Systémy výstrah zásadně ovlivňují bezpečnost provozu zařízení

Článek pojednává o spolehlivosti obsluhy rozsáhlých technologických zařízení, o konkrétních analýzách příčin havárií takovýchto zařízení a o významu výstražných hlášení (výstrah, alarmů), systémů jejich správy a dodržování předepsaných pravidel změnového řízení pro bezpečnost provozu zařízení.

Hlavním úkolem pracovníků na pozicích operátorů rozsáhlých technologických zařízení (nejčastěji v chemickém průmyslu a v energetice) je především důsledně udržovat hodnoty provozních veličin (teplota, tlak, průtok, poloha hladiny atd.) v technologickém zařízení v určených mezích – zásahy operátorů mají tudíž zejména charakter regulace procesu. Dalším důležitým úkolem operátorů je řešit poruchy a havarijní situace a minimalizovat jejich následky.

Co se týče interakce obsluhy (operátora chemické výroby) se zařízením, lze vysledovat tři možné kategorie zásahů, a to:

– *zásahy předcházející poruše*, což u operátora chemické výroby jsou zejména činnosti, které mohou vytvořit podmínky pro vyřazení ochranných mezí nebo kontrolních podmínek (jde např. o změnu konfigurace poloh ventilů, vyřazení výstrah při spouštění zařízení apod.),
– *zásahy vyvolávající poruchu*, kdy obsluha zařízení chybným zásahem způsobí poruchu v systému (nesprávné nastavení hodnoty technologické veličiny, opomenutí spuštění nebo odstavení procesu v případě, že nejsou tyto operace spouštěny automaticky, apod.),
– *zásahy jako odezva na iniciační poruchu*, tj. v situaci, kdy je zařízení v abnormálním stavu: jde o zásahy obvykle předepsané v havarijních předpisech a postupech (např. ruční aktivace ochranných systémů, odstavení zařízení apod.).

Článek je především zaměřen na poslední z uvedených kategorií operátorských zásahů, v níž jsou významným nástrojem pro detekci abnormálních podmínek tzv. alarmy (výstrahy, výstražná hlášení). To jsou automatizovaná, řídicím systémem generovaná upozornění na poruchu v chování řízeného (sledovaného) procesu, která vyžaduje zásah operátora. Výstražná hlášení by měla splňovat základní požadavky, které již v první polovině dvacátého století stanovil zakladatel glosematiky Louis Hjelmslev. Výstražný signál podle nich musí být jasný, zřetelný a jednoznačný, protože na jeho základě jsou zahájeny kognitivní a rozhodovací procesy, podle jejichž výsledků by operátor měl být schopen adekvátně zasáhnout do řízeného procesu, a zabránit tak případným nežádoucím situacím, či dokonce haváriím.

Bohužel ne vždy se však podaří haváriím předejít. Pro posuzování rizik spojených s technologickými provozy a hledání možných způsobů jejich redukce byla do české legislativy v souladu s evropskými předpisy zavedena vyhláška č. 256/2006 Sb., o analýze a hodnocení rizik závažných havárií. Tato vyhláška zahrnuje také analýzu vlivu lidského činitele na bezpečnost technologických zařízení. V české legislativě je vlastní postup analýzy zakotven v 6. metodickém pokynu odboru environmentálních rizik Ministerstva životního prostředí ČR (MŽP), kde je uložena povinnost provádět kvalitativní hodnocení vlivu lidského činitele na bezpečnost zařízení.

Někdy však (zejména u složitých technologických jednotek) samotná analýza lidského činitele nestačí k dostatečně hlubokému porozumění všem bezpečnostním aspektům výrobního zařízení. Vedle technologického zařízení a obslužného personálu je velmi důležitým hlediskem také tzv. ergonomičnost řízení, tedy správné uzpůsobení řídicích a ovládacích systémů lidské obsluze. V současné době lze s použitím moderních řídicích systémů automatizovat chod i velmi složitých jednotek. Moderní systémy umožňují dosahovat vyšších úrovní automatizace a jsou lépe konfigurovatelné, ale naproti tomu generují stále více různorodých údajů o průběhu řízeného procesu a jeho změnách, které jsou určeny operátorům. A právě srozumitelná prezentace relevantních údajů a informací operátorovi je tím nejdůležitějším faktorem, který ovlivňuje průběh řízení technologického procesu.

