

TECH FOR SUSTAINABILITY

Automationsnytt

2/2025 [siemens.se](https://www.siemens.se)



Jag är stolt över att
få ta över rollen som
**vd för Siemens i
Sverige och Norden**

Andrea Waenerlund

25

OT2IT MED HÖG CYBERSÄKERHET

8

Cirkulärt är modellen
– omvandlar biomassa
till kolnegativ energi

12

Resan mot
datadrivna
beslut

26

Hon är
expert på
cybersäkerhet

34

Så hjälper vi
dig möta de nya
regleringarna

44

AI-baserat
prediktivt
underhåll



Innehåll

Smarta samarbeten

OT2IT med hög cybersäkerhet när Benders framtidssäkrar i Uddevalla.....	4
Meva Energy omvandla biomassa till kolnegativ energi.....	8
Siemens är med på Ecoleans resa mot datadrivna beslut.....	12
Exjobb ger säkrare testrigg med ny teknik från Siemens.....	16

Serie | Maskinsäkerhet

Säkerhet, säkerhet och säkerhet – Ann Axelsson reder ut begreppen	20
--	----

Utbildning

SITRAIN utbildningscenter: höstens och vårens schema 2025/2026	22
---	----

Aktuellt

Nytt och aktuellt.....	24
Andrea Waenerlund ny vd	25
Hon är expert på cybersäkerhet	26
Nybliven doktor i informationssäkerhet.....	28
Ny era för cybersäkerhet	30
Så hjälper vi dig möta de nya regleringarna	34
Hållbarhet och produktivitet går hand i hand	36
Produktnytt	37

Smått & gott

Smarta tips.....	43
AI-baserat prediktivt underhåll	44
Att jobba smart kräver en underhållsstrategi.....	45

Kontakta oss

Så når du oss och våra partner	46
--------------------------------------	----



Mikael Leksell | ✉ mikael.leksell@siemens.com

Anja Eimer | ✉ anja.eimer@siemens.com

Grattis Mikael – välkommen Anja!

Vår tidigare vd för Siemens AB och Siemens i Norden samt chef för Digital Industries, **Mikael Leksell**, har sedan den 1 oktober gått vidare till en global roll som Digital Industries Sales Zone Head EMEA på Siemens, vilket innebär att han är globalt säljansvarig för Europa (exklusive Tyskland), Mellanöstern och Afrika. Vi säger stort grattis till Mikael och tack så mycket för insatserna under åren hos oss i Sverige och Norden!

Som ny **chef för Digital Industries** på Siemens i Sverige och Norden välkomnar vi **Anja Eimer**. Tillsammans med vår nya vd Andrea Waenerlund, som presenteras på sidan 25, kommer hon att ta Siemens vidare i Sverige och Norden och arbeta för ännu mer ökat samarbete och stöttning på våra kunders digitaliserings- och hållbarhetsresor.

Med sitt tidigare ansvarsområde på Siemens som Global Head of Verticals Water & Waste Water, Chemicals, Oil & Gas, Glass & Solar samt Minerals & Mining har Anja **gedigen erfarenhet** inom processindustri men har även **experterfarenhet** från diskret tillverkningsindustri från sin tidigare konsultbakgrund, såväl externt som inom Siemens Advanta Consulting.

I dessa roller hjälpte Anja kunder bland annat på den **digitala** transformationsresan, hjälpte dem att bli mer **hållbara** genom till exempel energioptimering och arbetade med att utveckla särskilda branschlösningar för att exempelvis stötta kunder att bli NIS2-redo.

För det är ju så att hand i hand med digital transformation går **cybersäkerhet** som en röd tråd. Och det är just vad du kan läsa om i detta nummer: en ny era för cybersäkerhet, digital transformation på resan mot datadrivna beslut och hållbarhet med cirkularitet som modell.

I allt detta blir **interoperabilitet** mellan produkter, system och människor allt viktigare. Däri ligger Anjas fokus och löfte framöver: att **göra våra kunders liv lättare** med oss. Som ett stort globalt företag vet vi att så kanske inte alltid är fallet. Vi vill, såväl internt som externt, arbeta mer som ett One Tech Company, med större samarbete mellan verksamhetsområden och länder – ett arbetssätt och framförallt förhållningssätt som Anja har varit med att arbeta fram. Detta blir bra – **varmt välkommen Anja!** ■



Ann-Louise Lindmark, chefredaktör och ansvarig utgivare
✉ ann-louise.lindmark@siemens.com

OT2IT med hög cybersäkerhet när Benders framtids-säkrar i Uddevalla

Med ökad förfrågan på markprodukter behövde Benders bygga en ny fabrik för effektivare produktion och bättre transportmöjligheter för mindre miljöpåverkan. Lösningen blev en ombyggd Volvofabrik i Uddevalla med hög automationsgrad: orderstyrd produktion, självkörande truckar och hög säkerhetsnivå både vad gäller personsäkerhet och cybersäkerhet utan att tillgängligheten påverkas.



Eftersom vi behöver samordna ett större antal PLC-system, både våra egna samt tredjepartssystem, var det naturligt med en Siemenslösning

UTMANING

Benders sökte en lokalisering som skulle optimera transporter ur ett klimatperspektiv.

Man ville ha en modern, fullt automatiserad markstensproduktion med hög maskin- och cybersäkerhet.

Det skulle även vara lätt att integrera tredjepartsleverantörer.

LÖSNING

En fabrik vid vatten med tågmöjlighet garanterar en framtidssäker transportlösning.

Genom att välja Siemens och TIA Portal får Benders en modern, integrerad lösning samt en leverantör med stor produktportfölj; det blir enkelt att integrera tredjepartsleverantörer som till exempel AGV:er och andra maskinbyggare.

Med Siemens felsäkra PLC:er kan en mer flexibel safetylösning integreras.

Via PN/PN-kopplare samordnas komplexa funktioner med tredjepartsleverantörer, där kommunikationsnätverket har byggts upp med högt säkerhetstänk genom segmentering.

RESULTAT

Benders har fått en modern tillverkningsenhet, vars placering minimerar transporter och miljöpåverkan.

Tack vare integratören AtLid och Siemens samordnas enkelt en stor mängd komplexa PLC-projekt med integrerade drivenheter, RFID-spårning och HMI.

Ökad flexibilitet, tillgänglighet och kontroll av produktion.

Förenklat underhåll genom Totally Integration Automation.



Som del i stödpaketet till Uddevalla efter nedläggningen av Uddevallavarvet byggdes på 1980-talet Volvo Uddevallaverken, fabriken som blev känd för att den traditionella löpande band-principen frångicks.

När Volvo Personvagnar senare lade ned anläggningen köptes den av Benders, tillverkare av betong- och granitprodukter och isoleringsmaterial. Med produktions- och lageranläggningar runtom i Sverige, Finland, Grekland, Tyskland och Norge passar den egna hamnen och järnvägsförbindelse på tomten utmärkt.

– För våra tunga produkter blir logistiken oerhört viktig. Nu kan vi optimera transporterna ur ett klimatperspektiv, säger **Sven-Erik Lagergren**, projektledare på Benders.

UTVECKLAR TILLSAMMANS

Benders har under många år samarbetat med Automations Teknik i Lidköping, AtLid, en integratör som med hjälp av den senaste tekniken utvecklar maskiner och systemlösningar tillsammans med Benders.

– Att bygga en maskin är enkelt, att integrera är det svåra. Där har vi stor hjälp av AtLid som är med från projektering till färdig anläggning, säger Sven-Erik Lagergren.

Tillsammans tar de fram lösningar för en såväl framtids-säker som person- och cybersäker produktion. Benders överlåter åt AtLid att sätta sin elstandard och medverka i upphandling av tredje parts maskiner.

– Att vi tar fram maskiner och teknislösningar ihop gör att vi utvecklas och stärker vårt arbete även med andra kunder och områden, säger **Gunnar Wikstrand**, teknikansvarig på AtLid.

STÄRKER FÖRETAG

AtLid gjorde tidigt en bedömning att satsa på beständiga områden som vägar, livsmedel, VA, sågverk, materialhantering och, som hos Benders, produktion av tunga produkter med låg förädlingsgrad. Detta baserat på att man för tio år sedan inte såg någon ljus framtid inom bil- och tillverkningsindustrin; ett beslut som visade sig vara fel men som ändå har gett företaget en stabil kundbas.

– Vi är genuint fascinerade av hur automatiserade industriella processer stärker företags produktion. Med vår expertkunskap hjälper vi svensk industri använda AI och processindustriell IT på nya sätt, säger Gunnar Wikstrand.

HÖG AUTOMATIONSGRAD

Till Uddevallafabriken levererar AtLid allt från MES- och SCADA-system till PLC-lösningar och apparatskåp. Här håller



Sven-Erik Lagergren, projektledare på Benders, Nina Rabe, kundansvarig på Siemens, och Gunnar Wikstrand, teknikansvarig på AtLid.

man hög automationsgrad med orderstyrd produktion och självkörande truckar – och hög säkerhetsnivå både vad gäller personsäkerhet och cybersäkerhet.

– Vi behöver en hög automationsgrad för att kunna driva en såpass stor anläggning, säger Sven-Erik Lagergren.

ENKEL SAMORDNING I TIA PORTAL

Att välja Siemens med sin breda produktflora i egenskap av stabil och långsiktig partner var ett enkelt val.

– Eftersom vi behöver samordna ett större antal PLC-system, både våra egna samt tredjepartssystem, var det naturligt med en Siemenslösning. Genom att koppla samman alla system i en nätverksstruktur kan vi via TIA Portal integrera både dataflöden och maskinsäkerhet och samtidigt hålla en hög cybersäkerhet, säger Gunnar Wikstrand och fortsätter:

– Med TIA Portal får vi en bra struktur och kan bygga avancerade safetylösningar på ett enkelt sätt.

Sven-Erik Lagergren är också nöjd med automationsplattformen.

– TIA Portal ger oss ett enhetligt verktyg där vi från en källa kan kontrollera maskiner, servon, frekvensomriktare, HMI och andra enheter som AGV:er.

I systemet används även Siemens RFID-enheter för att identifiera och spåra produkter i flödet; när en produkt dyker upp vet maskinen vilket program som ska köras.

OT2IT MED HÖG CYBERSÄKERHET

Tillsammans har man byggt upp en hög cybersäkerhet med hög integritetsnivå, både elektriskt och PLC-mässigt, där IT- och OT-nätverken pratar med varandra.

– Vi har ett administrativt nätverk, ett produktionsnätverk, ett fastighetsnätverk och lokala nätverk för maskinerna

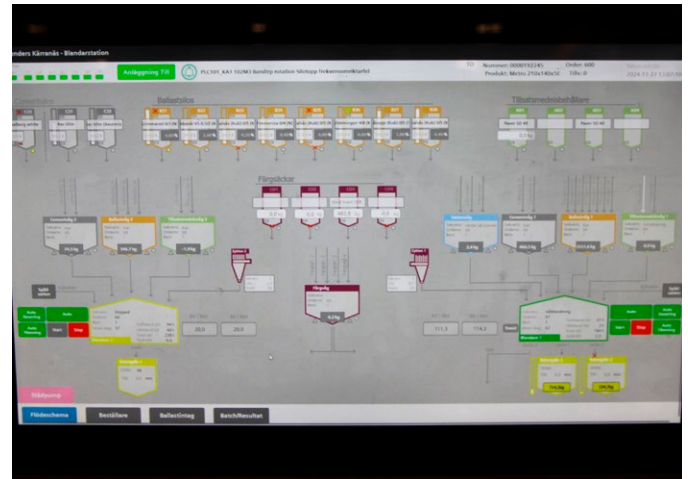


En nyttillverkad bricka plockas ut med jämna mellanrum till en teststation där kvaliteten kontrolleras med både provtagningsutrustning och manuella mätningar.

som kommunicerar via Profinet och kopplas ihop via PN/PN-kopplare, säger Sven-Erik Lagergren.

Robotarnas prioriteringar, orderköer för AGV:erna, övervakning, larm etc. ligger i master-PLC:n, via vilken även all säkerhet går; ingen trådad säkerhet här inte. Master-PLC:n samlar in och skickar upp produktionsdata till det av AtLid utvecklade produktionsuppföljnings- och orderhanterings-systemet som sedan pratar med affärssystemet.

– Master-PLC:n kommunicerar med alla enheter. Det vinner Siemens hårt på, att det är enkelt att integrera även med andra fabrikat. Öppenheten gör det enkelt att samordna och knyta ihop allt, avslutar Gunnar Wikstrand. ■



I fabriken sker all operatörsdialog via Simatic WinCC Scada och klienter. Recepten för blandarstationerna läses upp lokalt. Här en överblicksbild över betongstationen.



Det vinner Siemens hårt på, att det är enkelt att integrera även med andra fabrikat

TEKNIK

STYRSYSTEM

Simatic S7-1512, S7-1515, S7-1517-F, S7-1516-F;
PN/PN-kopplare

HUMAN MACHINE INTERFACE

Simatic WinCC Unified med klienter och paneler

BUSSKOMMUNIKATION

Profinet

DISTRIBUERADE I/O

Simatic ET 200SP

INDUSTRI-PC

Simatic Microbox PC

SERVOSYSTEM

Sinamics S120

FREKVENSOMRIKTARE

Sinamics G120D med Innomotics växelmotorer med integrerade felsäkra I/O

STRÖMFÖRSÖRJNING

Sitop PSU6200, Sitop UPS501S

LÅGSPÄNNINGSPRODUKTER & STARTAPPARATER

Motorskyddsbrytare Sirius 3RV, mjukstartare Sirius 3RW

LÅGSPÄNNINGSPRODUKTER & ELDISTRIBUTION

Dvärgbrytare Sentron 5SY

NÄTVERKSKOMMUNIKATION

Nätverksswitchar Scalance X

IDENTIFIERING

Simatic RFID

MER INFORMATION

[siemens.se](https://www.siemens.se) | [benders.se](https://www.benders.se) | [atlid.se](https://www.atlid.se)

Omvandlar biomassa till kolnegativ energi

Tillgången till service och support var viktiga faktorer när styrsystem skulle väljas för Meva Energys unika process som producerar förnybar gas och energi för industrin. Med den revolutionerande förgasningstekniken omvandlas lokalt genererade biogena rest- och avfallsströmmar från industrin till biosyngas med biokol som en värdefull restström.

När Meva Energy skulle välja styrsystem för sin första kommersiella anläggning för förgasning av biomassa gjordes en grundlig genomgång av olika leverantörer på marknaden.

– Viktiga faktorer för oss var tillgänglighet, service och support, kompetens och att det är ett väletablerat varumärke som är kompatibelt med andra system. Jag intervjuade flera stora systemintegratörer och fick entydiga svar: det är Siemens processtysystem vi ska ha, säger **Eric Palander**, automationsansvarig på Meva Energy.

