PM Kvantitativ 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 kvantitativ 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 Försvarsmakten.

FMV har behov av att ha löpande insyn i leverantörens systemsäkerhetarbete 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 Försvarsmakten.

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 siffervärden. Detta PM redogör för den kvantitativa 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 kvantitativa risklogg-mallen samt vad som ska redovisas i respektive cell för respektive olycksrisk.

Riskidentifiering

Riskidentifiering						
Risk nr	Risknamn	Delsystem	Fara	Egenskap	Möjlig vådahändelse eller farligt tillstånd	Exponering för vådahändelse
1:1	Avfyrning med luftvärnspjäs mot flygmål draget av målflygplan	luftvärns-projektil	Pjäs riktad mot målflygplan	Rörelse-energin i luftvärns-projektil	Pjäs avfyras men siktet inte är inställt på flygmålet. Bidragande orsaker kan vara felaktiga parameterinställningar för siktet, bristande kontrollrutin före skjutning, IFF (identify friend or foe) ger felaktig signal. Utlösande faktor är att skytt trycker på avtryckaren trots att vapnet är felriktat. Enligt driftsprofil uppskattas 5 skjutningar genomföras per pjäs och år. Bedömd sannolikhet för vådahändelse bedöms till 0,003 per avfyrning.	Målflygplan träffas, besättningen skadas eller omkommer. Givet vådahändelsen bedöms att flygplanet träffas 0,1 gånger. Givet träff i flygplan bedöms besättningen alltid exponeras.

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

Risknamn – Någon kortare rubrik på olycksrisken.

Delsystem – Här anges i vilket delsystem riskkällan förekommer eller vilket delsystem som ger upphov till olycksrisken. Delsystemet kan också definieras genom att ange ett identitetsnummer så som MIMI inom marinen eller motsvarande för armé och flyg.

Fara och Egenskap – I dessa två celler beskrivs riskkällan och det farliga tillståndet. Vad består riskkällan av, när är riskkällan förekommande och farlig samt dess farliga egenskap.

Möjlig vådahändelse eller farligt tillstånd – Beskriv vådahändelsen eller det farliga tillståndet. Vad är den oönskade händelsen? Beskriv också de bidragande orsakerna till vådahändelsen. 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.

Exponering för vådahändelse – Vådahändelsen (den oönskade händelsen när riskkällan befinner sig i ett farligt eller okontrollerat tillstånd) 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.

Riskvärdering före åtgärd

Riskuppskattning					Riskvärdering		
Före åtgärd					Riskmatris		
Sannolikhet/ frekvens för vådahändelse	Sannolikhet för exponering givet vådahändelse	Sannolikhet för olycka	Skadeklass	Procentuell andel	**p** för olycka med viss skadeklass	Risknivå resp. skadeklass	Risknivå hela risken
0,015	0,1	**PERSON** 1,5E-04	Dödsfall	70	1,1E-03	**ET**	**ET**
			Allvarlig	20	3,0E-04	**BT**	
			Mindre allvarlig	9	1,4E-04	**T**	
			Försumbar skada	1	1,5E-05	**T**	

Sannolikhet/ frekvens för vådahändelse – Den genom analys uppskattade kvantitativa sannolikheten eller den genom statistik härledda frekvensen för vådahändelsens inträffande ska anges i denna cell. Använd den enhet på sannolikheten eller frekvensen som är angett i systemets kravställda riskmatris.

Sannolikhet för exponering givet vådahändelse – Den genom analys uppskattade kvantitativa sannolikheten för att det skyddsvärda (som i tabellen ovan är person) exponeras givet att vådahändelsen inträffar, ska anges i denna cell.

Sannolikhet för olycka – Mallen räknar ut sannolikheten för olycka (sannolikheten för att vådahändelsen inträffar och att någon/något exponeras) baserat på de införda värdena i de två cellerna till vänster.

Skadeklass och Procentuell andel – Givet att en olycka inträffar kan dess konsekvenser variera från fall till fall. Riskmatrisen anger en indelning i fyra olika skadeklasser med olika allvarlighetsgrad. För personskada är skadeklasserna ”dödsfall”, ”allvarlig skada”, ”mindre allvarlig skada” och försumbar skada”. För ekonomisk skada definieras skadeklasserna utifrån kostnader till följd av olyckan. Stäm av mot den riskmatris som det tekniska systemet är kravställt mot och justera så att skadeklasserna stämmer med dessa. I cellen Procentuell andel ska den uppskattade procentuella sannolikhetsfördelningen mellan dessa fyra skadeklasser givet att olyckan inträffar, redovisas. Se exemplet ovan.

p för olycka med viss skadeklass – Utifrån sannolikheten för olycka och den införda procentuella skadeklassfördelningen, räknar mallen ut sannolikheten för olycka som resulterar i respektive skadeklass.

Risknivå resp. skadeklass – Utgå från sannolikheten för olycka med respektive skadeklass och stäm av mot riskmatrisen vilket sannolikhetsintervall respektive skadeklass ligger inom. Rutan man hamnar på anger risknivån 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). Skriv in sannolikhetsintervallet (benämnt med en bokstav) för respektive skadeklass samt markera rutan med färgen grön, gul eller röd beroende på om olycksrisken är tolerabel, begränsat tolerabel eller ej tolerabel enligt riskmatrisen. Se exemplet ovan.

Risknivå hela risken – "Hela" olycksrisken får samma risknivå som den skadeklass med högsta bedömda risknivån 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	Kostnad för åtgärd
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: – 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.

Risker 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.

Kostnad för åtgärd – Uppskattad kostnad, inklusive införande beräknat för ett exemplar av det tekniska systemet

Riskvärdering efter åtgärd

Riskuppskattning					Riskvärdering		
Före åtgärd					Riskmatris		
Sannolikhet/ frekvens för vådahändelse	Sannolikhet för exponering givet vådahändelse	Sannolikhet för olycka	Skadeklass	Procentuell andel	**p** för olycka med viss skadeklass	Risknivå resp. skadeklass	Risknivå hela risken
0,005	0,05	**PERSON** 5,0E-05	Dödsfall	50	1,3E-04	**T**	**T**
			Allvarlig	20	5E-05	**T**	
			Mindre allvarlig	10	2,5E-05	**T**	
			Försumbar skada	20	5E-05	**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 genom att minska sannolikhet för vådahändelse, minska sannolikhet för exponering eller förskjuta den procentuella fördelningen så att större andel av eventuella olyckor resulterar i mindre allvarliga skador.

Acceptansbeslut

Acceptansbeslut					
Åtgärd			Risk accepterad	Anmärkning (kan vara ref till beslutshandlingar eller övrig information)	STATUS
Beslut	Införd	Ver.			
Samtliga föreslagna åtgärder beslutas införas. Regler för vilka plan som får gå målflyg vid skjutning fastställda.	Ja,	Verifierings-rapport XXX. Instruktion XXX.	Ja 2015-01-01 Adam Bertilsson FMV		Stängd

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

Införd – Datum för införande.

Verifiering – Verifierad åtgärd samt referens till det dokument som dokumenterar verifieringen.

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 Anmärknings-kolumnen. Stängningen ska anges med datum, signatur, namnförtydligande och organisation. Det ska även framgå att en förutsättning för stängning är att åtgärder är verifierade.

Arbetet med risklogg

Riskloggen är ett arbetsdokument som gås 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 Försvarsmakten 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 Försvarsmakten och FMV.