Havárie v rafinerii BP Grangemouth

K ilustraci požadavků kladených na systémy správy výstražných hlášení si popišme situaci v ropné rafinerii Grangemouth společnosti BP plc (dříve British Petroleum plc), kde v roce 1987 došlo k nehodě neodhalitelné (nebo obtížně odhalitelné) metodami popsanými v 6. metodickém pokynu MŽP. Přestože vznik nehody souvisel i se závažnou konstrukční vadou, následné vyšetřování se soustředilo na chyby operátorů.

Technolologické zařízení

Nehoda nastala v jednotce hydrokrakování. Operace hydrokrakování se provádí podle typu hydrogenátu v přebytku vodíku při teplotě 370 až 480 °C a tlaku 15 až 30 MPa. V tomto procesu se produkty vystupující z hydrokrakovacího reaktoru vedou do systému separátorů, v němž se oddělí vodík a další lehké plyny (*obr. 1*). Kapalné produkty se z nízkotlakého separátoru vedou k dalšímu zpracování do frakční kolony. Nehoda vznikla v důsledku průniku vodíku z vysokotlakého do nízkotlakého separátoru, který však nebyl pro vysoké tlaky zkonstruován.

Vysokotlaký separátor byl vybaven ventilem řídícím polohu hladiny, který také fungoval jako uzávěr snižující tlak kapaliny přepouštěné do nízkotlakého separátoru a současně bránící průchodu vysokotlakého vodíku do nízkotlaké části zařízení.

Nádoba nízkotlakého separátoru byla dále chráněna před nebezpečným vnitřním přetlakem pojistným ventilem. V nízkotlakém separátoru v rafinerii BP Grangemouth nebyl pojistný ventil navržen pro průtok při tlaku vyskytujícím se ve vysokotlaké části zařízení, ale pouze k redukci tlaku par při nárůstu teploty v nízkotlakém separátoru.

Průběh havárie

K nehodě došlo v noci na 22. březen 1987, kdy byla jednotka hydrokrakování po odstávce uvedena do provozu. Asi ve 02:00 h místního času, tedy pět hodin před nehodou, byl odstaven jeden z hydrokrakovacích reaktorů z důvodu vysoké teploty v reaktoru. Průtok plynu byl přepnut na recirkulaci a bylo rozhodnuto vyčkat na příchod ranní směny. V 07:00 h nastal silný výbuch. Při nehodě byl smrtelně zraněn jeden pracovník externí firmy, který byl v době výbuchu ve velínu. Vzniklý požár se podařilo zvládnout až pozdě večer.

Šetření ukázalo, že tlaková nádoba nízkotlakého separátoru byla roztržena a fragmenty se rozletěly do okolí. Největší z fragmentů, třítunový, byl nalezen kilometr od jednotky. Z rozptylu fragmentů bylo určeno, že nízkotlaký separátor se roztrhl vnitřním přetlakem minimálně 5 MPa (projektován byl na přetlak 0,9 MPa).

