Försvarets Materielverk (FMV)
Handbook for Software in Safety Critical Applications
Part I, The Challenge

The System Safety Group

Svante Wåhlin

Örjan Hellgren **Lars Lange**

…plus part-time colleagues and consultants…

- Rules, regulations
- Courses/education/information
- Handbooks
- (Project support - consultants)

Background - regulations

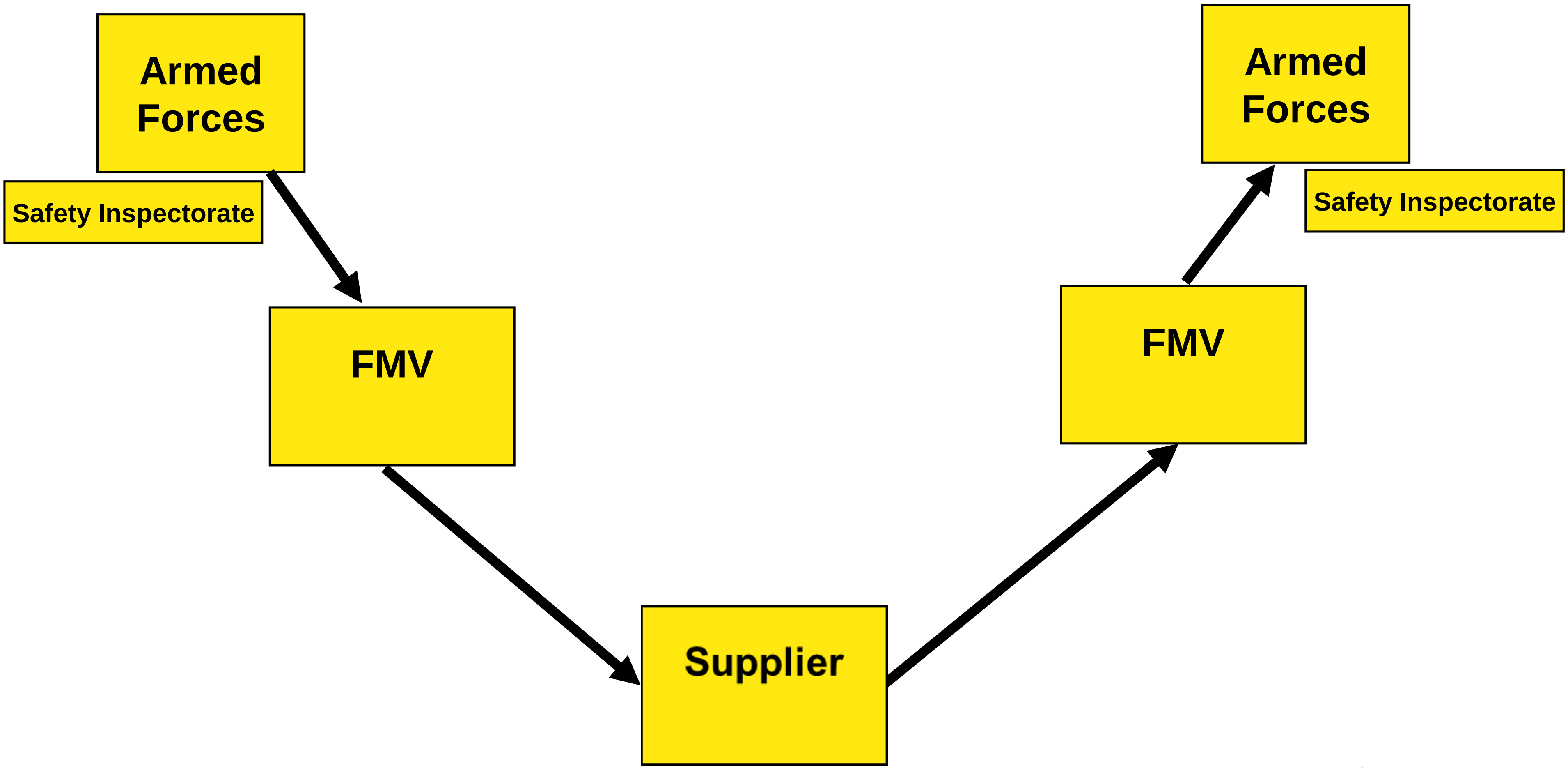
- Accidents
- Safety Legislation
  - Occupational Safety and Health Act (all systems)
  - Flammable and Dangerous Goods Act (ammunition)
  - Others…
- FM – FMV Coordination Agreement
- FMV Internal rules and regulations
- Manuals, Handbooks, templates, checklists *(designregelsamlingar)*
- Standards (Swedish FSD => STANAGS, MIL-STDs, Def-Stans, Civilian standards

Prioritations in order of effect

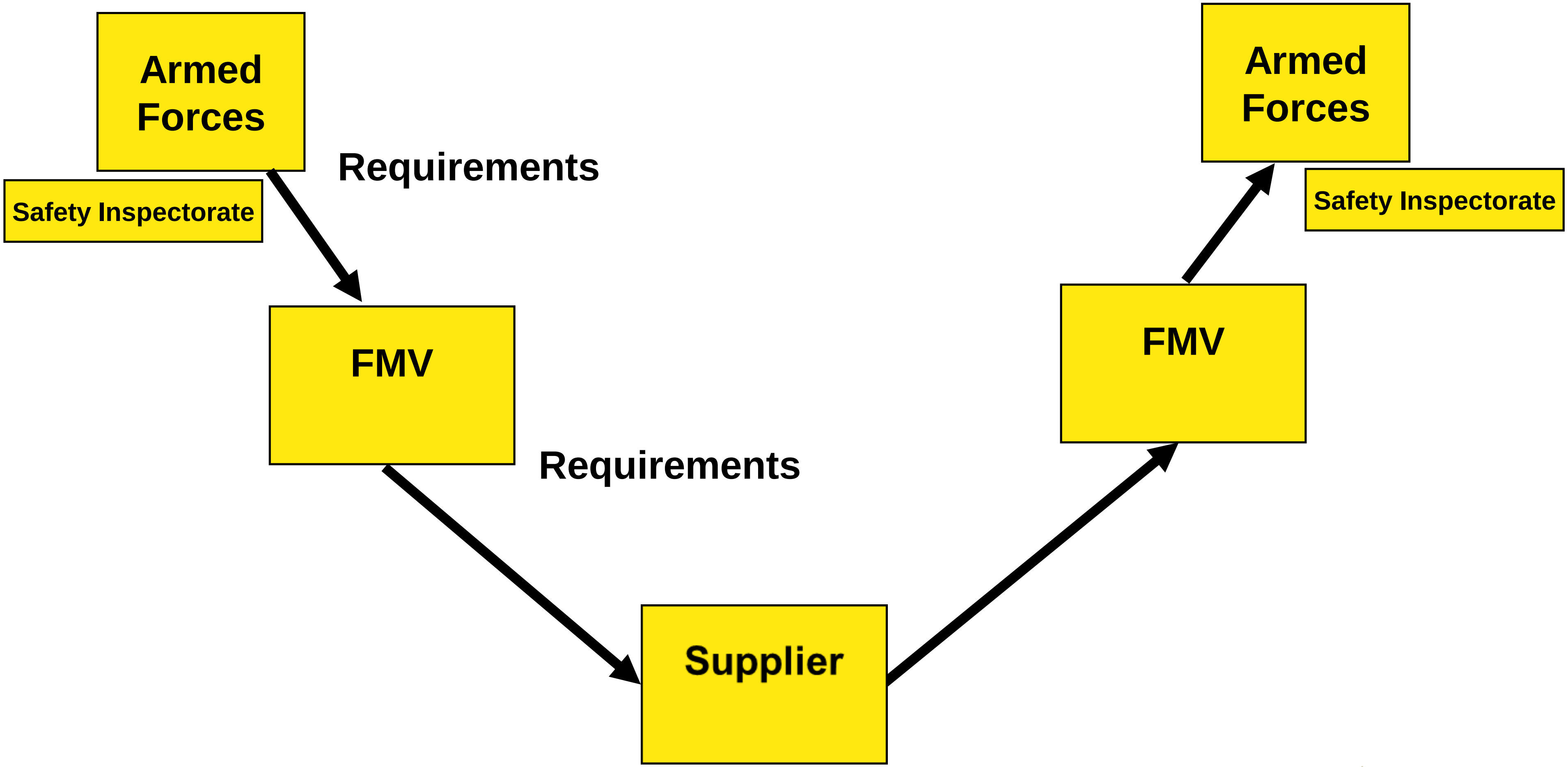
- **Eliminate hazards**
- **Safer construction**
- **Protection**
- **Warnings**
- **Personal protective gear**
- **Instruktions / signs**

- ***Education***

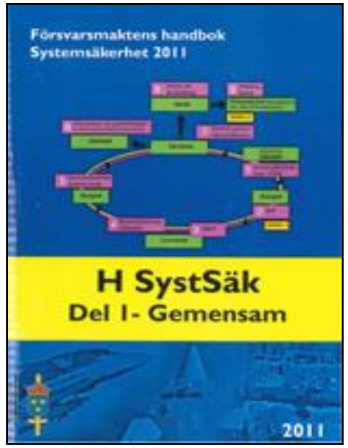
Actors, Role-play

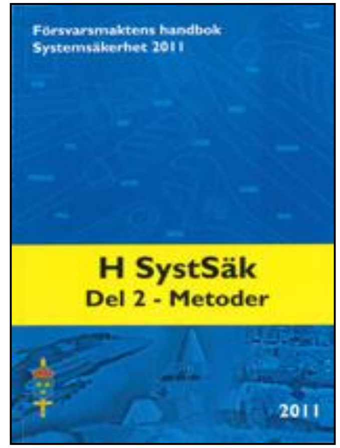


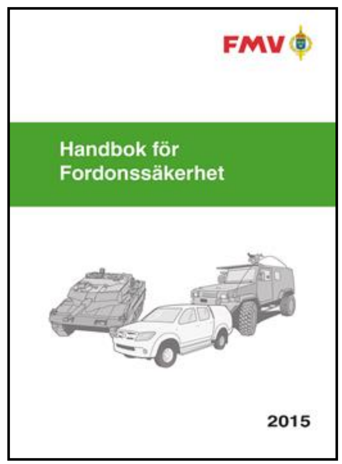
Actors, Role-play

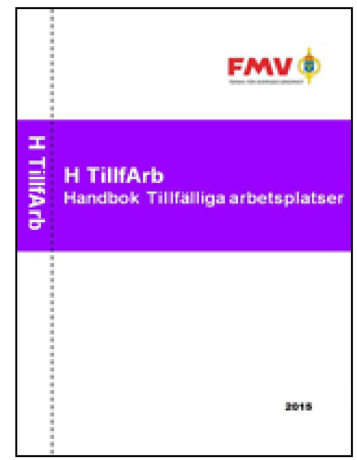


Handbooks / manuals









Our courses

- Systems Safety

  4-6 times / year, three days
- Weapons and ammunition Safety

  1 (- 2) times / year, three days
- Vehicular Safety

  2 (-3) times / year, three days
- **Software Safety**

  1 (- 2) times / year, Stockholm, one day (two?)
- FMV Electrical products and systems