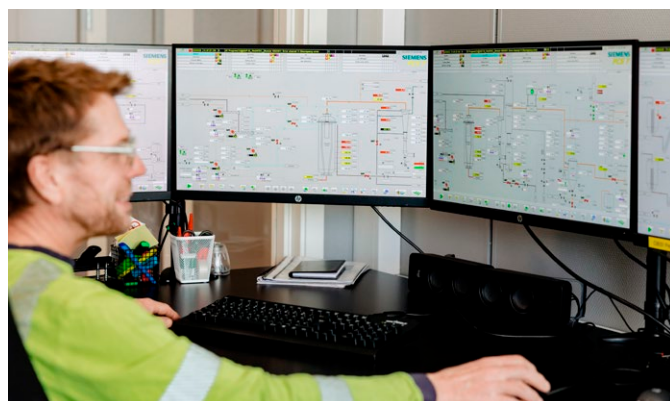
FRÅN BIOMASSA TILL BIOSYNGAS

I Mevas nybyggda anläggning i Kisa, som stod klar 2023, omvandlas biomassa till biosyngas i en patenterad process. Den förnybara gasen produceras genom att biomassa snabbt värms upp med en begränsad tillgång till syre. Gasen används sedan av ett intilliggande pappersbruk för att ersätta brukets fossila användning av gasol.

– Vi pratar om en årlig minskning för bruket på upp till 8 500 ton utsläppt koldioxid, säger Eric Palander.

RESULTAT AV FORSKNING

Meva Energy grundades 2008 i Sverige som resultat av forskning om biomassaförgasning vid Luleå tekniska universitet och Energitekniskt Centrums förgasningscenter.



Driftteknikern Staffan Andersson på Meva Energy har full koll på processen med Siemens processtysystem Simatic PCS 7 som kommunicerar med alla system och produkter.

Idag har Meva en anläggning i drift i Sverige och håller på att bygga sin andra i Polen till en möbelfabrik.

Nyligen tecknades ett 15-årigt avtal med Elcowire, en ledande europeisk tillverkare av koppartråd, för att leverera 9 MW förnybar biogas till en anläggning i Helsingborg, som idag använder naturgas som energikälla för att smälta metallen. Därmed blir Elcowire världens första koppartrådstillverkare som ersätter fossil gas med fossilfri energi i sin produktionsprocess.

ERSÄTTER FOSSILA BRÄNSLEN

Energikrävande industrier har länge varit beroende av fossila bränslen för att uppnå de temperaturer som krävs för tork- och smältapplikationer. Meva



MEVA ENERGY



Den viktigaste faktorn är att vi får hjälp och att det finns en utbredd kompetens



Energys innovativa lösning är framtagen för att kunna ersätta de fossila bränslena med den förnybara biosyngasen.

ANVÄNDER RESTAVFALL

I Mevas anläggning i Polen, som ska stå klar 2026, kommer Meva ta tillvara möbeltillverkarens eget restavfall från sin produktion och genom förgasning omvandla detta till biosyngas som ska driva motorer och generera el tillbaka till möbeltillverkarens fabrik.

– Det blir verkligen en win-win. Det är bra ur flera synpunkter. Kunden kan rå över sin egen energiproduktion och blir inte beroende av fossila källor och kostnaden blir mer stabil. Och framförallt: klimatavtrycket minskas, säger Eric Palander.

// Siemens produkter och system är kompatibla med alla andra system

VÄRDEFULL RESTSTRÖM

När biomassa omvandlas till gas genom Meva Energys teknik uppstår samtidigt en värdefull restprodukt: biokol. Biokol består av ett stabilt kol som kan lagras i marken under mycket lång tid, utan att släppas ut i atmosfären som koldioxid. På så sätt kan biokolet fungera som en långsiktig kolsänka.

Genom att kombinera två klimatpositiva effekter, ersättning av fossil gas med ett förnybart alternativ samt koldioxidinlagring via biokol, har tekniken potential att inte bara minska utsläppen, utan även att uppnå negativa utsläpp.

SUPPORT OCH ÖPPNA SYSTEM AVGJORDE

När Meva Energy skannade av marknaden och frågade systemintegratorer efter lämplig styrsystemsleverantör var det framförallt den tekniska supporten på Siemens som hyllades.



Eric Palander, automationsansvarig på Meva Energy, och Peter Henriksson, kundansvarig på Siemens.



Den unika processen producerar förnybar gas och energi för industrin.

– Den viktigaste faktorn är att vi får hjälp och att det finns en utbredd kompetens, vi måste veta att vi kan få hjälp när vi bygger och driftar våra kommande anläggningar oavsett var. Lika viktigt är också att Siemens produkter och system är kompatibla med alla andra system, avslutar Eric Palander. ■



TEKNIK

PROCESSTYRSYSTEM

Simatic PCS 7

DISTRIBUERADE I/O

Simatic ET 200SP HA (High Availability)

STRÖMFÖRSÖRJNING

Sitop PSU100S

Biosyngas är en förnybar gas som produceras genom termisk förgasning av lågkvalitativa biomassa-rester. Biosyngas kan användas för att ersätta fossil gas vid processuppvärmning eller för att producera el och värme. I jämförelse med andra biogaser består energibärarna i biosyngas främst av kolmonoxid (CO) och vätgas (H₂), med endast en liten mängd metangas (CH₄).

Biokol är en värdefull biprodukt från produktionen av biosyngas. Det är ett poröst material med mycket stor yta och högt kolinnehåll, som framställs genom att biomassa upphettas till höga temperaturer i en syrefattig miljö.

Ann-Louise Lindmark,
chefredaktör och ansvarig utgivare
på Siemens, Peter Henriksson,
kundansvarig på Siemens,
Charlotta Saghede, Business
Controller på Meva Energy, och
Eric Palander, automationsansvarig
på Meva Energy.



MER INFORMATION

[siemens.se](https://www.siemens.se) | [mevaenergy.com](https://www.mevaenergy.com)



Siemens är med på Ecolans OT2IT-resa mot datadrivna beslut

Ecolan, som tillverkar lättviktiga livsmedelsförpackningar i Helsingborg, har påbörjat sin OT2IT-resa för att framtidssäkra produktionen. En möjliggörare till digitaliseringen för att kunna fatta datadrivna beslut i realtid eller baserat på historik har varit mjukvaruverktyget PM-Analyze som hämtar in, presenterar och rapporterar data.

D en nya EU-förordningen om förpackningar och förpackningsavfall* sätter ambitiösa mål de närmsta åren för att minska, återanvända och återvinna förpackningar. Fokus ligger på att främja en cirkulär ekonomi genom standardiserade lösningar och tydliga krav på märkning och design. Som förpackningstillverkare gäller det att ha koll på sina data.

*PPWR, Packaging and Packaging Waste Regulation



Lättviktiga livsmedelsförpackningar där man får ut maximalt ur förpackningen.

– Ecolean kommer att vara väl förberedda. Vi insåg att vi behövde digitalisera, både för att effektivisera och för att ha koll på våra olika förpackningsmaterial. Spårbarhet och enkelhet blir allt viktigare, säger **Martin Trygg**, automationschef på Ecolean.

För Ecoleans del handlar det om flera aspekter: att säkerställa kvalitet, att effektivisera och att minska energi- och resursåtgång.

– För att kvalitetssäkra, effektivisera och resursspara behöver vi känna till våra siffror. Då behöver vi uppkopplade maskiner, säger **Jenny Jakobsson Evergren**, chef för automations-support på Ecolean.

LÄTTA OCH INNOVATIVA

Ecolean är en global leverantör av lättviktiga förpackningslösningar och fyllningsmaskiner för flytande livsmedel.

– Våra innovativa förpackningar kombinerat med hållbar teknik minskar miljöpåverkan och effektiviserar livsmedelsindustrin, säger Martin Trygg.

DATA MANAGEMENT FÖR DATADRIVET BESLUTSSTÖD

För att ha koll på sina data ville Ecolean samla dem på ett ställe.

– Vi behövde konsolidera data med en sanning. Istället för att gå in i flera olika system samlar vi nu in data till ett ställe för att snabbt få överblick, säger **Victor Sjöstrand**, automations-specialist på Ecolean.

UTMANING

För att optimera, effektivisera och höja kvaliteten i produktionen av förpackningar för flytande livsmedel måste aktuella och korrekta data analyseras för att identifiera rätt åtgärds punkter. Ecolean behövde därför skapa en samlad sanning av alla loggade data med tydlig semantik för alla intressenter. En helhetsbild av både process- och kvalitetsdata är särskilt viktig i branscher med höga hygien- och säkerhetskrav.

LÖSNING

Med Siemens SCADA-system Simatic WinCC Unified och tillvalsmjukvaran PM-Analyze för Process Management kan detaljerad analys utföras på historiska data från produktionsprocessen. Detta är särskilt värdefullt i tillverkning av livsmedelsförpackningar, där spårbarhet, kvalitet och effektivitet är avgörande. Genom att analysera trender och avvikelser kan man snabbt identifiera flaskhalsar eller kvalitetsproblem.

RESULTAT

Genom att visualisera och jämföra nyckeltal som till exempel OEE, kasseringsfrekvens, First Pass Yield och MTTR över tid kan Ecolean optimera maskininställningar, minska stillestånd och förbättra resursanvändningen. Detta leder till både ökad produktivitet och minskade kostnader. PM-Analyze fungerar sömlöst med visualiseringssystemet och andra Process Management-moduler från Siemens, vilket har minimerat tiden för utveckling, installation och idriftsättning.

Det började med att de medarbetare som hade beredskap ville ha möjlighet att även hemifrån kunna gå in i systemen för att kontrollera status och se när underhåll och service ska göras. Sedan har det spridit sig till alla enheter.

– Vi hade ju redan alla data, vi behövde bara plocka ut dem, säger Victor Sjöstrand.

Det handlar om att alla som är berörda ska ha tillgång till samma information.

– Det underlättar verkligen vardagen för många, säger **Edin Dedić**, automationsingenjör på Ecolean.



Pedagogiska dashboards presenterar insamlade data.

SAMLAR, VISAR OCH SKAPAR DATA MED PM-ANALYZE

I produktionslinjerna används Siemens styrsystem, bland annat Simatic S7-1200 G2, och Simatic WinCC Unified som visualiseringssystem mellan människa och maskin, där Process Management-tillvalet PM-Analyze samlar in och presenterar data.

Ecolean har byggt en applikation där mjukvaran PM-Analyze, som delar databas med SCADA-systemet, hämtar data från tioalet olika källor via OPC- och MQTT-kommunikation och presenterar dessa data eller skapar nya data från de data som hämtats in.

Med pedagogiska dashboards på tavlor ute i verksamheten går skiften på dagliga möten igenom vad som har hänt, vad det kan bero på samt bestämmer prio för arbetet. Operatörerna kan själva gå in i systemet för att se bakgrunden till varför något inträffade och beslut till åtgärder kan tas direkt på pulsmöten ute vid linjerna.



För att kvalitetssäkra, effektivisera och resursspara behöver vi känna till våra siffror



– Det blir ett väldigt bra underlag att diskutera kring för att kunna ta datadrivna beslut i realtid eller baserat på historik, säger Victor Sjöstrand.

KPI:erna som Ecolean jobbar med jämförs direkt – systemet uppdateras var femte sekund – och man kollar larm, trender etc. Användarna kan skapa anpassade diagram, dashboards och rapporter för olika användargrupper, från operatörer till kvalitetschefer.

REDO FÖR FRAMTIDEN

Det manuella arbetet kring rapporter har försvunnit.

– Vi kan skapa alla typer av rapporter, spara dem, dela och skicka. Man sätter bara åtkomstkriterier för vem som ska kunna titta på vad, och hur. Förut fick någon skriva ner och knappa in manuellt, säger Edin Dedić.

– Vi ville ha en plattform att kunna växa i. Nu kan vi bygga på med MES- och MOM-system och kan i framtiden även gå mer mot molnbaserade tjänster eller as-a-service med gemensam SQL-databas. Vi är redo för framtiden, säger Victor Sjöstrand. ■



Jenny Jakobsson Evergren, chef för automationssupport på Ecolean, Edin Dedić, automationsingenjör på Ecolean, Victor Sjöstrand, automationsspecialist på Ecolean, Martin Wernersson, automationsingenjör på Ecolean, Martin Trygg, automationschef på Ecolean, Maamoun Ali, automationsingenjör på Ecolean samt sittande Magnus Åberg, då kundansvarig på Siemens, och Jos Klein Woud, produkt- och säljansvarig för Simatic WinCC System på Siemens.

TEKNIK

AUTOMATIONSPLATTFORM

TIA Portal

STYRSYSTEM

Simatic S7-300, S7-1200 G2, S7-1500

HUMAN MACHINE INTERFACE

SCADA: Simatic WinCC Unified System med PM-Analyze som tillval för Process Management; paneler: Simatic WinCC Unified Panels, Simatic HMI Key Panels

DISTRIBUERADE I/O

Simatic ET 200SP, ET 200eco PN, ET 200M

INDUSTRI-PC

box-PC: Simatic IPC BX-39A

FREKVENSBOMRIKTARE

Sinamics G120, G120C

SERVOSYSTEM

Sinamics S120, S210, S150 med Simotics S-motorer

NÄTVERKSKOMMUNIKATION

nätverksswitchar: Scalance X

STRÖMFÖRSÖRJNING

Sitop

LÅGSPÄNNINGSPRODUKTER & ELDISTRIBUTION

startapparater: kontaktorer: Sirius 3RT, motorskyddsbrytare: Sirius 3RV; eldistribution: lastfrånskiljare: Sentron 3LD

PM-ANALYZE

Presentera och rapportera data med några klick!

Till Simatic WinCC, Siemens kraftfulla och skalbara visualiseringssystemfamilj (Simatic WinCC V7/V8, WinCC Professional, WinCC Advanced och WinCC Unified) finns ett antal tillval för Process Management. Baserade på standardmjukvara ger dessa tillval kostnadseffektiva lösningar på många av dagens digitaliseringsutmaningar. PM-Analyze är ett sådant tillval och används för att

- inhämta data
- presentera data
- rapportera data.

