Bezpečnost a redundance

Bezpečnost a redundance jsou dva rozdílné pojmy, kterým ne každý zcela rozumí jak jednotlivě, tak především jejich vzájemné souvislosti. Článek je stručně objasňuje a charakterizuje jejich vztah jak z technického, tak i z legislativního hlediska. Závěrem jsou uvedena základní doporučení pro praxi.

Dva pohledy na bezpečnost

Funkční bezpečnost (dále jen *bezpečnost*, anglicky *safety*) je definována velmi podobně, ale nikoliv stejně pro obor řízení strojů a pro obor řízení spojitých technologických procesů. U každé úlohy, kde není zřejmé, zda jde o stroj (strojní zařízení), nebo o proces, je třeba si položit dvě základní otázky.

První z otázek je: „Co je nebezpečné?“. Na ni se čeká odpověď buď „pokračovat v činnosti“, nebo „zastavit činnost“. Druhá otázka zní: „Co je bezpečné?“. Na druhou otázku se čeká odpověď „pokračovat v řízení“, nebo „zastavit řízení“.

Jestliže je nebezpečné pokračovat v činnosti a bezpečné je zastavit řízenou entitu (stroj, proces), jde o řízení stroje. Jako příklad lze uvést pohybující se robot. Bude-li jeho činnost zastavena, nehrozí dále žádné riziko, jehož zdrojem by byl (stojící) robot.

Je-li nebezpečné zastavit řízení a je bezpečné udržet řídicí systém entity v chodu, jde o řízení (bezpečnost) spojitého procesu. Příkladem může být parní kotel. Kdyby napájecí čerpadlo přestalo dodávat vodu, za které se generuje pára, a tím se ochlazuje kotel, mohlo by dojít k přehřátí kotle, porušení jeho stěny a k explozi. Tedy ne vždy je „povel“ zastavit danou entitu smysluplný a bezpečný.

Důležité pojmy

K usnadnění dalšího výkladu je vhodné definovat některé základní pojmy, jak je – v určitém zjednodušeném pojetí – autor chápe v tomto pojednání o vztahu mezi bezpečností a redundancí.

Řídicí systém

Řídicí systém je takový automatický prostředek k řízení, který nastavuje své výstupy na základě obrazů vstupů a při použití vnitřního softwaru, který toto automatické chování umožní. Pro potřeby v rámci tohoto textu je ponecháno stranou rozdělení vstupů a výstupů na digitální a analogové, rozdělení softwaru na firmware a další vrstvy apod.

Bezpečnostní systém

Bezpečnostní systém je systém splňující požadavky kladené na tzv. bezpečnostní komponenty. Pro účely tohoto článku postačí definice označující jako bezpečnostní takový systém, jehož vstupy a výstupy jsou určitým vnitřním způsobem sledovány a jejich chování je řízeno, stejně jako je jinými prostředky sledováno a hlídáno také chování softwaru. Vyskytne-li se chyba, následuje reakce závislá na povaze úlohy.

Redundantní systém

Systém s redundancí (tzv. redundantní systém) je systém, který nemusí mít nic společného s bezpečností (nezaměňovat automaticky s hledisky spolehlivosti, dostupnosti; anglicky *availability*). Vezměme si jeho pojmenování – slovo *redundance* znamená nadbytečnost, tedy laik nepoznamenaný praxí by řekl, že takový řídicí systém je při konkrétním použití zbytečně rozsáhlý. Redundantní řídicí systém má obvykle dvě procesorové jednotky (CPU), ty mohou mít dvojité napájecí obvody, dvojité komunikační sběrnice, dvojité obvody I/O, dvojité databázové prostředky, dvojitý zobrazovací podsystém, či dokonce i dvojitý archiv provozních údajů. Někteří výrobci umožňují ve svých zařízeních zdvojit pouze některé z uvedených komponent, přičemž ostatní mohou zůstat jednonásobné.

