Čo je bezpečnosť?

Ak sa technické procesy vymknú spod kontroly, môžu predstavovať pre ľudí, stroje, zariadenia a okolité prostredie vysoké nebezpečenstvo. Otázky bezpečnosti preto zohrávajú v dnešnom čoraz technickejšom svete stále dôležitejšiu úlohu. V nasledujúcom článku sa trochu bližšie pozrieme na túto problematiku.

Pri obyčajnom listovaní v odbornej literatúre narazí človek na mätúcu rôznorodosť pojmu bezpečnosť, ktorá má v praxi navyše rôzne stupne dôležitosti a výskytu (tab. 1). To vyvoláva u potenciálnych záujemcov automaticky celkom pochopiteľnú otázku: Čo vlastne znamená pojem bezpečnosť? Pokiaľ sa pri zodpovedaní tejto otázky použije zdravý rozum, dospeje sa k záveru (a to bez ohľadu na to, že v príslušných publikáciách existujú účelovo orientované, viac-menej ostré definície), že bezpečnostné problémy, resp. potreby a požiadavky v tejto oblasti vznikajú všade tam, kde sa dá uplatniť elementárny vzťah načrtnutý na obr. 1. Z neho teda vyplýva, že existuje zdroj ohrozenia, resp. nebezpečenstva N a obeť alebo objekt O, ktorý pre isté riziko nevyhnutne potrebuje ochranu. Potenciálne zdroje ohrozenia alebo nebezpečenstva sú pri tom všetky materiálne alebo virtuálne objekty, teda všetky

tematické oblasti	frekvencia výskytu
security	4 390 000 000
safety	1 500 000 000
dátová bezpečnosť	12 100 000
bezpečnosť IT	6 410 000
bezpečnosť pri práci	3 120 000
bezpečnosť reaktora	1 660 000
sieťová bezpečnosť	1 270 000
prevádzková bezpečnosť	1 110 000
bezpečnosť zariadení	708 000
bezpečnosť napájania	628 000
informačná bezpečnosť	609 000
produktová bezpečnosť	595 000
internetová bezpečnosť	548 000
systémová bezpečnosť	441 000
počítačová bezpečnosť	315 000
technická bezpečnosť	167 000
bezpečnosť strojov	166 000
bezpečnosť prístrojov	154 000
pasívna bezpečnosť	100 000
elektrická bezpečnosť	95 000
softvérová bezpečnosť	92 000
aktívna bezpečnosť	75 000
bezpečnosť výroby	49 000
komunikačná bezpečnosť	39 000
funkčná bezpečnosť	35 000

Tab.1 Tematické oblasti vzťahujúce sa na bezpečnosť a frekvencia ich výskytu na internete

Obr.1 Elementárny vzťah ohrozenia

živé i neživé súčasti, komponenty, systémy a fenomény v blízkom, ale aj vzdialenejšom prostredí človeka, ktoré sa vyznačujú nejakým nebezpečným potenciálom vo forme hmoty (zem, voda), energie (všetky druhy), informácie (napr. skrytej v škodlivých softvéroch) a pokiaľ ide priamo o človeka, aj vo forme nekontrolovanej činnosti.

Triedy ohrozenia

Z hľadiska ohrozených objektov S (človek, zviera, životné prostredie, technické komponenty, prístroj, hardvérový, resp. softvérový systém alebo nejaká iná štruktúra reálneho alebo virtuálneho sveta) sa rozlišujú tieto triedy ohrozenia:

- prírodné hrozby z bezprostredného alebo vzdialeného prostredia (napr. galaktické a atmosférické šumy, údery blesku, dopady meteoritov, zemetrasenie, zosuvy pôdy, veterné smršte, záplavy);
- neúmyselné hrozby spôsobené predovšetkým ľudskou neschopnosťou, nemohúcnosťou, zlyhaním alebo chybami (reprezentovanými organizačnými nedostatkami, zlým manažmentom, slabými vedomosťami, zlou koncentráciou, chybami v obsluhe, v údržbe, zlým prenosom informácií, nesprávnou interpretáciou predpisov alebo signálov, slabou kontrolou, nedbalosťou, ľahkomyseľným zaobchádzaním s nebezpečnými alebo ohrozenými objektmi), ale aj funkčným zlyhaním technických prostriedkov (spôsobeným poruchami a výpadkami základných stavebných prvkov, prístrojov a systémov v dôsledku nedostatočnej spoľahlivosti alebo nerozpoznanej vnútornej systematickej chybe vo forme konštrukčnej, programovej či spínacej chyby alebo nedostatočnej funkčnej stability);
- úmyselné alebo zlomyseľné ohrozenia (napr. frustrovanými zamestnancami, konkurenčnými podnikmi, hackermi, kriminálnymi živlami, tajnými službami, teroristami a inými útočníkmi).

