



Att tillämpa systemsäkerhet för att leverera och överleva på kort och lång sikt – för designer och användare av produktionsutrustning

Ett systemtänkande där människa, teknik och organisation samverkar har blivit allt vanligare inom säkerhetsarbete*. Patrik Moberg redogör för systemsäkerhet som ett sätt att stärka Sveriges industriella konkurrenskraft.

*Med säkerhet och systemsäkerhet avses genomgående safety och system safety. Med it-säkerhet avses IT security/cyber security.



Patrik Moberg, produktchef för simulering mot virtuell idriftsättning/träning och systemsäkerhet på Siemens.

Arbetet med säkerhet för att skydda människor från att skadas av produktionsutrustning har pågått under lång tid. Standarder, föreskrifter och ramverk såsom riskbedömning, utformning av barriärer, skyddsavstånd, robust design genom dubbling och övervakning etc. var och är en mycket god grund för att erhålla säkra stopp.

Över tid har dock ett mer systemtänkande vunnit mark där människa, teknik och organisation samverkar för att kunna ha både hög tillgänglighet av produktionsutrustning och ändamålsenliga säkerhetsfunktioner för användning under säkra förhållanden. I standarder, föreskrifter och ramverk som styr användandet och design av produktionsutrustning är detta systemtänkande genomgående – och

åtgärder för största praktiska riskreducering/systemsäkerhet är då en kombination av åtgärder mellan designer och användare.

Nyligen har även it-säkerhet och industriell it-säkerhet, det vill säga att skydda produktionsutrustningen från människor, introducerats för beaktande från säkerhetsperspektiv.

Bakgrund

Sedan många år framgår det med all önskvärd tydlighet vad som anses vara den **största möjliga praktiska riskreduceringen** eller **systemsäkerhet** och hur **bäst användning av tillgänglig teknik** är en del. De fyra faktorerna är följande och i den ordning de anges nedan, enligt state-of-the-art-standarderna för generella principer för design – riskbedömning och riskreducering:

- maskinens **säkerhet** under alla faser av sin livscykel
- maskinens **förmåga att utföra sin funktion**
- **användbarheten** av maskinen
- maskinens tillverknings-, drifts- och demonteringskostnad

Även följande finns poängterat:

- Den ideala tillämpningen av dessa principer **kräver kunskap** om maskinens **användning**, tillbud och olyckshistoria, **tillgängliga riskreduceringstekniker** och den rättsliga ramen för vilken maskinen ska användas.
- En maskindesign som är acceptabel vid en viss tidpunkt kan inte längre

motiveras när **teknisk utveckling** möjliggör konstruktion av en likvärdig maskin med lägre risk.

Siemens och systemsäkerhet

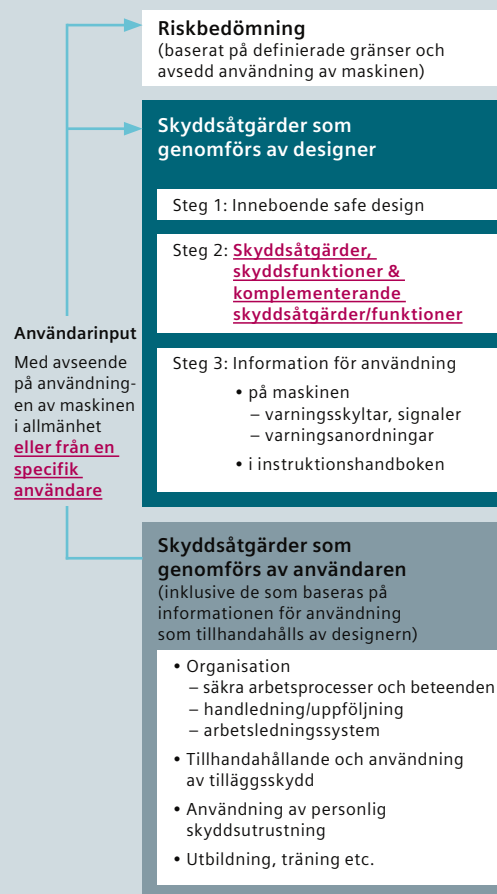
Siemens har både produkter och system för att bidra till att säkerställa systemsäkerhet. En del inom systemsäkerheten är då säkerhet för att skydda människan från att direkt skadas av produktionsutrustningen. Förutom produkter och system har vi dessutom kurser och även webbträningar inom ämnet.