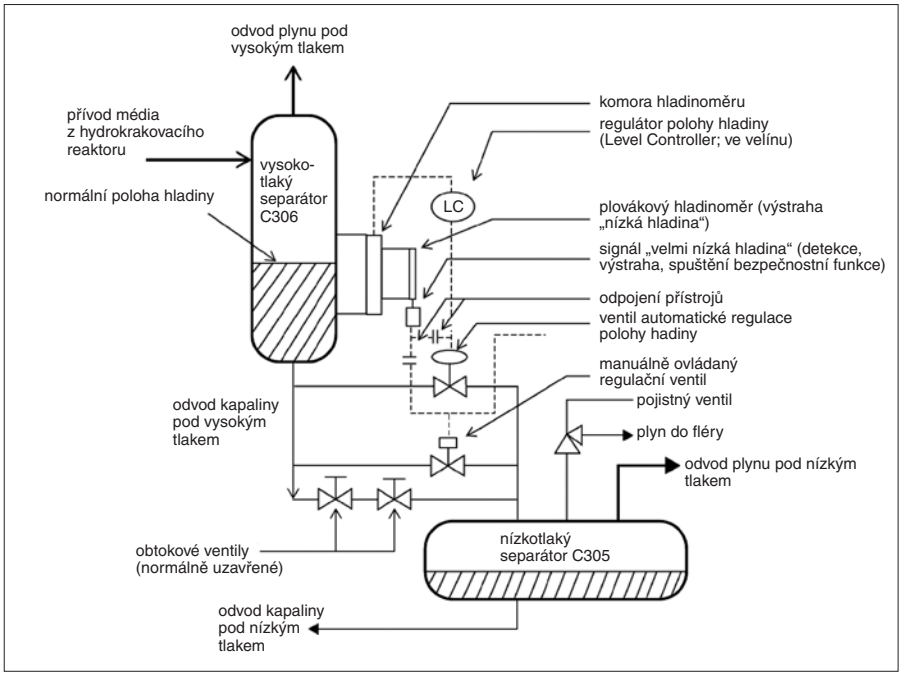
Záznam údajů z jednotky prokázal, že nehoda byla důsledkem prosazení plynu z vysokotlakého separátoru po poklesu hladiny kapaliny pod úroveň připojovacího potrubí do nízkotlakého separátoru. Hladina ve vysokotlakém separátoru sice byla regulována automaticky, ale tato regulace byla v průběhu odstávky a spouštění odpojena spolu se signalizací a výstrahou informujícími o poklesu hladiny na úroveň 10 % nad kritickou úrovní. Jednotka byla současně vybavena také záložním plovákovým hladinoměrem, který měl v případě potřeby dát automatickým ventilům

signál k uzavření průtoku kapaliny do nízkotlakého separátoru. Naneštěstí byl však tento snímač asi rok před událostí od ventilů odpojen. Za dané situace záviselo sledování polohy hladiny ve vysokotlakém separátoru pouze na ostražitosti obsluhy.

Závěry z vyšetřování nehody v rafinerii Grangemouth

Oficiálně bylo za příčinu nehody označeno selhání obsluhy zařízení. Nicméně je zřejmé, že nehoda nastala zejména v důsledku selhání řídicího systému, zanedbání údržby i kontroly zařízení a špatných pracovních návyků. Při dané konfiguraci a stavu zařízení bylo selhání obsluhy pouze otázkou času. Nebyl tosledek bývá problematický a mnohdy vede k přetěžování operátorů.

Je-li operátor zahlcen nadměrným počtem výstražných hlášení, tj. větším, než na jaký operátor dokáže efektivně reagovat, mluví se o „záplavě výstrahami“ (*alarm flood*). Podle definice asociace EEMUA (*Engineering Equipment and Materials Users' Association)* [7] je hranicí zatížení operátora více než deset výstrah během deseti minut trvající souvisle po dobu jedné hodiny [5]. Potenciální nebezpečí takovéto situace spočívá v tom, že operátor může v jejím průběhu mezi méně významnými přehlédnout důležitou výstrahu, což může vést ke vzniku nežádoucí situace, poškození zařízení či nebezpečné nehody. K předcházení takovýmto situacím je nezbyt-



Obr. 1. Technologické schéma separátorů hydrokrakovací jednotky v rafinerii BP Grangemouth

tiž v činnosti žádný ochranný či bezpečnostní obvod, který by musel být překonán.

