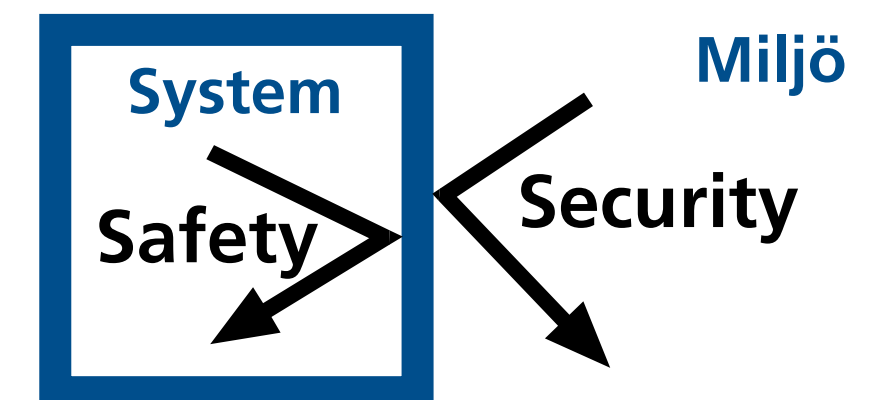


Safety - frihet från fara

Trots att de flesta människor i dagligt tal oftast syftar på skrivbordsdatorer när de pratar om datorer är majoriteten av dagens datorbaserade system sk inbäddade system. En programmerbar elektronisk krets kan användas för att styra så olika system som