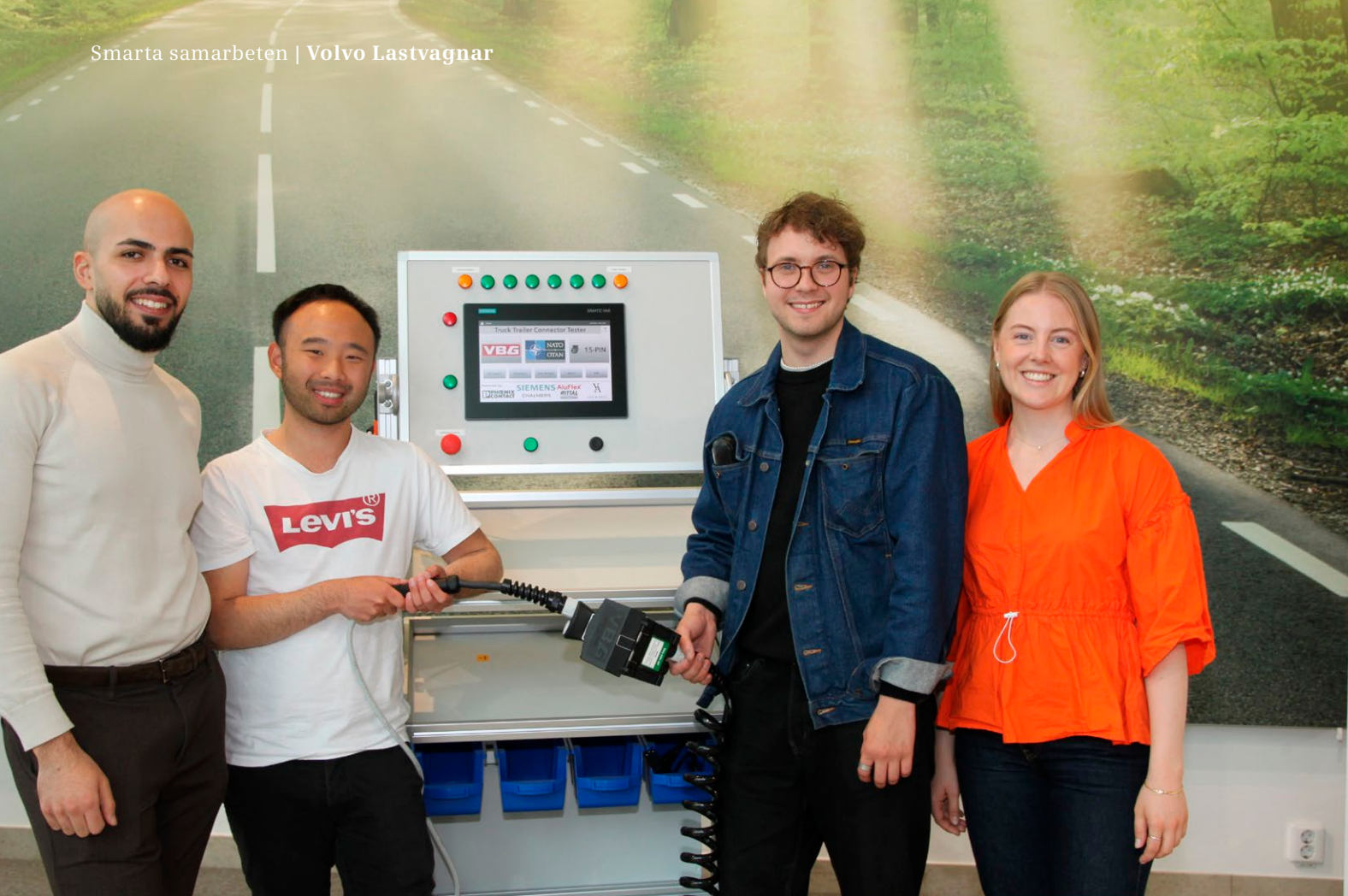


FRÅN DAGAR TILL TIMMAR

"Förut tog det mig två, tre dagar att skapa rapporter manuellt. Nu är det en digital process, som görs på några timmar, utan fel."

MER INFORMATION

 [siemens.se](https://www.siemens.se) |  [ecolean.com](https://www.ecolean.com)



Iliass Temsamani, produkt- och säljansvarig för industridatorer, HMI-paneler och IIoT på Siemens, Yan Gu, färdig student inom Production Engineering på Chalmers, Axel Malmberg, färdig student inom Product Development på Chalmers, och Emma Christensson, produkt- och säljansvarig för Simatic S7-1200 G2 och uppkoppling på Siemens.

Exjobb ger **säkrare testrigg** för lastbilar med ny teknik från Siemens

Testriggen för släpvagnskopplingar på Volvo Lastvagnar var gammal och uttjänt. Två Chalmersstudenter utvecklade en modern lösning med Siemens nya styrsystem Simatic S7-1200 G2.

Testrigheten för att testa elektriska signaler mellan lastbil och släp var gammal, klumpig och tidskrävande. I sitt examensarbete på Chalmers tekniska högskola i Göteborg tog sig

Yan Gu och **Axel Malmberg** an utmaningen att i samarbete med Volvo Lastvagnar utveckla en säkrare och mer tillförlitlig lösning. Tack vare de båda Chalmersstudenterna har Volvo Lastvagnar nu fått en pålitlig testtrigg som är modulär, skalbar och håller många år framöver.

Det handlar om att innan lastbilen kommer ut på marknaden säkerställa att lampor och ljussignaler fungerar genom ett testverktyg som simulerar att lastbilen har ett släp för att kunna testa signaler däremellan utan att släpet behöver kopplas in.

De tidigare testutrustningarna var gamla, manuella och hade länge orsakat problem; de var tunga, kunde lätt tappas och felsökningen skedde med en pol mot jord, en mot kontakt – inte så säkert för personalen. Nu ersätts tre olika testverktyg med ett enda som är mer hållbart och säkert för både personalen och framtiden.

STANDARDISERAT OCH ANVÄNDARVÄNLIGT

Chalmersstudenterna Yan Gu och Axel Malmberg byggde testutrustningen själva i samarbete med Volvo Lastvagnar och använde färdiga lösningar från Siemens.

– Vi gjorde en Chat GPT-bot som laddade ner alla manualer och så frågade vi boten när vi behövde, säger Yan Gu.

Att använda standardiserad teknik istället för hemmasnickrade system har många fördelar. Bland annat är det säkrare på lång sikt vad gäller tillgång till reservdelar och kompetens. Nu blir dessutom resultatet mer pålitligt; tidigare kunde man inte säkert veta om en felsignal berodde på lastbilen eller testutrustningen.

– Med modern teknik blir det plötsligt enkelt att utföra tester. Tack vare deras användarvänliga lösning är testningen nu ett enmansjobb istället för ett tvåmansjobb, säger **Albin Leyonlund**, Customer Adaptation Engineer och handledare på Volvo Lastvagnar, som värdesätter insatsen:

– Yan och Axels jobb har hjälpt oss att kunna bidra till en effektivare och snabbare efterkontroll av släpvagnskontakter kopplat till vår kundanpassningsverkstad. Deras arbete har alltid gjorts med ett glatt och positivt mindset, allt från att leta efter komponenter till att hålla presentationer kring testutrustningen. Deras bidrag till oss har varit värdefullt med deras utbildningar som grund för att lyckas med examensarbetet.



Flera olika kontaktanslutningar finns på den pålitliga testtriggen som är modulär, skalbar och håller många år framöver.

NY TEKNIK FRÅN SIEMENS

I testutrustningen används Siemens nya styrsystem Simatic S7-1200 G2 och operatörspanelen Simatic HMI MTP1200 Unified Basic Panel.

– Vi insåg att vi behövde pålitliga komponenter. Vi pratade med underhållsavdelningen på Volvo och de använder bara Siemens, säger Yan Gu som på webben såg att en ny PLC hade släppts.

– Simatic S7-1200 G2 är billigare och mer kompakt än den större Simatic S7-1500. Jämfört med den gamla S7-1200 har den nya G2 bättre prestanda och mer flexibilitet vad gäller maskinsäkerhet och Motion Control. Jag kollade Youtubeklipp och kom fram till att S7-1200 G2 var precis vad vi ville ha, fortsätter Yan Gu.



INTUITIVT MED TIA PORTAL

Konfigurationen av panelen gjordes i Siemens automationsplattform TIA Portal.

– Det var väldigt smidigt att jobba i TIA Portal, konstaterar Axel Malmberg.

– Ja, intuitivt och lätt att förstå, instämmer Yan Gu.

Volvo Lastvagnar har nu fått en testutrustning som är säker och pålitlig och som enkelt kan uppgraderas tack vare den modulära konstruktionen. Vill man registrera data från utrustningen i framtiden är det inga problem – utrustningen är framtidsredo för det.

– Det är väldigt roligt och smickrande att personalen uppskattar vårt arbete. Nu hoppas vi såklart att denna lösning kan bli en standard för fler anläggningar, säger Axel Malmberg. ■

TEKNIK

AUTOMATIONSPLATTFORM

TIA Portal

STYRSYSTEM

Simatic S7-1200 G2

HUMAN MACHINE INTERFACE

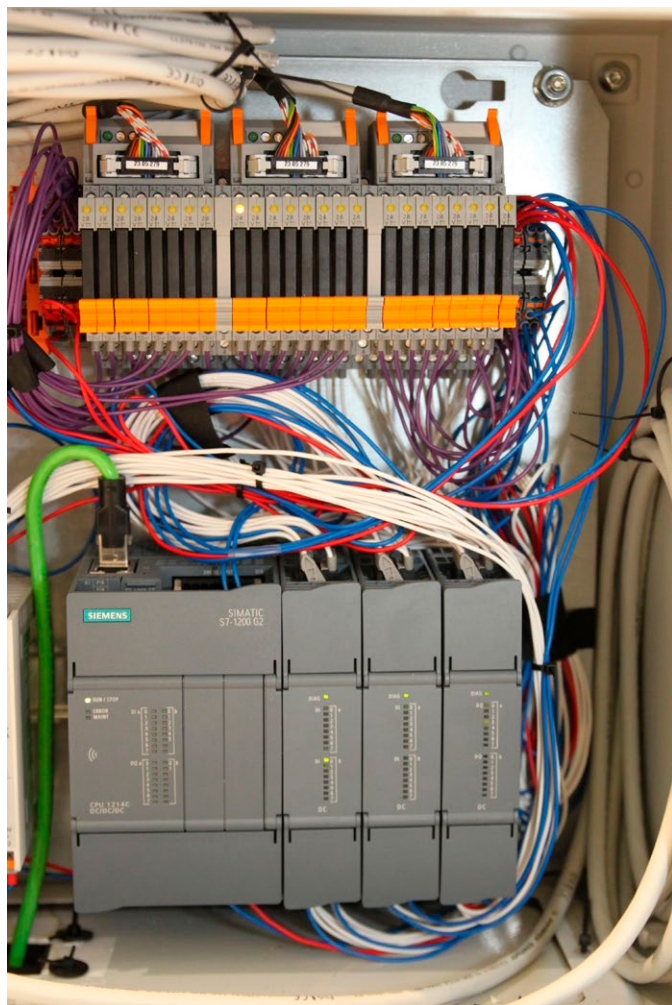
Simatic HMI MTP1200 Unified Basic Panels

BUSSKOMMUNIKATION

Profinet



Läs examensarbetet



KOMPAKT STYRNING FÖR ENKEL AUTOMATION – SIMATIC S7-1200 G2

Smarta, effektiva, tillförlitliga och skalbara lösningar som höjer produktiviteten behövs inom industrin.

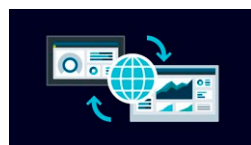
Den framtidsorienterade Simatic S7-1200 G2-serien består av kompakta programmerbara styrsystem som möter dessa krav med förbättrad prestanda och kraftfull funktionalitet med platssparande design.

- Förbättrad prestanda och skalbarhet
- Flexibel maskinsäkerhet
- Effektiv Motion Control

Yan Gu, färdig student inom Production Engineering på Chalmers.



ANVÄNDARVÄNLIGT HMI – SIMATIC HMI UNIFIED PANELS



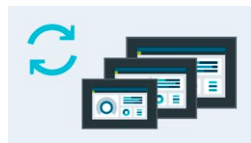
Webbklient för fjärrstyrning

Den underhållsfria webbklienten ger flexibel fjärråtkomst till visualiseringen.



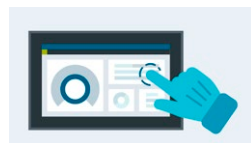
Security Integrated

Operativsystemet baserat på Simatic Industrial OS ger maximal säkerhet. Gränssnitt och appar som inte behövs kan enkelt avaktiveras eller avinstalleras.



Allt under kontroll

Säkerhets- och mjukvaruuppdateringar laddas ned till enheterna direkt från TIA Portal → enkelt att hålla dem uppdaterade och säkra.



Redo för tuff industri

Simatic Unified Panels är utformade för tuffa miljöer och kan användas med vanliga arbetshandskar. Smart detektering av felaktiga tryck gör panelerna robusta, användarvänliga och pålitliga.

Säkerhet, säkerhet och säkerhet

När vi pratar om säkerhet kan förvirring uppstå kring vad som avses. Det finns många typer av säkerhet och begreppen är många.

Ann Axelsson, Portfolio Consulting Professional på Siemens, reder ut begreppen.

När jag pratar om säkerhet pratar jag oftast om **maskinsäkerhet** men jag befinner mig ibland i situationer där det istället pratas om **processsäkerhet**, **cybersäkerhet** eller annan typ av säkerhet och då är det lätt att halka på begreppen och missförstånd kan uppstå. Därför är det viktigt att börja alla diskussioner med att komma överens om parametrarna: att ta reda på deltagarnas utgångspunkter och vad slutmålet ska vara och inse att vägen till slutmålet ser olika ut beroende på var vi startar.

MASKIN- OCH PROCESSSÄKERHET VS CYBERSÄKERHET

Maskin- och processsäkerhet har mycket gemensamt men också många olikheter men i jämförelse med cybersäkerhet kommer jag här för enkelhetens skull att likställa dem.

Vad är då skillnaden mellan maskin-/processsäkerhet och cybersäkerhet? På engelska är distinktionen mer tydlig då de beskrivs med olika ord: Safety och Security. På svenska används samma ord, säkerhet, och då kan det bli klurigare att hålla isär begreppen.

Cybersäkerhet handlar om att skydda digitala tillgångar från korruption; avsiktlig eller oavsiktlig. Vi ska skydda våra system mot intrång, skadlig programvara och datastöld. Cybersäkerhet uppnår vi genom att analysera risker och implementera tekniska lösningar såsom brandväggar, åtkomstkontroll etc., implementera säkerhetspolicyer och rutiner samt utbilda personal om dessa och vilka fällor de kan ställas inför.

Maskin- och processsäkerhet handlar om att skydda människor och miljö från fysisk skada. Det åstadkommer vi genom att analysera risker och vid behov implementera tekniska lösningar, tydliga rutiner och utbilda personal... Känner vi igen det här?



Vad vi skyddar och hur kan skilja sig avsevärt men när det kommer till arbetsflödet för att nå önskad säkerhet kan vi ändå se många likheter.

MASKINSÄKERHET VS PROCESSSÄKERHET

Utmaningarna i att skydda människor och miljö skiljer sig åt en hel del mellan tillverkningsindustri och processindustri.

