# Bezpečnostné systémy

Kľúčovou normou platnou pre túto oblasť je medzinárodná norma IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems), ktorá sa zaoberá bezpečnosťou z hľadiska celej životnosti bezpečnostných systémov. Prax totiž potvrdzuje, že drvivá väčšina príčin havárií leží mimo samotnej prevádzky a údržby. Štatistické rozdelenie typických vyšetrovaných a analyzovaných havárií poskytlo nasledujúce údaje:

- 44,1 % príčin havárií spočíva v zlom návrhu,
- 14,7 % príčin havárií spočíva v plánovaní a implementácii,
- 5,9 % príčin havárií spočíva v inštalácii a uvedení do prevádzky,
- 14,7 % príčin havárií spočíva v prevádzke a údržbe,
- 20,6 % príčin havárií spočíva v úpravách po uvedení do chodu.

Dôležité je tiež pripomenúť, že funkčná logika samotného systému sa podieľa v štatistike iba dielom 15 %, pričom snímače majú zastúpenie 35 % a akčné členy až 50 %.

Z rozdelenia vidieť, že samotnému návrhu systému treba z hľadiska bezpečnostných rizík venovať náležitý priestor. V tejto súvislosti bola zavedená trieda bezpečnosti SIL (Safety Integrity Level), od 1 (najmenšie požiadavky) do 4 (najvyššie požiadavky), ktorá vlastne definuje pravdepodobnosť výskytu bezpečnostného problému navrhnutého systému ako celku v rozmedzí od $10^{-(SIL+1)}$ do $10^{-(SIL)}$ pre nižšie požiadavky a pravdepodobnosť výskytu jednej nebezpečnej chyby za hodinu pre vysoké požiadavky kontinuálnej prevádzky v rozmedzí od $10^{-(SIL+5)}$ do $10^{-(SIL+4)}$. Technologické procesy spadajú vzhľadom na nepretržitú prevádzku pod vysoké požiadavky.

Treba si tiež uvedomiť, že akékoľvek zníženie rizika znamená náklady na opatrenia alebo zariadenia, ktoré riziko znižujú. V konkrétnom technologickom procese riadenom číslicovými systémami riadenia (DCS a PLC) možno riziká znižovať v samotnej technológii (v strojno-technologických zariadeniach a postupoch) a v systémoch riadenia (zvýšením spoľahlivosti a zlepšením informovanosti operátorov). Takto možno **celkové riziko** potlačiť za ekonomicky odôvodnené náklady na úroveň **akceptovateľného rizika**. Vždy zostáva tzv. **zvyškové riziko**. To musí zvládnuť **bezpečnostný systém**.

Jeho funkcia teda je, aby v prípade výskytu podmienky vedúcej k havárii takýto nebezpečný postup zastavil a v krajnom prípade technológiu bezpečne odstavil. Preto sa takýmto systémom hovorí aj ESD – Emergency Shut-Down. Sú to cyklické automaty ako PLC, ktoré však majú, ako vidieť z textu, úplne inú funkciu. Navyše ich technické aj programové prostriedky sú vyhotovené ináč, práve preto, že musia mať certifikovaný stupeň bezpečnosti (CASS – Conformity Assessment of Safety related Systems).

AXESS

**AXESS, spol. s r.o.**

**Ing. Vladimír Boďo, CSc.**
**Námestie hraničiarov 31 – 33**
**851 03 Bratislava**
**Tel.: 02/62 24 75 70**
**Fax: 02/62 24 75 38**
**e-mail: axess@axess.sk**
**http://www.axess.sk**