutrustning, kablar, givare etc installeras, kalibreras och kontrolleras. Om självtest kan ordnas ska sådan införas. I system för loggning/laging/protokollering ska risken för falsk identitet beaktas. Rimlighetskontroll gör att mätvärden från olika mätsystem ofta kan särskiljas så att kanalblandning upptäcks. Lagrade mätvärden kan ofta - om de lagras på fil - särskiljas med hjälp av datum och klockslag. Utöver filnamn ska man alltså i kritiska fall göra en dubbelkoll mot tidsinformationen. Data som lagras transient i arrayer löper mindre risk för sammanblandning eftersom en array endast kan innehålla data från en mätomgång i taget (indexera aldrig en array så att flera mätomgångar lagras i den).

Mätsystem ska kalibreras med regelbundna intervaller. Kalibreringsrutiner och intervall ska anges i anläggningsdokumentationen.

EMI och ESD

Ger upphov till störningar i system på många sätt. Tänk på att alltid begränsa bandbredd så att inte mer än nödvändigt släpps igenom. Undvik bussystem. Watch-Dog och Finite State maskiner med säkra återstartsrutiner. Checksumma och paritet etc.