Inom tillverkningsindustri används till stor del maskiner för att utföra arbetet. **Maskinsäkerhet** fokuserar på att minimera risken för olyckor och fysiska skador för människor som befinner sig runt maskinerna. Riskerna är ofta förknippade med rörelser.

Inom processindustrin hanteras farliga material, kemikalier, höga tryck med mera. **Processsäkerhet** handlar om att förebygga och hantera risker förknippade med till exempel explosioner och utsläpp av farliga kemikalier för att skydda både människor och miljö.

Självklart förekommer maskiner inom processindustri och processer inom tillverkningsindustri; det finns alltså ingen absolut gräns utan de överlappar varandra i mångt och mycket, vilket gör det ännu viktigare att förstå begreppen för att undvika missförstånd.

När jag försöker förklara vilka olika utmaningar vi ställs inför när vi jämför maskin- och processsäkerhet brukar jag falla tillbaka på tre punkter:

- **Konsekvenserna av en olycka kan vara väldigt olika** mellan maskin och process. När en olycka sker i en maskin är det oftast en eller ett fåtal människor som drabbas. I en processindustri kan det bli betydligt större konsekvenser för fler människor och för miljön.
- **Hög efterfrågan vs låg efterfrågan** – inom maskinsäkerhet pratar vi i princip uteslutande om hög efterfrågan, high demand mode, det vill säga våra implementerade säkerhetsfunktioner används regelbundet under maskincykeln eller testas regelbundet på annat sätt. Enligt maskinsäkerhetsstandarder är hög efterfrågan att funktionen används/testas ≥ 1 ggn/år. Inom processindustrin finns exempel på många säkerhetsfunktioner som inte används inom detta tidsintervall och då pratar vi istället om låg efterfrågan, low demand mode. Att säkerställa att en säkerhetsfunktion fungerar då den behövs ger oss då olika utmaningar inom maskin- och processäkerhet.
- **Slitage vs klibbning** – inom maskinsäkerhet där våra säkerhetsfunktioner används regelbundet drabbas vi av slitage på komponenter, till exempel att en kontaktor behöver bytas ut efter ett visst antal aktiveringar. Inom process, där funktionerna inte används lika ofta är risken istället att komponenter klibbar, en stor utmaning som behöver tas hand om.

FUNKTIONSSÄKERHET VS ELSÄKERHET

Maskin- och processäkerhet kan delas upp i olika inriktningar. Jag tänker främst på funktionssäkerhet och elsäkerhet.

Funktionssäkerhet inom maskinsäkerhet handlar om design av maskiner för att säkerställa att de fungerar på ett säkert sätt, ofta relaterat till mekaniska risker. Exempel kan vara kross- och klämskador orsakade av objekt i rörelse eller att förlora kroppsdelar i sågar eller saxar. Säkerhet uppnås genom lämplig konstruktion och implementering av säkerhetsfunktioner som kan upptäcka och reagera på farliga situationer.

När det kommer till processäkerhet fokuserar funktionssäkerheten på att processerna ska utformas för att vara säkra och att risker för olyckor och incidenter samt konsekvenserna av dessa minimeras. Exempel här kan vara samma som för maskinsäkerhet men även utsläpp av farliga kemikalier som kan skada både människor och miljö.

Elsäkerhet handlar om risker för personskador och skador på miljö och utrustning som kan ske av elektrisk utrustning och installationer. Detta gör elsäkerheten till en stor del av maskin- och processäkerheten då elektriska komponenter är mer regel än undantag i styrning av maskiner och processer.

För att en maskin eller process ska uppfylla kraven på säkerhet måste både funktionssäkerhet och elsäkerhet uppfyllas.

FÖRORDNINGAR, DIREKTIV, STANDARDER... OCH MÄNNISKOR

Vad som är tillräcklig säkerhetsnivå bestäms av lagar i form av förordningar och direktiv från EU. Lagar kan vara svåra att tolka. Därför har vi standarder som hjälper oss att ta fram arbetsmetoder och rutiner som vi sparar i våra verksamhets-system. Det är här lätt att bli fartblind och lägga allt fokus på att säkerheten ska vara dokumenterad. Missförstå mig inte, att ha dokumenterade arbetsmetoder och rutiner är viktigt och en stor del i att nå målen för säkerhet. Men vad händer om de inte följs?

Jag har själv besökt fabriker där jag, innan tillträde, måste genomföra en säkerhetsutbildning; vanligtvis en film på några minuter som beskriver risker jag kan utsättas för, hur jag ska bete mig och vilken skyddsutrustning jag ska använda. Rutinen är utförd och det är säkert att släppa in mig. Men tänk om jag inte förstått allt eller efter några timmar glömt vad som sas?

Återigen, missförstå mig inte, att få en säkerhetsgenomgång innan tillträde är en mycket viktig del i säkerhetsarbetet. Men det är lätt att det blir just en fråga om att bocka av saker i en checklista och att vi glömmar vikten av att bygga upp en kultur som uppmuntrar säkerhetstänkande. Vi kan inte endast informera om säkerhetsrutiner, vi måste också förankra dem i organisationen så att de blir en naturlig del av vardagen. Om vi upplever att skyddsbarriärer och skyddsutrustning försvårar för, eller förhindrar oss att utföra, vårt arbete på ett effektivt sätt, kommer vi då använda dem?

RISKANALYS I VARDAGEN

Vi människor är duktiga på att analysera risker och ta beslut om hur vi minimerar dem och vilka risker vi anser acceptabla. Vi gör det hela tiden i vår vardag; några av riskanalyserna gör vi väldigt medvetet men de flesta går mer på rutin.

Vi är då tillbaka till vikten av rutiner i säkerhetstänkandet. Det är bra att ha väl etablerade rutiner som är en del av vardagen. Men vi kan inte förlita oss på dem som en garanti för säkerhet, oavsett vilken typ av säkerhet vi pratar om.

FORTSÄTTNING FÖLJER

Nu har jag raljerat om vikten av att se bortom lagar. I nästa nummer dyker jag djupare i mitt specialområde maskinsäkerhet och tittar mer på förordningar, direktiv och standarder och vilka hjälpmedel vi kan erbjuda för att säkerställa att era maskiner är säkra. ■

MER INFORMATION

✉ ann.axelsson@siemens.com

SITRAIN utbildningscenter 2025/2026

		november					december		
Utbildningen	Pris	44	45	46	47	48	49	50	51
SIMATIC TIA Portal									
Simatic TIA Portal uppdatering från Step 7 V5.4/5.5	24 800								
Simatic WinCC SCADA i TIA Portal	25 000								
Simatic TIA Portal Safety	27 800						J:må-fr		
Simatic TIA Portal programmering 1 för plc	O 24 800		G:må-to	M:må-fr					G:må-to
Simatic TIA Portal programmering 2 för plc	24 800							G:må-fr	
Simatic TIA Portal service 1 för plc	O 24 300	G:må-fr					G:må-fr		
Simatic TIA Portal service 2 för plc	24 300					G:må-fr			
Simatic TIA Portal WinCC för paneler	20 200		G:må-on						
Simatic programmering med S7-Graph i TIA Portal	20 200				G:ti-to				
Simatic programmering 1 med S7-SCL i TIA Portal	19 700								
TIA Portal Programming Expert	19 700								
SIMATIC S7 Classic									
Simatic S7 service 1	24 300				S:må-fr				
Simatic S7 service 2	24 300								
Simatic S7 programmering 1	24 800						SK:må-to		
Simatic PCS 7 system grund standard	44 400								
Simatic PCS 7 system grund intensiv	31 300								
Simatic PCS 7 AS engineering	31 300					S:må-fr			
Simatic PCS 7 OS engineering	31 300								
Simatic PCS 7 service	29 900			S:må-fr					
Simatic PCS neo System Training, Basic	31 300								
Simatic Batch	31 300							S:må-fr	
Simit in Process Automation	24 900				S:ti-to				
Simit i diskret automationsteknik för nybörjare	24 900								
SIMATIC HMI									
Simatic WinCC system grund	24 900								S:må-fr
Simatic WinCC Unified 1, System Course	20 200			G:ti-to					
Simatic WinCC Unified 2	15 900							S:må-ti	
Simatic WinCC Unified 3	15 900							S:on-to	
SIMATIC NET									
Simatic Net Profibus/Profinet service	24 800				G:må-fr				
Profinet with Simatic Controllers	24 900								
Ethernet Fundamentals in Industrial Networks	15 200		G:må-ti						
Switching & routing in Industrial Networks	32 300						S:må-fr		
Wireless LAN in Industrial Networks	24 900								S:ti-to
Security in Industrial Networks	24 900							S:må-on	
Network Monitoring & Configuration SINEC NMS with SCALANCE	26 800								
SINUMERIK									
Sinumerik 840D pl/sl programmering grund	20 200			SK:må-on					
Sinumerik 840D pl/sl programmering fortsättning	20 500	SK:må-on							
Sinumerik 840D sl service	30 900							SK:må-fr	
Sinumerik 840D sl service fortsättning	27 500								SK:må-on
Sinumerik 840D Safety Integrated	30 900				SK:må-fr				
Sinumerik ONE Service Training	30 900		SK:må-fr						
SIMOTION/SINAMICS									
Sinamics S120 startup & service	28 100								
Sinamics S120 parametrering och idriftsättning/service i TIA Portal	28 400								
Sinamics G120 startup & service	11 400								
Övriga utbildningar – ej schemalagda; kontakta oss vid intresse									
Simatic S7 Engineering Tools	24 800								
Simatic Net Profibus	24 900								
Simatic S7-1200	18 100								
Simocode parametrering	15 900								
Simotion programmering	30 900								
Masterdrives service & underhåll	15 900								
Motion Control i TIA Portal	28 400								

Utbildningarna hålls i Stockholm (S), Göteborg (G), Jönköping (J), Malmö (M) eller Skövde (SK), alternativt online (O). Alla priser är exklusive moms. Med reservation för tryckfel.

O = finns som online-utbildning. Fler online-utbildningar finns på engelska. Kontakta oss vid intresse.

Allmänna villkor: Anmälan är bindande. Om avbokning sker mellan fyra till två veckor före start debiteras 50 procent av avgiften. Därefter debiteras full avgift. Detta gäller även vid sjukdom. Vid samtidig ombokning till annan utbildning ges 25 procent rabatt. Om anmäld deltagare inte kan komma går det bra att skicka någon annan. Vid färre än fem deltagare förbehåller vi oss rätten att ställa in utbildningen.

[illegible]

KONTAKTA OSS

Therése Fagerström: ☎ 08-728 14 48 | Susanne Bonde: ☎ 08-728 15 70 | ✉ sitrain.se@siemens.com | 🌐 siemens.se/sitrain



Zandra Nilsson, tidigare säljchef, är sedan april nordisk vd för Siemens Digital Industries Software med placering i Solna.

✉ zandra.nilsson@siemens.com



Anja Eimer, tidigare Global Head of Verticals Water & Waste Water, Chemicals, Oil & Gas, Glass & Solar samt Minerals & Mining, är sedan oktober Head of Digital Industries i Sverige och Norden med placering i Solna.

✉ anja.eimer@siemens.com



Svenja Kuczmera anställdes i april i Solna som CFO för Siemens Mobility AB. Svenja kommer närmast från Envirotainer och har tidigare arbetat inom Siemens Digital Industries.

✉ svenja.kuczmera@siemens.com



Kristina Gjørde, OEM Sales inom Digital Industries med placering i Mölndal, är sedan oktober Global Account Manager för JBT Marel.

✉ kristina.gjoerde@siemens.com



Jörgen Blomqvist anställdes i juli i Solna inom Digital Industries som Sales Specialist och produktansvarig för Mechatronics Systems med Simotics E-motorer för 24/48 V-matning. Jörgen kommer från Ebm-papst som förvärvades av Siemens i juli.

✉ jorgen.blomqvist@siemens.com



Jenni Moberg, tidigare chefsassistent inom Digital Industries, är sedan oktober vd-assistent till Andrea Waenerlund samt CFO-assistent för Siemens AB och Siemens i Norden med placering i Solna.

✉ jenni.moberg@siemens.com



Daniel Kjellberg anställdes i augusti i Malmö inom Digital Industries som Account Manager inom Territory Sales. Daniel kommer närmast från Rejlers.

✉ daniel.kjellberg@siemens.com



Jessica Boqvist, chefsassistent till Andreas Hillerström som är ekonomichef för Digital Industries i Sverige samt CFO för Siemens i Danmark, är sedan oktober även chefsassistent till Anja Eimer, Head of Digital Industries i Sverige och Norden, med placering i Solna.

✉ jessica.boqvist@siemens.com



Mikael Leksell, tidigare vd för Siemens AB och Siemens i Norden med placering i Solna, har sedan oktober en global roll som Digital Industries Sales Zone Head EMEA.

✉ mikael.leksell@siemens.com



Nusha Heit, tidigare inom Siemens Mobility, är från november CFO för Siemens i Sverige och Norden med placering i Solna.

✉ nusha-susanne.heit@siemens.com

MER INFORMATION

🌐 siemens.se/jobb

Andrea Waenerlund ny vd för Siemens i Sverige och Norden

Den 1 oktober tillträdde Andrea Waenerlund som ny verkställande direktör för Siemens AB samt för Siemens i Norden.

Andrea Waenerlund efterträder Mikael Leksell som vd för Siemens i Sverige och Norden. Mikael Leksell går vidare till en global roll som försäljningschef för EMEA-zonen inom Siemens Digital Industries.

Andrea Waenerlund har sedan tidigare varit vd för Siemens i Danmark och har lång erfarenhet av att leda komplexa organisationer i förändring. Med över 20 års internationell erfarenhet inom ledarskap, strategi, affärsutveckling och digital transformation, bland annat från ledande roller på Schneider Electric, Eon och

Bravida, har hon en gedigen bakgrund för att ta Siemens vidare i Sverige och Norden.

– Jag är stolt över att få ta över rollen som vd för Siemens i Sverige och Norden. Tillsammans med våra engagerade medarbetare ser jag fram mot att bygga ett vinnande team och stärka det nordiska samarbetet. Siemens har en unik kombination av tekniskt ledarskap och möjligheter till utveckling och innovation som ger oss förutsättningar att skapa värde och stötta våra kunder på deras digitaliserings- och hållbarhetsresor, säger Andrea Waenerlund. ■



MER INFORMATION

✉ andrea.waenerlund@siemens.com | [siemens.se/press](https://www.siemens.se/press)

Hon är expert på cybersäkerhet

Med en bakgrund inom IT bidrar Amalie Lønning med en stor mängd erfarenhet och insikter inom cybersäkerhet – en expertis som är ovärderlig inför framtidens utmaningar.

