Så kan IIoT byta till Ethernet

Säkerhet, determinism, och migreringen i sig – så möter du utmaningarna

Av Uday Mudoi, Microsemi Corporation

Uday Mudoi är vice vd för marknadsföring på Microsemi Corporation med över tjugo års erfarenhet i kommunikations- och halvledarbranschen. Han har en fil kand i elektroteknik från Indian Institute of Technology, en masterexamen i datateknik från North Carolina State University och en dito i företagsekonomi från Columbia University.

I en värld där nätstörningar är helt enkelt inte får förekomma, är det nödvändigt för IIoT-branschen att lämna gammal teknik och gamla protokoll bakom sig, inklusive första generationens industriella Ethernet-nätverk.

Vid denna migrering ställs du inför tre utmaningar: säkerhet, determinism, och migreringen i sig. Utmaningarna möts med en kombination av Ethernet-switchar, programmerbara enheter, högprecisionstimrar, Power over Ethernet, och tillämpningsoptimerad programvara.

34 miljarder – det är den senaste uppskattningen av antalet ”things” i Internet of Things år 2020. Enligt källan BI Intelligence kommer företag och myndigheter att stå för över 55 procent av dessa enheter.

M2M-kommunikation mellan smarta produkter blir allt vanligare i både kommersiella, industriella och offentliga tillämpningar. Drivkraften är IoT:s löften om lägre driftskostnader, högre produktivitet och andra effektiviseringar.

INOM INDUSTRIELL IOT (IIoT) är kraven på dataintegritet, tillförlitlighet och säkerhet mycket högre än i konsumentinriktade IoT-tillämpningar. De potentiellt katastrofala konsekvenserna vid fel eller driftstörningar svävar som ett svart moln över IIoT-nätet, men de förhoppningar som knyts till IIoT om dess överlägsna transparens och effektivitet väger ändå tyngre.

Att övervaka och styra uppkopplade IIot-objekt i realtid kräver nätverk med hög prestanda och låg latens. Ethernet bär på en mängd fördelar som gjort det till standardvalet för företag, datacenter, och tjänsteleverantörer – standardisering, mångsidighet, hög prestanda och låg kostnad.

Dagens IIoT-nät använder dock i hög grad specialiserade protokoll och har en installerad bas av äldre utrustning. Detta gör det mer komplext att modernisera till en ren IP-Ethernet-infrastruktur. I uppgraderingsstrategin för sådana heterogena nät måste man balansera industriella krav på tillförlitlighet, determinism, och säkerhet mot den kostnadsminskning som migration till standard-Ethernet ger.

Flerskiktad säkerhet är nödvändig i industriella nätverk. Med hjälp av det kan man upprätthålla tillförlitlighet och tillgänglighet i nätverket utan att begränsa verksamheten.

Säkerhet i industriella nätverk idag bygger typiskt på att företagsnätet är isolerat från Internet med en brandvägg. Ambitiösare försök att säkra industriella nätverk innebär typiskt att man får räkna med nätverksstopp och dyra förändringar av nättopologin, eller både-och. Det kan sätta både produktiviteten, intäkterna, och till och med säkerheten på spel.

Men att anta ett nätverk är skyddat bara för att vi tror att det är isolerat från Internet är en missuppfattning. Som de senaste cyberattackerna visat är verkligheten den att ett modernt industriellt nätverk faktiskt kan bli mindre säkert om det isoleras från Internet, eftersom isoleringen gör det svårare att hantera och diagnostisera problem.

ISOLERADE NÄT ÄR OCKSÅ svåra att skala upp och omkonfigurera när man behöver uppdatera leveranskedjan, adoptera en ny tekniklösning, eller när man behöver göra utveckling för att möta nya utmaningar och introducera ny teknik.

Det krävs åtgärder på många nivåer i ett Industriellt IoT-nät för att skydda dataplan, administration (noder och nät) och kontrollplan (protokoll). De behöver alla skyddas, särskilt vid M2M-kommunikation.

Ett typiskt upplägg är att kryptera data, administration och kontrolltrafik för att möta kraven på både dataintegritet och ”AAA” (autentisering, auktorisering och redovisning, accounting).

På nästa nivå säkras även nättrafiken genom kryptering. I Ethernet används MACsec (IEEE 802.1AE) och Keysec (numera en del av IEEE 802.1X) som L2-kryptering respektive nyckelprotokoll för att säkra fysiska portar och VLAN. Vissa myndigheter kräver IEEE 802.1AEbn med 256-bitarskryptering för att ytterligare öka konfidenialiteten.

Visserligen är kryptering ensamt otillräckligt för att säkra ett nätverk, men stark 256-bitars kryptering, som MACsec, i nätverksutrustning och slutpunkter kan användas för den autentisering, dataintegritet, och sekretess som krävs i Ethernetbaserade IIoT-nät.

