

PM Kvalitativ Risklogg till stöd för leverantörer

Detta PM innehåller information om FMV:s förväntningar på leverantörens riskdokumentering som ska redovisas i risklogg. PM:et redogör för ifyllnad av Risklogg för kvalitativ bedömning av olycksrisk enligt den risklogg-mall som tillhandahålls av FMV.

Bakgrund

FMV anskaffar årligen en stor mängd materiel som på ett eller annat sätt omfattas av krav på systemsäkerhetsverksamhet inklusive krav på tolerabel risknivå. Tekniska system, produkter eller koncept som omfattas av krav på systemsäkerhet behöver på ett eller annat sätt få den tekniska designen och dokumentationens kvalitet utvärderad i syfte att FMV på ett tydligt sätt ska kunna gå i god för systemsäkerheten och därmed kunna ta sitt tekniska designansvar gentemot Försvarmakten.

FMV har behov av att ha löpande insyn i leverantörens systemsäkerhetsarbete och få visshet om att leverantören uppfyller ställda krav, hanterar identifierade olycksrisker och redovisar detta på ett öppet och systematiskt sätt. Detta kommer att underlätta för FMV vid olika genomgångar/möten och vid leveranskontroller.

Leverantören ska, som en del av systemsäkerhetsarbetet, i en risklogg dokumentera vilka olycksrisker som identifierats under analysarbetet samt hur dessa har värderats och hanterats. Riskloggen är, under tiden leverantören genomför systemsäkerhetsarbete, ett arbetsdokument som fortlöpande fylls i under analysarbetet fortskrider. Riskloggen kan användas för att dokumentera resultatet av de specifika riskanalyser som genomförs som systemsäkerhetsaktiviteter, såsom PHL, PHA, SHA, SSHA, FHA, EHA, HHA, O&SHA och RADS. Se vidare H SystSäk för mer information om dessa aktiviteter.

Syftet med riskloggen är att leverantören på ett tydligt sätt till FMV ska redovisa en sammanställning från riskanalyserna över vilka olycksrisker som det tekniska systemet omfattas av samt vilka åtgärder man genomfört för att minimera dessa. Riskloggen tillsammans med leverantörens systemsäkerhetsutlåtande (SCA), systemsäkerhetsrapport (SAR) och eventuella övriga säkerhetsrelaterade dokument utgör grunden för FMV vid fastställande av systemsäkerhetsgodkännande i samband med överlämning av systemet till Försvarmakten.

Mallar för Risklogg

På FMV:s hemsida finns mallar för kvalitativ och kvantitativ risklogg. Kvalitativ bedömning innebär en värdering mot en verbal beskrivning av sannolikhet medan kvantitativ bedömning är en värdering mot sannolikheten uttryckt i siffrvärden. Detta PM redogör för den kvalitativa risklogg-mallen. Vilken risklogg som ska användas beror på det tekniska systemets beskaffenhet. Finns tillräckligt med data för att kunna uppskatta kvantitativa sannolikheter ska detta göras. I annat fall bör den kvalitativa riskloggen användas. Leverantören bör rådfråga FMV vilken risklogg som systemsäkerhetsarbetet ska dokumenteras i. Riskloggmallarna kan vid behov anpassas genom att lägga till eller ändra kolumner, men ska endast göras efter samråd med FMV.

Språk

Riskloggen kan skrivas på svenska eller på det språk om detta anges i anbudsinfordran.

Riskdokumentation i risklogg

Ur ett FMV-perspektiv är det viktigt att olycksrisker dokumenteras enhetligt, då flera produkter eller system – ofta från olika leverantörer – ska integreras och samverka enligt definierade användningsområden.

Riskloggen ska kort och gott redovisa riskhanteringsprocessen för respektive olycksrisk. Något förenklat kan man säga att olycksriskerna utgör cellrader i dokumentet och riskhanteringsprocessen utgör cellkolumner från vänster till höger. Nedan följer en redogörelse över de kolumner som ingår i den kvalitativa risklogg-mallen samt vad som ska redovisas i respektive cell för respektive olycksrisk.