Trots examen i företagsekonomi och nationalekonomi ledde passionen för ny teknik och framtidsinriktade lösningar henne snabbt till cybersäkerhet. Idag är **Amalie Lønning**

Cyber Portfolio Manager på Siemens för Norden.

– Jag tillhör generationen som växte upp med datorer och internet men det var spelvärlden och min nyfikenhet som först introducerade mig till cybervärlden. Då handlade det inte om cybersäkerhet, det handlade om att krascha spelservrar när vi insåg att kod kunde användas till mer än att bygga hemsidor.

– Det var också coolt att utforska vad som hände på dark web, även om jag hade väldigt liten förståelse för hur man skyddar sig mot cyberattacker. Låt oss bara säga att några laptops fick gå i graven... Jag brukade säga till mina föräldrar att det bara var dåligt antivirusprogram.

ATT VARA VAKSAM PÅ HOTBILDEN

Verkligheten idag är att vi lever i ett geopolitiskt klimat präglad av stora spänningar, både globalt och lokalt. Vi måste erkänna att det finns kriminella grupper och aktörer som vill göra våra liv svårare. När detta kombineras med samhällets ökande digitalisering blir vi ännu mer sårbara.





Vi har ett starkt team med ingenjörer, utvecklare och säkerhetsexperter i hela Norden och i kombination med vårt globala nätverk är vi redo att stödja våra kunder på deras digitala resa på ett säkert sätt

DIGITALISERING FÖRST, SÄKERHET SEDAN

Detta märks särskilt i den digitala omvandlingen av industrin och kritisk infrastruktur. Alla vill få ut mer av sina system med färre resurser för att stödja den gröna omställningen. Digitalisering är en nyckel till lösningen. Utmaningen är att vi ofta tänker på säkerheten först efteråt.

Vi öppnar nu upp system och processer som traditionellt har varit avskilda från omvärlden. Detta för samman två mycket olika världar: Operational Technology (OT) och Information Technology (IT).

Amalie Lønning påpekar att dessa två områden fungerar enligt fundamentalt olika säkerhetsprinciper:

– Det är en diplomatisk övning i sig att få ihop höglackat och loafers med skyddsskor och hjälmar i samma rum för att samarbeta kring morgondagens säkerhetslösningar.

TAR VÅRT SAMHÄLLSANSVAR PÅ ALLVAR

Vilken roll spelar vi på Siemens i att möta framtidens utmaningar?

– En sak är säker: vi tar vårt samhällsansvar på allvar. Vi är en leverantör av hårdvara och mjukvara för industri och kritisk infrastruktur och våra kunder förlitar sig på våra lösningar för att hålla samhället igång.

– Vi har ett starkt team med ingenjörer, utvecklare och säkerhetsexperter i hela Norden och i kombination med vårt globala nätverk är vi redo att stödja våra kunder på deras digitala resa på ett säkert sätt, säger Amalie Lønning.

VAR BÖRJAR VI?

Vilka är de viktigaste stegen för nordiska företag när det gäller industri och kritisk infrastruktur?

– Svaret beror delvis på kundens situation. Det viktigaste första steget är att göra en grundlig kartläggning och riskbedömning av kritisk utrustning ur ett cybersäkerhetsperspektiv. Generellt ser vi att många organisationer har förbättringspotential när det gäller patchhantering och säkerhetsövervakning av kärnkomponenter.

Amalie Lønning betonar att många organisationer redan har implementerat olika cybersäkerhetsåtgärder men att dessa ofta inte är väl integrerade med företagets operativa miljö.

– Med lite hjälp att reda ut dessa frågor ser vi ofta att säkerhetsnivån kan förbättras avsevärt.

Framöver rullas nya regleringar ut över hela EU, som NIS2-direktivet som måste tas i beaktande.

– Om du redan har börjat arbeta med detta har du lagt en solid grund att bygga vidare på. ■

MER INFORMATION

✉ amalie.lonning@siemens.com

Industrin visar god cybersäkerhet – men **kommunikationen mellan IT och OT** måste förbättras

Automationsnytt tog ett snack med Kristian Kannelønning, doktor i informationssäkerhet och kommunikationsteknik, som nyligen avslutat ett fyraårigt forskningsarbete om cybersäkerhet inom Industri 4.0. Vi pratar om vad industrin gör rätt, var förbättringspotentialen finns och hur företag kan ta sina första steg mot bättre cybersäkerhet.

Förutom att vara Cybersecurity Officer på Siemens i Norge och Product & Solution Security Officer för Smart Infrastructure i Norden har **Kristian Kannelønning** nyligen avslutat sin forskning som visar att den norska industrin generellt presterar bra inom cybersäkerhet men att det finns förbättringsutrymme.

– Människan betraktas ofta som den svagaste länken men mina resultat visar att deltagarnas faktiska beteende stämmer överens med hur de själva bedömer sin säkerhetsmedvetenhet, vilket är mycket positivt.

– Det är särskilt glädjande att se att anställda följer företagets regler och att säkerhetsåtgärder som används ligger i linje med internationella standarder. Dessutom betar sig anställda i organisationer som inte har drabbats av incidenter lika ansvarsfullt som de som har drabbats och båda grupperna använder liknande säkerhetskontroller. Det tyder på att cybersäkerhet är en prioritet, oavsett tidigare erfarenheter. Men det finns förbättringsområden. Det största är styrningen av cybersäkerhet inom OT. Vi ser tydliga kommunikationsbarriärer mellan IT och OT, vilket försvårar förståelsen för hur säkerhetsåtgärder påverkar det dagliga arbetet. När en säkerhetskontroll upplevs som ett hinder hittar personalen ofta kreativa sätt att kringgå den vilket försämrar säkerheten. Min

främsta rekommendation är att inkludera OT-personal i cybersäkerhetsstyrningen. Dessutom behövs mer specifik utbildning inom OT-cybersäkerhet och bättre återställandeplaner.

VILKA UTMANINGAR SER DU INOM OT?

– Ett tydligt problem är användningen av cybersäkerhetsstandarder. Dessa bör fungera som kunskapskällor men används inte i den utsträckning man skulle önska – särskilt inte av mindre företag. Våra data visar att det främst är större organisationer som följer sådana standarder.

– Mitt råd är att börja med det grundläggande. Se till att alla medarbetare känner till regler och riktlinjer – det kräver inte stora utbildningsbudgetar. Ett annat viktigt steg är att ha kontroll över sin installerade bas. Man behöver inte ett avancerat system men en uppdaterad tillgångsförteckning gör det möjligt att senare lägga till verktyg för sårbarhetshantering och patchhantering. Tre områden där OT ofta ligger efter jämfört med god IT-praxis är:

- tillgångsinventering
- sårbarhetshantering
- patchhantering.

– En positiv observation är att backup av kritisk mjukvara är vanligt förekommande. Däremot behöver användningen av återställandeplaner förbättras för att undvika kostsamma driftstopp.



Kristian Kannelønning, PhD, Cybersecurity Officer på Siemens i Norge och Product & Solution Security Officer för Smart Infrastructure i Norden.

HUR KAN FÖRETAG FÖRBÄTTRA SIN CYBERSÄKERHET?

– Det är svårt att ge generella råd eftersom behoven varierar beroende på företagets typ och storlek. Men en bra startpunkt är att fråga sig: Har vi kontroll över vår installerade bas? Det är grunden för att kunna arbeta med sårbarhetshandtering och patchhantering.

– Ur ett Chief Information Security Officer-perspektiv skulle jag också fokusera på att förbättra kommunikationen mellan IT och OT. Börja med att undersöka förekomsten av workarounds inom företaget. Följer alla medarbetare reglerna? Börja med att bjuda in nyckelpersoner från OT, öppna en dialog om deras utmaningar och se hur kraven kan justeras utan att kompromissa med säkerheten. Vi rekommenderar att OT-personal inkluderas i cybersäkerhetsstyrningen, det är kanske det långsiktiga målet. Men det finns

flera sätt att förbättra kommunikationen så börja med att skapa en kanal för öppna samtal.

– På ett mer teoretiskt plan föreslår jag att företag tänker i termer av vad man inom den akademiska världen kallar ett sociotekniskt system, det vill säga ett system där både mänskliga och tekniska element är sammanflätade och ömsesidigt beroende av varandra. Det innebär att säkerheten inte bara förbättras med teknik utan också genom att ta hänsyn till den sociala dimensionen, alltså människorna i organisationen. Ett exempel är Intrusion Detection Systems, IDS, som genererar många larm. Innan man installerar ett sådant system bör man fråga sig: Har vi kompetensen att tolka och agera på dessa larm? Om svaret är nej räcker det inte att bara stärka det tekniska skyddet utan man behöver även stärka kunskapen i företaget. ■

MER INFORMATION

✉ kristian.a.kanneloenning@siemens.com

Lowering cybersecurity entry barriers
for Industry 4.0 – läs PhD-avhandlingen



Ny era för cybersäkerhet i EU

Eftersom digitala hot ökar i både omfattning och komplexitet har EU tagit krafttag för att stärka den digitala säkerheten genom Cyber Resilience Act, en ny lag som syftar till att höja säkerhetsnivån för alla produkter med digitala komponenter som säljs inom EU.

För företag innebär Cyber Resilience Act, CRA, inte bara nya juridiska krav utan också en möjlighet att bygga förtroende genom att framtidssäkra sina produkter. För Siemens berörs stora delar av vår produktportfölj av den nya lagen. Men även till exempel maskinbyggare, som bygger en maskin baserat på många komponenter, har ett ansvar för att helheten är säker på maskinen på lösningsnivå.

VAD FÖRETAG BEHÖVER TÄNKA PÅ

För att möta kraven i CRA bör företag som säljer produkter eller maskiner med digitala komponenter fokusera på:

- **säkerhet från början** – säkerhetskrav måste integreras redan i designfasen
- **CE-märkning** – alla nätverksanslutna produkter måste uppfylla CRA:s krav för att få CE-märkas och säljas inom EU
- **sårbarhetshantering** – företag måste övervaka sina produkter för att hålla koll på sårbarheter och tillhandahålla kostnadsfria säkerhetsuppdateringar i minst fem år
- **incidentrapportering** – säkerhetsincidenter måste snabbt rapporteras till relevanta myndigheter
- **livscykelansvar** – säkerheten ska beaktas under hela produktens livscykel, från utveckling till avveckling.

FRAMÅT: FRÅN EFTERLEVNADE TILL KONKURRENSFÖRDEL

Att anpassa sig till CRA är inte bara en fråga om regelefterlevnad, det är en strategisk investering. Företag som tidigt implementerar robusta cybersäkerhetsrutiner kommer inte bara att undvika sanktioner utan också stå starkare i en marknad där digitalt förtroende blir allt viktigare.

SÅ IMPLEMENTERAR DU CRA

För att uppfylla kraven i CRA krävs mer än bara tekniska lösningar; det handlar om att bygga in cybersäkerhet i hela produktens livscykel. Med sju konkreta steg kan du gå från regelefterlevnad till konkurrensfördel:

1. **Kartlägg era produkter:** identifiera vilka produkter som omfattas av CRA – både hårdvara och mjukvara med digitala komponenter. Gör en analys av de risker som finns med produkterna.
2. **Bygg in säkerhet från början:** säkerhetsfunktioner ska vara en del av produktens design, inte ett tillägg i efterhand. Säkerställ säkerheten i leverantörskedjan; kan du ta ansvar för komponenterna i maskinen under hela maskinens livscykel?
3. **Inför sårbarhetshantering:** etablera rutiner för att upptäcka, åtgärda och rapportera sårbarheter – även efter att produkten lanserats.
4. **Dokumentera allt:** CRA kräver tydlig dokumentation av riskbedömningar, säkerhetsåtgärder och uppdateringsrutiner.
5. **Utbilda personalen:** säkerställ att alla relevanta roller förstår lagens krav och hur de påverkar utveckling och drift.
6. **Förbered CE-märkning:** produkter måste genomgå en konformitetsbedömning och uppfylla cybersäkerhetskraven för att få säljas inom EU.
7. **Planera för hela livscykeln:** säkerheten ska upprätthållas under hela produktens livstid, inklusive uppdateringar och avveckling. ■



EU Cyber Resilience Act

For safer & more secure
digital products

#DigitalEU #CyberSecEU

Checklista för CRA-implementering

- ☐ Identifiera berörda produkter
- ☐ Säkerställ "security by design"
- ☐ Etablera sårbarhetshantering och incidentrapportering
- ☐ Dokumentera cybersäkerhetsåtgärder
- ☐ Utbilda utvecklare och ledning
- ☐ Förbered CE-märkning enligt CRA
- ☐ Planera för långsiktig säkerhetsförvaltning

Cyber Resilience Act

CRA är en EU-förordning som syftar till att stärka cybersäkerheten för produkter med digitala element. Den gäller för alla produkter med digitala inslag som släpps ut på marknaden i EU. Det innebär att företag som tillverkar, importerar eller distribuerar sådana produkter måste se till att de uppfyller de nya cybersäkerhetskraven.

CRA trädde i kraft i 2024 men de huvudsakliga skyldigheterna börjar tillämpas först 2027. Under denna tid har tillverkare av produkter med digitala inslag en övergångsperiod på sig för att anpassa sig till de nya kraven.

De viktigaste delarna av CRA är:

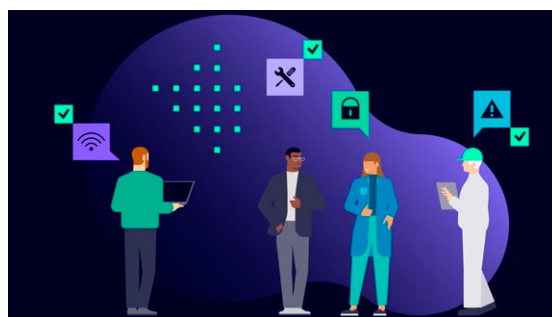
- **Skärpta säkerhetskrav:** produkter måste utformas och tillverkas på ett sätt som minimerar sårbarheter och säkerställer att de är motståndskraftiga mot cyberattacker.
- **Rapportering av sårbarheter:** Tillverkare måste rapportera allvarliga sårbarheter som upptäcks i sina produkter till en central myndighet.
- **CE-märkning:** produkter måste CE-märkas för att visa att de uppfyller de krav som ställs i CRA.

CRA är ett viktigt steg för att öka cybersäkerheten i EU och säkerställa att digitala produkter är säkra att använda.

Är det du levererar säkert?

Vet du vad produkten eller maskinen som du levererar egentligen innehåller? Det är det som Cyber Resilience Act handlar om: du ska veta att produkten eller maskinen som du levererar till kund är säker. "Starta dialogen med oss", uppmanar Michael Dufva, Cybersecurity Officer på Siemens i Sverige.

