Integrovaná bezpečnost

Jelikož se i v průmyslovém prostředí z mnoha důvodů stává zavedeným standardem komunikačních sítí Ethernet, je přirozené, že technici začali uvažovat o jeho vhodnosti i pro bezpečnostní úlohy.

Bezpečnostní komunikační sítě mají ve srovnání s tradičně zapojenými bezpečnostními systémy s architekturou bod-bod mnoho předností, zejména pokud jde o diagnostiku celého systému. Namísto toho, aby se při problému musel odstavit celý výrobní provoz, dokáže bezpečnostní síťová řídicí jednotka rychle rozhodnout, které jednotlivé procesy a zařízení je třeba odstavit a které mohou pokračovat v provozu. Bezpečnostní sítě tak nejen snižují četnost nehod, nýbrž také přispívají k omezování jejich důsledků a zvyšování produktivity.

Proč Ethernet?

Velkou výhodou průmyslového Ethernetu, jako je např. EtherNet/IP, je skutečnost, že je založen na otevřených standardech. Má malé náklady na instalaci, protože využívá univerzální síťové komponenty. To také usnadňuje případné modifikace a rozšiřování systému.

Náležitou pozornost je však nutné věnovat výběru konkrétního komunikačního systému. Jestliže se systémy na bázi průmyslového Ethernetu spoléhají na specifické síťové prvky od konkrétních dodavatelů nebo k oddělení segmentů sítě vyžadují specifický mechanismus, ztrácí uživatel mnohé z výhod Ethernetu jako obecného standardu.

CIP Safety: jeden protokol pro všechny sítě CIP

Pro sítě EtherNet/IP i DeviceNet, které jsou součástí skupiny protokolů CIP (*Common Industrial Protocol*), je k dispozici společný bezpečnostní protokol CIP Safety, umožňující integraci bezpečnostní komunikace do sítí, jež používají běžná řídicí zařízení (provozní úroveň komunikace), i do těch, jež jsou základem komunikačního systému celého podniku (podniková úroveň komunikace). O bezpečnostní protokol CIP Safety jsou rozšiřována pouze samotná bezpečnostní zařízení; běžná zařízení sice nadále nejsou schopna plnit funkci bezpečnostních zařízení, ale mohou sdílet stejný síťový komunikační kabel s bezpečnostními zařízeními.

O tom, zda pro protokol CIP Safety použít síť EtherNet/IP, nebo DeviceNet, rozhoduje uživatel podle vzdálenosti mezi účastníky, podle velikosti datových paketů, doby odezvy, požadovaného příkonu připojených zařízení a podle jejich ceny. EtherNet/IP je vhodnější pro delší datové pakety, větší šířku pásma a větší vzdálenosti mezi účastníky; pro úlohy, kde je šířka pásma sítě DeviceNet dostačující, může být tato sběrnice ekonomicky výhodnějším řešením.

V rámci sítí DeviceNet nebo EtherNet/IP lze vytvářet bezpečnostní buňky s velmi rychlou odezvou na vybavení bezpečnostního signálu. Tyto buňky je možné propojit s dalšími buňkami prostřednictvím komunikační sítě, která umožňuje jejich vzájemnou interakci. Výhodou této architektury je to, že většina bezpečnostní komunikace probíhá v lokální buňce, pouze malá část je určena pro komunikaci mezi buňkami. Bezpečnostní komunikace tak jen minimálně omezuje šířku přenosového pásma nadřazené sítě. Kombinace místních, rychle reagujících bezpečnostních buněk a funkce směrování bezpečnostních dat mezi buňkami umožňuje vytváření rozsáhlých bezpečnostních systémů. Větší pružnost, kterou s sebou protokol CIP Safety nese, navíc urychluje konfiguraci, testování a zprovozňování systémů. Bezpečnostní sítě DeviceNet Safety a EtherNet/IP Safety vypadají a pracují stejně jako běžné sítě DeviceNet či EtherNet/IP, se zachováním všech výhod diagnostiky a snadného uvádění do provozu, na které jsou jejich uživatelé zvyklí. Bezpečnostní systém založený na sítích DeviceNet Safety či EtherNet/IP Safety dovoluje připojovat bezpečnostní i běžná zařízení ke stejné síti, přičemž v architektuře systému mohou, ale nemusí být použity bezpečnostní programovatelné automaty (PLC). To je obrovská výhoda ve srovnání s těmi bezpečnostními protokoly, které vyžadují oddělené sítě pro bezpečnostní a standardní řídicí prvky, čímž zvyšují cenu i složitost systému.

Je však umístění bezpečnostních zařízení a běžných řídicích jednotek ve stejné síti bezpečné?