  2 (- 3) times / year, Stockholm, one day

Kontakt: sakerhetskurser.fmv@fmv.se

Info: Svante Wåhlin: svante.wahlin@fmv.se

Handbook for Software in Safety Critical Applications

Björn Koberstein

= 1980 - 1997 at Saab Aircraft Linköping

37 Viggen, Saab 340, 39 Gripen

= 1997 -> FMV

39 Gripen, Helicopter NH90 / HKP14

Handbook for Software in Safety Critical Applications

Table of Content

= About FMV
= Exemples
= The challenge of procuring software
= The software growth (explosion)
= Software ”maintenance” in long lived systems
= Software cost versus functional growth

Handbook for Software in Safety Critical Applications

Försvarets Materielverk FMV = Swedish Defence Materiel Administration

Procures military materiel for the Swedish Armed Forces since 1630.
As a result of the loss of HMS Wasa 1628, it was decided that the King could not handle this himself, so the Government Administration called ”Kungliga Krigskollegium” was created, the predesessor of todays FMV.

Handbook for Software in Safety Critical Applications

Some of the material FMV buy for the Swedish Defence Force…

This presentation is mainly about software for aircrafts, but the reasoning will apply to other types of systems.

FMV

Handbook for Software in Safety Critical Applications

Software Failure
EXEMPLE 1

www.defenseindustrydaily.com

While attempting its first overseas deployment to the Kadena Air Base in Okinawa, Japan, on 11 February 2007, six F-22s flying from Hickham AFB, Hawaii, experienced multiple computer failures while crossing the International Date Line (or 180^{th} meridian of longitude dependent on software programming).
The failures included navigation and communication.

The fighters were able to return to Hawaii by following a tanker aircraft.

Within 48 hours, the error was resolved and the journey resumed

Handbook for Software in Safety Critical Applications

Software Failure
Exemple 2

Norwegian C-130 Hercules crashes on mars 15, 2012 at Kebnekaise, Sweden.

C-130J is a four engine military transport aircraft for passenger and cargo.

Handbook for Software in Safety Critical Applications

Software Failure Exemple 2

Fig 4: Kartbild över Skandinavien. I det rödmarkerade området har TAWS i läge Tactical *ingen terrängvarningsfunktion. Haveriplatsen är markerad med en röd stjärna.*

Handbook for Software in Safety Critical Applications

The Challenge

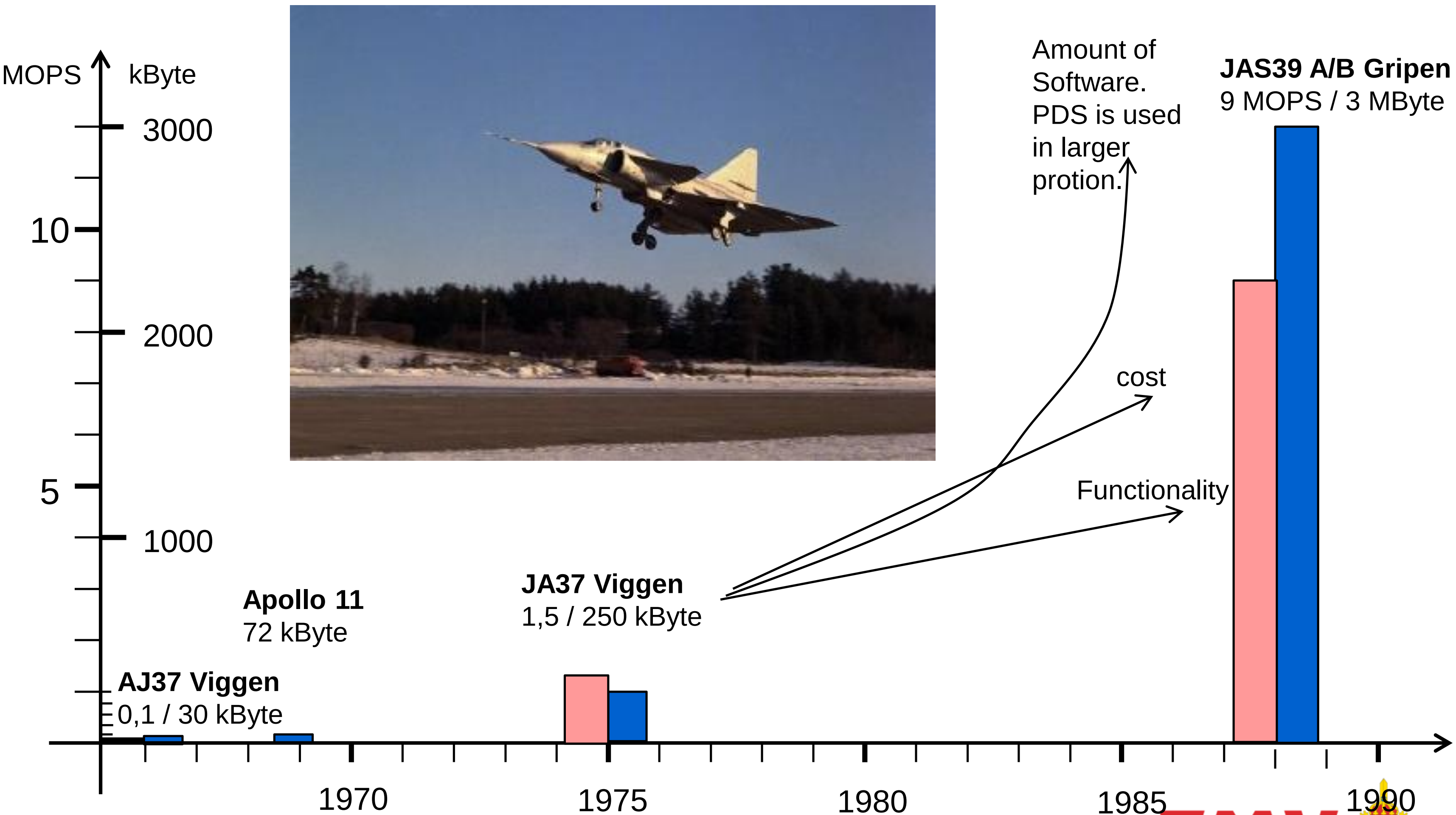
According to Swedish Defence Force System Safety Handbook, Safety includes:

Protect	Branch	Consequense	Complexity			System Lifecycle
Person (1-3)	Army	Catastrophic	System of system	War	Operation	Procure
Property	Air Force	Critical	Plattform	Crisis	Exercise	Operation
Environment	Navy	Marginal	Unit	Peace	Training	Maintenance
	Command & Control	Negligible	Software			Decommission
		No Effect				