hushållsapparater, tillverkningsmaskiner, flygplan och kärnkraftverk. Fel som uppträder i systemen

kan få katastrofala effekter och äventyra människors liv och hälsa.

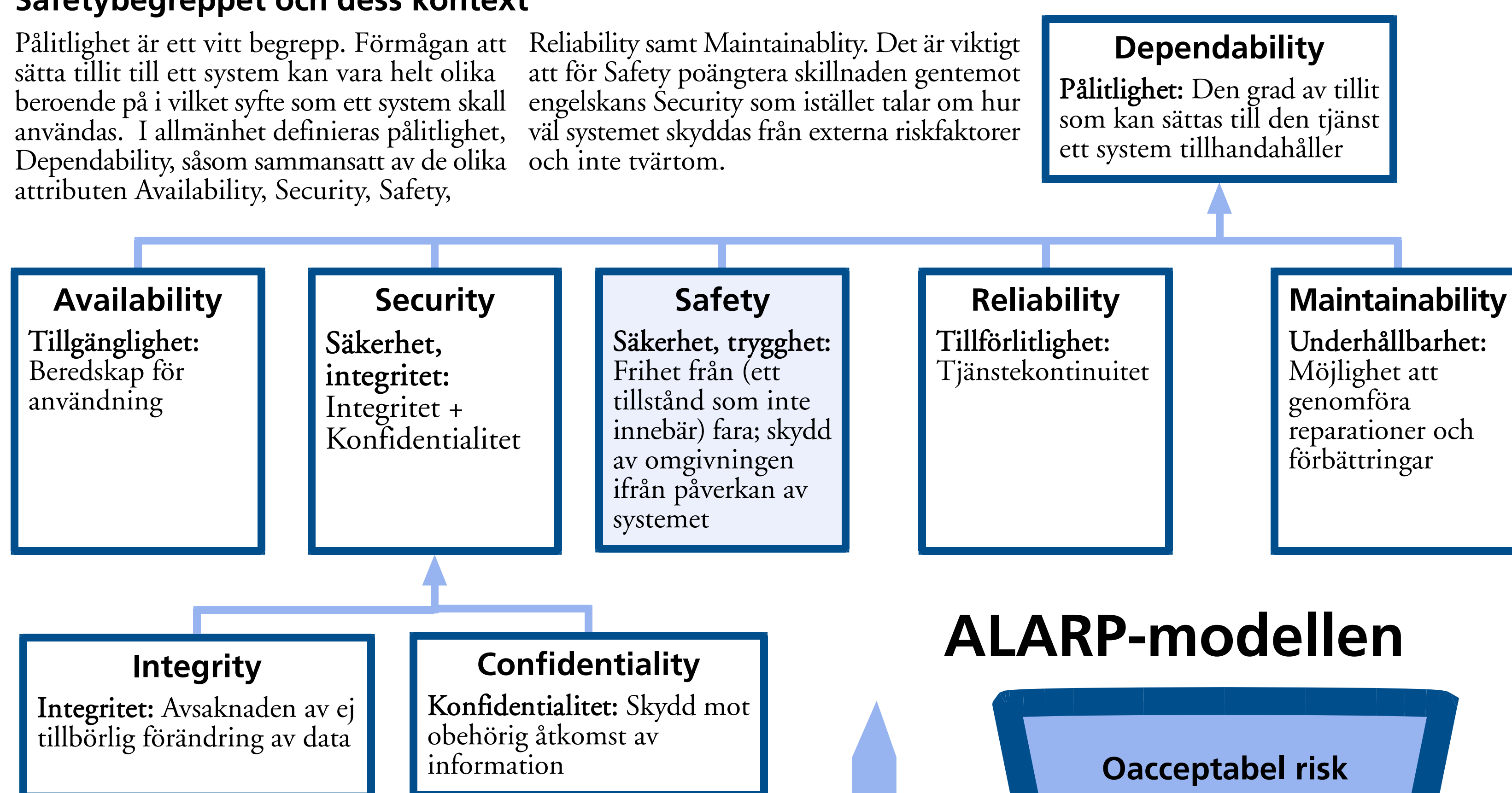
Systemen blir mer komplexa och introduceras inom nya områden. Behovet av att utveckla funktionssäker programvara ökar.