Proč dvojité zařízení? V případě poruchy je tato detekována a daná oblast je přepnuta na druhý z okruhů či druhou z komponent – např. na druhou procesorovou jednotku nebo na záložní větev komunikační sběrnice. Přepnutí je zobrazeno operátorovi a porucha, např. přerušený komunikační kabel, musí být do určité doby odstraněna. Následně si operátor zvolí, zda chce systém opět přepnout do předchozího stavu, nebo ponechat běh na druhou, záložní větev a až v případě její poruchy přepnout zpět na větev první. Z naznačeného vysvětlení je patrné, že zmíněný laik má ze značné části pravdu: motivem k používání řídicích systémů s redundancí jsou ekonomické ztráty spojené s odstavováním a opětovným spouštěním technologického zařízení – především v provozech, kde opětovné započetí výroby trvá dlouho a ekonomické ztráty jsou příliš velké, jako např. v elektrárnách, chemických a petrochemických závodech a dalších provozech se spojitými technologickými procesy.

Další skupinou systémů jsou *kombinace* předchozích dvou typů systémů, tedy bezpečnostní a redundantní systém v jednom. Z pohledu uživatele je takové uspořádání výhodné, protože pořizovat samostatné redundantní a bezpečností systémy je značně nákladné (*de facto* se pořizují dva systémy místo jednoho, přičemž je nutné vyřešit vzájemnou komunikaci těchto systémů a jejich napojení na podsystém vizualizace, což při použití kombinovaného systému není zapotřebí).

Na trhu jsou nabízeny také speciální výrobky splňující nejvyšší požadavky na bezpečnost a redundanci označované jako TMR (z anglického *Tripple Modular Redundancy*), které jsou trojnásobně zálohovány a současně jsou klasifikovány jako bezpečnostní. Takové systémy jsou využívány např. při řízení primárních okruhů jaderných elektráren, refrakčních kolon v rafineriích, plošin pro těžbu ropy a zemního plyn a v podobných provozech s vysokou úrovní rizika.

Legislativní hledisko

Jak na danou problematiku nahlíží legislativa? Jde o záležitost poněkud složitější. Základním kritériem při rozhodování je, zda daná řízená entita splňuje definici stroje (strojního zařízení). Jestliže ano, je třeba následovat strojírenskou směrnici 2006/42/ES, jak předepisuje zákon 22/1997 Sb. Nejde-li o stroj, půjde s největší pravděpodobností o spojitý technologický proces.

Strojní zařízení

Strojní zařízení (stroje) podléhají působnosti zákona 22/1997 Sb. a na něj navázaných nařízení vlády nebo směrnic EU, např. zmíněné strojírenské směrnice. Podle toho, do které skupiny stanovených výrobků daný stroj patří, takové nařízení vlády či směrnice musí výrobce splnit. Jestliže chce uživatel zvolit levnější a jednodušší prohlašování shody podle přílohy VIII nebo X strojírenské směrnice 2006/42/ES, je nutné použít harmonizované normy. V oficiálním věstníku ke strojírenské směrnici jsou ze všech možných k dispozici normy EN ISO 13849-1 nebo EN 62061, ovšem zavést podle nich řídicí systém s redundancí je velmi nesnadné.

Spojité technologické procesy

Pokud jde o bezpečnost nikoliv strojů, ale spojitých technologických procesů, je daleko efektivnější použít soubor norem EN 61508, nebo spíše EN 61511. Situace není ani zde zcela jednoznačná, protože zejména norma EN 61508 je použitelná i pro řídicí systémy strojů, nicméně není harmonizována a při prohlašování shody by bylo nutné použít postup podle přílohy IX směrnice 2006/42/ES, vyžadující přezkoušení typu, a tím celé řešení značně prodražit.

Každopádně oba soubory norem, EN 61508 i EN 61511, pracují s pojmem pravděpodobnosti selhání systému při požadavku na jeho činnost (*Probability of Failure on Demand* – PFD), a to ve dvou podobách v závislosti na četnosti výskytu požadavků na činnost systému (komponenty). U systémů pracujících v režimu s velkou četností požadavků na činnost (tzv. *high demand*) se užívá veličina PFH_d (*Probability of Dangerous Failure per Hour*), zatímco u systémů pracujících v režimu s malou četností požadavků na činnost (tzv. *low demand*) veličina PFD.

Co si pod uvedenými pojmy představit? Jako názornou ukázku lze uvést příklad z běžného automobilu. Bezpečnostní komponentou pracující v režimu velké četnosti požadavků na činnost je systém provozních brzd, zatímco bezpečnostní komponentou s malou četností požadavků na činnost je airbag. Stejné je to s řídicími a bezpečnostními systémy v průmyslu.

