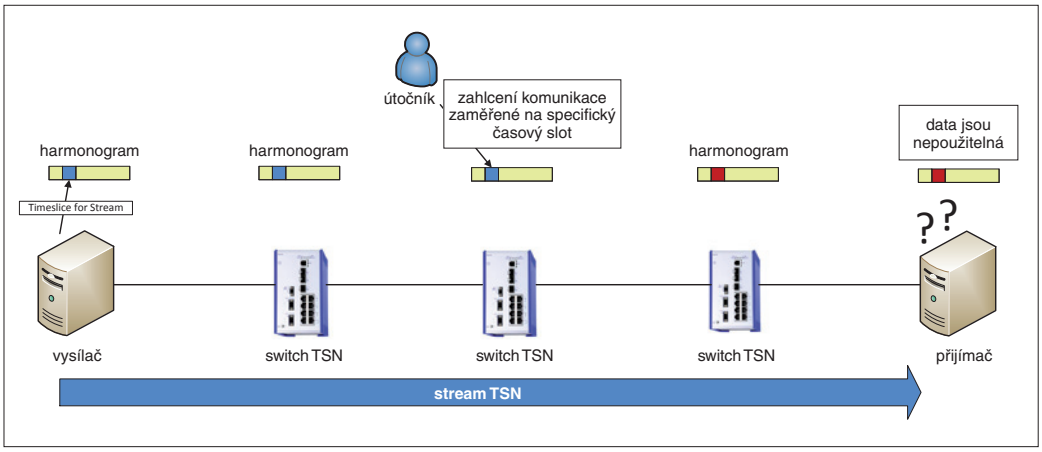
Zabezpečení sítí TSN v moderní automatizaci

Sítě podle standardů TSN (*Time-Sensitive Networking*) jsou dalším krokem ve vývoji Ethernetu a mají všechny předpoklady k tomu, aby se staly základním stavebním kamenem pro sítě IIoT (*Industrial Internet of Things*) a Industry 4.0. Přinášejí vlastnosti reálného času a garantované služby, ale naproti tomu představují problém z hlediska zabezpečení komunikace – tzv. kybernetické bezpečnosti. Ovšem nikoliv neřešitelný – jak popisuje tento článek, stačí správně použít existující a osvědčené zabezpečovací mechanismy a implementovat pravidla pro zabezpečení průmyslových komunikačních sítí.

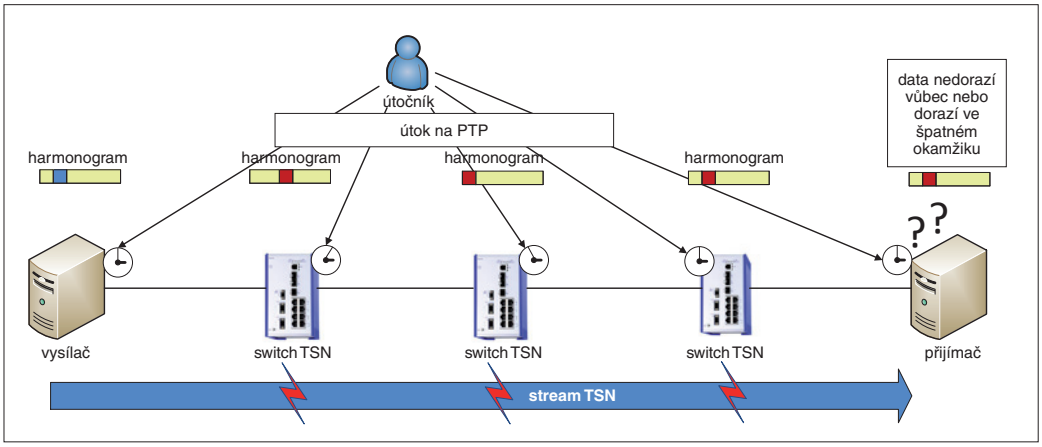
Rozhodující je čas

Sítě TSN jsou založené na skupině standardů specifikovaných pracovními skupinami IEEE 802.1 a IEEE 802.3. Některé z těchto standardů již byly schváleny a publikovány, jiné se teprve připravují. Pro tyto standardy je však společné, že všechna zařízení v síti TSN musí mít společnou časovou základnu. To je nutné k tomu, aby bylo možné datové rámce přenášet deterministicky, podle plánovaného harmonogramu, s jasně stanovenou hranicí maximálního zpoždění (*latence*) a jejím co nejmenším rozptylem – *jitter*.