Handbook for Software in Safety Critical Applications

Software development in military aircraft and space

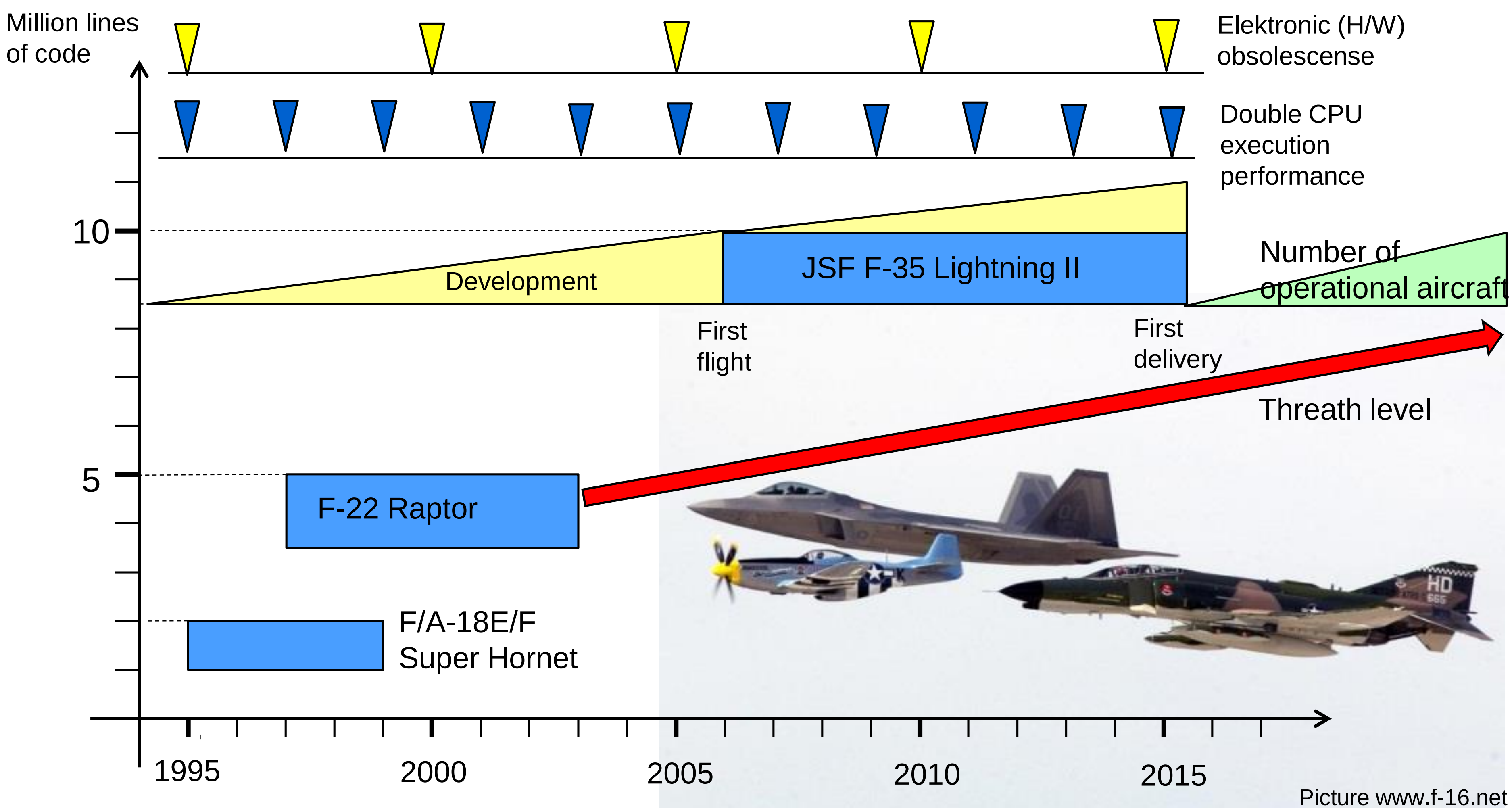
MOPS = Miljoner operationer per second



Handbook for Software in Safety Critical Applications

P-51 Mustang: 15 586
F-4 Phantom II : 5195
F-22 Raptor: 187

Software development during design phase

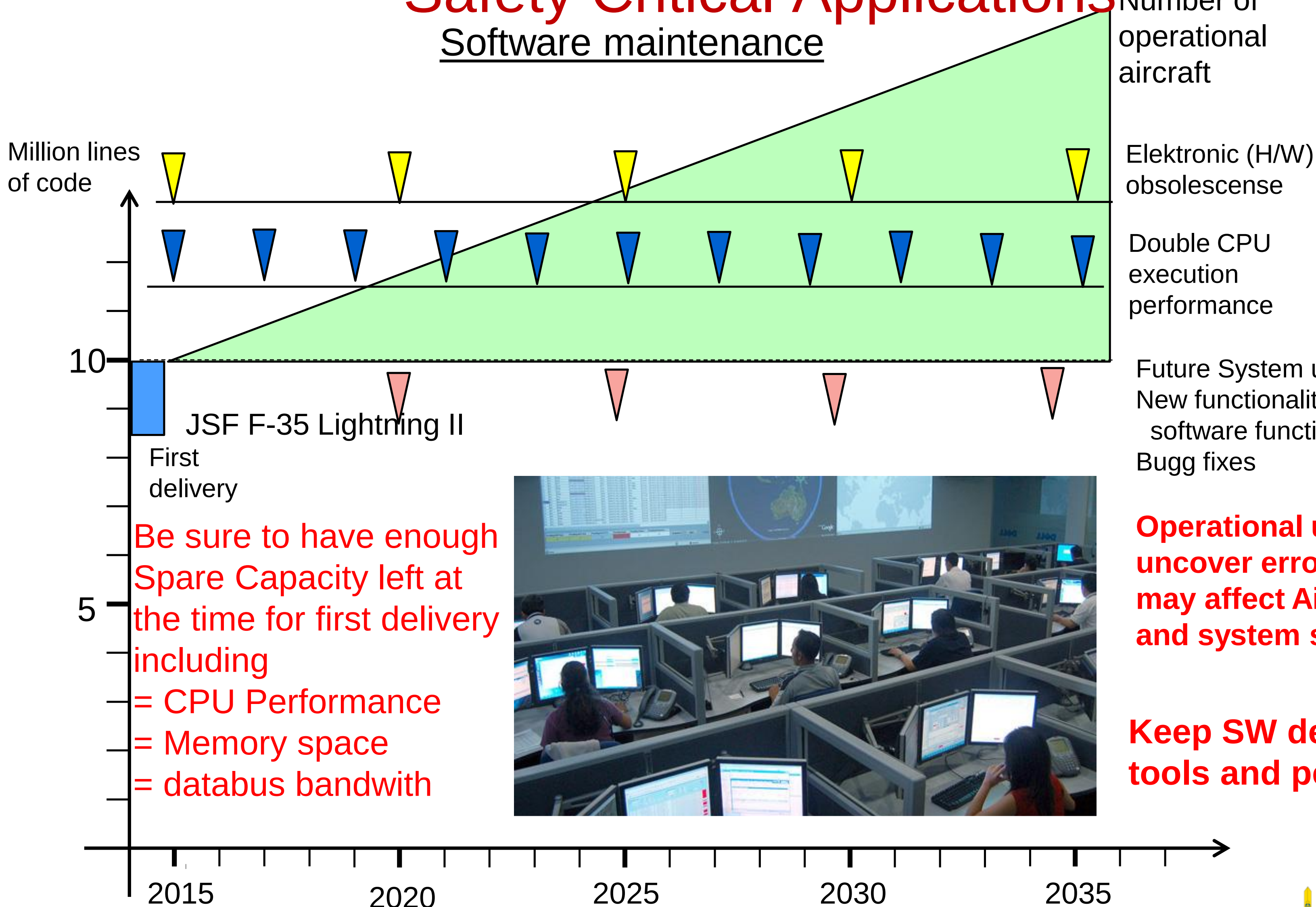


Picture www.f-16.net

FMV

Handbook for Software in Safety Critical Applications

Software maintenance



Be sure to have enough Spare Capacity left at the time for first delivery including
= CPU Performance
= Memory space
= databus bandwith

Operational use may uncover errors that may affect Air worthiness and system safety!

Keep SW development tools and people!(?)

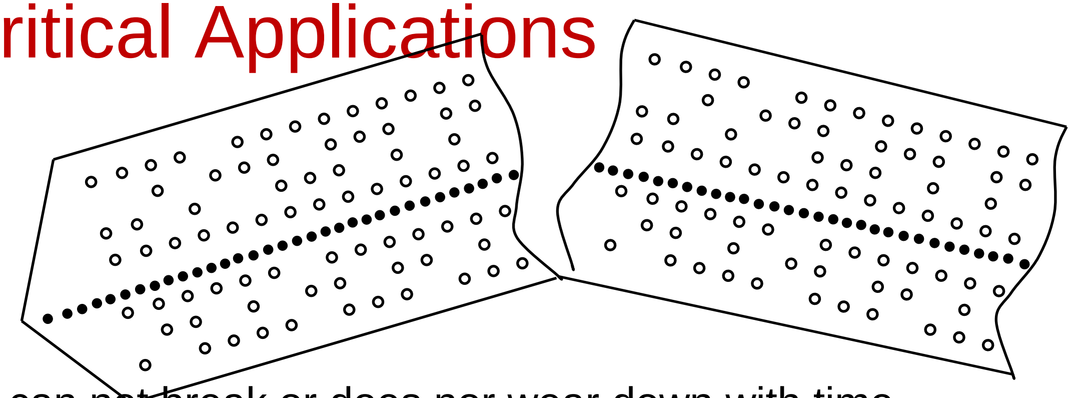
Handbook for Software in Safety Critical Applications

<u>Definition of Safety Critical Computer system</u>

A Computer system that controlls, indirect controls or monitors energy that due to a fault, could cause damage to a person, to the environment or to property.

Ett datorsystem som styr eller indirekt styr eller övervakar energier som vid ett okontrollerat förlopp kan orsaka en vådahändelse

Handbook for Software in Safety Critical Applications



Software:

- Has no weight (weightless)

- Software can take unwanted actions, but can not break or does nor wear down with time.
 Computer memory can unintentional change content.
 To make a memory checksum of the memory / data may be needed to check for unintended data change.

- All software errors are introduced during development process. Eitherfrom the specification or from the coding. This makes all software errors (buggs) systematic, not random.

- There is no way to predict how or when a software will do an unvanted action (Frequency). It is possibel to designate the worst case criticality level. This will affect the Risk assessment:
 Risk = Consequens x Frequens.

- The criticality of the software is determind by the systems where it resides.

- That part of a software, that is developed to the lowest criticality level determinds the hole software criticality level in that particular software / computer.

Handbook for Software in Safety Critical Applications

AIRWOTHINESS
(Supplier)

Airworthiness (Supplier)	Seaworthiness (Supplier)	Traffic / ”ground” worthiness (Supplier)
Is the ability of an aircraft or other airborne equipment or system to be operated in flight and on the ground without significant hazard to aircrew, ground crew, passengers or third parties. It is a technical **attribute of Materiel** throughout its lifecycle.		

Handbook for Software in Safety Critical Applications

FLIGHT SAFETY (FMV)

Flight Safety (FMV)

Is the state of freedom from unacceptable risk of injury to persons or damage throughout the lifecycle of military air systems.