Systémy a komponenty, u kterých se předpokládá časté zasahování do chodu daného procesu (technologického zařízení), budou pracovat v režimu *high demand* a půjde o úlohy, při nichž často dochází ke styku člověka se strojem. Naopak tam, kde systémy pouze sledují výrobní proces a zasáhnou až v případě rizika vzniku nebezpečné události vlivem ojedinělé poruchy, půjde o systémy pracující v režimu *low demand*.

Systémů, které mohou pracovat pouze v režimu *low demand*, je velmi mnoho, ale je třeba si uvědomit, že zatímco přípustná pravděpodobnost vzniku nebezpečné poruchy je např. jedna ku sto milionům u systémů v režimu *high demand* v úrovni SIL 3 (*Safety Integrity Level;* integrita bezpečnosti), pro stejně nebezpečný případ v režimu *low demand* je to pro tutéž SIL 3 jedna ku deseti tisícům, tedy o čtyři řády méně. Pozor, schválně neříkáme hůře, ale méně, protože pro *režim low demand* je to postačující. Byla by tedy velká chyba si myslet, že má-li systém v katalogovém listu uvedeno SIL 2, lze ho použít v jakékoliv úloze. Mohl by totiž vzniknout vážný rozpor s legislativou, který by mohl mít velmi závažné následky.

Při hodnocení bezpečnostních systémů (komponent) je tedy třeba vědět, zda pravděpodobnost selhání při požadavku na činnost je v daném případě charakterizována veličinou PFH_d (tj. pro režim *high demand*), nebo veličinou PFD (tj. pro režim *low demand*).

Pokud jde o systémy TMR, tyto většinou mají certifikáty pro oba typy pracovního režimu, neboť často řeší kombinované úlohy v oblasti bezpečnosti.

Čemu věnovat pozornost

Časté reakce na již uvedené jsou: „To je pěkné, že toho mám v hlavě zase o něco víc, ale jak se to celé projeví v mé praxi? Co se zase musím učit?“. Pracuje-li odborník se stroji nebo na jejich konstruování již minimálně dva roky, nemusí se učit nic zásadně nového. Za zmínku snad stojí pouze nová norma EN 14119, která značně zpřísní používání bezpečnostních krytů; ve verzi ČSN by měla vyjít v létě 2014. Pracuje-li v oboru řízení spojitých technologických procesů, poslední změna se objevila v roce 2010, kdy byl zásadně novelizován soubor norem řady EN 61508. Zde lze doporučit zakoupení tohoto souboru novelizovaných norem. Dobrý pozor je však třeba si dávat v případě, že tento odborník vstupuje ze zaběhnutých kolejí do jiných, byť na první pohled příbuzných odborných oblastí – tedy např. jestliže firma běžně řeší bezpečnost technologických procesů a najednou je zákazníkem oslovena s požadavkem na vyřešení bezpečnosti stroje. Bezpečnost strojů a bezpečnost spojitých procesů jsou sice obory velmi příbuzné, ale přístupy, které jsou v nich používány, se přece jenom poněkud liší a jiným se způsobem je též prohlašována shoda.

Doporučení pro praxi

Na závěr několik základních doporučení pro praxi. V oboru bezpečnosti strojů je ideální pro malé stroje použít bezpečnostní moduly. Při dodržení schémat doporučených výrobcem stačí k ověření správnosti jednoduchý výpočet. Pro středně velké stroje s odděleným klasickým řídicím systémem a bezpečnostním systémem je ověření složitější pouze o oblast softwaru. Pro velké stroje a strojní zařízení je nejlepší použít integrovaný bezpečnostní systém, což je systém, který umí řídit výrobní proces a zároveň je schopen vyhodnocovat obvody bezpečnostních snímačů. Ohodnotit celý integrovaný systém je mnohem jednodušší než u varianty odděleného hardwaru. K řízení a zajištění bezpečnosti procesů lze rovněž použít integrovaný systém jak v klasickém uspořádání – tedy neredundatním, tak v redundantním uspořádání, a to v těch případech, kde by v důsledku neplánované odstávky mohly vzniknout ekonomické škody, nebo daleko častěji – kde by porucha mohla být příčinou vzniku nebezpečné situace.

Karel Stibor