Så säkrar du din verksamhet

EXPERTARTIKEL

Oväntade driftstopp kan bli dyra och farliga. Internetuppkoppling kräver dessutom nya säkerhetslösningar.

Av John Mossman, Maxim Integrated

John Mossman började på Maxim Integrated som FAE för över tio år sedan och idag är han marknadsansvarig för affärsområdet Control & Automation. Han är också medlem i företagets strategiska marknadsföringsteam. John har arbetet inom elektronikindustrin i över 20 år med allt från industri- och konsumentelektronik till militära och medicinska produkter. Likaså har han flera amerikanska patent.

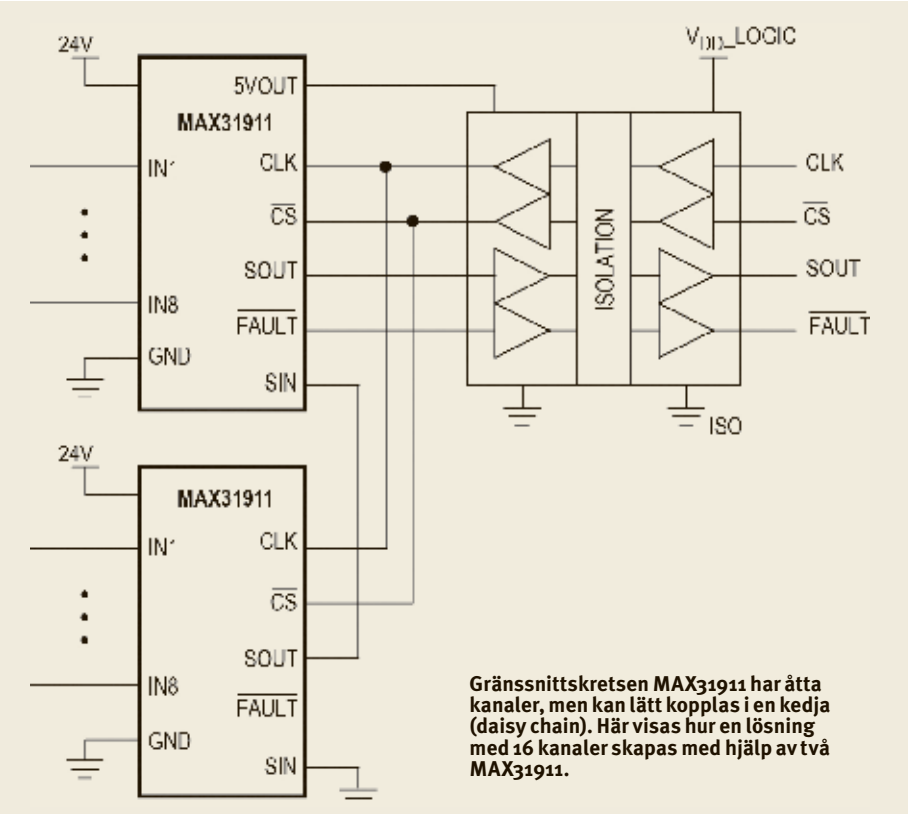
Om du har varit i branschen ett tag har du säkert hört det förut: maximera avkastningen på investeringen (return on investment – ROI) så håller du företaget friskt och växande. Det är ett enkelt mål, men inte lätt att nå. För att få ut maximal avkastning från en industrianläggning måste den hållas igång 24 timmar om dygnet, sju dagar i veckan, året om. Drifttiden är godhetstalet – och således ett mått på prestanda.

Det är inte bara moln-servrar och kritiska militära säkerhetssystem som måste klara det man betecknar 5 9s eller 6 9s, där 5 9s motsvarar en tillgänglighet på 99,999 procent eller ett driftstopp på som mest fem minuter per år. Samma krav gäller fabriker, kraftverk och kommersiella anläggningar, ja överallt där investeringar och samhällets behov överensstämmer med ägarnas och användarnas strävan att maximera drifttid och kapacitet.

Oväntade driftstopp kan bli extremt dyra, inte enbart på grund av att produktionen stannar utan även för att man kan komma att förlora de produkter som håller på att tillverkas (Work In Progress) samt att de produkter som tillverkas direkt efter en omstart inte säkert uppfyller specifikationerna. Vissa produktionsanläggningar kan behöva flera dagar på sig för att stabiliseras innan produkterna som tillverkas åter uppfyller de krav som ställs. Om ett driftstopp beror av ett katastrofalt fel finns det även risk för föroreningar, allvarliga säkerhetsproblem, juridiska konsekvenser, mänskliga skador och till och med dödsfall.

Driftstopp i offentliga byggnader kan orsaka andra liknande problem. En flygplats som inte kan användas på grund av att belysningssystemet slås ut kan exempelvis drabba flera tusentals människor.