Pro zajištění těchto funkcí využívají sítě TSN mechanismus TDMA (*Time Division Multiple Access*), který rozděluje čas do cyklicky se opakujících úseků. V rámci každého cyklu jsou sloty vyhrazené pro datový tok s vysokou prioritou, který musí být izolován od zbytku komunikace. Obsazení vyhrazených slotů musí být sdílené všemi účastníky na přenosové cestě. Jinými slovy, vyhrazením slotů se vytváří virtuální kanál zahrnující dvě nebo více koncových zařízení v síti TSN. Aby všechna zařízení v takovém kanálu dodržovala vyhrazení časových slotů, musí být synchronizována. Vysoké přesnosti synchronizace, která je pro sítě TSN nutná, se obvykle dosahuje prostřednictvím protokolu podle IEEE 1588, který je lépe známý pod názvem *Precision Time Protocol* (PTP).



Obr. 1. Útok na vyhrazený časový slot zasáhne celý datový stream



Obr. 2. Útok na hodiny reálného času v protokolu PTP

Čas jako vektor útoku

Jestliže chce útočník ochromit provoz moderních komunikačních sítí, používá často útoky typu DoS (*Denial of Service*). Takový útok se realizuje zahlcením sítě tak velkým množstvím dat, že nemůže dále fungovat. Bylo již uvedeno, že sítě TSN potřebují synchronizaci času, ovšem jak synchronizační protokol PTP, tak mechanismus TDMA mohou být snadno zneužity jako vektory útoku. Útok DoS je v síti TSN jednodušší než u klasického Ethernetu: postačuje vybrat si jako cíl útoku jeden vyhrazený časový slot, protože jeho přetížení postihne celý specifický komunikační stream kritických dat (*obr. 1*). Kromě možnosti přetížení komunikace v kritických vyhrazených časových slotech mohou být cílem útoku i samotné synchronizační protokoly IEEE 1588.

Protokol PTP používají pro synchronizaci hodin mnohé moderní komunikační sítě. Přitom tento protokol nemá žádný vlastní integrovaný zabezpečovací mechanismus a zcela se spoléhá na zabezpečení sítě.

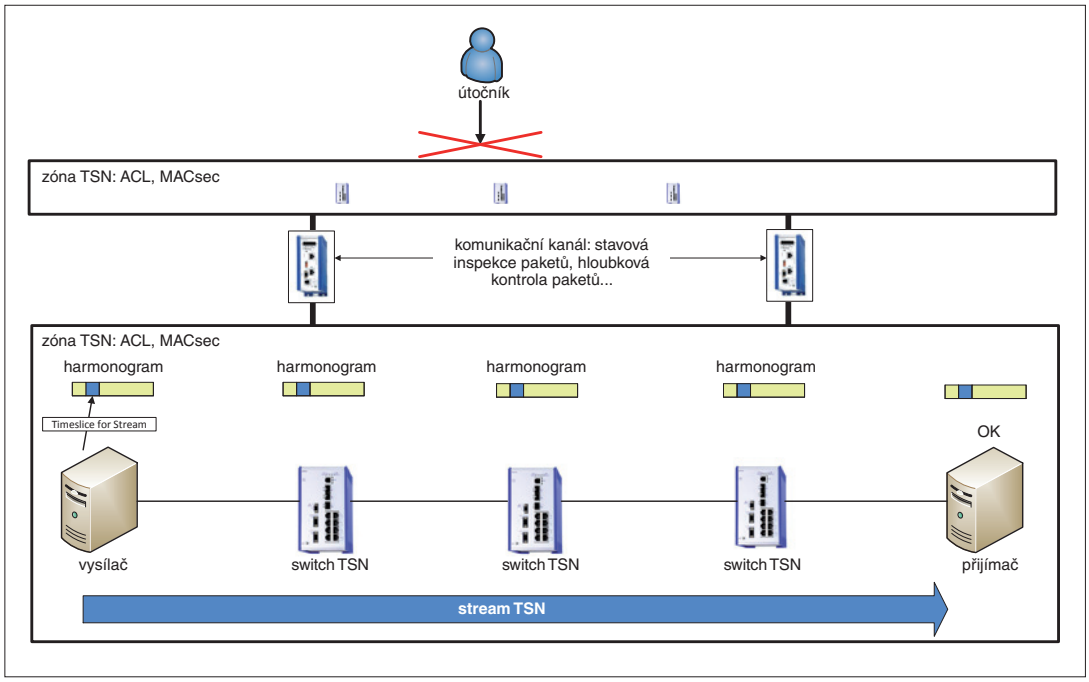
Kdyby v samotné síti nebyly implementovány žádné zabezpečovací mechanismy, útočník by mohl např. ovládnout funkci centrálních hodin. Centrální hodiny by potom mohly např. posílat informace potřebné k synchronizaci s velkým rozptylem a tak sabotovat správné uspořádání časových slotů v jednotlivých zařízeních (*obr. 2*). Útočník navíc může vyvolat diskontinuitu času, což přiměje mnoho časově citlivých aplikací v koncových zařízeních k okamžitému bezpečnostnímu ukončení.

