Denna mall stöder metodbeskrivningen 'STAMP/STPA, Faktablad för Grundorsaks- & Riskkälleanalys mha STAMP-metoden, FMV-dokument 14910:44132/2007' (nedan kallad 'faktabladet').

Blå text har använts för instruktioner samt exempel.
Numrering i blått refererar till motsv. punkt i faktabladet.

Syftet med mallen är att vid enklare prov av STAMP/STPA kunna jämföra tekniken med övriga, klassiska systemsäkerhetsanalysmetoder, utan att behöva skaffa de specialverktyg som finns framtagna.

1 Analysförutsättningar

- Systemets omfattning:
- Analysens syfte:

2 Analysgrupp

Deltagarlista, datum

3 Ingångsmaterial

- Dokumentation över aktuellt system[1]:
- CIL[2]*:*
- Tidigare framtagna riskkällelistor för systemet:

4 Arbets- o mötesplan

Mötes-nr	**System-konfiguration**	**Analysobjekt**	**Datum**	**…**

5 Analysresultat

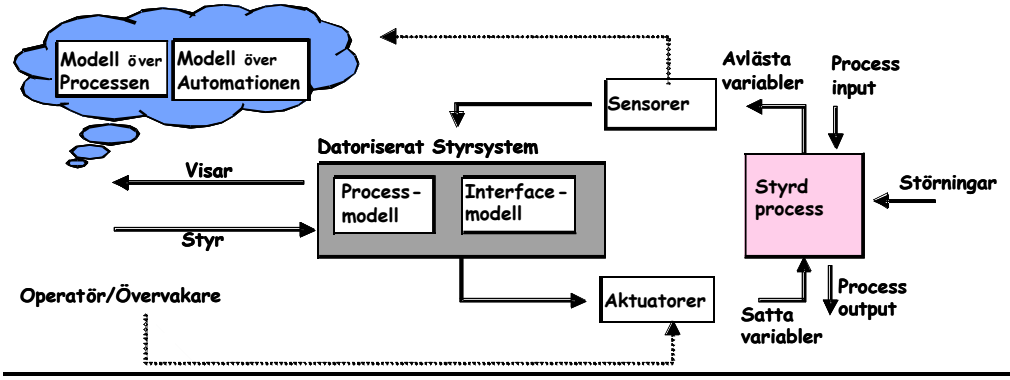
(1) **Generella krav:**
(1a) **Generella systemkrav** (toppnivå)**:**
(1b) **Systemomgivningsrestriktioner:**

(2) **Systemgraf[3]:**

Ersätt nedanstående principskiss över grundläggande styrmekanismer (basic control structure process model) med dito för aktuellt system.
Processmodellen skall avspegla
(a) Erforderliga relationer mellan processvariablerna
(b) Aktuell status (värden hos processvariablerna)
(c) Det sätt på vilket processen kan ändra status.

---

[1] *(Infoflöde mellan) Subsystem/komponenter/funktioner/driftspersonal samt grundläggande styrstrukturer inom o mellan det tekniska systemet, involverad personal o organisation. Operationell användning vid olika systemmod o omgivningar för angivna systemkonfigurationer.*
[2] *Critical Item List: en förteckning över kritiska systemelement (upprättad vid tidigare analys eller med annan analysmetod).*
3 *Systemet på toppnivå med ingående delar o grundläggande styrmekanismer (basic control loops). Detaljeras för underliggande nivåer allt eftersom systemdesignen fortskrider.*



(3) **Riskkälleanalys** (systemnivå) **:**

Löp-nr <*Hazard _id*>	**Analys-objekt** (system/ subsy-stem)	**System-konfi-gura-tion**	**System-mod/fas**	**Riskkälla** (3a) (4) <beskriv-ning>	**Orsak / Bidragande faktorer**[4] (3b)	**Konsekvens**	**Åtgärd =** Säkerhets-restriktion-er (3c,4)	**Kom-mentarer**
STPA-1	*ACC-systemet*	*Turbo-varianten*	*ACC **on: Brake/ Clutch***	*ACC bi-drar till att **bakom**lig-gande bil kör in i egen bil.*	*i) Kraftig in-bromsning ⇒ förkortad re-sponstid för bakomvarande förare ii)Fördröjd tändning av bromsljus iii)Trasiga bromsljus*	*Person-/ for-dons-/ omgiv-ningsskador*	*SC1, SC4, SC5, SC6*	*Itera-tion via pkt (4).*
			*ACC **on: Coast***	*Se ovan*		*Se ovan*	*SC2*	
			*ACC **on: Time gap+***	*Se ovan*		*Se ovan*	*SC3, SC7, SC8*	

Löp-nr <*Hazard _id*>	**Kritikalitet/ Allvarlig-hetsgrad**	**Felfrekvens/ Sannolikhet**	**Upptäckts-datum**	**Förslag till styrning**	**Verifiering**	**Status**[5]	**Slutlig struktur**

