

NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET

FAKULTET FOR INFORMASJONSTEKNOLOGI, MATEMATIKK OG
ELEKTROTEKNIKK

INSTITUTT FOR DATATEKNIKK OG INFORMASJONSVITENSKAP



HOVEDOPPGAVE

Student : Gunhild Sivertsen Sørvig

Fag: Hovedoppgave, Systemutvikling

Oppgavens tittel (norsk) : Feil- og risikoanalyse i en programvareutviklingsbedrift

Oppgavens tittel (engelsk) : Failure and Hazard Analysis in a Software Development Company

Oppgavens språk : Norsk

Oppgavens ordlyd : Hvordan kan feil- og risikoanalyse brukes til å forbedre kvaliteten på et helseinformasjonssystem?

Oppgaven gitt:	20. januar 2003
Besvarelsen leveres innen:	23. juni 2003
Besvarelsen levert:	19. juni 2003
Utført ved:	NTNU, Trondheim
Veileder:	Tor Stålhane, NTNU

Sammendrag

Jeg har gjennomført en feil- og risikoanalyse i en bedrift som aldri har gjort dette tidligere. Hensikten med arbeidet, er å øke kvaliteten på produktet til bedriften, et helseinformasjonssystem for norske sykehus.

Helseinformasjonssystemet er stort og komplekst, med mange muligheter for konfigurering slik at det i stor grad kan spesialtilpasses hvert enkelt sykehus. Dette fører til at testrutinene må være svært omfattende for å sikre at systemet ikke inneholder feil. Bedriften har erfart at på tross av omfattende testing, klarer man ikke å teste hele systemet. Det er derfor et behov for å prioritere hvilke deler av systemet som må utsettes for mest omfattende testing. Risikoanalyse kan være et viktig hjelpemiddel til å identifisere de mest kritiske delsystemene.

Jeg valgte å gjennomføre risikoanalysemetoden funksjonell HazOP på noen utvalgte delsystemer for å undersøke om dette er en metode som egner seg for bedriften. I funksjonell HazOP har vi brukt use-case-diagrammer som systemdokumentasjon. I stedet for HazOP-ledeord, ble feilhendelser og konsekvenser identifisert ved å stille spørsmålene:

1. Hvordan kan denne funksjonen feile? – hva er funksjonenes feilhendelser?
2. Hva kan konsekvensene bli for pasientene og sykehuset?

Risiko er en kombinasjon av alvorlighetsgraden av en inntruffet hendelse og sannsynligheten for at den skal inntreffe. Siden sannsynlighet er en kompleks størrelse å beregne, valgte jeg i stedet å bruke feilhyppighet. I den forbindelse ble det foretatt registrering av alle meldte feil i en syvukers periode.

Både feilanalyse og risikoanalyse krever en konsistent oppfattelse av hvilke hendelser som kan betegnes som alvorlige. Siden et helseinformasjonssystem har stor innvirkning på sykehusets pasientbehandling og totale servicetilbud, anså jeg tradisjonelle informasjonssikkerhetsbegreper som for snevre. Derfor tok jeg utgangspunkt i konsekvenstabeller fra et byggeprosjekt i helsevesenet og intervjuer med bedriftens ansatte når jeg skulle utarbeide en klassifiseringstabell for feilhendelser. Et helseinformasjonssystem er svært omfattende, og feilhendelser har forskjellige konsekvenser for interessenter som pasienter, brukere og helseforetak. Bedriftens sterke kundefokusering gjorde at jeg valgte å dele klassifiseringstabellen inn i helseforetak og pasienter, framfor å vurdere alvorlighet ut i fra betydningen for bedriften.

Funksjonell HazOP viste seg å være velegnet for delsystemer som har brukerinteraksjon, mens det for andre delsystemer er mer hensiktsmessig å gjennomføre HazOP med ledeord. Feilanalysen krevde store endringer i rutinene for feilregistrering i bedriften, noe som var vanskelig å gjennomføre. Feilanalysen ble derfor noe mangelfull, men ble likevel vurdert som nyttig i vurdering av risiko.

Feil- og risikoanalysen førte til økt oppmerksomhet på kvalitetssikring i bedriften. Dessuten bidro utarbeidelsen av klassifiseringstabellen til økt bevissthet på hvilke vurderinger bedriften legger til grunn når feilhendelser gis alvorlighetsgrad. På grunnlag av erfaringene jeg har gjort, mener jeg at funksjonell HazOP og feilanalyse er en enkel og nyttig måte å gjennomføre risikoanalyse på for programvarebedrifter som utvikler systemer med høy grad av brukerinteraksjon.