Riskidentifiering

Riskidentifiering		
Risk id / nr	Riskkälla	Olycksbeskrivning (Förklara risken)
1.1	Rörelse-energin i luftvärnsprojektil	<p>Pjäs avfyras men siktet är inte inställt på flygmålet. Bidragande orsaker kan vara felaktiga parameterinställningar för siktet, bristande kontrollrutin före skjutning, IFF (identify friend or foe) ger felaktig signal.</p> <p>Utlösande faktor är att skytt trycker på avtryckaren trots att vapnet är felriktat.</p> <p>Exponering innebär att målflygplan träffas samt att besättningen skadas eller omkommer.</p> <p>Givet vådahändelsen bedöms att projektilen missar flygplanet som betydligt troligare. Givet träff i flygplan bedöms besättningen alltid exponeras.</p>

Risk id / nr – Varje olycksrisk förses med ett unikt ID-nummer för att underlätta hänvisningar och referenser i övriga systemsäkerhetsdokument.

Riskkälla – I denna cell beskrivs riskkällan. Det vill säga vad den består av samt dess farliga egenskaper.

Olycksbeskrivning – Beskriv vådahändelsen, vad är den oönskade händelsen? Beskriv också de bidragande orsakerna till att vådahändelsen inträffar. Hur, när och varför den kan tänkas uppstå? Man bör även fundera på kompenserande faktorer avseende att vådahändelsen inte inträffar och om sådana finns beskriva dessa. Det kan vara olika typer av skyddsbarriärer som redan finns i systemet.

Vådahändelsen kan leda till en olycka om någon eller något skadas av riskkällan, med andra ord; exponeras för riskkällan. Redogör för vilken typ av skada som olyckan kan ge upphov till, personskador eller ekonomiska skador. I ekonomiska skador ingår skador på egendom men även skador på yttre miljö inkluderas som här omräknas i kostnader för sanering m.m. Redogör också för de eventuella bidragande orsaker som leder till att person, egendom eller den yttre miljön exponeras för riskkällan vid vådahändelsen. Man bör även fundera på kompenserande faktorer avseende exponering och om sådana finns beskriva dessa. Det kan till exempel vara olika typer av skyddsanordningar eller skyddsutrustningar som ingår i det befintliga systemet.

Om en vådahändelse bedöms kunna generera personskador och ekonomiska skador ska olycksrisken beskrivas på flera rader i riskloggen. Detta dels för att sannolikheten för olika allvarliga skador kan variera mellan de skyddsvärda givet att vådahändelsen inträffar, dels för att kraven på tolerabel risknivå kan variera beroende på om det avser person eller ekonomisk skada.

Risikvärdering före åtgärd

Riskvärdering		
Riskmatris		
Skadeklass före åtgärd	Sannolikhet/ Frekvens (A-E enligt riskmatris) för olycka per skadeklass I-IV	Risiknivå T, BT, ET (Alla fyra nivåer ska vara ifyllda)
I - Dödsfall	D	ET
II - Allvarlig	D	BT
III – Min. allvarlig	E	T
IV - Försumbar	E	T

Skadeklass före åtgärd – Denna kolumn är i riskloggmallen redan ifyllda med skadeklasser. I exemplet ovan är det för personskada. För ekonomisk skada definieras skadeklasserna utifrån kostnader till följd olyckan. Stäm av mot den riskmatris som det tekniska systemet är kravställt mot och justera så att skadeklasserna stämmer med dessa.

Sannolikhet/ Frekvens – Här ska redovisas den genom analys uppskattade kvalitativa sannolikheten eller frekvensen för att en olycka inträffar och ger den konsekvens som skadeklassen anger. Utgå från de sannolikhetsintervall som finns definierade i den kravställda riskmatrisen för systemet.

(Givet att en olycka inträffar kan dess konsekvenser variera från fall till fall. Riskmatrisen anger en indelning i fyra olika skadeklasser med olika allvarlighetsgrad.)

Risiknivå – Utgå från den uppskattade sannolikheten för olycka med respektive skadeklass och stäm av mot riskmatrisen vilken ruta man hamnar på. Rutan i riskmatrisen anger risiknivån som antingen är tolerabel (dvs. grön och markerad med T), begränsat tolerabel (dvs. gul och markerad med BT) eller ej tolerabel (dvs. röd och markerad med ET). Markera rutan med färgen grön, gul eller röd beroende på om olycksrisken är tolerabel, begränsat tolerabel eller ej tolerabel enligt riskmatrisen. Se exemplet ovan.

"Hela" olycksrisken får samma risiknivå som den skadeklassen med högsta bedömda risiknivå fick. I exemplet ovan är olycksrisken ej tolerabel då sannolikheten för en av skadeklasserna enligt matrisen ligger på ej tolerabel nivå.

