# 5 steg för säker IT/OT-integration

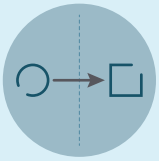
Vi har listat 5 steg för hur du säkert kan integrera IT/OT! Metoden är baserad på standarden IEC 62443 – ett måste för den som jobbar med säkerhet inom OT.

## 1. Identifiera systemet

Huvudsyftet i detta steg är att grovt bestämma vilka system som ska omfattas och vad som ska segmenteras. SCADA-systemet kan innehålla information som man vill exportera till kontorsmiljön. Man kan även ha behov av att underhålla OT/SCADA-miljön och behöver då importera data från kontorsmiljön.

## 2. Initial riskanalys

Nästa steg är att göra en initial, enkel riskanalys och i den identifiera det värsta som kan hända idag utan att ha introducerat några riskreducerande åtgärder. Baserat på detta gör man sedan en första gruppering av system och flöden. Du måste definiera dina mest kritiska systemtillgångar, konsekvenser och sannolikheten för dessa konsekvenser och baserat på det kan man räkna ut en worst case-risk som de olika delarna i systemet blir utsatta för utan säkerhetsfunktioner eller segmentering. Genom att sortera scenarierna efter konsekvensnivå blir det tydligt vilket scenario som anses mest allvarligt.



## 3. Zonindelning och dataflöden

Basera grupperingen på riskanalysen, men även på best practices och referensarkitekturer (exempelvis Purdue). När systemen ska placeras in i zoner delar man in dem i exempelvis Kontor, DMZ, SCADA och Anläggningar. När det gäller identifering av dataflöden kan det vara en utmaning att reda ut vilka de är men trafikanalys är ett sätt att ta reda på vilka protokoll man har i sitt nätverk. Ett sätt att göra detta är att spela in trafik från sitt nätverk och sedan titta på trafiken med ett eller flera analysverktyg. Efter att man gjort en trafikanalys får man ut vilken slags data det är som flödar mellan zonerna.

## 4. Detaljerad riskanalys

Enligt IEC 62443 gör man en detaljerad riskanalys om den initiala risken överskrider den acceptabla risken. I den detaljerade riskanalysen gör man en riskanalys per zon och flöde. Samma riskmatris och metod bör användas som i den initiala riskanalysen. När den reducerade risken understiger den acceptabla risken har man kommit i mål med sina riskreducerande åtgärder.

## 5. Design

När man färdigställt den detaljerade riskanalysen är det dags att fokusera på design. Designen blir resultatet av våra analyser – den slutgiltiga segmenteringslösningen. En lösning på att dataflödet blir enkelriktat ut ur zonerna är att använda datadioder. Exempelvis kan man skapa en enkelriktad exportkanal av mätdata med hjälp av en datadiod. IEC 62443 definierar 5 säkerhetsnivåer som hjälper till att härleda säkerhetsrelaterad kravställning och ringa in styrkan på segmenteringslösningen.



ISO 9001 CERTIFIED
ISO 14001 CERTIFIED