Safetybegreppet och dess kontext

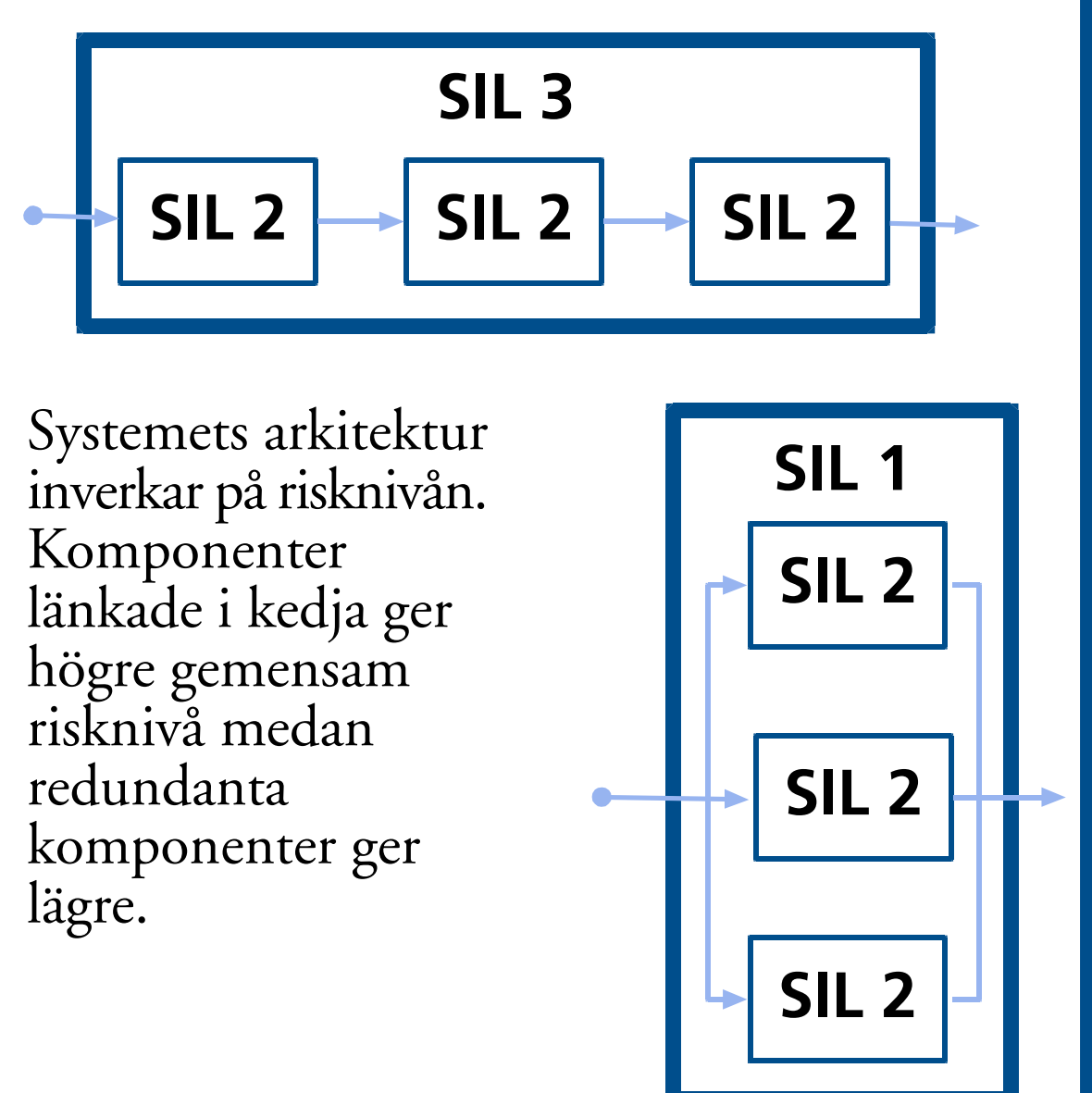
Pålitlighet är ett vitt begrepp. Förmågan att sätta tillit till ett system kan vara helt olika beroende på i vilket syfte som ett system skall användas. I allmänhet definieras pålitlighet, Dependability, såsom sammansatt av de olika attributen Availability, Security, Safety,