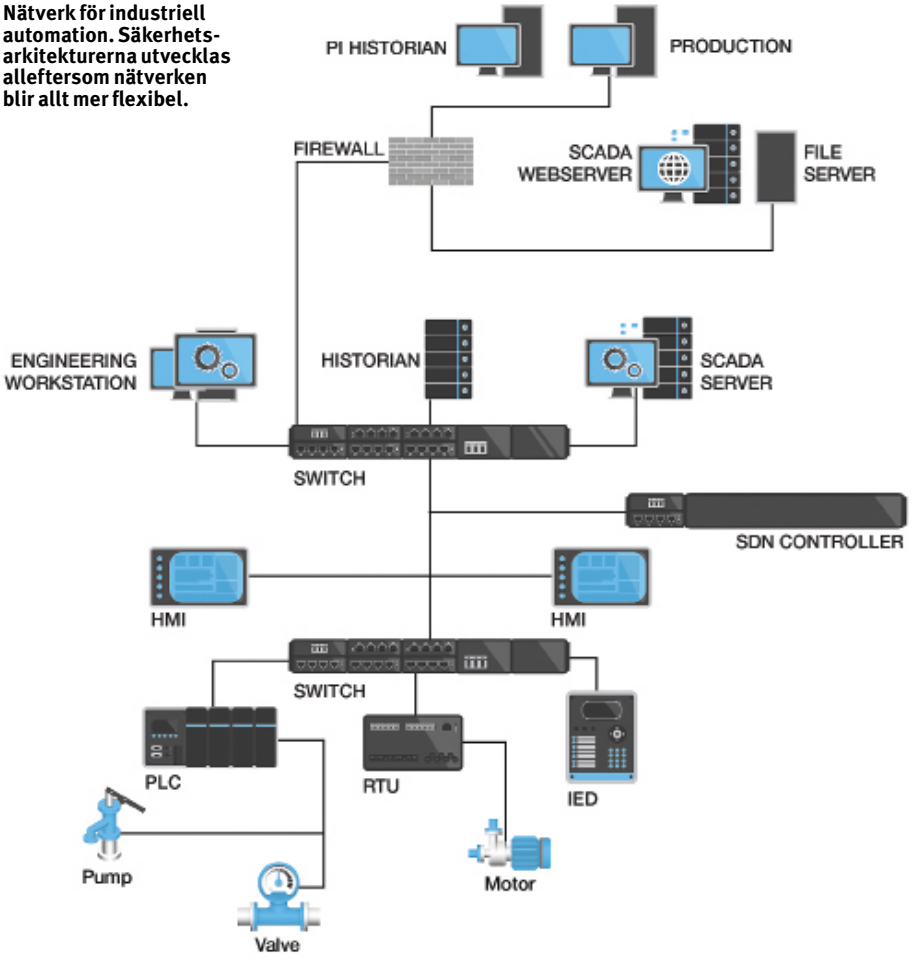
Utöver detta kan man använda FPGA:er med inbyggda säkerhetsfunktioner för att

FAKTA:

TSN (AVB Gen2) är en standardsvit med följande funktioner:

- Timing och synkronisering för tidskritiska tillämpningar (IEEE 802.1ASbt)
- Förbättringar för schemalagd trafik (IEEE 802.1Qbv)
- Frame preemption (IEEE 802.1Qbu)
- Path control and reservation i redundanta nät (IEEE 802.1Qca)
- Förbättringar av SRP (Stream reservation protokoll) i stöd för Qbu/Qbv/Qca/CB (IEEE 802.1Qcc)
- Sömlös redundans (IEEE 802.1CB)

IEEE 802.1ASbt förenklar och höjer prestandan. Dessutom stöder den one-step-tidsstämpling vilket minskar antalet paket som krävs för att kommunicera nätverkstid jämfört med två-stegsprocessen i den tidigare standarden. Att behovet av pakettrafik och datorkraft minskar är en klar fördel i seriekopplade breda tidsanvändande nät. IEEE 802.1ASbt ökar också tillgängligheten på tidsinformations genom att den erbjuder flera nivåer av synkronisering vilket ger exakt timing på individuella nätverksnoder.



Nätverk för industriell automation. Säkerhetsarkitekturerna utvecklas alleftersom nätverken blir allt mer flexibel.

skapa en root-of-trust i systemet. Sådana anordningar används för säkra startprocessen i externa processorer. Detta skapar ytterligare en nivå av säkerhet; det hindrar att nätverkets delar manipuleras för att hitta nycklar.