Säkerhet från designerperspektiv

I state-of-the-art-standarderna för generella principer för riskbedömning och riskreducering finns tydligt beskrivet att designer ska ha förståelse för användaren rent generellt eller till och med skapa förståelse från en specifik användare.

I reportaget där Evomatic beskriver hur de har gått tillväga i arbetet med att bygga om presslinjer är kunskapen och förståelse för användaren central ihop med hur säkerhetskritisk mjukvara hanteras och testas.

Riskreduceringsprocessen från designerperspektiv från A-standarderna som beskriver "maskiner, generella principer för design – riskbedömning och riskreducering".



Automationsingenjörens och maskinupphandlarens roll – ihop med praktisk riskreducering

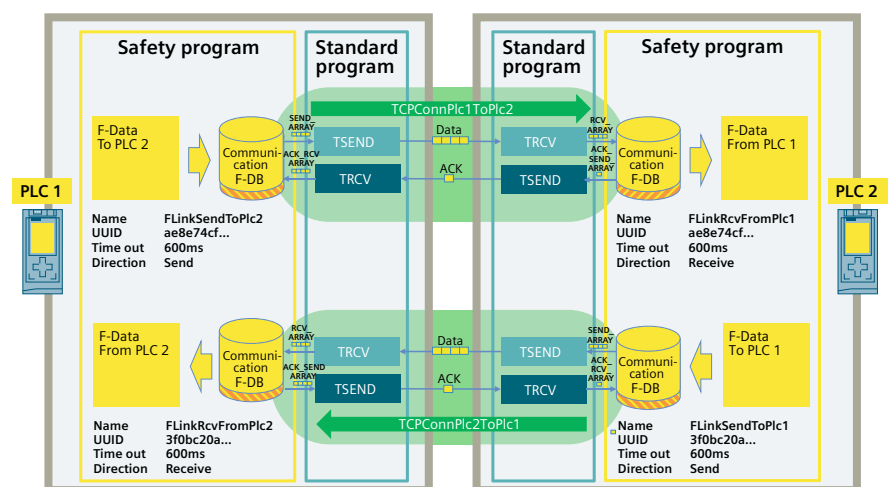
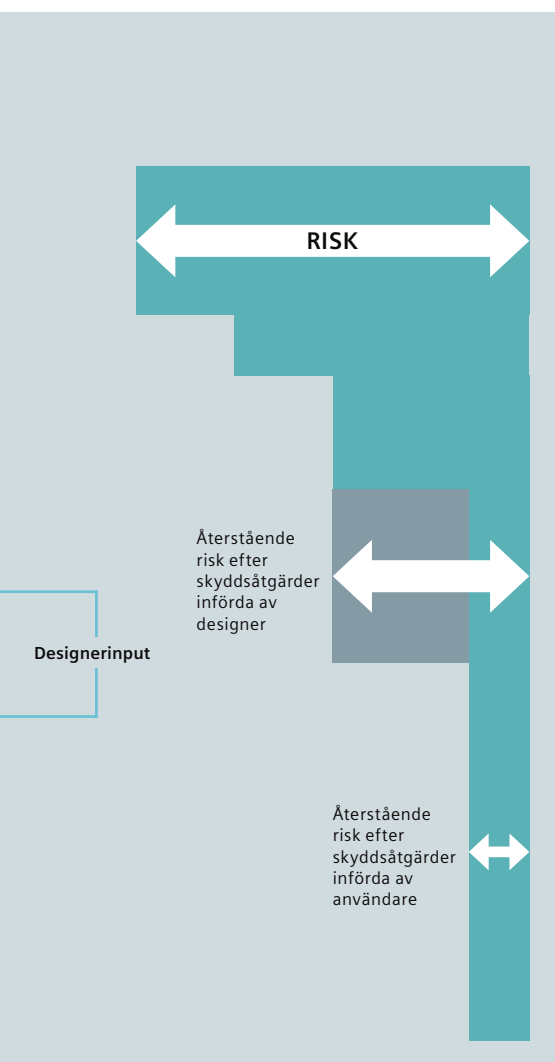
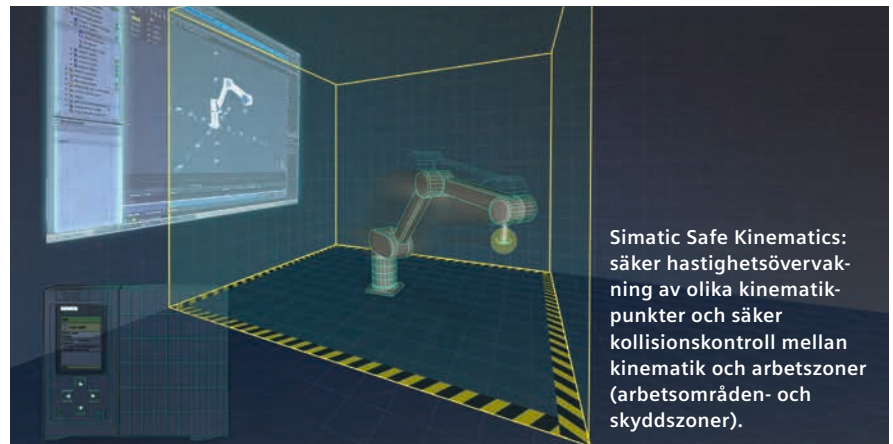
Automationsingenjörens roll och upphandlarens roll i praktisk riskreducering är omfattande liksom att behovet av att simulera är ökande då:

- säkerhetskritisk programvara är ökande eftersom behovet av ändamålsenlig funktionalitet är ökande
- kunden ska förvissas om att utrustningen har förmågan att utföra sin funktion
- operatörer ska tränas för att säkerställa optimerad användbarhet
- kostnadsaspekten för maskinen ska innefatta drift- och demonteringskostnader.

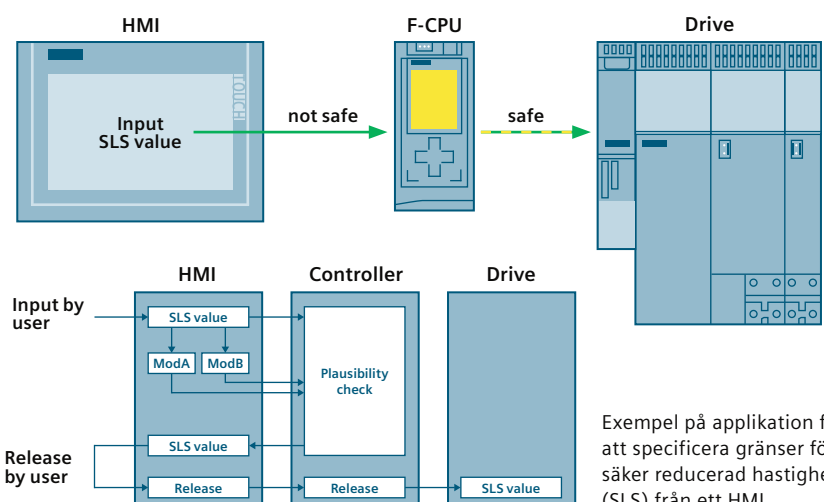
Siemens produkter, system, integrerade funktioner och applikationsstöd för systemsäkerhet

Att integrera säkerhetsfunktionalitet i automationssystemen med innovativa integrerade funktioner ihop med hjälp av applikationer ger kostnadsfördelar, effektivitet i implementeringen och inte minst flexibilitet.

Forts. nästa sida



Exempel på applikation: Flexibel F-link-kommunikation.



Exempel på applikation för att specificera gränser för säker reducerad hastighet (SLS) från ett HMI.

Systemsäkerhet som en del av att förstärka sin industriella konkurrenskraft

Det är av yttersta vikt att vi har både duktiga designers av produktionsutrustning liksom duktiga företag som kan producera för att behålla och förstärka vår industriella konkurrenskraft. Att utveckla och motivera befintliga medarbetare och locka nya är då avgörande.

Nedan beskrivs ett systematiskt arbete som bygger på Evomatics projekt vad gäller säkerhet i produktionslinjer. Fokus i artikeln är avgränsat till att:

- förstå användarna och kunna optimera produktionslinjer från användarens perspektiv, behov och erfarenheter
- systematisera för att kunna effektivisera programmering och testning av säkerhetsfunktionerna.