Reliability samt Maintainability. Det är viktigt att för Safety poängtera skillnaden gentemot engelskans Security som istället talar om hur väl systemet skyddas från externa riskfaktorer och inte tvärtom.

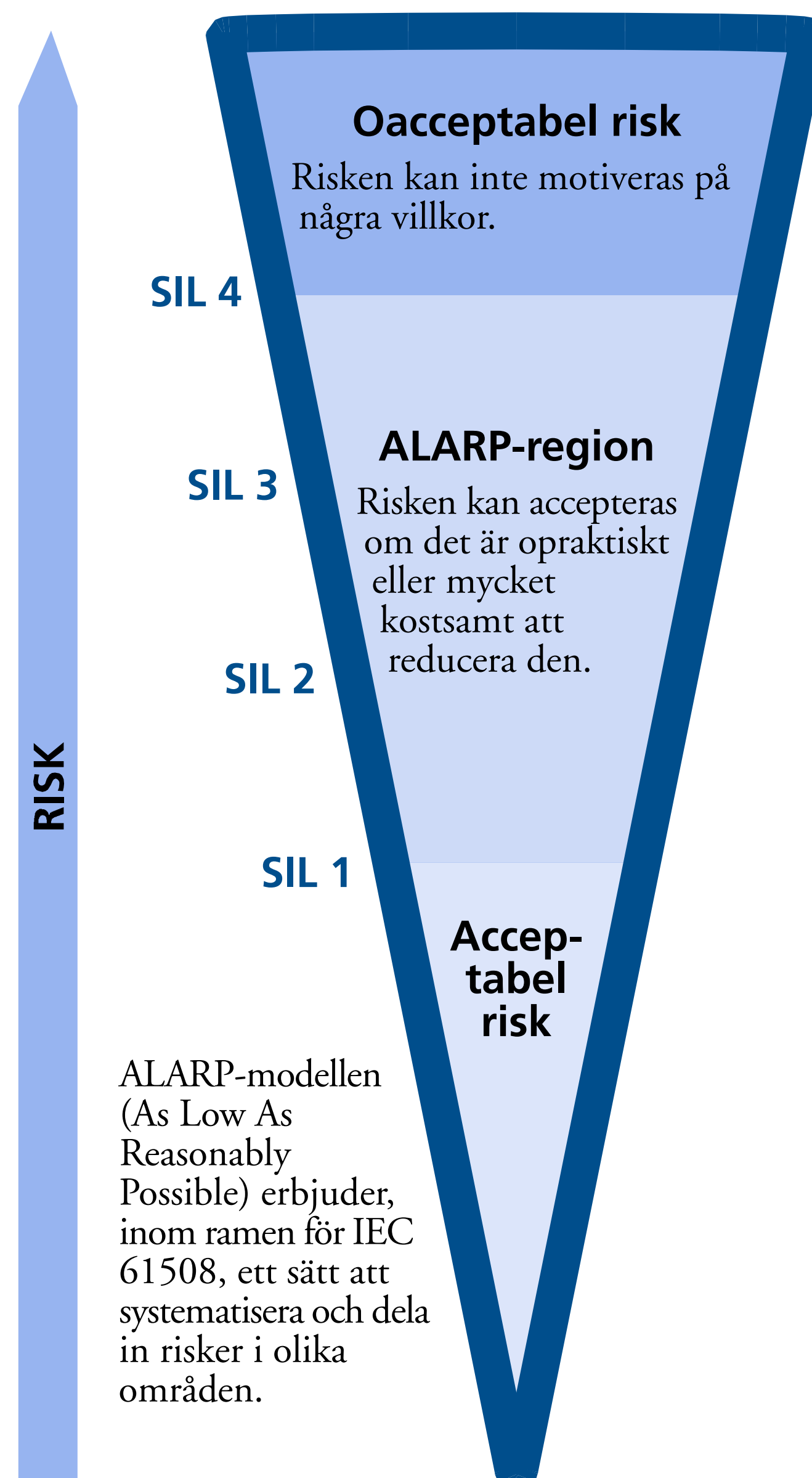


SIL – Safety Integrity Level

Safety Integrity Level (SIL) är ett mått på risknivå för en komponent och beräknas utifrån en kombination av sannolikhet, konsekvens och kostnad för att undvika de olyckor som komponenten kan vålla. En högre SIL-nivå innebär allvarigare risk.



ALARP-modellen



ALARP-modellen (As Low As Reasonably Possible) erbjuder, inom ramen för IEC 61508, ett sätt att systematisera och dela in risker i olika områden.

Standarder

IEC 61508

Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PESs)