Air Traffic Control

Runway

Pilot

Weather

Fuel

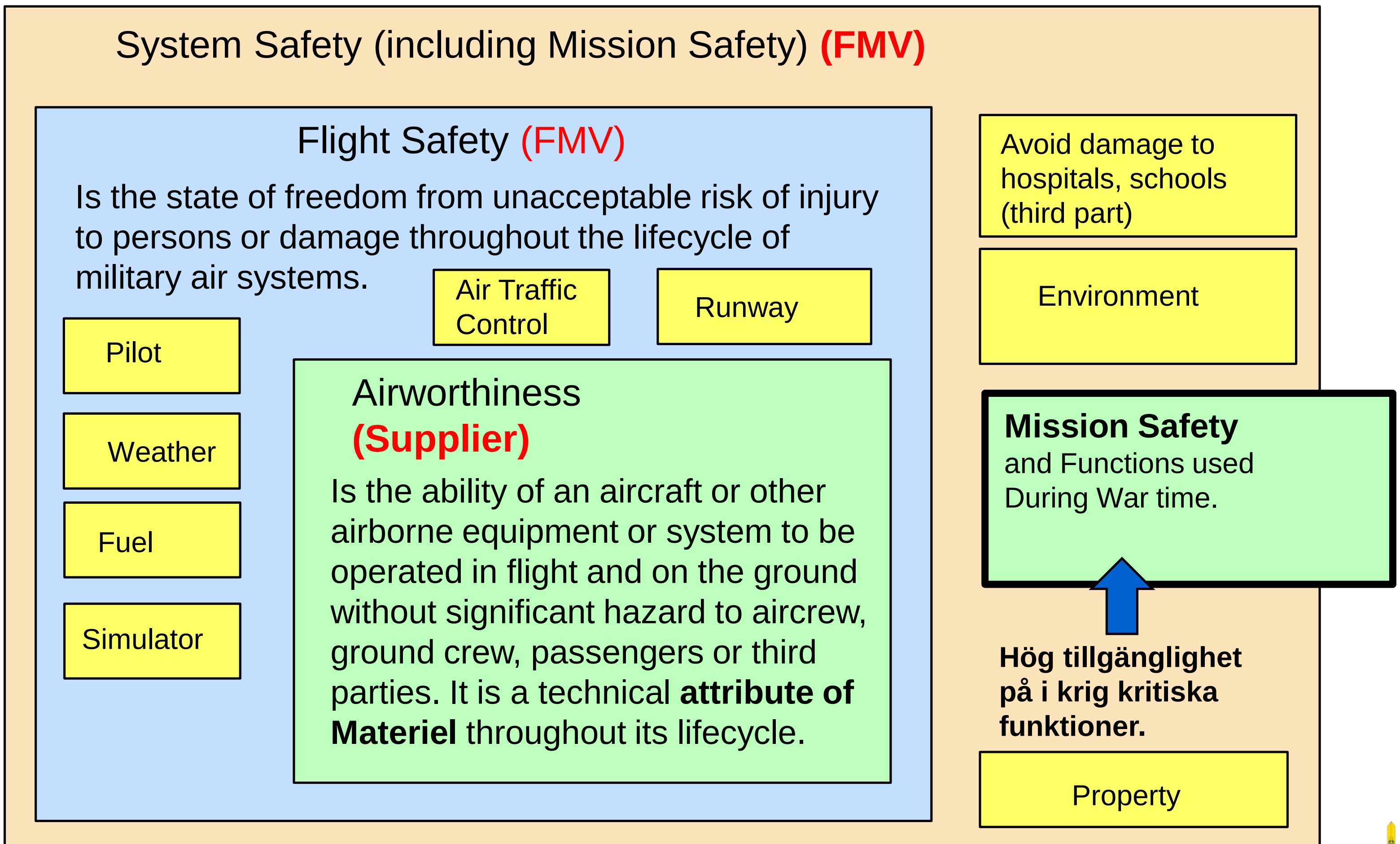
Simulator

Airworthiness
(Supplier)

Is the ability of an aircraft or other airborne equipment or system to be operated in flight and on the ground without significant hazard to aircrew, ground crew, passengers or third parties. It is a technical **attribute of Materiel** throughout its lifecycle.

Handbook for Software in Safety Critical Applications

SYSTEM SAFETY (FMV)



Handbook for Software in Safety Critical Applications

Operational Safety **(Defence Force)**

System Safety (including Mission Safety) **(FMV)**

Flight Safety (FMV)

Is the state of freedom from unacceptable risk of injury to persons or damage throughout the lifecycle of military air systems.

- Air Traffic Control
- Runway
- Pilot
- Weather
- Fuel
- Simulator

Airworthiness **(Supplier)**

Is the ability of an aircraft or other airborne equipment or system to be operated in flight and on the ground without significant hazard to aircrew, ground crew, passengers or third parties. It is a technical **attribute of Materiel** throughout its lifecycle.

- Avoid damage to hospitals, schools (third part)
- Environment

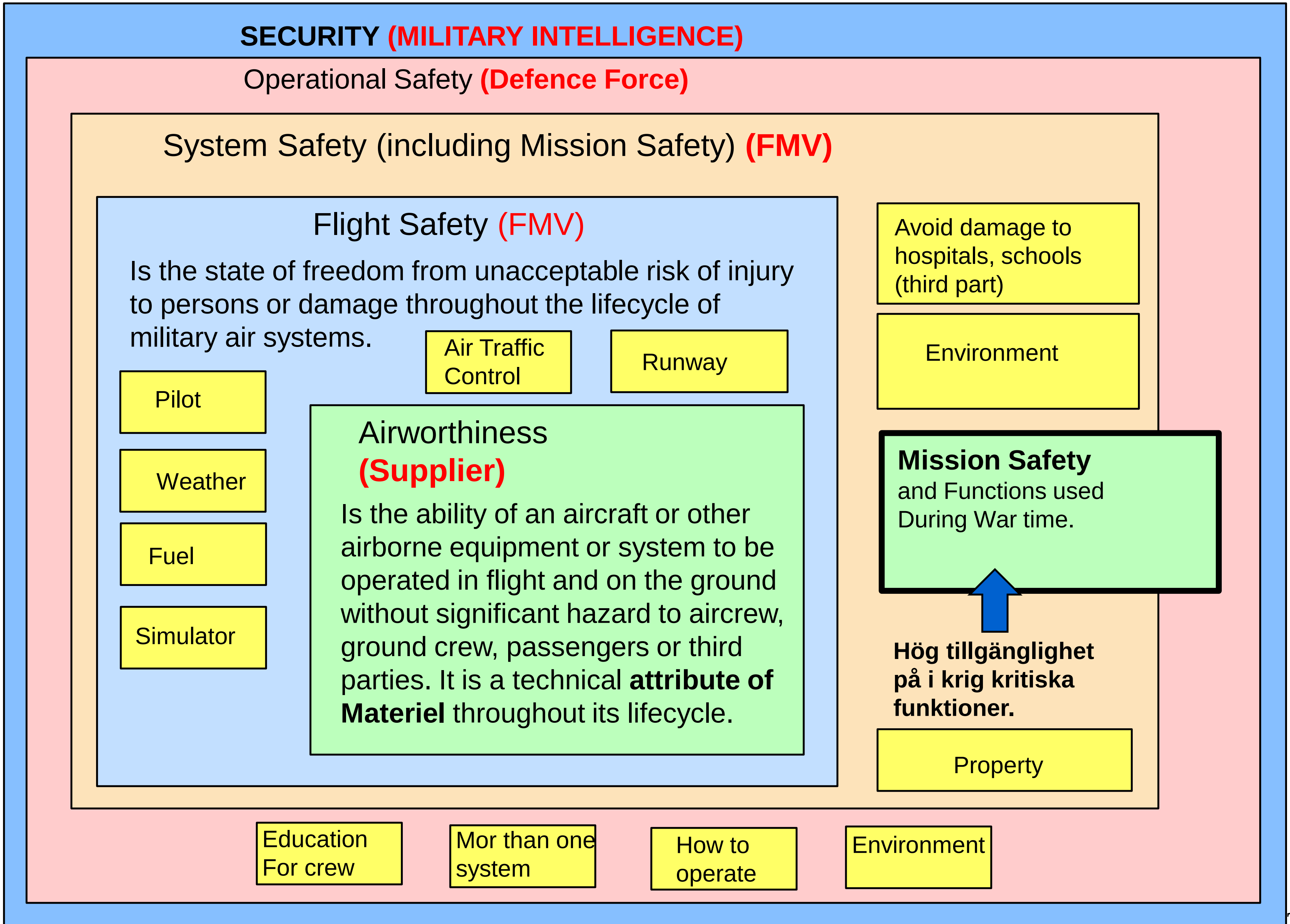
Mission Safety
and Functions used
During War time.

Hög tillgänglighet på i krig kritiska funktioner.

- Property

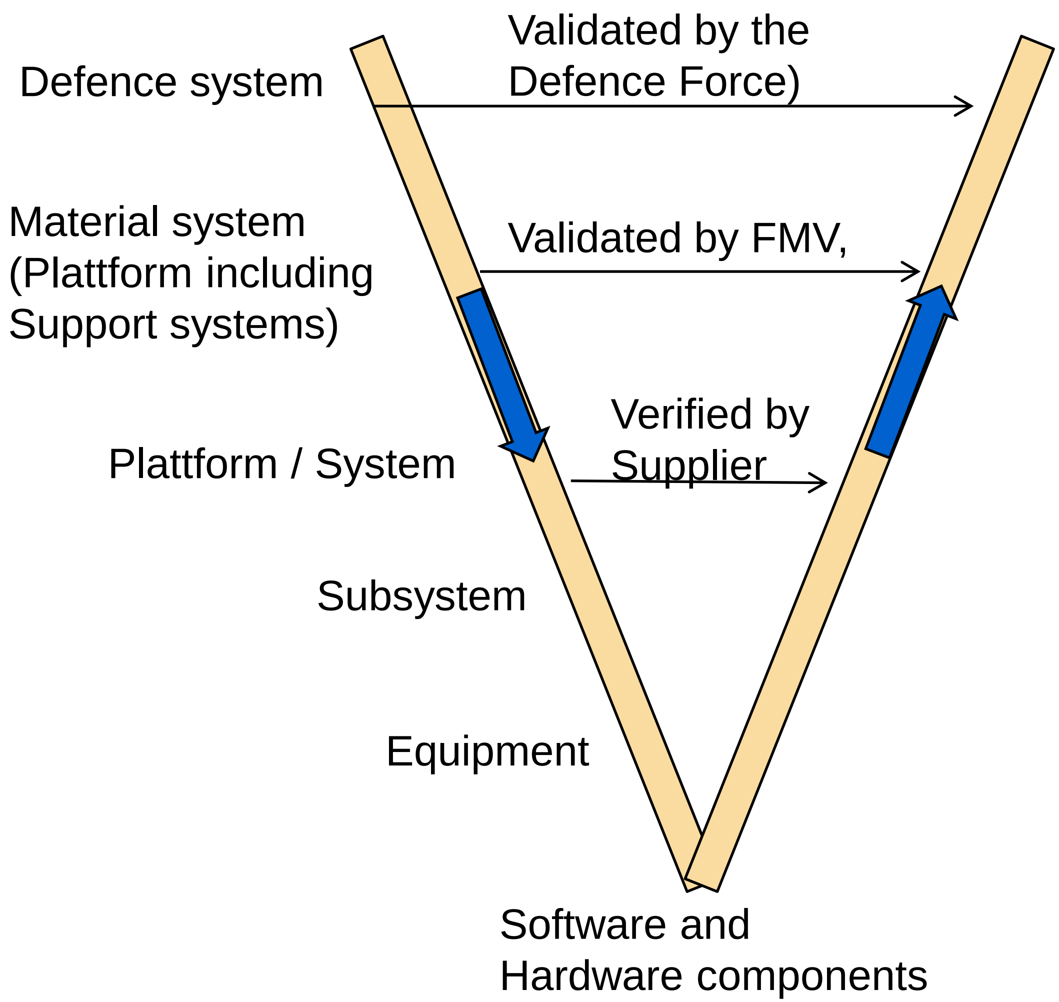
- Education For crew
- Mor than one system
- How to operate
- Environment