Tillskott till systemsäkerhet

– industriella it-säkerhets- och maskinsäkerhetsprinciper för riskbedömning och riskreducering

TECHNICAL
REPORT

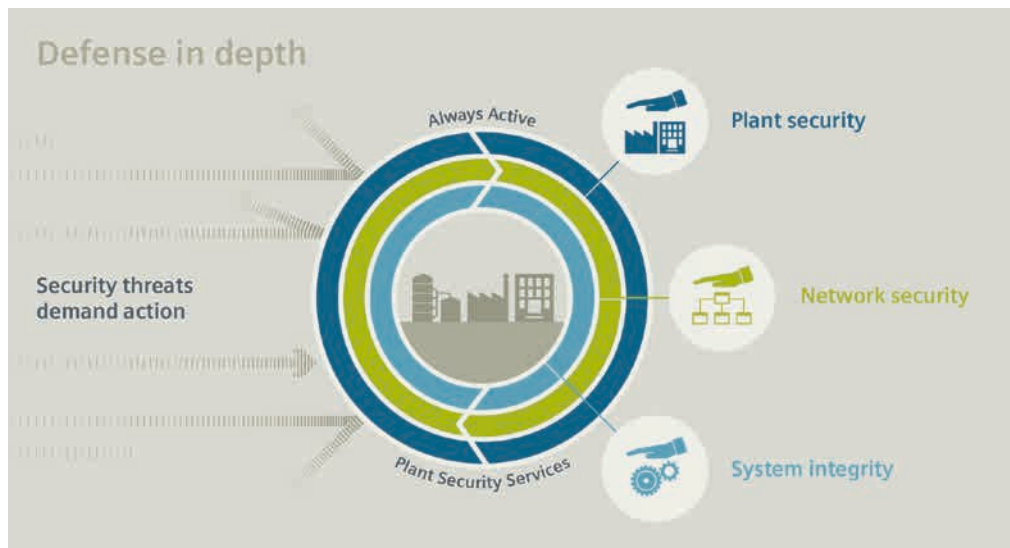
ISO/TR
22100-4

First edition
2018-12

Safety of machinery – Relationship
with ISO 12100 —

Part 4:
Guidance to machinery manufacturers
for consideration of related IT-security
(cyber security) aspects

Det primära syftet med detta dokument är att ta itu med aspekter på säkerheten hos maskiner som kan påverkas av it-säkerhetsattacker relaterade till direkt eller fjärråtkomst till,



och manipulation av, ett säkerhetsrelaterat styrsystem av personer för avsiktligt missbruk (oavsiktligt bruk). It-säkerhetsattacker blir alltmer ett potentiellt hot mot maskinens säkerhet. Även om avsiktligt missbruk faller utanför tillämpningsområdet för ISO 12100 och den riskbedömningsprocessen är det också rimligt för maskintillverkare att överväga sådana hot.

I dokumentet hänvisas till standarder som hanterar industriell it-säkerhet som bygger på att "defence in depth" tillämpas och vad som vilar på tillverkarens, integratörens och användarens ansvar för utrustning för industriellt bruk.

Competence Group och erbjudande till medlemmar

Inom vår "Competence Group – We make future of automation & digitalization work" erbjuder vi oss att under en dag komma till ditt företag för att beskriva maskinsäkerhet från automationsperspektiv, från vilka krav en automationsingenjör ska ställa på riskbedömnings- och riskreducerings-

teamet innan automationsingenjören/programmeraren börjar programmera säkerhetsfunktionerna till hur man ska säkerställa och förvissa slutkunden att produktionsutrustningen är säker med alltmer mjukvara.

På förmiddagen arbetar vi med ett system som de flesta av oss använder hemma och som de flesta har en förståelse för hur det funkar och applicerar kraven på detta allmänna system enligt systemsäkerhet som beskrivs i denna artikel. På eftermiddagen går vi över till produktionssystem och gör samma arbete på typiska, moderna produktionsutrustningar. Då fås även information om och tillgång till det arbete och material som unga och engagerade industridesigner och programmerare har utfört åt Siemens för att täcka in användbarhet och vad en ung programmerare tänker om hur ungdomar ska lockas till att programmera produktionsutrustning. ■

[siemens.com/safety](https://www.siemens.com/safety)
[siemens.com/industrial-security](https://www.siemens.com/industrial-security)
[siemens.com/tia](https://www.siemens.com/tia)
patrik.moberg@siemens.com