Alla pratar om det men nu är det dags att börja göra något.
– Vi vill uppmana våra kunder att ställa krav på sina leverantörer. Det går inte längre att vara luddig och allmängiltig i sin kravspecifikation kring cybersäkerhet. Du måste ta ansvar för din egen riskbild, säger **Michael Dufva**, Cybersecurity Officer på Siemens i Sverige.



MODERNISERA MER

Michael Dufva vill också uppmana till modernisering.

– Släng ut det gamla och investera i nya komponenter så att du kan lita på att det är säkert. En produkt kan innehålla kod som inte är uppdaterad och som därmed kan innehålla sårbarheter. I värsta fall finns inga uppdateringar att få för att den produkten har nått slutet på sin livscykel.

UPPRÄTTA INNEHÅLLSFÖRTECKNING

För att få koll på din produkt eller maskin behöver du upprätta en innehållsförteckning över vilka mjukvarukomponenter som ingår, en Software Bill of Materials.

– Många gånger använder man en tredjeparts-programvara som man sedan glömmer bort att man har laddat ned. Du behöver gå igenom dina produkter för att få koll på om komponenterna och mjukvarorna är korrekta och uppdaterade. Det här kan vi hjälpa till med men det är du som kund som har ansvaret. Det du köper från oss kan du lita på är säkert men du måste själv se till att det är uppdaterat. ■



– Vi som leverantör måste leverera säkra produkter som är skyddade mot cybersäkerhets-attacker. Vi ska också tillhandahålla uppdateringar om det uppstår en sårbarhet. Det bygger in ett behov av en livscykelhantering för sina produkter.

Det är något som Siemens gör men som även våra kunder behöver göra.

– De behöver göra en riskanalys och inventering av ingående komponenter i sina produkter för att bli medvetna om eventuella sårbarheter och risker kopplade till produkterna.

MER INFORMATION

✉ michael.dufva@siemens.com



Vi ger kraft åt var tredje maskin i världen – i **varje ögonblick**

Du kanske inte alltid ser oss. Men vi finns där.

Siemens ger kraft åt var tredje maskin världen över. Våra tekniska lösningar är en del av vardagen och gör ögonblicken smidigare, tryggare och mer hållbara.

Vår styrka ligger i det vi möjliggör tillsammans med våra kunder, partner och samhället. Vi visar vägen och driver utvecklingen framåt så att du får uppleva en värld som fungerar som den ska.

Varje dag ser vi till att livets självklarheter fungerar. Vi tror på en framtid där tekniken för oss närmare varandra, öppnar dörrar och skapar möjligheter. För alla.

[siemens.se/transform-the-everyday](https://www.siemens.se/transform-the-everyday)

Så hjälper vi dig möta de nya regleringarna

Anläggningar som är kritiska för samhället omfattas av NIS2. Vi på Siemens kan hjälpa till i förberedelserna inför den nya cybersäkerhetslagen.

Omfattas du av NIS2, då finns arbete som måste göras. Det handlar om att göra sin riskanalys, åtgärdsplan och att upprätthålla säkerheten under anläggningens hela livscykel. Hur kan vi på Siemens hjälpa er?

Det finns flera nivåer på hur vi på Siemens kan hjälpa till. Dels har vi vår tjänsteportfölj, där vi kan hjälpa till med riskanalys och genomlysning av verksamheten för att se hur den möter OT-cybersäkerhetsstandarden 62443.

Sedan har vi vår gigantiska produktportfölj där vi kan ge stöd kring produktfunktionalitet, dels hur man bygger sin automationslösning för en fabrik, dels hur man använder de individuella komponenterna och hur de konfigureras.

– Där har vi en helt ny funktionalitet som har släppts i senare releaser av TIA Portal gällande till exempel användarhantering, loggning och rollbaserad åtkomstkontroll. Vi har fått en helt ny nivå på användarhanteringen i industrisystemen, med individuella säkerhetsfunktioner i individuella produkter. Vi jobbar hela tiden aktivt med att svara

upp mot komponentstandarden för 62443, det vill säga 62443 4-2. Vi tar även fram mer dokumentation som hjälper dig i arbetet med att implementera säkerhetsfunktioner för att möta de säkerhetsnivåer som är definierade i 62443, säger **Urban Haglund**, Product & Solution Security Officer på Siemens för Digital Industries i Norden.

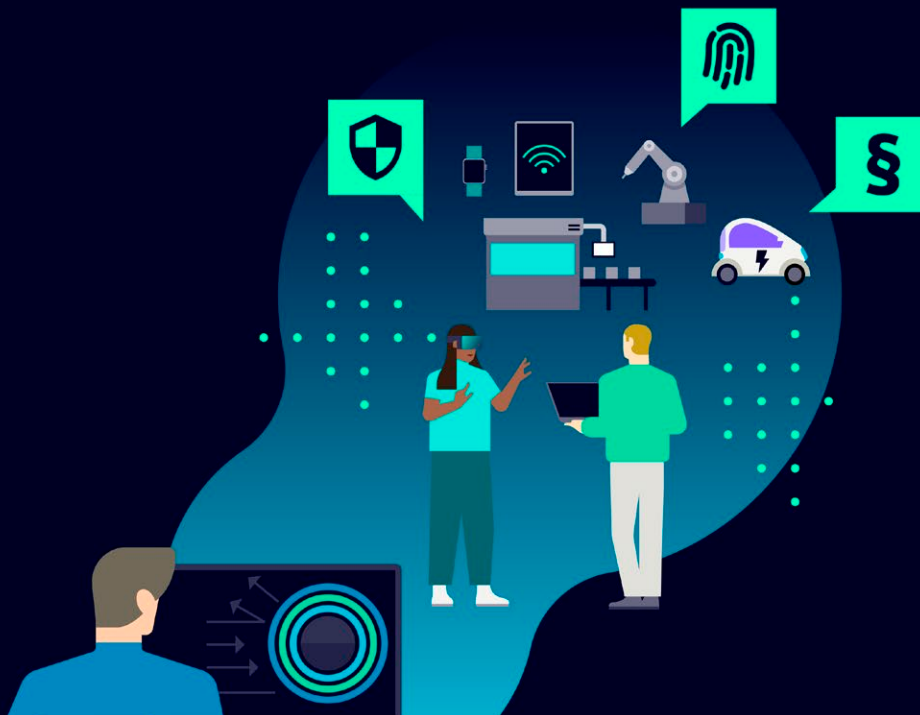
Siemens har mer än 120 fabriker världen över. Vi vet vad vi pratar om.

– Det viktigaste är att säkerställa tillgängligheten på anläggningen. Att förlora e-posten en timme på kontoret spelar inte så stor roll men förlorar du processen en timme i produktionen kan det gå riktigt illa. ■



Cybersäkerhet på Siemens i siffror

39	års cybersäkerhetsexpertis
1 300+	cybersäkerhetsexperten inom företaget
1 000+	incidenter hanterade månadsvis
100 000+	attackförsök årligen



SIEMENS PRODUCT CERT

Vårt centrala team med säkerhetsexperter som tar emot, utreder och rapporterar säkerhetsproblem relaterade till Siemens produkter, lösningar eller tjänster.



SINEC SECUREITY GUARD

Vår mjukvara som automatiserar sårbarhetshandlingen av komponenterna i en fabrik för att säkerställa och upprätthålla säkerheten i OT-nätverket.



SIEMENS INDUSTRIAL ASSET HUB (IAH)

Inventeringstjänst som upptäcker, identifierar och hanterar industriella tillgångar i hela verksamheten, oavsett leverantör eller typ, och bidrar till effektivare tillgångshantering.



INDUSTRIAL AUTOMATION DATACENTER (IADC)

Vårt specialanpassade datacenter för att säkerställa tillgängligheten på tillverkningen och kontroll på informationsflödet mellan IT och OT och som underlättar övergången till en framtidsäkrad, digitaliserad infrastruktur i en industri.



REMOTE INDUSTRIAL OPERATIONS SERVICES (RIOPS)

Modulära dygnet-runt-övervakade tjänster för IT/OT-infrastruktur med hårdvara, mjukvara, nätverk och service för att bland annat övervaka och uppdatera industriella processer, maskiner och enheter.

MER INFORMATION

✉ urban.haglund@siemens.com



Hållbarhet och produktivitet går hand i hand: 72 % mindre utsläpp, 145 % högre produktion

Siemens fabrik i tyska Fürth har tagits upp på World Economic Forums lista över ledande hållbara produktionsanläggningar.

World Economic Forum granskar tusentals fabriker världen över för att lyfta fram pionjärer som använder den senaste tekniken, varav vissa får ett särskilt erkännande för sitt arbete inom hållbar utveckling.

2021 utsågs Siemens fabrik i Amberg, Tyskland, till ett så kallat Sustainability Lighthouse. Två år senare utsågs även Siemens fabrik i Chengdu, Kina, och nu har även Siemens fabrik i tyska Fürth utsetts. Dessa fabriker använder innovationer för att främja effektivitet, konkurrenskraft, flexibla affärsmodeller och ekonomisk tillväxt samtidigt som de värnar om arbetskraft och miljö.

UPPNÅ NETTONOLL 2026

Fabriken i Fürth, där bland annat våra Simatic HMI-paneler tillverkas, siktar på att uppnå netto-

nollutsläpp senast 2026, fyra år tidigare än Siemens globala mål. Tack vare de utvecklingsprojekt som ett tvärfunktionellt hållbarhetsteam har drivit har man lyckats minska industriavfallet med 47 procent, energiförbrukningen med 64 procent och växthusgasutsläppen med 72 procent per producerad enhet samtidigt som produktionen har ökat med 145 procent.

RIKTADE INSATSER OCH EXAKTA BERÄKNINGAR

Ett holistiskt energihanteringssystem med över 350 energimätare som samlar in data från hela anläggningen gör att riktade insatser för att minska energiförbrukningen kan göras. Produkternas koldioxidavtryck beräknas exakt med mjukvaru-verktyget Sigreen. ■

MER INFORMATION

 siemens.com/press

TIA Portal V20



TOTALLY INTEGRATED AUTOMATION

Ökad prestanda och effektivitet med TIA Portal V20

Engineeringsmiljön i version 20 av engineeringplattformen TIA Portal erbjuder utökad funktionalitet, inklusive stöd för nya styrsystem med omfattande funktioner för Motion Control och Safety.

Det nya styrsystemet Simatic S7-1200 G2 och den ökade prestandan hos Simatic S7-1516, S7-1517 och S7-1518 ger avsevärt förbättrad effektivitet.

TIA Portal version 20 erbjuder också möjlighet till större planeringseffektivitet oavsett plats: optimerat datautbyte mellan TIA Portal, TIA Portal Cloud och Project Server Cloud säkerställer sömlöst samarbete.

TIA PORTAL I MOLNMILJÖ

Med TIA Portal Cloud behöver du inte installera mjukvaran lokalt.

FÖRBÄTTRAD SÄKERHET

Med User Management Access Control, UMAC, kommer servicetekniker enkelt åt automationsutrustningen med hjälp av standardinloggning.

GENERATIV AI

Siemens Industrial Copilot integrerar generativ AI med TIA Portal för att stödja automationsingenjörer i det dagliga arbetet.

TESTDRIVEN UTVECKLING

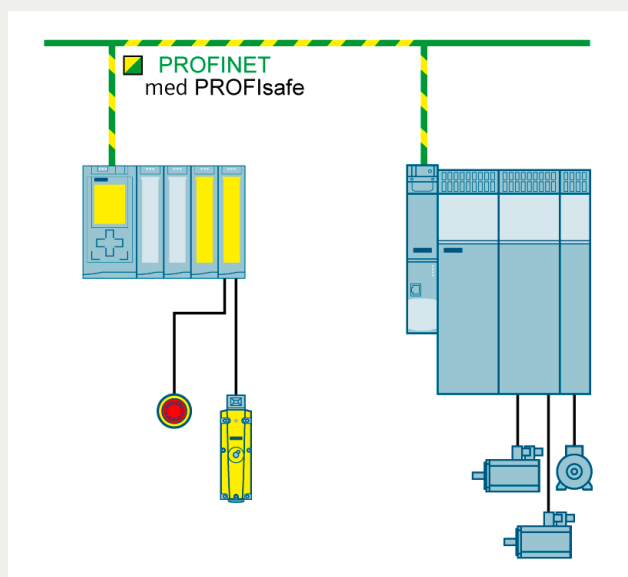
Ett steg mot förbättrad prestanda är testfunktionen TIA Portal Test Suite, där kontinuerliga regressionstester säkerställer tillförlitlig kodkvalitet. ■

MER INFORMATION

✉ ralf.folke@siemens.com

Safety Validation Assistant i TIA Portal

Validera hela kedjan i en säkerhetsfunktion från sensor till frekvensomriktare eller ställdon med Safety Activation Test.



Definiera tester med ingångsvillkor och förväntade reaktioner; wizards tillhandhålls därefter för att utföra testerna och resultaten sparas i en testrapport i Safety Activation Test. Resultaten kan i efterhand exporteras till en enda testrapport för att bevisa att säkerhetsfunktionerna fungerar korrekt. Testrapporten integreras som en del av maskindokumentationen.

Safety Activation Test var i tidigare versioner en del av Startdrive Advanced men i och med TIA Portal V20 är den en integrerad del av TIA Portal och stödjer såväl Simatic- som Sinamicsprodukter. ■

MER INFORMATION

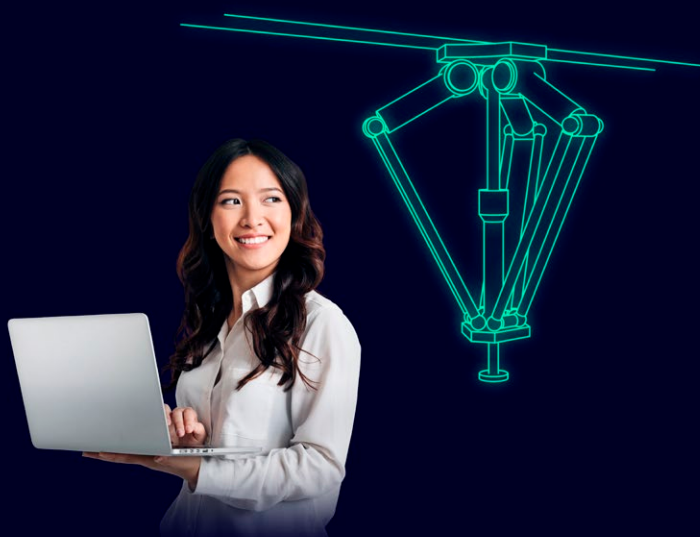
✉ ann.axelsson@siemens.com

Ny hårdvara inom **Simatic Motion Control**

Med releasen av TIA Portal V19 uppdaterades CPU:er i Simatic S7-1500 familjen från S7-1510 upp till S7-1516. I samband med version 20 av TIA Portal förbättras prestandan även på de större CPU:erna.