Handbook for Software in Safety Critical Applications

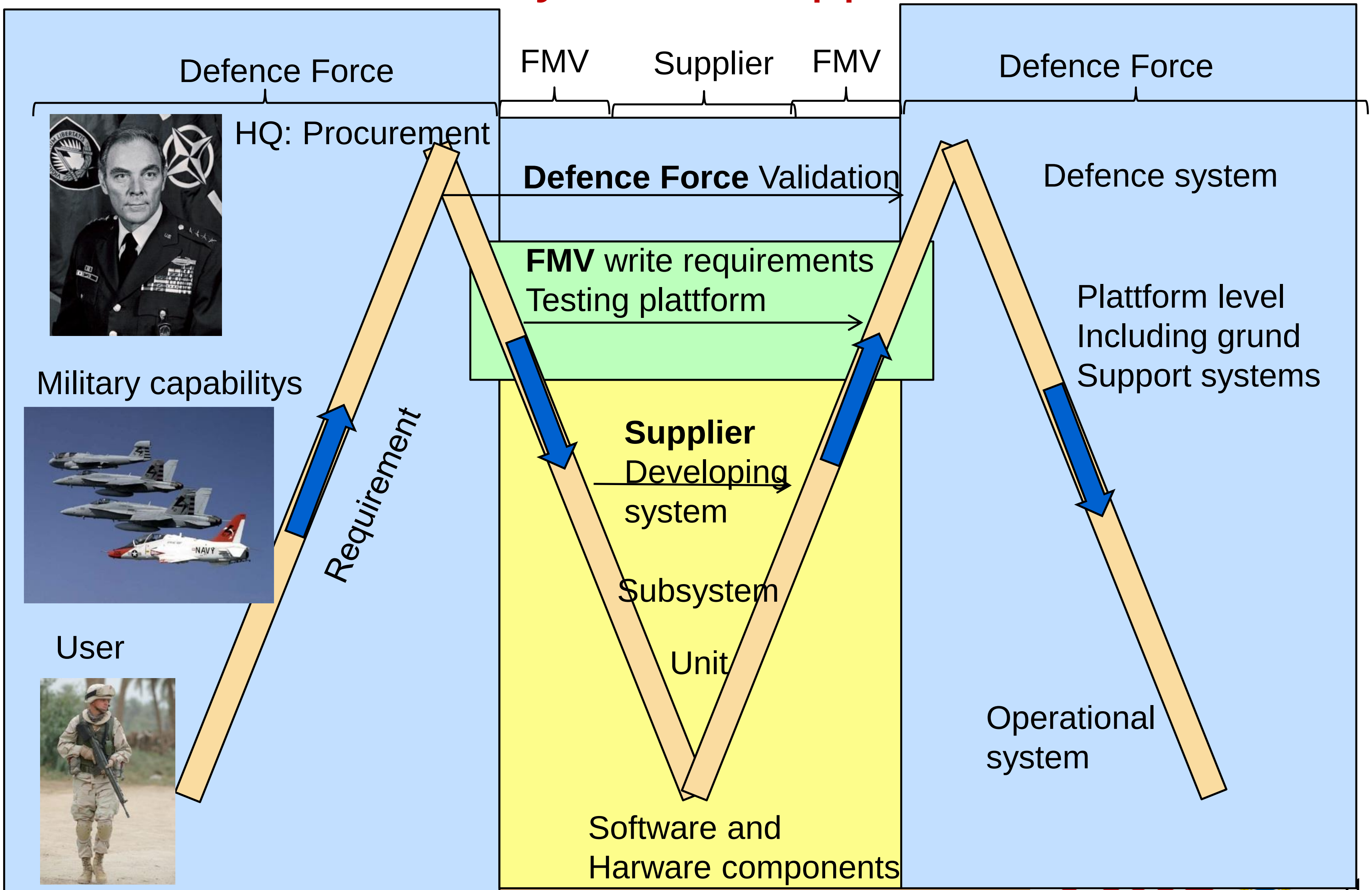


Handbook for Software in Safety Critical Applications

Systemdevelopment ackoring to the V-modell / The waterfall method



Handbook for Software in Safety Critical Applications



Handbook for Software in Safety Critical Applications

Different countries has different background and view on Hazards, criticality and risk. This is a challenge when operating together.

Handbook for Software in Safety Critical Applications

Difficulty to work together when systems / plattforms from different arenas operate together (airplanes / ships / groundbased). Different safety standards and requirements.

Handbook for Software in Safety Critical Applications

The orientation / environment of the Swedish Defence Force

= Cold War

From WWII until the fall of Berlin Wall / The Iron curtain
Safety not very high priority
Swedish made systems

= International operations, ”The War on Terror”

The Defence Force cut down 90 – 95%
Bosnia, Afghanistan, Op Atalanta, Mali…
NATO led => NATO compatibility
Safety more priority

= Defence of Sweden

Russian aggression Georgia, invasion of Krim,…
NATO compability continues
Safety high priority and more ”organized”

Handbook for Software in Safety Critical Applications

<u>Exposure + Hazardous event => Accident</u>

The Defence Force knows in what environment and how the system is intended to be used. They have the requirements on SAFETY on the system, and this is an input to the Safety work at FMV and at the supplier.

<u>Exposure</u>

<u>Accident</u>

The number of accidents Depends on how and in what Environment the system Is used. (FMV)

<u>Hazardous event</u>

The Supplier can / shall predict the reliability Of the delivered system. ”How often will a System fail and create a Hazardouz event.

Handbook for Software in Safety Critical Applications

Questions?

Försvarets Materielverk (FMV)
Handbook for Software in Safety Critical Applications
Part 2, The Handbook

Björn Koberstein
= 1980 - 1997 at Saab Aircraft Linköping
37 Viggen, Saab 340, 39 Gripen
= 1997 -> FMV
39 Gripen, Helicopter NH90 / HKP14

Handbook for Software in Safety Critical Applications

MIL-STD-882E
(USA DoD)

↓

System Safety Handbook
(Defence Force)

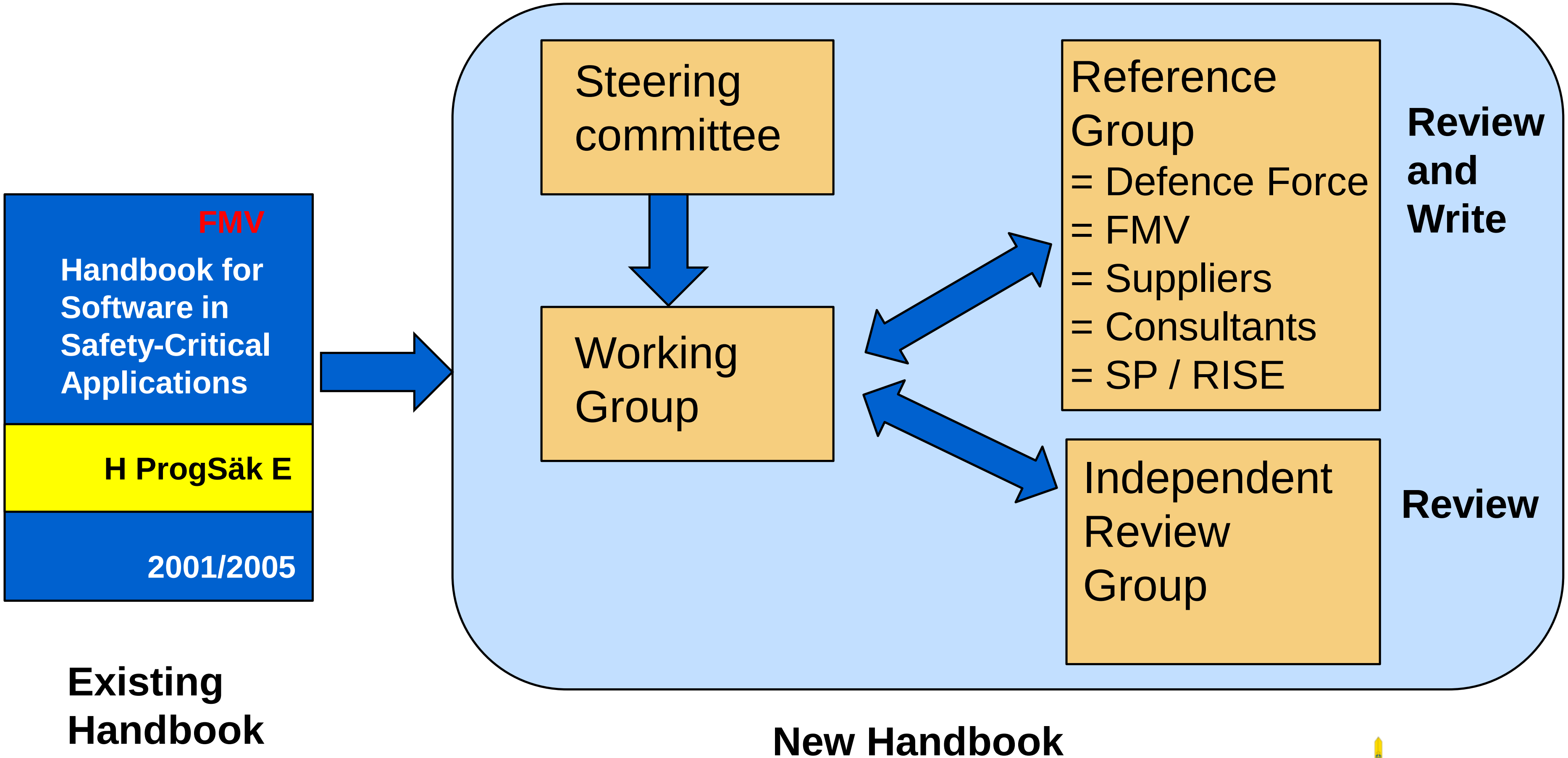
↓

Software for Safety Critical Systems Handbook
(FMV)

FMV

Handbook for Software in Safety Critical Applications

FMV Safety handbooks can be downloaded from www.fmv.se
FMV has several seminars on Safety, including safety critical software.
(RISE = Research Institute of Sweden, SP Borås)



Handbook for Software in Safety Critical Applications

There is no Standard for writing a Safety Standard.