Komunikovat protokolem CIP Safety jsou schopna pouze bezpečnostní zařízení, čímž je účinně zabráněno tomu, aby se běžné zařízení mohlo vydávat za bezpečnostní jednotku: běžná zařízení nemohou rušit funkci bezpečnostních zařízení a naopak.

Bezpečnostní protokol CIP Safety zajišťuje, že bezpečnostní systém na vybavení bezpečnostního signálu reaguje během předem známého časového intervalu tak, že přechází do předem stanoveného bezpečnostního stavu.

Ochranná opatření, která jsou součástí protokolu CIP Safety, zajišťují vysokou úroveň integrity zpráv i tehdy, když jde o smíšenou bezpečnostní a běžnou komunikaci. Tato ochranná opatření, schválená organizací TÜV, ovšem nemohou ochránit síť proti selhání, protože všechny komunikační sítě jsou ze svého principu více nebo méně náchylné k chybám způsobeným např. rušením, přerušením kabelu nebo zkratem. Může také vzniknout závada některého zařízení v síti, která způsobí, že jsou data do sítě odesílána opakovaně nebo jsou poškozena. Bezpečnostní opatření v CIP Safety však bezpečnostní jednotce umožní rozeznat, že došlo k poškození bezpečnostního telegramu, jeho zpoždění, ztrátě, opakovanému vysílání nebo podobné závadě, a to nezávisle na komunikační síti a nezávisle na běžných telegramech. I v tomto případě se zařízení uvede do bezpečného stavu. Mohou tak fungovat bezpečnostní snímače vedle měničů frekvence i bezpečnostní řídicí jednotky vedle běžných PLC. Bez ohledu na to, jaká kombinace zařízení je použita, bezpečnostní smyčka nemůže být nepříznivě ovlivněna kterýmkoliv z běžných řídicích zařízení.

Bezpečnostní zařízení je uvedeno do bezpečného stavu bezpečnostním hardwarem a v něm uloženým bezpečnostním programem, který je součástí každého zařízení. Tento hardware má typicky redundantní architekturu a je schválen pro bezpečnostní úlohy. Tak je zajištěna maximální spolehlivost vykonání bezpečnostní funkce. Komunikační stack EtherNet/IP Safety není součástí bezpečnostního programu, protože CIP Safety pracuje na vyšší úrovni komunikace; lze tedy použít běžný, komerčně dostupný stack.

Závěr

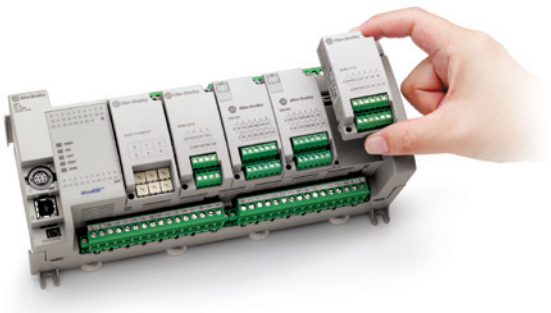
Výhody bezpečnostních komunikačních sítí jsou zřejmé, takže rozhodující otázkou již není volba mezi pevně propojeným bezpečnostním systémem a systémem s bezpečnostní komunikační sítí, nýbrž spíše volba takové sítě, která má co nejflexibilnější topologii a současně nejvyšší úroveň ochrany investic. Tím, že protokolem CIP Safety je možné doplnit běžné sítě DeviceNet a EtherNet/IP, dává rozšíření o protokol CIP Safety záruku, že dřívější investice nebyly vynaloženy zbytečně, přičemž současně poskytuje obrovský potenciál pro další budoucí rozšíření.

(Rockwell Automation)

LISTEN.
THINK.
SOLVE.®

Řada PLC Allen-Bradley® Micro800™ pro širokou škálu menších strojních aplikací – včetně polohování až tří servo os. Navržen pro možnost individuálního přizpůsobení, flexibilitu a úsporu nákladů.

Jelikož se jedná o součást nabídky produktů Connected Components, používá se jediný programovací software Connected Components Workbench™, čímž se usnadňuje instalace, konfigurace, připojení a údržba. Snadného individuálního přizpůsobení lze dosáhnout díky prostorově úsporným zásuvným a rozšiřujícímV/V modulům Micro800 u široké palety našich procesorů. Zvýšená flexibilita díky integrovaným komunikačním možnostem, jako například síť Ethernet, sériové připojení a USB, činí z tohoto řešení ideál pro menší strojní aplikace.



Načtěte QR kód a získejte virtuální brožuru o Micro800™.
www.rockwellautomation.com/go/micro800

Rockwell Automation

Allen-Bradley • Rockwell Software