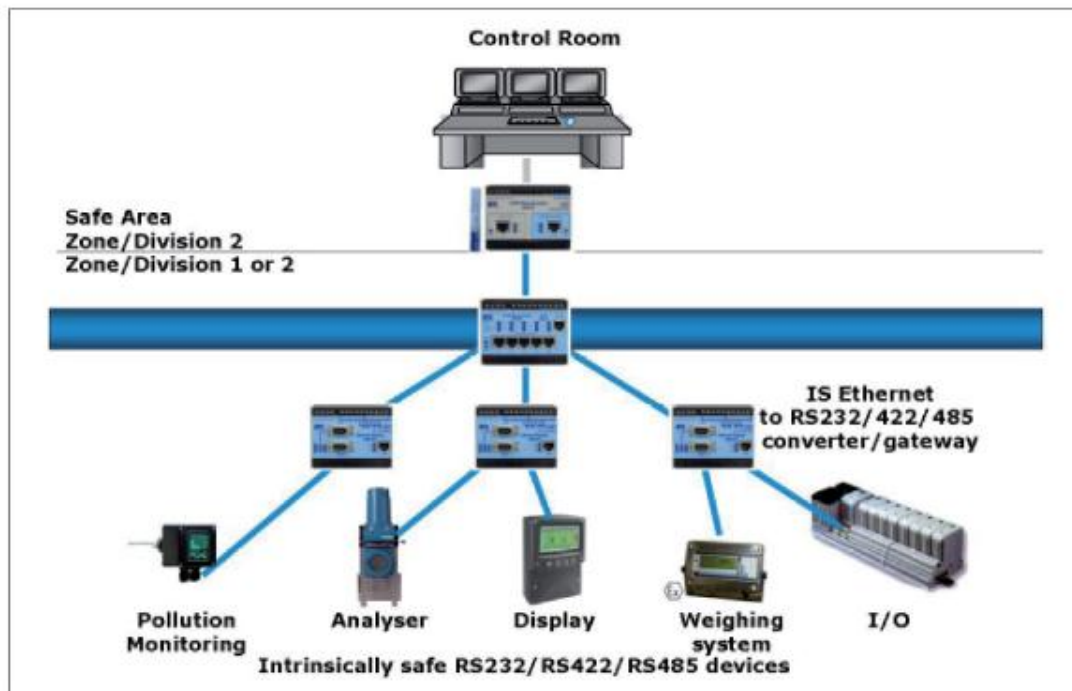


## Sikker kommunikasjon

**Kommunikasjonssystemer er en vesentlig del av et automatiseringsanlegg, og blir stadig viktigere – hvordan sikrer vi at alt går riktig for seg i eksplosjonsfarlige områder?**

Av: Einar S. Huse, Siv. Ing og Markedssjef i NOREX AS



*Feltbusser og annet periferiutstyr som tilkoples kontrollsystemet, må håndteres på samme, sikre måte i eksplosjonsfarlige soner – men er ikke alltid like standardisert som for bl.a. instrumenter.*

Tradisjonelt har kommunikasjonssystemene ligget i sikkert område, som et nettverk mellom kontrollere og datasystemer/operatørstasjoner. Med økende distribusjon av systemer og I/O-grensesnitt, mer intelligente instrumenter, og ikke minst trådløs teknologi, får vi flere kommunikasjonssystemer i eksplosjonsfarlig område. Kommunikasjonssystemene er med på å redusere kablingsbehovet, det øker fleksibiliteten og tilgangen på data fra prosessen.