= Different number of criticality levels (3 – 6 levels)
= The Levels have different designation
and same designation can have different meaning

IEC 62061	SIL 1 – SIL 3
EN 50128	SIL 0 – SIL 4
RTCA/DO-178C	Level E – Level A

= Words have different meaning i different standards
Hazard, fault, error, failure…
= Standard cover different areas: Railway, vehicles, machinery…
= Standard for protecting: people, environment, Property…

Handbook for Software in System Critical Applications

The Challenge / The Scope

According to Swedish Defence Force System Safety Handbook, Safety includes:

Protect	Branch	Consequense	Complexity			System Lifecycle
Person (1-3)	Army	Catastrophic	System of system	War	Operation	Procure
Property	Air Force	Critical	Plattform	Crisis	Exercise	Operation
Environment	Navy	Marginal	Equipment	Peace	Training	Maintenance
	Command & Control	Negligible	Software			Decommission
		No Effect				

Handbook for Software in Safety Critical Applications

The Scope of the Handbook for Safety Critical Software

1 Scope of the Handbook
2 Law's and standards
3 Workflow between The Defence Force, FMV and the supplier
4 Safety critical architecture and methodology
5 The life cycle, Quality Management and Configuration Control of the software
6 Expectation from the Defence Force
7 The requirements on FMV
8 The requirements on the Supplier
9 Requirement on Documentation
10 CE marked/cerified equipment and equipment certified by third party
11 Perviously Developed Software (PDS)
12 Methodology and techniques

Handbook for Software in Safety Critical Applications

The handbook assumes that it is not possible to predict how often or when a software will fail.

This since all software errors are Systematic, not Random.

Only the consequence of a Software Error can be predicted.

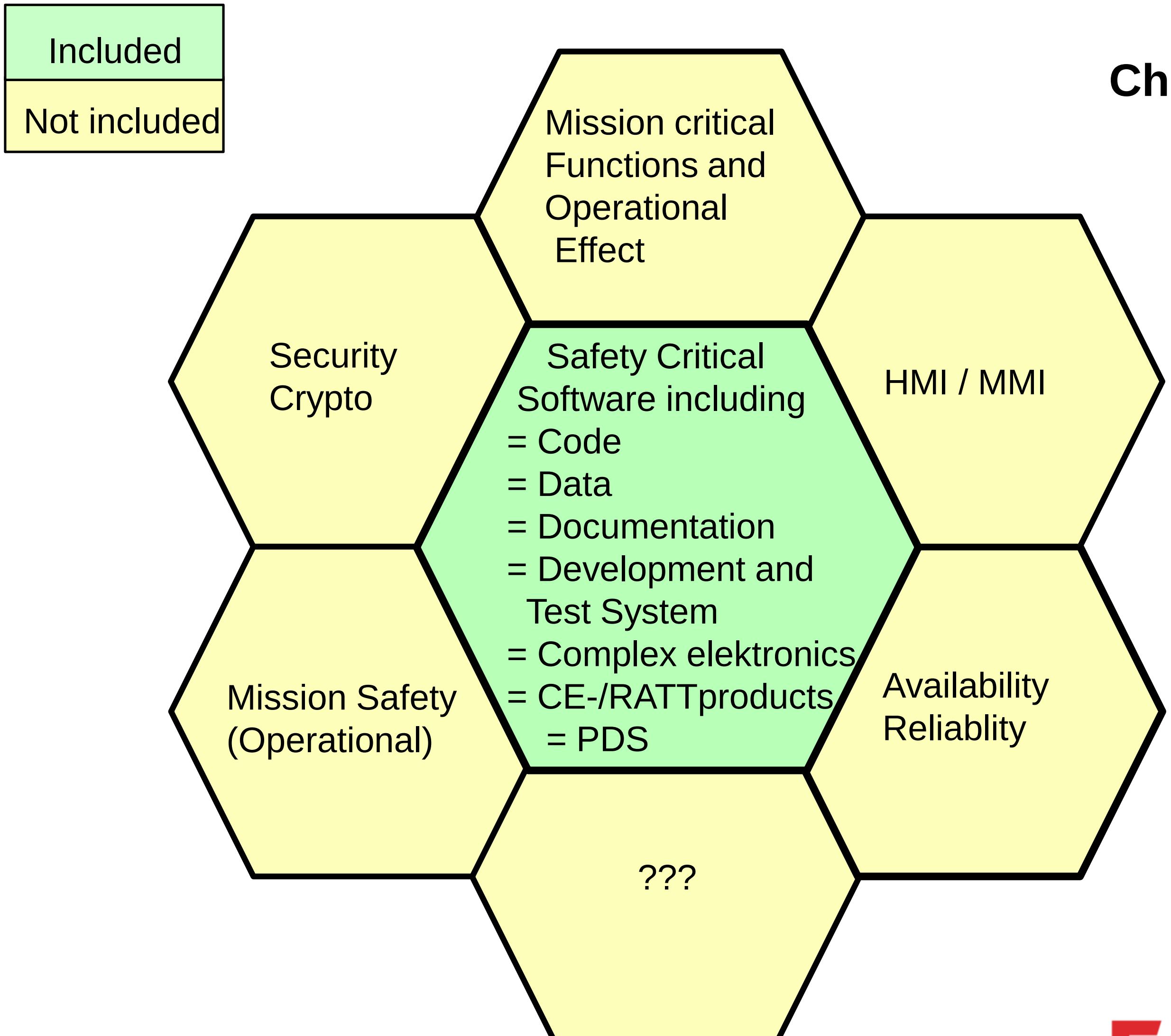
Handbook for Software in Safety Critical Applications

The goal of the handbook is to Encourage to use as little critical Software as possible. Non if possible!

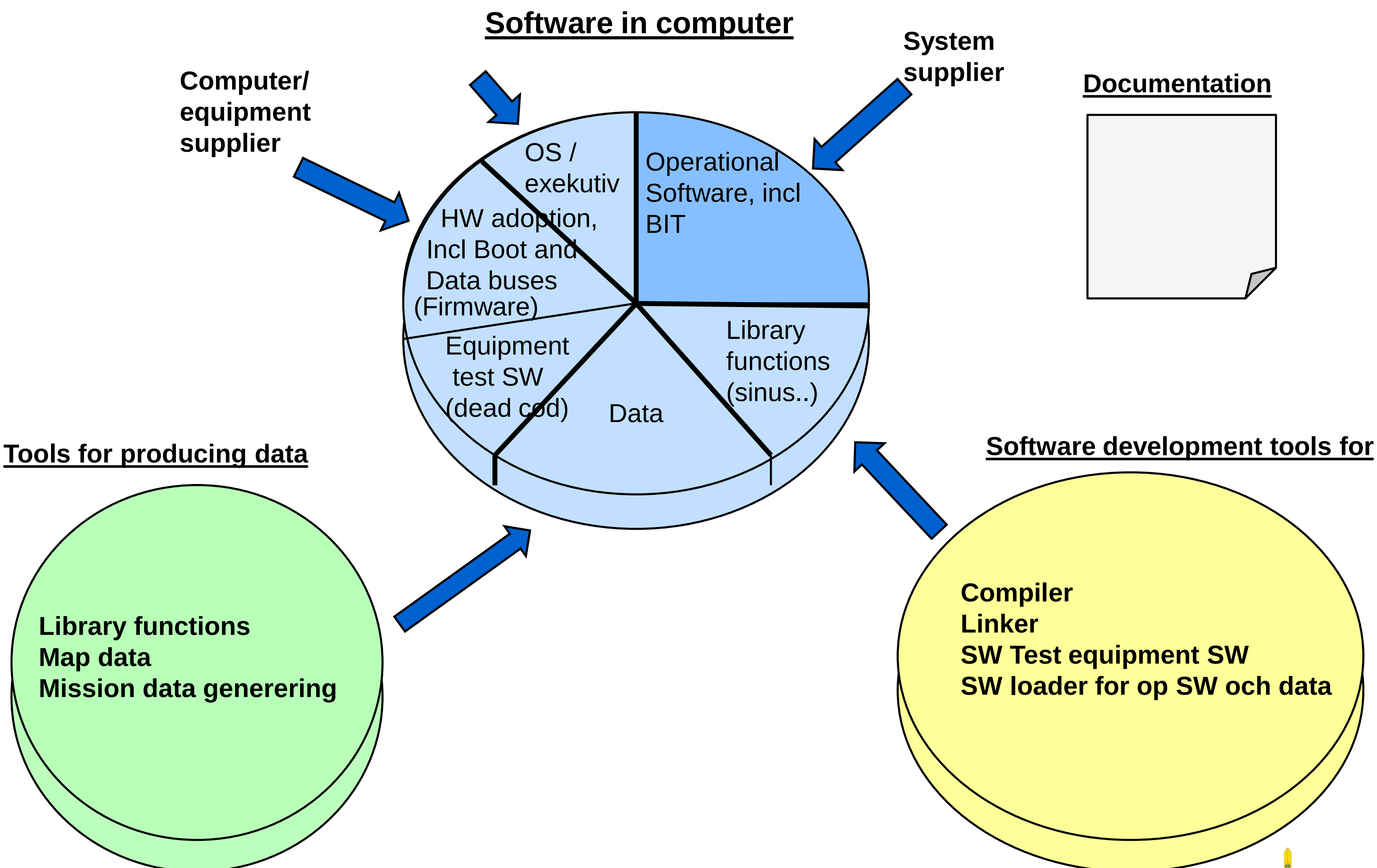
Develop the system with as low criticality as possible.