ALLTEFTERSOM IIOT blir vanligare, kommer företagen att börja samla på sig data i nätverkets periferi och ta big data-analys och molnet i bruk dels för att skala upp sin datorkapacitet och dels för att hitta praktisk användning av all denna data. Uppkopplingen mot Internet är grunden för det hela, och här kan man använda en centraliserad säkerhetsstruktur, hårt integrerad med distribuerade nätverksprodukter, för att effektivt att säkra sitt IIoT-nät.

Vad gäller determinism i Ethernet-nät, handlar det om att se till att specifika operationer sker inom bestämda tidsramar. Noderna i nätet håller reda på tiden och kan avgöra om de levererat Ethernet-paket i tid. Samtidigt är detta bara en del av lösningen.

En mekanism för att synkronisera och dela exakt tid i Ethernet finns i IEEE 1588v2. Den senaste standarden inom TSN (Time Sensitive Networking) innehåller ett mycket tidsorienterat sätt att schemalägga trafik.

TSN-standarden är utvecklad inom IEEE 802 och utvidgar Ethernetprotokollet till industriell kvalitetsnivå när det gäller realtidskommunikation. Bland funktionerna finns klocksynkronisering, tidsbaserad meddelandehantering, Frame preemption (gräddfiler för datapaket) och sömlös redundans.

De nya TSN-funktionerna ger realtidsdeterminism och låg latens till Ethernet-nätverk. Detta är något som IIoT-tillämpningar kräver. Därmed försvinner det sista hindret mot att använda Ethernet som ryggrad i IIoT-nätverk. Det här är ett stöd för trenden att kritisk och icke-kritisk styrning och datatrafik börjar konvergera till att använda gemensamma nät.

SAMTIDIGT SOM ETHERNET med TSN äntligen kommer att kunna göra ett rimligt jobb som deterministisk ryggrad i industriella nätverk, kommer företagsegna gränssnitt att finnas kvar, åtminstone för överskådlig framtid.

Därmed blir det kritiskt att FPGA:er och systemkretsar som översätter mellan Ethernet, IEEE 1588, TSN, och specialiserade industriella protokoll, också kan hantera determinism.

Här har FPGA:er en stor fördel gentemot MCU:er. Ett exempel på en tillämpning som kan dra nytta av FPGA:ns deterministiska natur är en nätverkad motorstyrningstillämpning som använder Ethercat. En FPGA kan konvertera protokollen och implementera motorstyralgoritmerna med minsta möjliga latens. FPGA:er kan till skillnad från MCU:er sända data deterministiskt och klarar deterministisk motorstyrning synkroniserad med fjärrnoder.

ATT IIOT-NÄT TILL SLUT kommer att migrera till IP/Ethernet är självklart, men det finns två saker som är viktiga att inse: att Ethernet-standarder, -komponenter och -system för LAN egentligen är en onaturlig miljö för IIoT-nät, och att det krävs en fin balansgång för att både kunna migrera IIoT-nätverk och stödja befintliga icke-standardprotokoll, samtidigt som man förbereder nätet för nya innovationer.

När man gäller ett typiskt industriellt nätverk – som består av en heterogen bas av äldre utrustning och specialiserade nätverksprotokoll – finns flera nyckelelement som systemkonstruktörer kan använda för att förenkla migreringen till Ethernet:

- Multi-protokollstöd för Ethernet och fältbussgränssnitt för att säkerställa kompatibilitet och skalbarhet i storskaliga heterogena nätverk
- Optimerade programvarustackar för Ethernet-switchar för enkel driftsättning och styrning
- Unifierad hård- och mjukvara som på ett tillförlitligt sätt kan leverera den realtidsdeterminism och låga latens som krävs för industriell kommunikation.
- Flexibilitet i portkonfigurering och synkroniseringsval samtidigt som miljö- och operativa krav inom IIoT tillgodoses
- Möjlighet till Power over Ethernet (PoE) upp till 95 W för att med marginal kunna strömförsörja fjärrenheter, för förenklad driftsättning

ALLT OVANSTÅENDE ÄR MÖJLIGT i en pragmatisk kombination av hårdvara och mjukvara med följande innehåll:

- Strömsnåla och säkra FPGA-lösningar
- Ethernet-switchkretsar optimerade för industriella installationer
- Programvarustackar som inte bara erbjuder smidig administration och övervakning, utan också ett ekosystem av av mjukvara för att bygga säkerhetsfunktionalitet.
- Ruggade PoE-lösningar utformade för industriella miljöer

OBSERVERA ATT DET ALDRIG kommer att finnas en one-size-fits-all-lösning för IIoT. PoE, synkronisering och datakryptering är några tilläggsfunktioner som kan underlätta en uppgradering till grundläggande maskin- och programvaruplattformar. I andra scenarier kan eventuell extra datorkraft som krävs tillgodoses av en fristående processor, eller av en CPU integrerad i switch eller FPGA. ■