För att öka drifttiden och produktionskapaciteten måste man välja den utrustning som är mest pålitlig och samtidigt införa ett program för underhåll som får utrustningen att prestera maximalt (se faktarutan sid 27).



Gränssnittskretsen MAX31911 har åtta kanaler, men kan lätt kopplas i en kedja (daisy chain). Här visas hur en lösning med 16 kanaler skapas med hjälp av två MAX31911.

MEN NÄR DET GÄLLER DRIFTTIDEN inom industrin och resultatet på nedersta raden är underhåll av utrustningen inte allt. I vissa situationer är det inte kostnaden för underhåll som driver besluten. Vid satsvisa processer – exempelvis i bryggerier och vid läkemedelstillverkning – kan underhållet skötas mellan satserna. Samtidigt kan det i dessa fall bli extremt dyrt, till och med farligt, om ett driftstopp uppstår mitt under en sats. Därför är det av avgörande betydelse att ha övervakande utrustning och felsäkra system i dessa miljöer.

Diskret tillverkning är ett annat processexempel. Här handlar det om monteringslinor där enskilda artiklar monteras eller tillverkas. Det kan vara allt från bilar till mobiltelefoner. I dessa tillverkningslinor handlar det ofta om snabba moment, då är drifttiden kritisk.

I en produktionsanläggning kan utrustningen påverkas av många olika yttre be-

tingelser, såsom höga spänningstransienter, skador på kablar, felaktig anslutning vid reparationer eller andra ändringar, extrema temperaturer, elektromagnetisk interferens (EMI/RMI), frätande och explosiv atmosfär, starka vibrationer samt fukt eller damm. Om yttre betingelser påverkar noggrannheten hos sensorer och signalbehandlingen finns det risk för felaktig avläsning och felaktiga styrsignaler. Detta kan, i bästa fall, leda till ett sämre resultat och i värsta fall få katastrofala följder.

I SYSTEM DÄR KOSTNADEN för redundans inte kan motiveras måste man istället konstruera väldigt tillförlitligt. Olika metoder – såsom FMEA (Failure Mode Effects Analysis), FMECA (Failure Mode Effects and Criticality Analysis) och FMEDAs (Failure Mode Effects and Detection Analysis) kan användas för att säkerställa att systemet upptäcker, reagerar på och minimerar alla möjliga fel som kan uppstå.

Analyserna görs ända ner på komponentnivå i elektriska och mekaniska system för att säkerställa att utrustningen möter gällande industristandard. Resultatet av analyserna leder ofta till att mer elektronik adderas för att övervaka signalvägar och kraftelektronik. Åtgärden är bra för att öka tillförlitligheten och säkerheten, men den extra elektroniken gör det samtidigt besvärligt att förenkla och minska storleken på konstruktionen och att göra den energisnålare.

Maxim Integrated har uppmärksammat dessa utmaningar. Företaget har därför utvecklat kretsar som integrerar funktioner för att minska behovet av externa komponenter som annars behövs för att klara en FMECA-analys. Likaså har företaget tagit fram referensdesigner för att korta konstruktionstiden och för att minska effektförbrukningen hos konstruktionen.

Idag är det ett vanligt problem att digitala gränssnittsmoduler som ska hantera 24 V-signaler på ingången dras med stora effektförluster. När man försöker minska storleken på dessa moduler orsaker effektförlusterna att värme utvecklas, vilket begränsar modulens temperaturområde. Samtidigt måste utrustningen tåla höga temperaturer för att kunna placeras nära en maskin.

DET ÄR ALLTSÅ VIKTIGT med effektsnåla lösningar. För att tackla detta problem har Maxim Integrated utvecklat MAX31911, en gränssnittskrets med åtta kanaler som serialiserar digitala 24V-signaler och översätter dessa till CMOS-kompatibla 5 V-signaler. Modulen minskar effektförlusterna med upp till 60 procent jämfört med då traditionell teknik med diskreta motstånd används samtidigt som den möter IEC61131-2 PLC-standarden för digitala signaler, typ 1, 2 och 3.