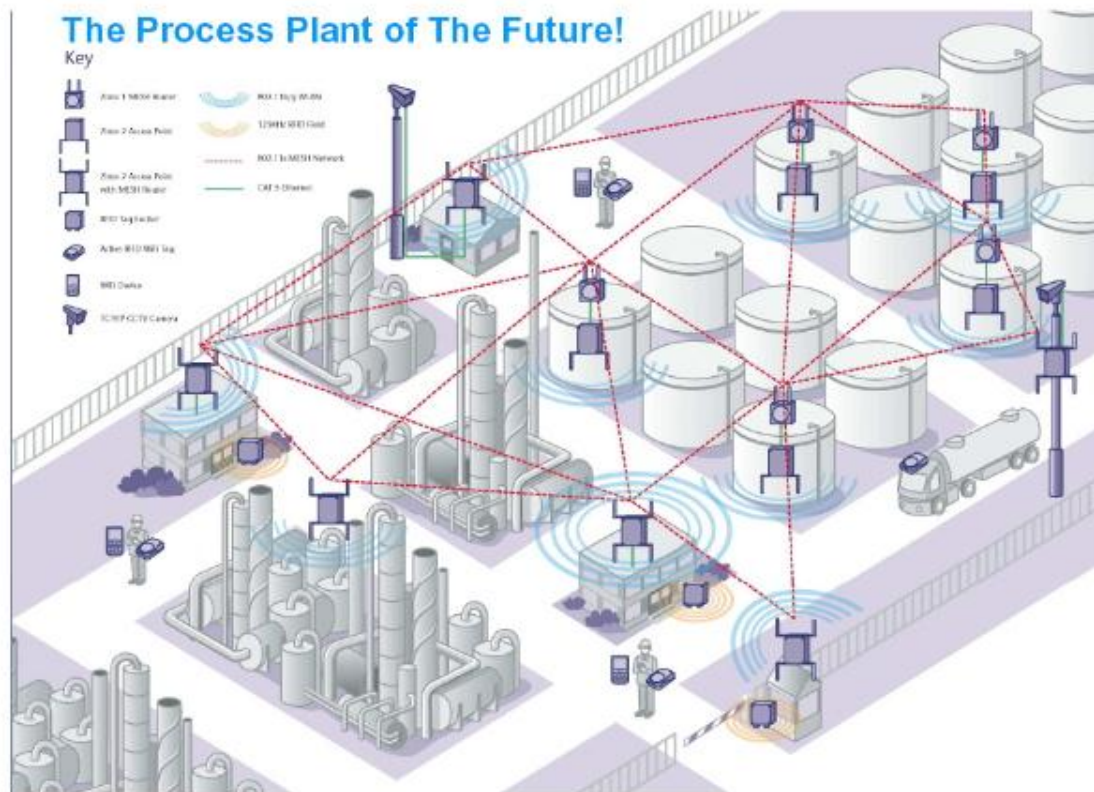
Når det gjelder eksplosjonsbeskyttelse av kommunikasjonssystemer, gjelder de samme prinsipper som for annet elektronisk utstyr. Man kan benytte de samme beskyttelsesmetodene, men mest vanlig er løsninger som:

- Ex-i egensikker
- Ex-me kombinasjon av innstøpt og tennsikker
- Ex-q innkapslet

Det er ikke samme grad av standardisering innen kommunikasjonssystemer som for eksempel innen instrumentering. Enhetene er ofte laget for å fungere mot komponenter i et spesielt system og kan ikke benyttes mot andre systemer.

For sone 2 finnes det etter hvert en god del sertifiserte standardprodukter. For sone 1 er derimot utvalget mindre og man må gjøre tilpasninger eller kapsle inn kommunikasjonsproduktene i en Ex d-boks.

Husk å benytte riktig kabel og installer den i henhold til gjeldende forskrifter.



Morgendagens prosessanlegg får trolig et større innslag av trådløs kommunikasjon, også i eksplosjonsfarlige områder.

## KOMMUNIKASJON I SONE 1

### Egensikre kommunikasjonsløsninger

Det benyttes en barriere i sikkert område. Dette er som regel en spesialbygget barriere eller isolator. I noen tilfeller kan det benyttes zenerbarrierer, men kun for lavere frekvensområder da sperrediodene ved høye frekvenser vil fungere som kapasitanser (kondensator-effekt) og ødelegge signalet.

Det finnes barrierer for RS232, RS422, RS485, Profibus DP og Ethernet. Utvalget er imidlertid begrenset. Sikkerhetsparametrene og kabelparametrene må sjekkes som for en «vanlig» egensikker krets.

### Innstøpte kommunikasjonsomformere

Det finnes på markedet flere ATEX-sertifiserte kommunikasjonsomformere som er eksplosjonssikre ved at de er innstøpt, Ex d, og har terminering på tennsikre klemmer Ex e (for power og kommunikasjonskabel). Kommunikasjonen kan dermed gå direkte fra PLS/DCS i sikkert område, til utstyret i eksplosjonsfarlig område.

Noen enheter kan også omforme signalet fra en protokoll til en annen (GATEWAY), eller fra fiberoptikk til kobber (MEDIA CONVERTER).