Handbook for Software in Safety Critical Applications

Chapter 1

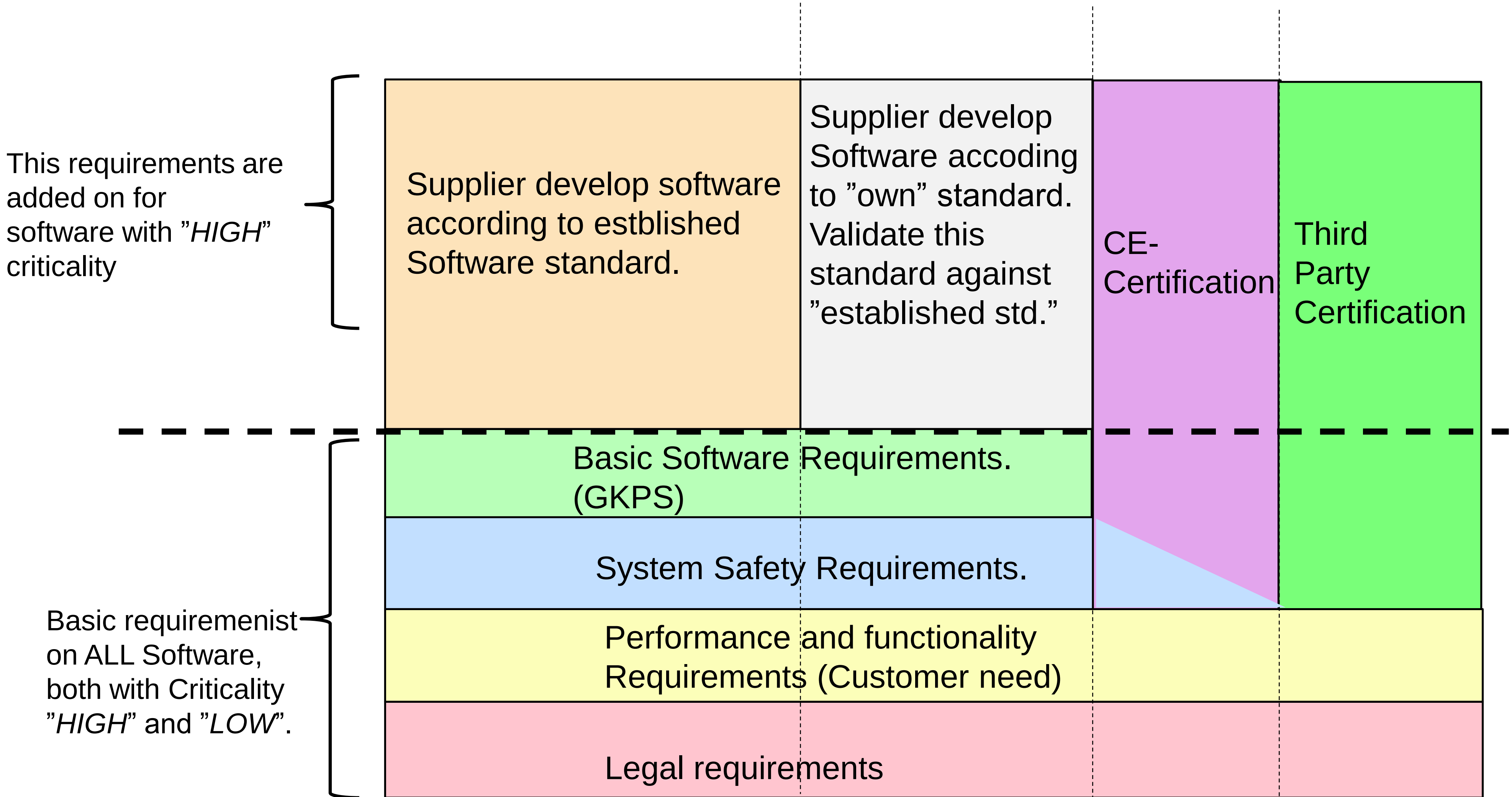


Handbook for Software in Safety Critical Applications



Handbook for Software in Safety Critical Applications

Chapter 2



Handbook for Software in Safety Critical Applications

Chapter 6

The Swedish Armed Forces

Accident (FM)

&

Exposure (FM)

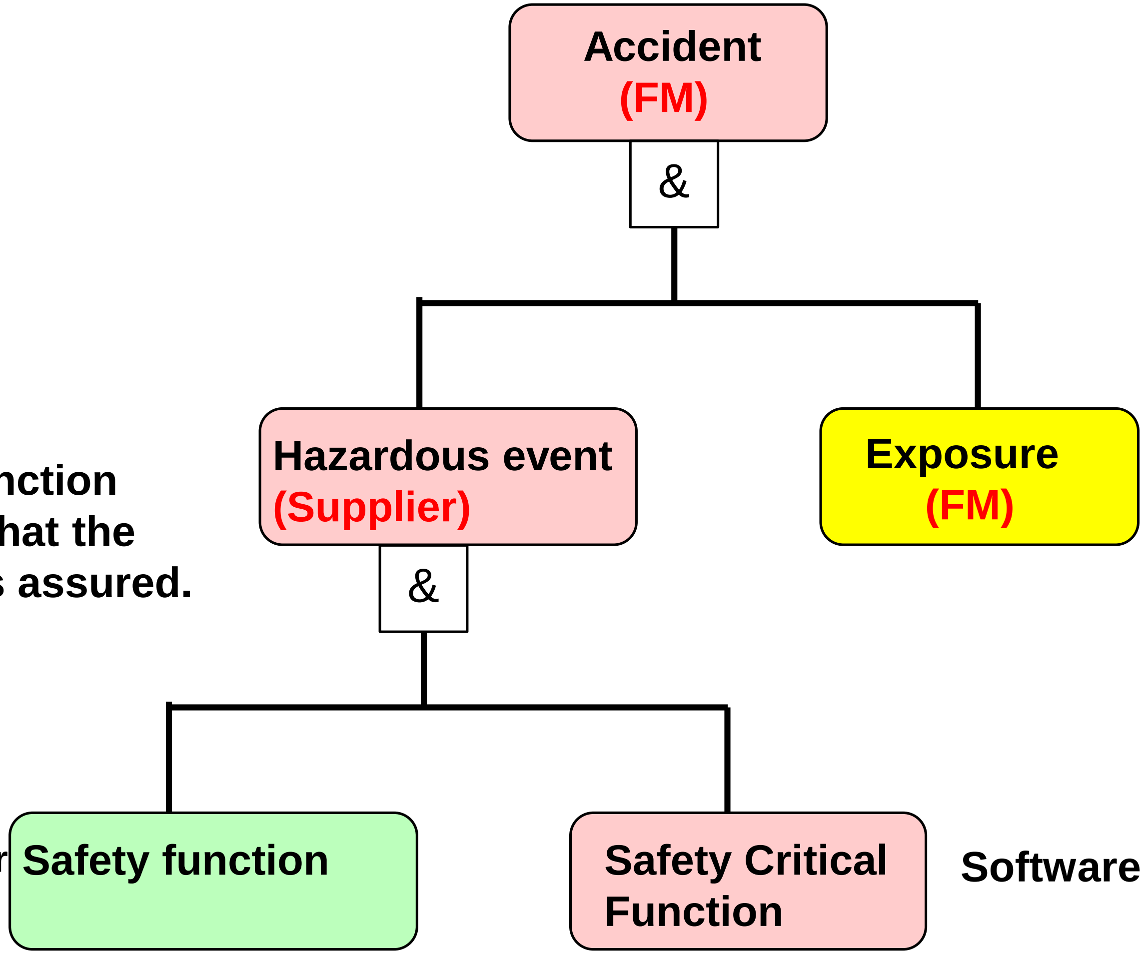
FMV

Hazardous event (Supplier)

Supplier

Handbook for Software in Safety Critical Applications

Chapter 4



The Safety function has to proof that the Safety level is assured.

May be a Safety switch or a monitoring Function.