Jak tedy zabezpečit sítě TSN?

Ochrana sítě

Rozhodujícím prvkem pro ochranu sítí TSN zůstávají tradiční firewally. Ty však mají negativní vliv na komunikaci v reálném čase. Například procházejí-li data firewallem s funkcí DPI (*Deep Packet Inspection*), software musí zkontrolovat každý paket, který má být propuštěn do zabezpečené oblasti. Tím se do komunikace zanáší dodatečné zpoždění. Jestliže toto zpožděn-

ní není bráno v úvahu, může nastat situace, kdy datový paket získá takové zpoždění, že není doručen ve svém vyhrazeném časovém slotu, ale až ve slotu následujícím, což v komunikaci způsobí chaos. Jednou z možností, jak tento problém vyřešit, je používat firewally, které jsou určené pro práci v reálném čase. Druhou možností je zviditelnit účastníkům komunikace dobu zpoždění, aby se s ní mohlo v mechanismu TDMA počítat a rezervace časových slotů mohla být podle ní upravena.



Obr. 3. Ochrana sítě TSN rozdělením do zón

Stejný postup může být použit také u switchů, které podporují bezpečnostní mechanismy na hardwarové úrovni – např. seznamy pro řízení přístupu ACL (*Access Control List*) nebo stavové filtry datových paketů. Tyto mechanismy v běžné ethernetové síti nemají na komunikaci podstatný vliv, protože způsobují jen malé zpoždění. Avšak sítě TSN, kde je třeba data přenášet s mikrosekundovou i lepší přesností, jsou z tohoto hlediska velmi citlivé, a dokonce i malé zpoždění může vést k selhání komunikace.

Zdá se, že nejlepší způsob, jak se vyhnout zpoždění, je v sítích TSN žádné zabezpečení nepoužívat. To ovšem není dobrý nápad. Lepší způsob je se zpožděním počítat. Je velmi důležité, aby při výpočtu zpoždění a stanovení harmonogramu časových slotů sítě TSN byla brána v úvahu všechna zpoždění, která mohou vzniknout po cestě vlivem zabezpečovacích funkcí, včetně zpoždění vznikajících ve firewallu.

Ve specifických úlohách, kde je požadována velmi malá latence a krátká doba cyklu, však nemusí být dlouhé zpoždění tolerovatelné, ani když je známé. V těchto případech lze použít dva rozdílné druhy funkcí pro zabezpečení sítí: v prvním případě je zabezpečovací mechanismus implementován přímo v komunikační cestě v síti TSN a v druhém na jejích hranicích.