Riskreducering och åtgärd

Riskreducering
Förslag till åtgärd(er) i kategori(er) (D) = Design (S) = Skyddsanordning (V) = Varning (I) = Instruktion (U) = Utbildning
Skyddsmekanism för att reducera sannolikhet för vådahändelse kan vara att skjutledaren förses med en strömbrytare som aktivt måste aktiveras för avfyrning ska kunna ske.
Skyddsbarriärer för att reducera exponering kan vara <ul style="list-style-type: none">– Längre avstånd mellan flygplan och flygmål– Ballistiskt skydd i flygplan– Två motorer– Reducerat antal personer ombord till piloten– Katapultstol

Förslag till åtgärd – Här anges förslag till åtgärd för att reducera olycksrisken. En viss åtgärd kan minska sannolikhet för vådahändelse, sannolikhet för exponering eller fördelningen på olika skadeklasser eller möjligen påverka flera av dessa faktorer samtidigt. Åtgärder kan utgöras av konstruktionsförändringar, skyddsanordningar, varningsanordningar, instruktioner eller utbildning.

Olycksrisker som i den initiala riskvärderingen bedömts vara ej tolerabla eller begränsat tolerabla behöver hanteras med någon form av åtgärd för att risken ska kunna reduceras ner till tolerabel nivå. I vissa fall kan det bli nödvändigt med flera åtgärder för att risken ska kunna bedömas ligga på tolerabel nivå. Om en åtgärd kan ske till låg kostnad och samtidigt ha stor riskreducerande effekt, så kan det vara lämpligt att genomföra den även för en risk som initialt bedömts vara tolerabel.

Riskvärdering efter åtgärd

Riskvärdering		
Riskmatris		
Skadeklass efter åtgärd	Sannolikhet/ Frekvens (A-E enligt riskmatris) för olycka per skadeklass I-IV	Risknivå T, BT, ET (Alla fyra nivåer ska vara ifyllda)
I. – Dödsfall	E	T
II. – Allvarlig	E	T
III. – Min. allvarlig	E	T
IV. – Försumbar	E	T

Riskvärdering efter åtgärd genomförs efter att åtgärderna är genomförda eller mot beaktan att åtgärderna kommer att genomföras. Uppskattning och värdering sker på samma sätt som för riskvärdering före åtgärd men skillnaden att man nu räknar med att åtgärderna reducerar olycksrisken.

Acceptansbeslut

Acceptansbeslut			
Åtgärd	Risk accepterad/stängd Namn/org/ underskrift	Anmärkning	Status S/Ö
Samtliga föreslagna åtgärder beslutas införas. Regler för vilka plan som får gå målflyg vid skjutning fastställda.	Ja 2015-01-01 Adam Bertilsson FMV	Verifierings-rapport XXX. Instruktion XXX.	S

Åtgärd – Här dokumenteras beslut om att föreslagen åtgärd ska genomföras alternativt att ingen åtgärd ska genomföras. Också referens till beskrivning och andra dokument.

Risk accepterad / Anmärkning / STATUS – Stängning av risk ska göras antingen direkt i riskloggens acceptanskolumn alternativt i separat dokument eller risknummerblankett som då ska refereras i Anm-kolumnen. Stängningen ska anges med datum, signatur, namnförtydligande och organisation. Det ska även framgå att en förutsättning för stängning är att åtgärder är verifierade. Ange därför verifierad åtgärd samt referens till det dokument som dokumenterar verifieringen.

Arbetet med risklogg

Riskloggen är ett arbetsdokument som går igenom vid SSWG- och/eller SSPR-möten mellan leverantören och FMV under ett anskaffnings- eller modifieringsprojekt. Inledningsvis, under riskidentifieringsfasen, läggs fokus på riskidentifieringsdelen. Senare under projektet går man igenom riskvärderingar och åtgärder. Om en olycksrisk inte kan hanteras av leverantören då det tekniska systemets helt eller delvis inte har påverkan på risken är det viktigt att FMV meddelas detta så tidigt som möjligt. Slutligen, innan leverans, hålls ett SSWG- eller SSPR-möte för att i samråd stänga kvarvarande risker som hanterats och bedömts vara tolerabla efter att åtgärder genomförts.

Riskloggen är även tänkt att vara ett arbetsdokument för Försvarmakten och FMV under vidmakthållandefasen samt som ingångsvärde till riskanalys inför avveckling (RADS) i samband med avveckling. Det är därför viktigt att riskloggen levereras till FMV som en bilaga till SCA, dels som en PDF samt som en Word- alternativt Excelfil vilket underlättar vidare systemsäkerhetsarbete inom Försvarmakten och FMV.