Detta är ett viktigt steg mot att fullt ut kunna migrera Motion Control-systemet Simotion till teknologi-CPU:erna Simatic S7-1500 T-CPU. Simatic S7-1516 T(F), S7-1517 T(F) och S7-1518T(F) uppdateras och får därmed många fördelar, som mer minne, högre prestanda, förbättrad kommunikationsprestanda och ett andra Profinet IRT-interface.

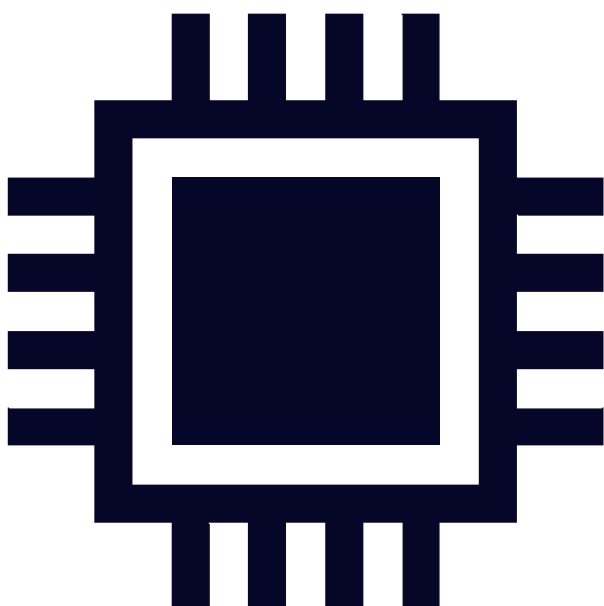
CPU:erna är funktionskompatibla med tidigare versioner förutom att Profibus DP nu saknas. I och med detta släpps även ny firmware, FW 4.0, som kräver den nya hårdvaran.



Även en mer kraftfull teknologi-CPU kommer att släppas framöver: soft-PLC:n 1508S T(F) som tillsammans med vår nya box-PC Simatic IPC BX-59A kommer att svara mot alla högt ställda krav på Motion Control i den övre prestandaklassen. ■

MER INFORMATION

✉ stefan.kaeck@siemens.com



Simatic S7-1200 G1 blir **säkrare med ny firmware**

En ny firmware-version för Simatic S7-1200 generation 1-CPU:er har lanserats och höjer säkerhetsnivån ytterligare.

Firmware-versionen 4.7 höjer säkerhetsnivån ytterligare i våra Simatic S7-1200 G1-CPU:er med hjälp av User Management Access Control (UMAC) och systemloggningsfunktioner (Syslog).

V4.7 kan konfigureras från och med Step 7 Basic V20 respektive Step 7 Pro V20. ■

MER INFORMATION

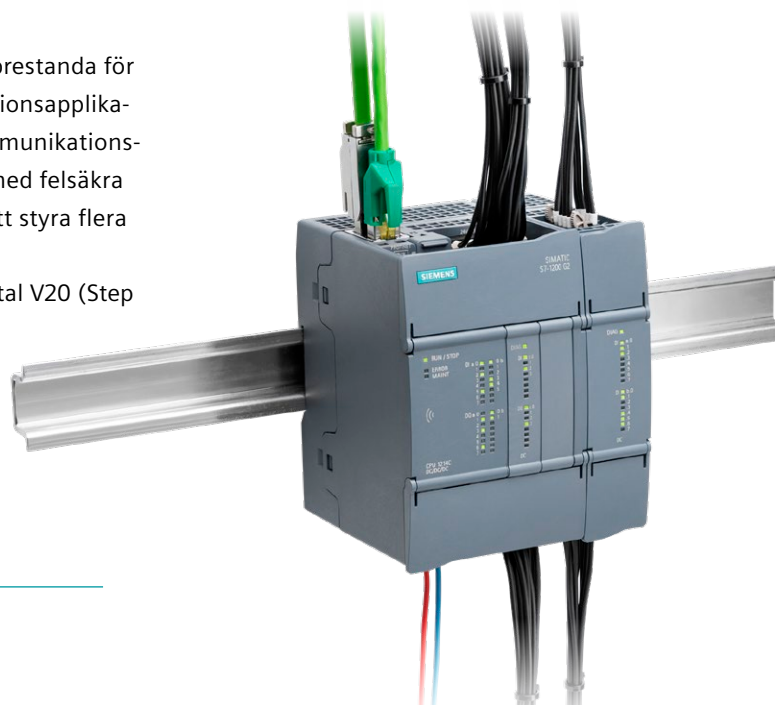
✉ lars.jonsson@siemens.com

Flexiblare maskinsäkerhet med **SIMATIC S7-1200 G2**

Nya Simatic S7-1200 generation 2-CPU:erna har lanserats och möjliggör integrerad Motion Control och flexiblare maskinsäkerhetslösningar i en kompaktare design.

Nya Simatic S7-1200 generation 2 erbjuder mer prestanda för mångsidiga och högprecisionskrävande automationsapplikationer genom förbättrad processorkraft och kommunikationsprestanda, mer minne, utökad felsäker portfölj med felsäkra signalkort och mixade I/O:n, samt möjligheten att styra flera koordinerade axlar och enkel kinematik.

Simatic S7-1200 G2 konfigureras med TIA Portal V20 (Step 7 Basic / Step 7 Professional). ■



MER INFORMATION

✉ emma.christensson@siemens.com



Säkrare och mer prestanda med firmware V4.0

Simatic S7-1500- och ET 200SP-CPU:er blir säkrare och får mer prestanda med nya firmware V4.0 som kan konfigureras från och med Step 7 V20 i TIA Portal V20.

Firmware version 4.0 höjer säkerhetsnivån ytterligare i våra CPU:er med User Management Access Control (UMAC) och systemloggningsfunktioner (Syslog).

Ett antal andra nya funktioner tillkommer för flertalet av de befintliga Simatic S7-1500-CPU:erna. Dessutom ökas prestandan väsentligt när det gäller snabbhet, kommunikation, Motion Control och minnesutrymme. Under året lanseras även nya CPU:er med ny hårdvara med V4.x. ■

MER INFORMATION

✉ lars.jonsson@siemens.com

RED 3.3 compliant



INDUSTRIAL COMMUNICATION

Nytt EU-direktiv: **Radio Equipment Directive**

Ett nytt direktiv, Radio Equipment Directive, RED3.3, trädde i kraft i augusti, vilket påverkar våra enheter för trådlös industriell kommunikation. Om man inte följer direktivet kommer man att förlora CE-märkningen.

Det nya EU-direktivet RED3.3 påverkar våra Scalance M-routrar för fjärråtkomst och Scalance W-enheter för trådlös kommunikation.

SCALANCE M

Scalance M-enheter behöver uppgraderas till ny firmware, FW V8.3. Berörda enheter: Scalance M876-4, MUM853-1 EU, MUM853-1 (A1), MUM856-1 EU, MUM856-1 (A1) samt MUB852-1 (A1).

SCALANCE W

Scalance W Wi-Fi 6 behöver uppgraderas till ny firmware, FW V3.2. Berörda enheter är Scalance WAB760, WUB760, WAM760 och WUM760.

Scalance W Wi-Fi 4 behöver uppgraderas till ny firmware, FW V6.6, som släpps i oktober. Observera att enheterna kommer att behålla sin CE-märkning tills den nya mjukvaran är tillgänglig. Berörda enheter: Scalance W760/720, W770/730, W788/748 och W786. ■

MER INFORMATION

✉ christoffer.karlsson@siemens.com | ✉ wally.hariz@siemens.com

INDUSTRIAL CONTROLS | SIRIUS MONITOR

SIRIUS 3RQ4

– ny serie plintreläer

Den nya serien Sirius 3RQ4 består av tre olika varianter av plintreläer som till 80 procent är tillverkade av biobaserad plast.



Välj mellan mekaniskt relä eller halvledarteknik, ett ypperligt komplement för kommunikation mellan Simatic-PLC:er och lågspänningsapparater; en mycket flexibel lösning då plintreläerna har en bredd på 6,2 mm och klarar strömmar upp till 6 A.

Till systemet finns dessutom en ny stiftskena som klarar 10 A vilken förenklar montage. Som vanligt finns möjlighet att välja mellan skruv- och fjäderanslutning. ■

MER INFORMATION

✉ tony.sjoelander@siemens.com

TEKNISKA FRÅGOR?

Du kan registrera ett supportärende direkt på vår supportwebbsida. På våra internationella supportsidor kan du söka efter teknisk information, manualer, applikations-exempel och mycket annat. Där finns också ett forum där du kan ställa egna frågor och läsa andras frågor och lösningar.



INDUSTRIAL AUTOMATION | PROCESS CONTROL

Säkerhetsfunktioner i SIMATIC PCS neo V6

Version 6 av användarvänliga Simatic PCS neo tar processtyrning till en ny nivå genom att kombinera intelligens, effektivitet och säkerhet.

Det webbaserade processtyrssystemet Simatic PCS neo erbjuder ett modernt användargränssnitt och en skalbar arkitektur för krävande industrimiljöer.

Utöver allmänna förbättringar och ett gäng efterfrågade funktioner har nu valbar säkerhetsfunktionalitet tillkommit. Certifierade säkerhetsfunktionsblock, flexibla arkitekturer, möjligheter till simulering och testning samt individuella åtkomsträttigheter gör DCS-systemet både säkert och effektivt.

Dessutom har den nya versionen förbättrad larmhantering, samlad händelselogg, mer detaljerad enhetsdiagnostik utan separat licens, snabbare objektadministration samt ett ännu mer intuitivt användargränssnitt.

- Basic Process Control System (BPCS) och Safety Instrumented System (SIS) på samma eller separerade enheter
- Singel- eller redundanta system
- F-I/O anslutna via Profinet (S1, S2 eller R1)
- Dedikerade engineeringsrättigheter för safety
- Omfattande säkerhetsbibliotek med certifierade funktionsblock
- Användardefinierade säkerhetsfunktionsmallar
- Simulering med Simit Virtual Controller & Unit

Systemet uppfyller kraven enligt standarderna IEC 61508 och IEC 61511. ■

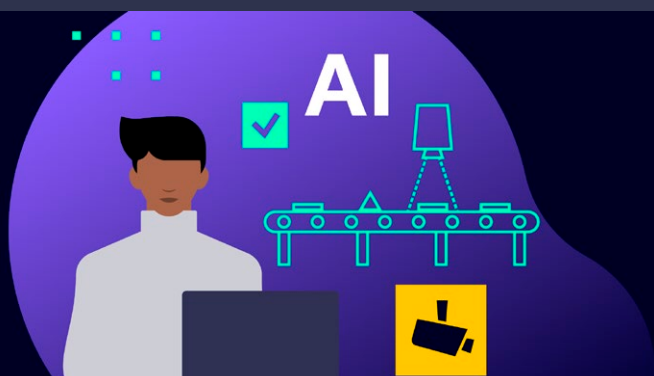
MER INFORMATION

✉ robert.wallin@siemens.com

INDUSTRIAL AI | INSPEKTO VISUAL INSPECTION

Plug & Inspect med **Inspekto** för kvalitetsinspektion på nolltid

Inspekto är vårt nya AI-baserade visionsystem för kvalitetskontroll av olika typer av produkter, anpassat för att operatörer ska kunna sätta upp, använda och underhålla systemet utan krav på tidigare erfarenhet av visionsystem.



Siemens AI-baserade Inspekto löser komplexa kvalitetsinspektioner och kan enkelt integreras med automationssystemet för att få en fullständig och automatiserad kvalitetskontroll.

Traditionellt har det varit osäkert om en vision-lösning är skalbar och lönsam i längden. Inspekto kan utvärderas extremt snabbt med dina produkter för att se om lösningen fungerar: inom två timmar har vi ett beslut på go eller no-go. Ingen expert-kunskap eller erfarenhet av visionsystem krävs; Inspekto kan helt och hållet hanteras av operatörer.

VAD KAN INSPEKTERAS?

Produkter inom exempelvis formsprutning, metall-gjutning/-bearbetning, kretskortsmontering och mycket mer kan inspekteras. Kravet är endast att objektet har en hård yta som exempelvis plast, metall eller en kombination av hårda material. Inspekto kan även placeras var som helst: i början av en produktionslinje, i mitten för verifiering av monteringsmoment och i slutet för slutgiltig kvalitetsinspektion. ■

SÅ SÄTTER DU IHOP SYSTEMET

Packa upp Inspekto.
Alla komponenter följer
med beställningen.

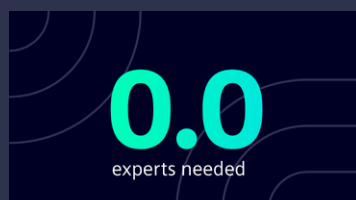
Montera på plats och anslut till
ström. Möjlighet finns även att
integrera med TIA Portal.

Träna AI:n genom att presentera
20 godkända exemplar och påbörja
sedan inspektionen. Inga defekter
behöver presenteras för Inspekto.

Klart på ett klick!

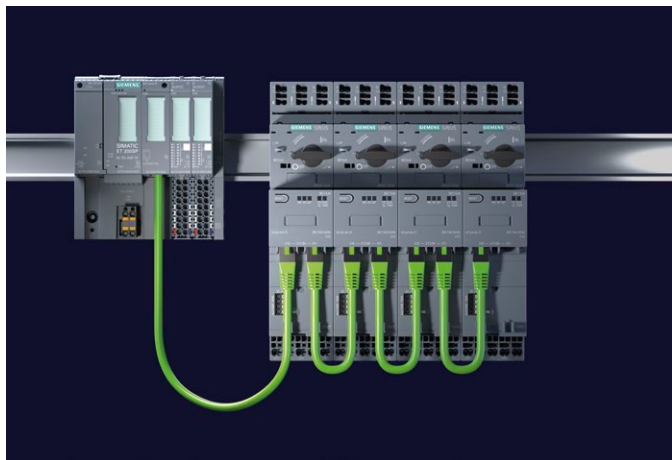
Lättanvänt!

Prisvärt!



MER INFORMATION

✉ iliass.temsamani@siemens.com



Uppgradera startgrupper med intelligenta länk-modulen SIRIUS 3RC7

Nu kan du enkelt göra startgrupper med kontaktor och motorskyddsbrytare digitala och intelligenta.

Addera den nya länkmodulen Sirius 3RC7 för integration i Totally Integration Automation för full kontroll och diagnostik. Snabb installation i kombination med intuitiv konfiguration gör att du kommer igång snabbt. ■

MER INFORMATION

✉ tony.sjoelander@siemens.com

Så jobbar du med **energi-hantering** med SENTRON Powercenter 3000

Sentron Powercenter 3000 är ett användarvänligt och effektivt verktyg för lokal datahantering och visualisering av kraftdistributions- och lågspänningslösningar.