Každá z týchto hrozieb vystavuje ohrozený objekt riziku, resp. situácii predpokladajúcej spôsobenie škody, ktorá môže za istých, veľmi nepriaznivých okolností viesť až k zničeniu daného objektu. K tomu patria:

- ujmy na zdraví (zdravie a život človeka, resp. zvierat),
- vecné škody (škody na majetku, poškodenie a zničenie materiálnych statkov, škody na životnom prostredí),
- straty v prevádzke (straty v produkcii, meškanie dodávok spôsobené napr. poruchami technických prostriedkov, strojov a zariadení),

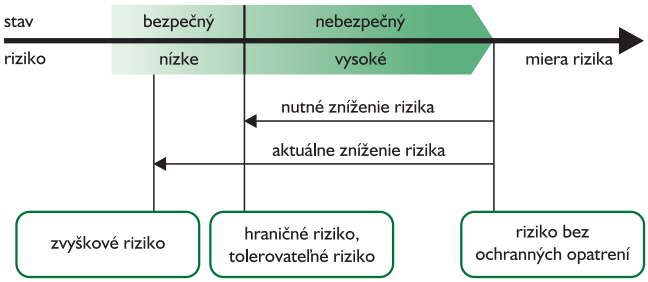
- morálne škody (napr. strata povesti či dôvery, ktorá má spravidla aj vážny dosah na finančné príjmy).

Treba dodať aj to, že v princípe môže byť každý objekt zdroj ohrozenia a zároveň aj ohrozený objekt. Pri neopatrnej manipulácii s elektrickým prístrojom si môže niekto privodiť ujmu na zdraví, ale naopak, prístroj sám o sebe môže spôsobiť funkčným zlyhaním škody na majetku.

Implementácia bezpečnosti

Akým spôsobom však možno implementovať bezpečnosť cielene a účelovo do prístrojov, strojov a zariadení a predovšetkým do čoraz komplexnejších systémov kategórie človek – stroj? Základné alternatívy sú tieto:

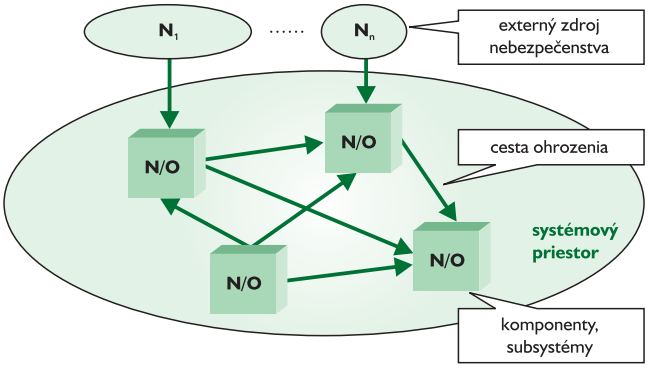
- eliminácia zdrojov ohrozenia (pokiaľ je to realizovateľné), resp. zredukovanie potenciálu ohrozenia na minimálnu možnú mieru;
- zabránenie účinku nebezpečenstva v čo najrozsiahlejšej miere, inými slovami minimalizovanie pravdepodobnosti výskytu udalosti spôsobujúcej škodu, t. j. zníženie s tým spojeného rizika prostredníctvom vhodných opatrení pod isté hraničné riziko (obr. 2); k týmto opatreniam patrí cielené nasadenie monitorovacích a bezpečnostných funkcií, aby sa prípadné udalosti vedúce k škodám zachytili čo najskôr a odvrátili napr. pomocou alarmov, poplachov a automatických protiopatrení;
- pri vzniku škody promptne aktivovať vopred starostlivo naplánované obmedzenie škôd tak, aby bolo možné poškodený objekt čo najrýchlejšie uviesť do pohotovostného stavu.



Obr.2 Základná schéma posudzovania rizika

Štruktúrovaný reálny systém sa potom môže považovať za bezpečný, keď sa spomínané úvahy transformujú do reality, čím sa docieli, že riziko pre všetky spôsoby ohrozenia systému z externých zdrojov alebo aj medzi jednotlivými komponentmi systému, resp. subsystémov leží pod tolerovateľnou hranicou (obr. 3).