Software included

Handbook for Software in Safety Critical Applications

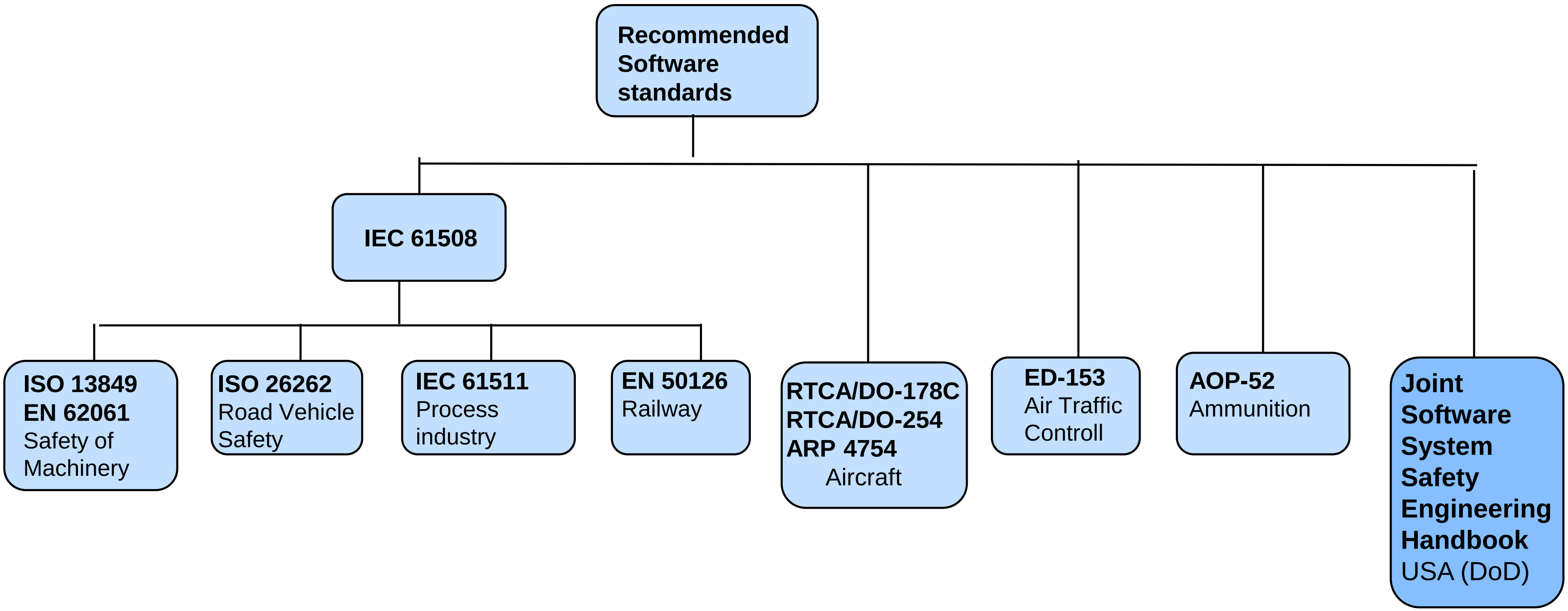
”Advertising”

FMV have received a lot of support from RISE, former SP Borås in evaluating different software standards for the handbook.

From 2017 SP became part of RISE.

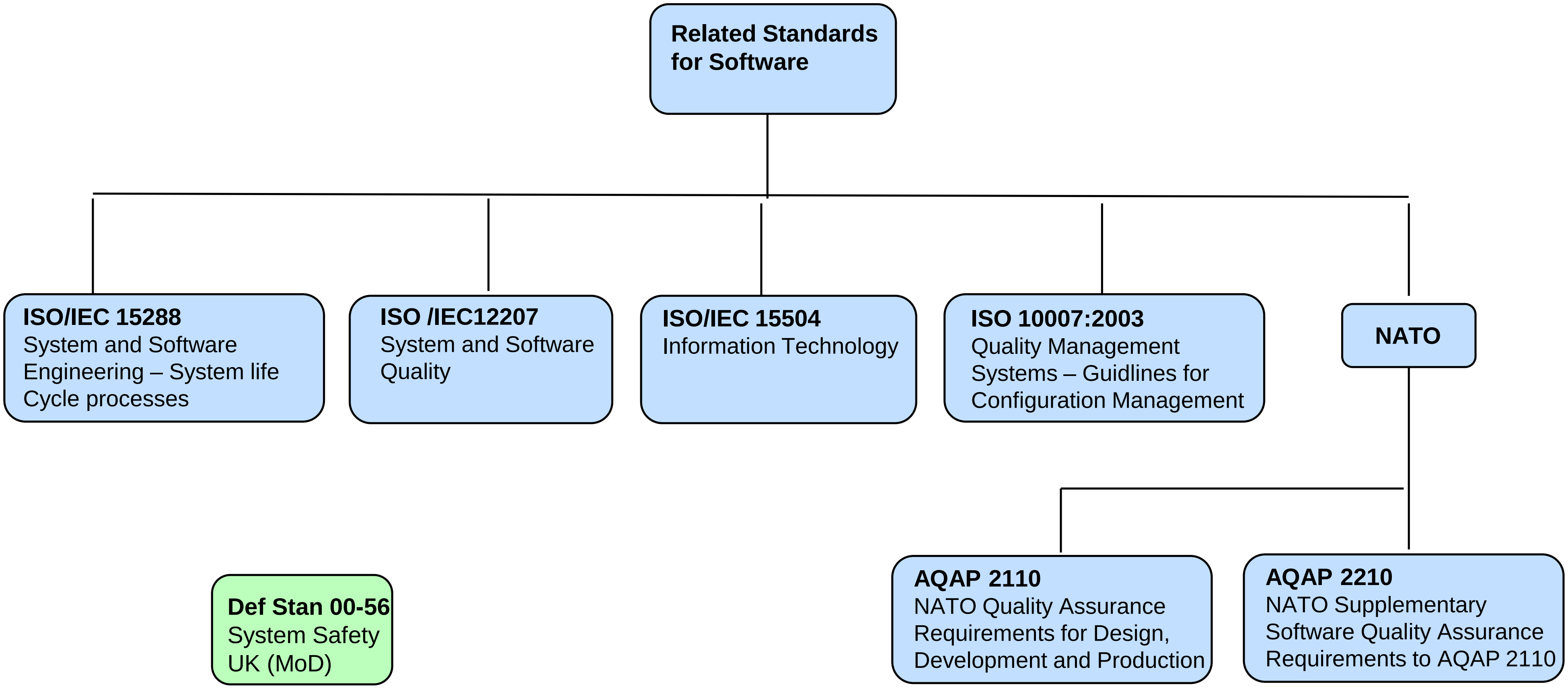
Handbook for Software in Safety Critical Applications

Chapter 2



Handbook for Software in Safety Critical Applications

Chapter 2



Commonly used Software standards Audrey Canning, Safety Critical Systems Symposium 2017(SSS´17)

Bransch	Standard	H ProgSäk 2018
Industry	IEC 61508 Ed 2, (2010) EN 50402 (2005) IEC 61511 Ed 2, (Feb 2016)	X X
Railway	EN50128, (2001) EN50129, (2003) EN50128, (2008)	X X X
Avionics	DO178C, (2012)	X
Defence	Def Stan 00-56, (2007)	X
Competency	IET Guidelines, (2016)	
Machinery	IEC 62061, (2005) ISO 13849-1, -2, (2006)	X X
Electrical Drives	IEC 61800-5-2,,(2007)	
Electrical Appliances	IEC 60335, (2010)	
Explosive Atmosphere	EN 50495, (2010) IEC 60079-29-3, (2014)	
Nuclear C&I	IEC 61513, (2011)	
Automotive	ISO 26262, (2011)	X
Water Management	IEC 60730, (2013)	
Medical Devices	IEC 62304, (2006)	
Farm vehicles	ISO 25119, (2010)	

Handbook for Software in Safety Critical Applications

Tabell 6 **Kritikalitetsnivåer för olika programvarustandarder.**

FM och FMV FHA	H ProgSäk 2018	IEC 61508 Progr. elektr. System	ISO 26262 fordon	ISO 13849 maskiner	EN 62061 maskiner	IEC 61511 process-industri	EN 50128 järnväg	RTCA/ DO-178C flygande	RTCA/ DO-254 flygande	ARP 4754A flyg	RTCA/ DO-278A flygledning	ED-153 flygledning	MIL-STD-882E militära system
HÖG *Kritikalitet*	Grundkrav + vald standard & kritikalitet	SIL 4 SIL 3 SIL 2 SIL 1	ASIL D ASIL C ASIL B ASIL A	PL e PL d PL c PL b PL a	SIL 3 SIL 2 SIL 1	SIL 4 SIL 3 SIL 2 SIL 1	SIL 4 SIL 3 SIL 2 SIL 1	Level A Level B Level C Level D	Level A Level B Level C Level D	Level A Level B Level C Level D	AL 1 AL 2 AL 3 AL 4 AL5	SWAL1 SWAL2 SWAL3 SWAL4	SwCI 1 SwCI 2 SwCI 3 SwCI 4
LÅG *Kritikalitet*	Grundkrav		QM				SIL 0	Level E	Level E	Level E	AL 6		SwCI 5

Handbook for Software in Safety Critical Applications

Appendix 1 Comparison between software standards

Below are comparison tables for selected standards regarding applicability

Tabell 1. Administrativa aspekter

	IEC 61508	ISO 26262	EN ISO 13849 -1	EN 62061	RTCA/ DO 178C	RTCA/ DO -254	ARP 4754A	ED -153	EN 50128	IEC 61511
Area of application	Progr. elektr. system	Väg - fordon	Maskin - styrning	Maskin - styrning	Flyg (SW)	Progr. logik (HW)	Flyg (system)	Flyg	Järnväg	Processindustri
Issue	2010	2011	2015	2015	2011	2000	2010	2009	2011	2016
Number of parts	7	10	2	1	1	1	1	1	1	3

Handbook for Software in Safety Critical Applications

Tabell 2. Kritikalitetsklassning

	IEC 61508	ISO 26262	EN ISO 13849-1	EN 62061	RTCA/ DO 178C	RTCA/ DO-254	ARP 4754A	ED-153	EN 50128	IEC 61511
Basis for Classification	Allvarlighet, sannolikhet	Allvarlighet, exponering, styrbarhet	Allvar-lighet, frekvens, möjlig-het att undvika	Allvar-lighet, sanno-likhet	Allvar-lighet	Allvar-lighet	Allvar-lighet	Allvar-lighet, sannolik-het	Allvar-lighet, frekvens (enligt exempel)	Allvarlighet, sannolikhet
Method for Classification	Riskgraf	Riskgraf	Riskgraf	Tabell	Bedöm-ning allvarlig-het	Bedöm-ning allvarlig-het	Bedöm-ning allvarlig-het	Riskgraf	Riskgraf	Flera metoder i IEC 61511-3
Levels for Classification	SIL 1 – 4	ASIL A – D	PL a – e	SIL 1 – 3	Level A – E	Level A – E	Level A – E	SWAL 1 – 4	SIL 0 - 4	SIL 1-4
Highets Criticality Level	SIL 4	ASIL D	PL e	SIL 3	Level A	Level A	Level A	SWAL1	SIL 4	SIL 4

Handbook for Software in Safety Critical Applications

Examples of Safety techniques recommended in the handbook

Criticality Classification	Redundancy
Failure detection, Built in test	Diversity
Use of Safe State	Software Safety Architecture
Watchdog	Deterministic behaviour
Checksum of memory / data