Mjukvaruverktyget erbjuder funktioner som webbaserad energihantering, anpassade aviseringar, grafer, diagram och molnanslutning. Mjukvaran är förinstallerad och därmed utformad som plug-and-play-lösning, vilket är tidsbesparande samtidigt som den är flexibel och lätt att uppgradera. Den säkerställer också säker dataöverföring och cybersäkerhet, med alternativ för molnbaserad datalagring och analys. ■

MER INFORMATION

✉ karlsson.joakim@siemens.com

Snabbt, enkelt och smart med **TIA Selection Tool**

Enkel och snabb projektplanering med TIA Selection Tool som stöd!



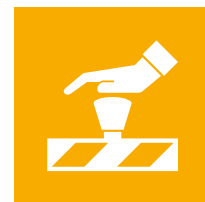
Skippa katalogerna – med TIA Selection Tool kan du välja, dimensionera och konfigurera lösningar och får samtidigt information om produkternas klimat- och miljöpåverkan. Du får enkelt fram certifikat och data såsom EPD*.

Mjukvaruverktyget finns för gratis nedladdning eller som molnbaserad variant. ■

*Environmental Product Declaration

OPC UA **Safety**

Tidigare i år släpptes standarden för OPC UA Safety. Med släppet av update 3 till TIA Portal V20 kan vi gå från att läsa standarder till att implementera OPC UA för felsäker kommunikation mellan PLC:er på riktigt.



Titta gärna på våra applikationsexempel för idéer om hur du kan använda OPC UA Safety. Tveka inte att höra av dig om du har en applikation där du tror att det här kan vara en bra lösning. ■

MER INFORMATION

✉ ann.axelsson@siemens.com

Prediktivt underhåll med Senseye Predictive Maintenance

Jobba smartare! Senseye Predictive Maintenance kan hjälpa dig öka produktiviteten och få koll på tillgångarna, inte enbart för enskilda maskiner utan för hela anläggningar. På så sätt kan du minska stillestånd, öka kunskapsdelning och påskynda den digitala transformationen.

Med Senseye Predictive Maintenance får du en intelligent tillgångshantering utan att manuell analys behövs, vilket hjälper dig att öka produktiviteten, arbeta mer hållbart och påskynda den digitala omvandlingen.

Att digitalisera en organisation är utmanande. Siemens har verktygen, expertisen och erfarenheten inom modernisering, uppkoppling, tillståndsovervakning och prediktivt underhåll och hjälper dig att kartlägga, planera och genomföra kostnadsminskningar, effektivare underhåll och förbättrad kunskapsinsamling och -delning.

ANALYS AV DRIVSYSTEM OCH MASKINER

Få värdefulla insikter från dina drivsystem och maskiner med avancerade analysverktyg som optimerar underhåll och ökar effektiviteten. Standardisera processer, minska stillestånd och få en smidig produktion med datadrivna lösningar i realtid.

Att utveckla skräddarsydda modeller manuellt för varje maskin är tidskrävande. Senseye Cloud Application gör att prediktivt underhåll kan skalas upp genom att kombinera AI med mänsklig expertis för att rikta din uppmärksamhet och kompetens dit den behövs mest. ■



Vad uppnår du med Senseye Predictive Maintenance?



Öka tillgängligheten

Öka tillgängligheten i anläggningen genom att minska produktionsstoppen med hjälp av prediktivt underhåll. Du får en korrekt bild av skicket på tillgångarna och kan agera därefter.



Utför rätt slags underhåll

Gör aldrig för mycket eller för lite: med prediktivt underhåll vet du exakt vad som behöver underhållas och när det ska göras, med tillräcklig framförhållning för att kunna planera åtgärderna.



Främja kunskapsdelning

Bevara kunskapen från erfarna medarbetare genom en gemensam informationskälla som är lättillgänglig för framtida användning och underlättar samarbete i organisationen.



Säkerställ hållbarhet

Rätt underhåll i rätt tid förlänger utrustningens livslängd, förbättrar energieffektiviteten och minskar risken för miljöpåverkan från trasig utrustning.

Att jobba smart kräver en underhållsstrategi

Prediktivt underhåll handlar om att få tillgång till bra beslutsunderlag för att kunna planera underhåll proaktivt och effektivt. Det viktiga är att lyckas få med organisationen på tåget.

Att jobba smart handlar om att ha en strategi: hur vill du att ert underhåll ska säkerställa att era företagsmål nås så att ni kan ha hög tillgänglighet och få ut så många produkter med så hög kvalitet och liten resursåtgång som möjligt?



– Prediktivt underhåll är inte teknik, det är en strategi. Och vi kan stötta med kanonbra verktyg för att uppnå den strategin. Men det krävs att företag ser över och bestämmer sig för att det är så man vill jobba och inte heller bortser från den organisatoriska förändring som krävs, säger **Katarina Lundgren Gestlöf**, säljspecialist inom service på Siemens.

Prediktivt underhåll bygger på tillståndsbaserat underhåll, så kallat Condition Monitoring.

– Det är samma data som samlas in men vi gör det kontinuerligt 24/7, nyttjar Machine Learning och AI och får ett riktigt kraftfullt verktyg som stöd för underhållspersonalen.

PREDIKTIVT UNDERHÅLL AS-A-SERVICE

Sensey är en molnbaserad SaaS-plattform för prediktivt underhåll där data samlas in från olika system i produktionen, exempelvis från befintliga eller nya sensorer, PLC:er och drivsystem.

Sensey samlar in aggregerade data, som till exempel min-, max- och medelvärden för tryck, ström, vibrationer och

vridmoment, men istället för att fokusera på att hitta fel har Sensey en modell som tränas på att förstå vad som är normalt för tillgången och flaggar sedan för avvikelser.

– Vi arbetar med ett uppmärksamhetsindex för att säkerställa att företagen inte ska få fler ärenden per dag än vad som är hanterbart. Det är ofta en kombination av en degraderande trend, eventuellt tröskelvärde och en avvikande händelse som gör att ett underhållsärende skapas.

FÖRLÄNGER LIVSLÄNGDEN

Förutom att minska oplanerade stopp och effektivisera underhåll kan man med tiden även se en effektivisering av det planerade underhållet. Dessutom förlängs livslängden på maskinparken, en stor fördel ur hållbarhetsaspekt.

Många försök till prediktivt underhåll misslyckas dock.

– Det kan ofta handla om att tekniken inte är skalbar. Man får det kanske att fungera för en maskintyp men kan inte tekniskt skala upp lösningen eller så blir det på tok för kostsamt. Eller så kan det bero på att man inte får med sig organisationen i den kulturella förändringen. Det kräver en engagerad inställning, som i all typ av förändringsarbete. Vi delar jättegärna med oss av våra dokumenterade erfarenheter här för att hjälpa till en bit på vägen.

AI HJÄLPER OCH GER RÅD

Siemens Industrial Copilot arbetar i kombination med Sensey.

– Den integrerade Siemens Industrial Copilot lär sig och blir som en grym och erfaren kollega som aldrig slutar. Den möjliggör även att du som inte är en Data Scientist kan tillgodogöra dig informationen. Du kan fråga om tidigare underhåll som har gjorts på maskinen, få grafer och data förklarade och rekommendationer kring möjlig felsökning. Och eftersom Siemens Industrial Copilot bygger på LLM:s, Large Language Models, kan du fråga på vilket språk som helst. Det finns mycket att tjäna på det här. I framtiden kommer det vara en no-brainer. ■

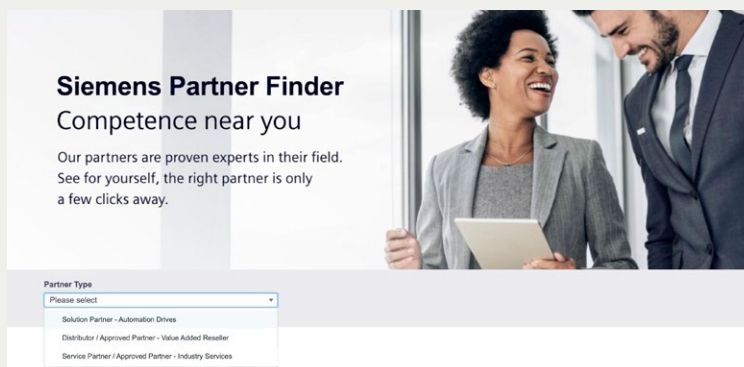
MER INFORMATION

✉ katarina.lundgren_gestloef@siemens.com

Siemens Solution Partner

Siemens globala partnerprogram för systemintegratörer, Siemens Solution Partner Automation Drives, består av certifierade partnerföretag med god branschkunskap och stor kunskap i programmering och tillämpning av Siemens automations- och drivprodukter.

Partnerprogrammet ska garantera att anläggningsägare får en optimal automationslösning som ger en kostnadseffektiv investering genom hela anläggningens livscykel. Partnerföretagen genomgår regelbundet utbildningar och certifieringar inom de områden som de har valt att specialisera sig inom, till exempel Factory Automation, processkontrollsystem, Drives & Motion, industriella nätverkslösningar, IIoT, cybersäkerhet m.m. Vi har även partner som är certifierade inom olika branscher.



Svenska Solution Partner

Behöver du hjälp med ditt projekt?

Kontakta någon av våra svenska Solution Partner!

Siemens Partner Finder

Med vårt globala sökverktyg kan du hitta partner över hela världen.

DISTRIBUTÖR: APPROVED PARTNER – VALUE ADDED RESELLER

Ahlsell

08-685 70 00

ahlsell.se

Solar

031-382 50 00

solar.se

DISTRIBUTÖRER

Busck

031-87 09 00

busck.se

Sonepar

08-92 35 00

sonepar.se

Rexel

08-556 214 00

rexel.se

AUKTORISERADE DISTRIBUTÖRER

Nätverkskommunikation:

Alcadon

08-657 36 00

alcadon.se

Processinstrument:

Axel Larsson

08-555 247 00

axel-larsson.se

Gustaf Fagerberg

031-69 37 00

fagerberg.se

Vägningsssystem:

Sitech Sverige

010-456 80 00

sitechsolutions.com/se

VÄXELMOTORER, LÅGSPÄNNINGSMOTORER OCH TIDIGARE MOTORPARTNERPROGRAM

Innomotics

order.se@innomotics.com

innomotics.com

Rörick

0221-45 75 00

rorick.se

TECHNOLOGY PARTNER

Elektromontage

0121-344 00

elektromontage.se

Digital Industries

Order Management

Telefon: 08-728 15 00

- 1 Order/lagerstatus
- 2 Pågående leveranser
- 3 Reservdelar/reparationer/utbytesköp
- 4 Garantier/returer/övriga reklamationer

Nyförsäljning: ✉ industry.om@siemens.com

Reservdelar/utbyten/reparationer:

✉ reservdelar.se@siemens.com

Garantier/returer/övriga reklamationer:

Registrera ditt ärende på engelska på

🌐 siemens.se/reklamationer

Kontakt på engelska gällande pågående ärenden

✉ reklamationer.se@siemens.com

Digital Enterprise Services

Beställa servicetekniker

☎ 0200-28 28 00

Utlandet: ☎ +46 8 728 12 72

✉ industriservice.se@siemens.com

🌐 siemens.se/industriella-tjanster

E-handelsbutik & support

🌐 siemens.se/sieportal

Sittrain utbildningscenter

✉ sittrain.se@siemens.com | 🌐 siemens.se/sittrain

Din digitala
assistent för
vägledning och svar



Automationsnytt med Stories

Prenumerera på nyhetsbrevet!

Anmäl dig på 🌐 siemens.se/automationsnytt

FÖLJ OSS

📘 facebook.com/siemens.sverige

📺 youtube.com/siemens

🌐 linkedin.com/company/siemens

📷 instagram.com/siemens

📷 instagram.com/siemens_sverige

MER INFORMATION

🌐 siemens.se

Solna

Post: Box 4044, 169 04 Solna

Besök: Evenemangsgatan 21, 169 79 Solna

Gods: Evenemangsgatan 25, 169 79 Solna

Växel: 08-728 10 00

Jönköping

Post: Box 3070, 550 03 Jönköping

Besök: Fordonsvägen 17, 553 02 Jönköping

Växel: 036-570 75 00

Linköping

Post: Gillbergagatan 39D, 582 73 Linköping

Besök: Gillbergagatan 39D, 582 73 Linköping

Växel: 013-460 61 00

Malmö

Post: Hyllie Stationsväg 41, 215 32 Malmö

Besök: Hyllie Stationsväg 41, 215 32 Malmö

Gods: Basargränd 4 (mån–fre 08–12)

Växel: 040-59 25 00 (gods: 040-44 20 30)

Mölnadal

Post: Box 14153, 400 20 Göteborg

Besök: Östergårdsgatan 2–4, 431 53 Mölnadal

Växel: 031-776 86 00

Sundsvall

Post: Box 776, 851 22 Sundsvall

Besök: Bergsgatan 130, 851 22 Sundsvall

Växel: 060-18 56 00

Övriga lokalkontor hittar du på 🌐 siemens.se

Siemens är ett ledande globalt teknikföretag som i mer än 175 år har stått för teknisk spetskompetens, innovation, kvalitet och tillförlitlighet. Räkenskapsåret 2023 hade Siemens Group cirka 305 000 anställda över hela världen och genererade intäkter på 74,9 miljarder euro och en nettovinst på 8,5 miljarder euro.

Siemens Digital Industries är en innovationsledare inom automatisering och digitalisering. Tillsammans med kunder och partner driver vi den digitala omvandlingen inom industrin och skapar hållbara industriella innovationer för en värld vi vill leva i idag och i framtiden.

I **Sverige** grundades det första Siemensbolaget 1893. Idag består Siemens i Sverige av Siemens AB, Siemens Mobility AB, Siemens Financial Services AB, Siemens Healthcare AB, Siemens Industry Software AB och Siemens Electronic Design Automation AB. Medarbetarantalet uppgår till cirka 1 500 och omsättningen under räkenskapsåret 2023 var 6,9 miljarder kronor.

Siemens Automationsnytt utges och distribueras av:
Siemens AB, Box 4044, 169 04 Solna

Adressändring: industry.om@siemens.com

Chefredaktör och ansvarig utgivare:
ann-louise.lindmark@siemens.com

Layout: Susanne Apel

Tryck: EO Grafiska

Upplaga: 6 000 ex. Två nummer per år.

© 2025 Siemens AB Sverige

MER INFORMATION

🌐 siemens.se | 🌐 siemens.se/automationsnytt



Returadress

Siemens AB
Box 4044
169 04 Solna

Adressändring görs till

✉ industry.om@siemens.com

© 2025 Siemens AB

På väg mot nettonollutsläpp med **Tech for Sustainability**

siemens.se



SIEMENS