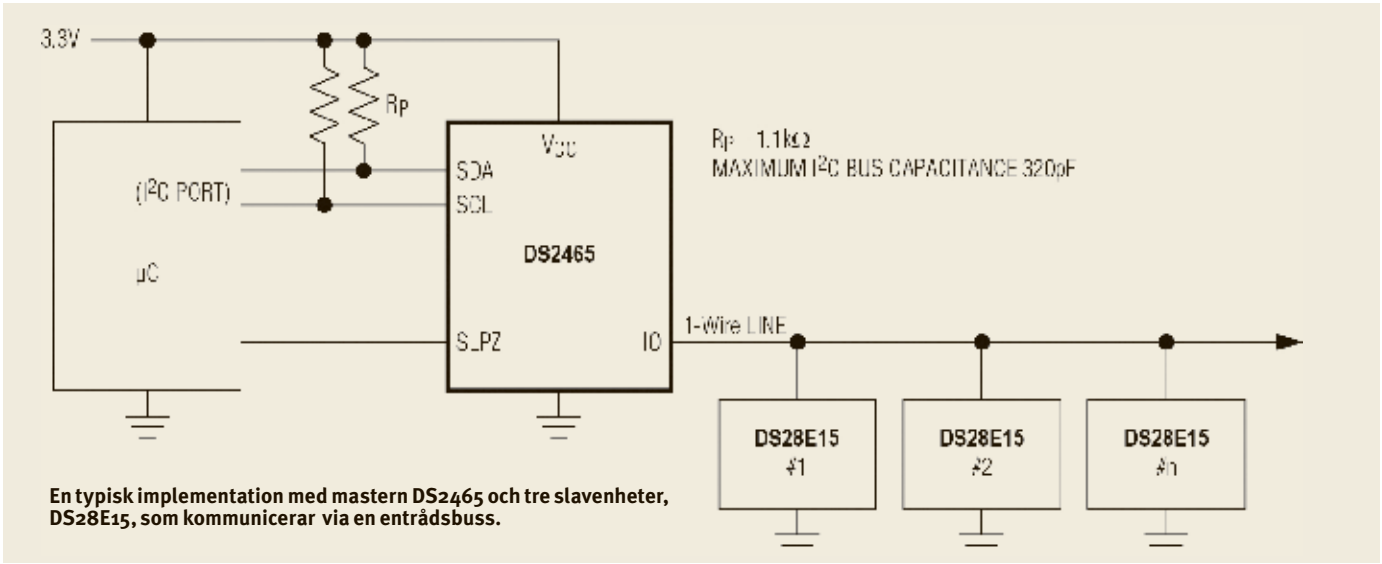
Modulen integrerar ett justerbart lågpassfilter för flexibel hantering av ringningar (debouncing). Det seriella SPI-gränssnittet på utgången minskar antalet optokopplare, vilket också minskar effektförbrukningen, storleken och priset på konstruktionen. För att säkerställa giltigt data på SPI-gränssnittet genereras en checksummekod (CRC) för varje 8-bitars data.

För tillämpningar som kräver extremt låg effektförbrukning finns även MAX31910 som inkluderar avancerad strömstyrd teknik, vilket minskar energiförbrukningen med upp till 40 procent, jämfört med MAX31911.

För system som har mer än åtta ingångar kan flera MAX31911 lätt kopplas i en kedja – daisy chain. I figuren på sid 24 visas hur man kan skapa en lösning med 16 kanaler med hjälp av två MAX31911.

I SYSTEM MED PARALLELLA INSIGNALER och seriella utsignaler är den första frågan alltid: ”Hur snabbt går det att sampla ingångskanalerna och behålla giltigt data och genomströmning?”

Det snabbaste läget är utan filtrering. Utsignalen från de åtta interna komparatorerna låses i serialiseraren på den fallande flanken av Chip Select (CS). Varje klockflank kommer därefter att klocka ut en bit som motsvarar respektive ingång. I detta fall är hastigheten begränsad till ingångsbandbredden som är 1 MHz, så en klockning av serialiseraren med 8 MHz ger en genomströmning per kanal motsvarande 1 Mbit/s (i 8-bitarsläge). Om fyra kretsar daisy-chain-kopplas för en 32-bits-tillämpning så kommer den maximala klockningen av serialiseraren att begränsa genomströmningen. Anledningen är att om man ska klocka 32 bitar ur en serialiserare vid maximal klockhastighet på 25 MHz, så blir genomströmningen per kanal 25MHz/32



En typisk implementation med mastern DS2465 och tre slavenheter, DS28E15, som kommunicerar via en entrådsbuss.

vilket motsvarar 0,8 Mbit/s. Om man istället använder filtrering så kommer genomströmningen att begränsas ytterligare.

För att stödja industriella tillämpningar har MAX31911 inbyggda ±15kV ESD-skydd (HBM) på alla ingångar. Kretsen är också klassad för upp till +150°C (junction temperature). Den kommer kapslad i en TSSOP-EP med 28 anslutningar som mäter 6,5 x 9,8 x 1,1 mm.

TRENDEN ATT ANSLUTA industriutrustningen till Internet ger många fördelar, men den medför också större säkerhetsrisker. Cyberkrigsföring är ett verkligt hot mot drifttiden och resultatet på nedersta raden.