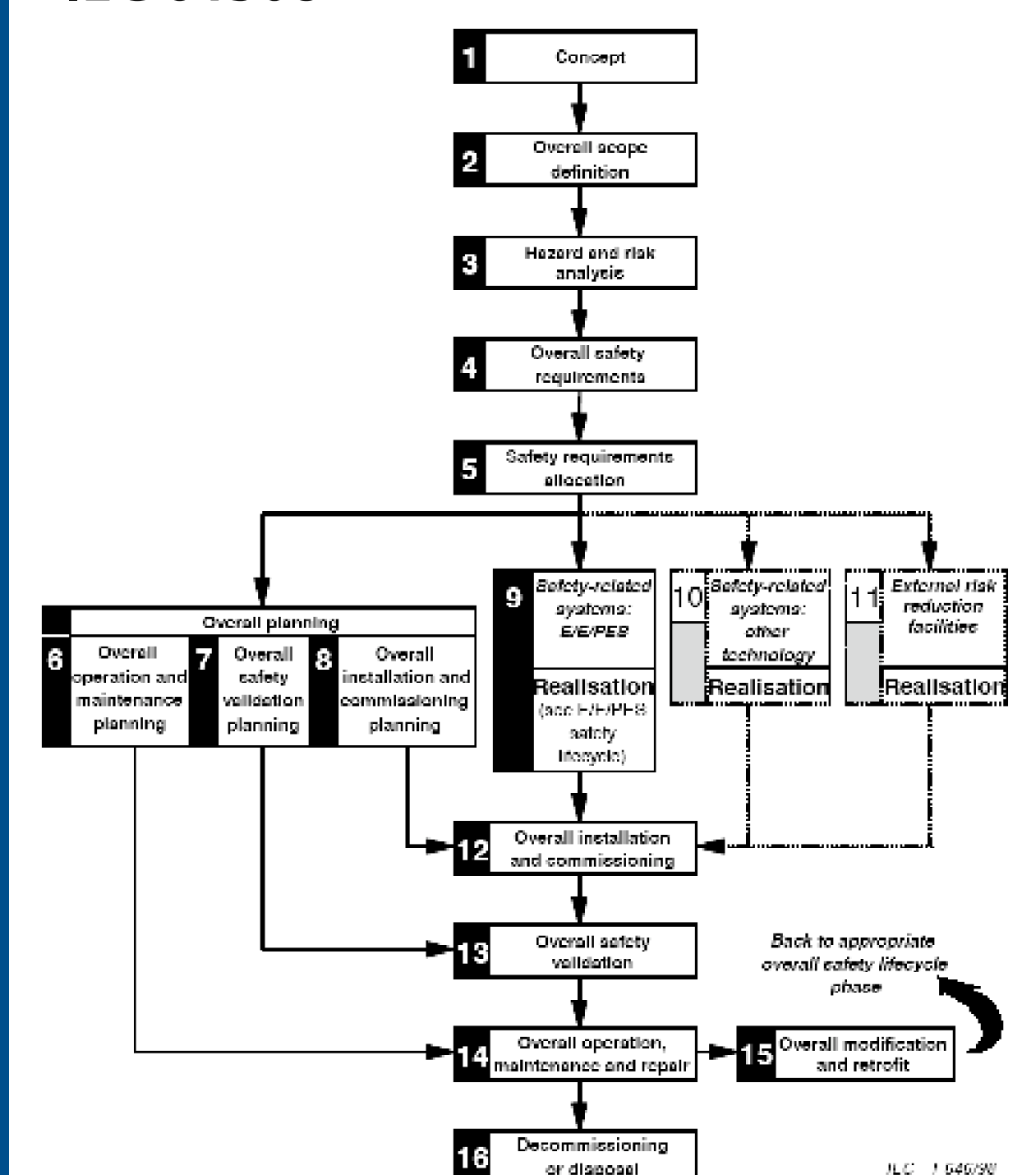
IEC 61511 Functional safety:

Safety Instrumented Systems for the process industry sector

IEC 62061 Safety of machinery:

Functional safety of electrical, electronic and programmable control systems

Utvecklingsprocessen enligt IEC 61508



I IEC 61508 är "safety lifecycle" (livscykel för funktionssäkerhet) ett centralt begrepp. Standarden är strukturerad i enlighet med denna. Syftet är att definiera en hållbar systemövergripande utvecklingsprocess för funktionssäkerhet. Det bör dock poängteras att den inte ska betraktas som någon definitivt föreskriven indelning av processen i tidsordning, utan skall mer ses som ett riktmärke som definierar hur information flödar mellan olika processsteg.

Forskningsområden

Kartläggning

För att identifiera problemområden behövs en kartläggning rörande safety för programvara inom svensk industri. Resultatet av denna jämförs sedan mot forskning samt mot hjälpmedel som utvecklats i form av t ex standarder och verktyg.

Metoder och tekniker för funktionssäkra PLC-tillämpningar

PLC:er (Programmable Logic Controllers) blir allt vanligare inom automationsindustrin. Dessa kan enkelt programmeras med olika programmeringsspråk (t ex de i IEC 61131). Metoder och tekniker för dessa områden är för närvarande under intensiv utveckling och ett intressant område för fortsatt forskning.

Metoders effektivitet för safety

Det existerar i dag en uppsjö metoder och tekniker för att bygga säkrare system. Detta forskningsområde avser kartlägga vilka av dessa som är effektivast i fråga om säkerhet och kostnad.