### Innkapslede løsninger

I mange sammenhenger blir kommunikasjonsenheten bygget inn i en Ex-d kapsling, og gjerne sammen med PLS/DCS-en eller kontrollutstyret den kommuniserer med. I slike tilfeller står man svært fritt til valg av kommunikasjonsprotokoll og medium. Ulempen er imidlertid kostnadene og vedlikeholds kravet forbundet med Ex-d kapsling.

## Ethernet og WiFi

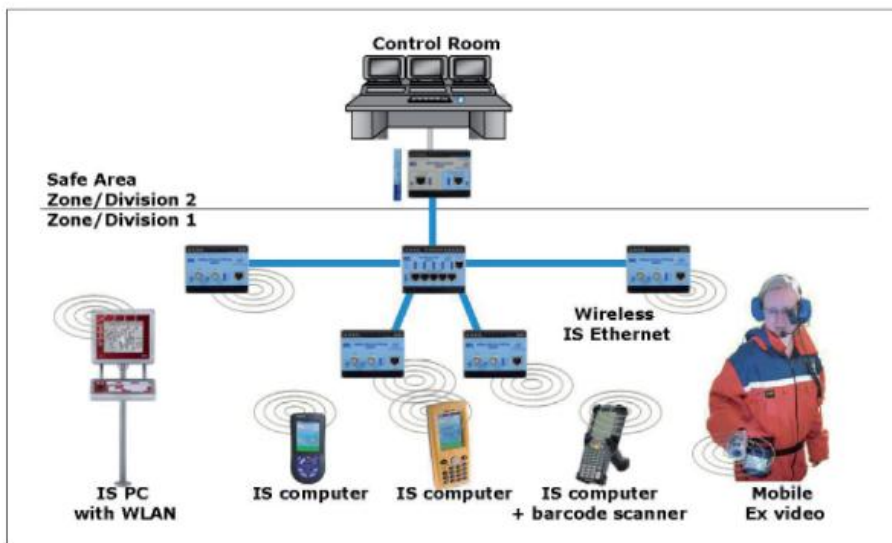


*For WiFi teknologi har den mest benyttede beskyttelsesmetoden til nå vært å plassere aksesspunkter i en Ex-d kapsling, men flere andre konsepter er tilgjengelig.*

Bruken av Ethernet og WiFi er sterkt økende i automatiseringsindustrien. Nå finnes det et relativt godt utvalg av produkter for sone 2. For kablet Ethernet eksisterer det ATEX sertifiserte switcher og mediekonvertere med Ex n - sertifisering. For sone 1 er utvalget mindre, men MTL har en komplett serie med IS-Ethernetprodukter.

Når det gjelder WiFi teknologi, har den mest benyttede beskyttelsesmetoden til nå vært å plassere aksesspunkter i en kapsling, Ex-d. Antennen settes på utsiden, og er som oftest en Ex me-løsning. Et viktig punkt vedrørende verifisering av eksplosjonssikkerhet, er å bekrefte at den utstrålte effekten fra antennen ikke overgår kravet til sonen og gassgruppen. Kravene til antenner og utstråling blir omtalt i «EN60079-0 General Requirements».

Aksesspunktet kan også plasseres i sikkert område, og så kan antennen kables ut i eksplosjonsfarlig område. Antennen må selvfølgelig være sertifisert. Det samme kan gjøres med en «leaky feeder», dvs. en spredkabel. For en «leaky feeder» må en eventuelt ende-terminering plasseres i en Ex d-boks. Husk og installer kabelen i henhold til EN 60079-14, og at den skal være mekanisk beskyttet.



*IS Ethernet for Sone 1 fra MTL.*

De første egensikre aksesspunktene har kommet på markedet. Disse er mindre, lettere og enklere å montere enn de relativt store Ex-d kapslingene. Det finnes også på markedet aksesspunkt med egensikre antenneutganger. Da kan man benytte et langt større utvalg av retningsgivende antenner. Dette øker kommunikasjonsavstanden betraktelig.

Det er fullt mulig å designe telemetri-linker med redundans, og WiFi kan derfor også benyttes i kritiske systemer med krav til høy oppetid. Dette er allerede tatt i bruk som kommunikasjonsløsning mellom skip eller på FPSO-er, mellom fast dekk og turreten.

Med WiFi, også i eksplosjonsfarlig område, åpnes det for mange nye og spennende teknologier; trådløse vedlikeholdssystemer som HART, videoinspeksjon, IP-telefoni, tracking av utstyr med RFID, osv.