To odpovídá koncepci rozdělení komunikační sítě do zón a vytváření komunikačních kanálů (*Zones and Conduits*). Cílem tohoto rozdělení je vytvořit oddělené oblasti, které spolu komunikují jen po ověření požadavku na komunikaci. Uvedená koncepce však byla vytvořena s ohledem na zabezpečení běžných ethernetových sítí; v sítích TSN je dalším parametrem, který je třeba vzít v úvahu, časování.

To ale není neřešitelný problém, protože jak požadavek na komunikaci, tak časování komunikace jsou založené na stejném typu komunikační relace *end-to-end* mezi zařízeními v síti. Pro zabezpečení sítě lze tudíž na hranici mezi zabezpečenými zónami použít např. firewall s hloubkovou inspekcí paketů (DPI), zatímco uvnitř zóny, přímo v komunikační cestě v síti TSN, se použije výrazně rychlejší switch se stavovým filtrováním paketů podle seznamu povolených přístupů ACL (*obr. 3*).

Jinou koncepcí zabezpečení, kterou lze zavést v sítích TSN, je hloubková obrana a diverzita (*Deep Defence and Diversity*). Tato koncepce doporučuje pro zabezpečení sítě kombinovat bezpečnostní mechanismy, které pracují různým způsobem, a zařadit je do série. Podle zmíněné koncepce lze pro ochranu přímého přístupu do sítí TSN využít klasické mechanismy řízení přístupu, např. IEEE 801.1X, které jsou často implementovány v routerech a switchích. Pro zvýšení odolnosti sítí TSN proti útokům lze navíc využít bezpečnostní mechanismy druhé, linkové vrstvy modelu ISO/OSI (L2).

Zabezpečení na linkové vrstvě

Jedním z mechanismů linkové vrstvy komunikačního modelu, na jehož začlenění do standardu TSN se aktuálně pracuje, je *Ingress Filtering and Policing* (IEEE 802.1Qci). Tento mechanismus umožňuje kontrolovat, zda jsou datové rámce a jejich čas přijetí součástmi vyhrazeného datového streamu. Jestliže tomu tak není, paket je odmítnut dříve, než může mít negativní vliv na provoz sítě. Pro autentizaci, kódování a ochranu integrity dat různých streamů mezi účastníky sítě lze navíc použít MACsec (*Media Access Control Security*) nebo podobné mechanismy.

Ovšem právě bezpečnostní mechanismy typu MACsec mají negativní vliv na latenci přenosu dat mezi dvěma účastníky v síti TSN, a to i tehdy, jsou-li realizovány na hardwarové úrovni. Již bylo uvedeno, že i zde je možné dobu zpoždění způsobeného kontrolou přístupu zveřejnit, aby s ní účastníci mohli počítat. Doba zpoždění silně závisí na tom, zda jsou bezpečnostní mechanismy realizovány hardwarem nebo softwarem.

Shrnutí

Sítě TSN jsou novým krokem vývoje Ethernetu. Velká šířka pásma a služby reálného času jsou předpokladem pro to, aby sítě TSN mohly být nyní i v budoucnu využívány jako moderní komunikační prostředek v průmyslové automatizaci. Sítě TSN nejsou firemním nebo pseudofiremním standardem, proto je lze v průmyslové automatizaci používat zcela univerzálně, kdekoliv a kdykoliv. Pro zajištění kybernetické bezpečnosti sítí TSN není třeba vymýšlet nic nového: bezpečnostní mechanismy, které existují pro zabezpečení ethernetových sítí, lze použít i pro sítě TSN. Celou situaci ovšem komplikují přísné požadavky na reálný čas, na něž je třeba brát při navrhování sítě a jejího zabezpečení ohled. Současné koncepce zabezpečení umožňují těmto požadavkům vyhovět.

Ačkoliv celá skupina standardů TSN ještě není dokončena, ty z nich, které byly schváleny, se již v praxi používají. Specifikací zbývajících standardů se intenzivně zabývají pracovní skupiny IEEE 802.1 a 802.3 a standardizační proces by měl zaručit, že i bezpečnostní mechanismy TSN budou kompatibilní se standardním Ethernetem.

Dr. René Hummen, Dr. Oliver Kleineberg,
Belden, Inc.