V konkrétnom prípade sa počas koncipovania bezpečného systému analyzuje a posudzuje očakávané riziko pomocou presných zásad, postupov a praktík a zároveň sa reguluje na rozumnú hranicu (obr. 2). Pri všeobecnom posudzovaní miery rizika hrajú dôležitú úlohu kritériá, ako pravdepodobnosť výskytu neželanej udalosti, rozsah škôd, geografické a časové rozšírenie škôd, odstránenie škôd, oneskorenie medzi vznikom udalosti a neskoršími následkami, ako aj spoločenské reakcie, ktoré sa môžu objaviť pri porušení individuálnych, sociálnych alebo kultúrnych záujmov. V rámci príslušného rozhodovacieho procesu sa uplatňuje tzv. princíp ALARP (As Low As Reasonable Possible). Práca



Obr.3 Vysvetlenie systémového rizika

v tomto smere vyžaduje veľké skúsenosti a spravidla ju vykonáva špecializovaný tím expertov. Výsledky potom reprezentujú do istej miery kvantifikovanú mienku expertov, v každom prípade sú však subjektívne a často ovplyvnené záujmami jednotlivcov alebo skupín. Objektívne formálne posúdenie rizika preto neexistuje. V technickej sfére sa na výpočet rizika používa nasledujúci matematický vzťah:

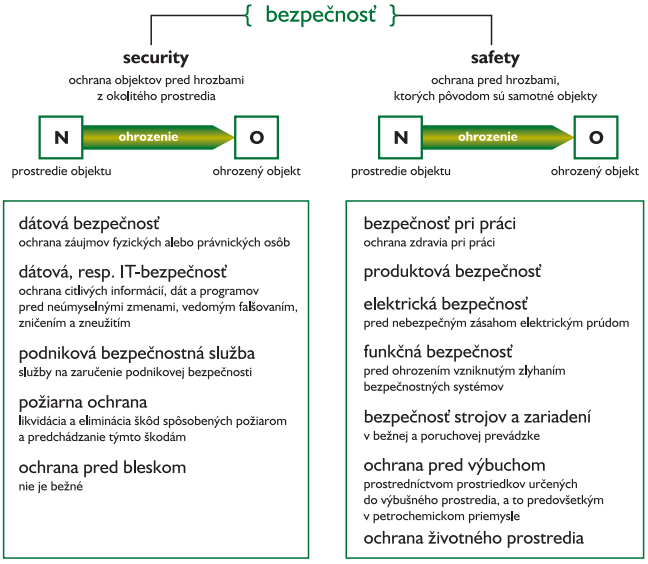
$$R = P \cdot S$$

kde P je pravdepodobnosť výskytu škôd $[P = 0 \ldots 1]$,
S – výška škôd vyjadrená vo vhodných jednotkách (financie, zranení, mŕtvi atď.).

Z vedeckých teoretických poznatkov, ale aj z hospodárskych dôvodov vyplýva, že absolútna bezpečnosť v zmysle zamedzenia akéhokoľvek rizika neexistuje a v každom prípade sa vyskytuje akési minimálne zvyškové riziko, s ktorým sa treba jednoducho vyrovnať. Na analýzu možného nebezpečenstva a posudzovanie rizika, takisto ako na formovanie bezpečných technických objektov je k dispozícii rozsiahly súbor predpisov.

Safety a Security

V praxi je výhodné pri riešení problémov z oblasti bezpečnosti, a to najmä v priemyselnej sfére rozlišovať angloamerický význam slov Security (ochrana objektov pred hrozbami z okolitého prostredia) a Safety (ochrana pred hrozbami, ktorých pôvodom sú samotné objekty). Obr. 4 názorne ozrejmuje jednotlivé rozdiely.



Obr.4 Názorné vysvetlenie rozdielu medzi pojmami Security a Safety

Záver

Bezpečnosť je vo svete vyspelej techniky vysoko aktuálna téma. Tento článok ponúka krátky prehľad najrôznejších bezpečnostných aspektov špeciálne sa týkajúcich priemyselnej sféry. Systémoví inžinieri musia pri tvorbe, konštrukcii, vývoji, projektovaní, realizácii, starostlivosti a údržbe zariadení, strojov a prístrojov venovať bezpečnosti adekvátnu pozornosť. Na to slúži obsiahly a neprehliadnuteľný súbor noriem.

Zdroj informácií: www.AuD24.net

Branislav Bložon