(3c) **Säkerhetsrestriktioner** (systemnivå)[6]**:**

Löp-nr	**Säkerhetsrestriktion** (3c)	**Motiveringar**[7]	**Antaganden/ Design-förutsättningar**[8]	**Motverkad riskkälla**
SC1	*ACC skall ge röst- o ljudvar-ning vid urkoppling.*	*Ger tydlig påminnelse till föra-re om att ACC kopplas ur vid inbromsning/ manuell växling*		*STPA-1, STPA-5, STPA-15*
SC2	*ACC-inbromsning skall ske mjukt.*	*Ger bakomliggande förare möjlighet att hinna reagera*		*STPA-1*
SC3	*ACC-genererat bromsnings-kommando skall vara högprio-*	*Begränsad bandvidd o hög buss-trafik får ej fördröja au-*		*STPA-1, STPA-6*

4 Causal factors/Asumptions: Beskrivning av situationer där/när riskkällan kan föreligga.
5 Öppen/Stängd.
6 SafetyConstraint (System Safety Design Constraint): Detaljer ang krav- o designrestriktioner i separat tabell bl a därför att en säkerhetsrestriktion kan vara motmedel till flera riskkällor.
7 Rationale: Förklaringar till på vilket sätt denna restriktion bemöter angiven riskkälla.
8 Antagande m a p systemets design, omgivning, operation, drift, administrativa föreskrifter/rutiner/strukturer.Vid varje förändring omprövas dessa antanganden. Om något av dessa visar sig inadekvat, kan utformningen av dessa faktorer behöva modifieras.

	riterat på CAN-busen.	*tomatisk inbromsning eller signal att tända bromsljus*		

(5a) **Processmodell** (komponentnivå):

<graf med styrande o styrda komponenter: en detaljering av den övergripande systemgrafen enl punkt (2)>

(5b-c, 6) **Säkerhetsrestriktioner** (komponentnivå)**:**

Kom-po-nent_id	**Komponent-krav/ -åtagande**[9] (5b) <beskrivning>	**Säkerhets-restriktio-ner** (5c)	**Styr-meka-nism**[10] (6), (6b1)	**Identifierade brister**[11] (6a), (6b2), (6b4)	**Bidragande faktorer** (6b)	**Åtgärd:** ref till risklind-ring & styr-mekanism i utökad pro-cessmodell (6b3)
Kompo-nent_1	*1. xxx* *2. yyy*	*SC1.1:<text>* *SC2.1:<text>* *SC3.1:<text>*	*Styrflöde_1: Uppgift* *Feed-back-flöde_1: Återmatad info* *Styrflöde_2: Uppgift* *Feed-back-flöde_2: Återmatad info*	*(6a1_i): …* *(6a1_ii): Osäkert då bromsljus ej av-speglar bromsmod* *(6a1_iii): …* *(6a1_iv): …* *(6a1_v): …* *(6a2_i): …* *(6a2_ii): …* *(6a2_iii): …* *(6a2_iv):För sent vid fartminskning före bromsljus.*	*Halka* *Hinder framför ACC-bil*	*<dvs utöka med nya sä-kerhetsre-striktioner i (5c)>*

6 Referenser

[1] …
[2] …

7 Dokumenthistorik

Mellanliggande versioner ligger som dold text.

Version	Datum	Beskrivning
1.0	07-10-10	Första mallutkast
1.1	07-10-23	Ensning mot ’STAMP/STPA, Faktablad för Grundorsaks- & Riskkälleanalys mha STAMP-metoden, FMV-dokument 14910:44132/2007, version 1.1’
1.2	08-02-13	Rättning av huvud för sid>1. Tillägg (fotnot 8-9).

9 Exempel: För komponent=operatör beskrivs 1) Organisationens förberedelser av rollinnehavare: Anställningsförutsättningar, introduktioner, 2)Rollens ansvarsåtaganden:Ålagda uppgifter under normala omständigheter, 3) Rollens befogenheter: Föreskrivna säkerhetsåtgärder i risksituationer, 4)Skyldigheter i förhållande till övriga nivåer i organisationshierarkien. Jfr faktabladets ref [8]: Fig 5.

10 Control action: Namngivna styrflöden med riktning (förslagsvis <Source> to <Destination_1> to <Destination_2> to <Destination_3>, t ex ’Styrmodul Bromsar’ till ’Bromsljus’ till ’Bakomliggande bil’ till ’Förare’ til ’Accelerator’) efterföljt av text beskrivande flödets uppgift (t ex ’Signalöverföring för tändning av bromsljus som varning till bakomvarande förare’)

11 Inadequate/hazardous control action:Fyll i identifierade brister enl punkt 6a i faktabladet.