Nya säkerhetslösningar måste tillhandahålla standardiserad kryptering, autentisering och säker nyckellagring på kiselnivå. Lösningarna ska inte kräva att man följer komplexa datahanteringsregler och förfaranden för att upprätthålla anläggningens brandväggar. Nya lösningar från Maxim Integrated förhindrar obehörig kommunikation samt krypterar all godkänd kommunikation. De reagerar också aktivt på en lång rad fysiska och elektriska attacker. Risken för påverkan av skadlig kod, stöld av krypteringsnycklar och kloning minskar således kraftigt. Lösningarna har använts i många år i exempelvis uttagsautomater och kassaapparater, där de skyddat finansiella transaktioner och personliga identiteter.

En av flera säkerhetslösningar som Maxim erbjuder är SHA-256, en autentiseringslösning bestående av två kretsar, mastern DS2465 som är en säkerhetsprocessor samt slavenheten DS28E15 1-Wire SHA-256 för säker autentisering. Kretsarna kommunicerar via en enkel ledning och stöder så kallad challenge-response-autentisering. Det innebär att algoritmen avvisar alla anslutna moduler som inte beräknar rätt värde – för att kunna beräkna rätt värde krävs tillgång till den interna nyckeln. Både master och slavenheten måste använda nyckeln tillsammans med ett slumptal. Om resultaten inte är identiska misslyckas autentiseringen, varvid den anslutna enheten inte tillåts att kommunicera.

DS2465 HAR EN INBYGGD MASTER som hanterar busstimingen och tillhandahåller krypteringsalgoritmen så att systemet inte behöver belasta värdprocessorn med dessa uppgifter. Säkerhetsprocessorn har också 64 byte EEPROM med flera skyddstillval och förbinds med värdprocessorn via ett enkelt I2C-gränssnitt. Den ryms i en TSOC med sex anslutningar och är 4,0mm x 4,45mm x 1,5mm.

DS28E15 kombinerar säker challenge-response-autentisering baserad på kryptoalgoritmen FIPS180-3 SHA256. Den har 512 bit EEPROM samt ytterligare ett säkerhetsminne som innehåller den hemliga nyckeln. Varje enhet har ett unikt ID-nummer som ligger i ett 64 bit ROM programmerat i fabriken. Två kretsar är aldrig identiska. Med hjälp av en säker billig fabrikstjänst kan data förprogrammeras – även hemlig data om så önskas. Det finns en mängd olika metoder för att hålla säkerheten under fullständigt kontroll, även då kretsarna används hos kontraktstillverkare. ■

FAKTA:

Olika nivåer av underhåll

Det finns en mängd metoder att välja mellan när det gäller att underhålla en anläggning. Olika metoder är lämpade för olika utrustning och behovet beror av den aktuella installationen.

- **Reaktivt underhåll** – eller kör tills det brister – är den metod som initialt kostar minst eftersom inga ansträngningar görs för att underhålla utrustningen. Den används helt enkelt tills dess att den går sönder. Det kan verka oansvarigt att använda reaktivt underhåll, men metoden har sin plats i tillämpningar som inte är kritiska och som endera är för dyra eller omöjliga att underhålla och där fel kan förutsägas och är förväntade. Vissa redundanta systen, och system som sällan fallerar, passar väl för denna metod.
- **Förebyggande** – preventivt – underhåll är standard i många installationer. Trots att metoden visat sig vara en av de mest kostsamma har den sin plats. Det är motiverat att använda den där exempelvis slitage, erosion och andra väsentliga förändringar direkt kan korreleras med användningstid eller åldrande.
- **Förutsägbart** – prediktivt – eller tillståndsbaserat (Condition based Maintenance – CBM) underhåll ökar i de flesta fall drifttiden samtidigt som metoden blir kostnadseffektiv i längden, även om den initiala kostnaden är högre än tidigare nämnda metoder. Stickprovskontroll av utrustningen är ett steg i rätt riktning, men kontinuerlig tillståndskontroll (Continuous Condition Monitoring – CCM) baserat på sensorer och datainsamling ger det mest ultimata skyddet. Den initiala kostnaden för utrustningen, liksom utbildning och upphandling, är relativt hög men den betalar sig eftersom den förebygger katastrofer.
  Denna metod är ofta den bästa eftersom väldigt många fel är slumpmässiga i tiden och sensorer kan användas för att upptäcka förändringar och varna i tid.
- **Proaktivt underhåll** är ett framåtblickande system som lär sig av underhållshistoriken och som inför förändringar för att minska framtida behov av underhåll.
- **Självunderhåll** är den metod som är mest framåtblickande. Utrustningen kan själv övervaka, diagnostisera och kalibrera sig så att driften kan fortsätta tills dess att det är lämpligt för andra åtgärder.