Klíčovou roli při rozvoji nehody sehrálo selhání systému správy výstražných hlášení. Někdy je totiž ve výjimečných provozních situacích nutné vyřadit bezpečnostní vybavení z provozu. Bezpečnostní výbava by však měla být odpojena až po písemné autorizaci kompetentní osobou a toto odpojení by mělo být zřetelně označeno např. signalizací na ovládacím panelu, aby operátor (zejména operátor z další směny) věděl, že ochrana není funkční.

Nehoda v rafinerii Texaco v Milford Havenu

Naproti tomu je také přílišné „zalarmování“ technologického zařízení. Svádí k němu relativní jednoduchost, s jakou lze v moderních řídicích systémech konfigurovat nová výstražná hlášení, někdy bez rozmyslu. Výné stav systému výstražných hlášení a jeho správy průběžně sledovat, udržovat a racionalizovat např. odstraňováním duplicitních výstražných hlášení, přehodnocováním nastavení mezních hodnot příslušných jednotlivým výstražným hlášením, přehodnocováním priority výstrah apod. (viz např. [5], [8] a [9]).

Odstrašujícím příkladem následků špatné údržby systému správy výstražných hlášení je nehoda v rafinerii ropy společnosti Texaco v Milford Havenu v roce 1994 [8]. Důsledkem bylo 26 zraněných a finančních ztráta ve výši 48 milionů liber. Vyšetřovací komise zjistila, že příčinou události byla špatně nastavená priorita výstražných hlášení, dále nevhodná zobrazení, která měli operátoři k dispozici, a nedostatečné vyškolení pracovníků pro podobné zátěžové situace. Pro ilustraci, v posledních jedenácti minutách před výbuchem museli dva operátoři čelit celkem 275 výstražným hlášením, tj. měli každé z 275 výstrah porozumět, potvrdit ji a učinit náležitá opatření.

Ponaučení z uvedených havárií („*lessons learned*“)

V moderních řídicích systémech lze snadno měnit nastavení existujících výstražných hlášení i konfigurovat nová. Z hlediska konzistence systému výstražných hlášení je ovšem nezbytné jednak stanovit pravidla, podle kterých se provádějí změny v nastavení výstrah, a jednak zajistit jejich dodržování. K osvědčeným pravidlům patří např. zákaz zavést trvalou změnu bez schválení vedoucím operátorem a technologem, požadavek zrušit dočasné změny před nástupem nové směny, dále uchovávání záznamů o všech změnách v databázi s možností zpětného přezkoumání apod.

Jen dobré prvotní nastavení výstražných hlášení a dodržování pravidel při jejich změnách však nestačí. Vedle výměn jednotlivých částí zařízení není neměnný ani samotný technologický proces. Mění se pracovní režimy, složení vstupních surovin apod. Systém výstrah je tedy třeba s ohledem na tyto změny udržovat funkční a aktuální, a to nástroji dohromady tvořícími systém správy výstražných hlášení.

Při práci vykonávané uvedeným způsobem nemuselo dojít k vážné nehodě v rafinerii v Milford Havenu, jejíž příčinou byla přemíra výstražných hlášení, která nebyla účelně zkonfigurovaná tak, aby vedla obsluhu zařízení ke správnému zvládnutí abnormální situace a k jejímu vyřešení. Uživatelská rozhraní sloužící operátorům k porozumění aktuální situaci byla naopak zahlcena nepřehlednou spoustou údajů s nejasnou prioritou a vzniklá stresová situace vedla k velmi závažné havárii.

U starších zařízení, která netrpí přemírou konfigurovatelných výstrah, je naopak třeba věnovat mimořádnou pozornost všem mimořádným situacím. Měly by být také pravidelně prováděny kontroly nebo audity bezpečnostních obvodů, aby bylo jisté, zda jsou aktivní. Takové kontroly mohou zejména ve společnostech, které se tomuto aspektu zatím nevěnovaly, přinést nečekaná zjištění. Audit ochran v nejmenované společnosti provozující spojité technologické procesy ukázal, že ze čtrnácti nainstalovaných fotoelektrických bezpečnostních senzorů byly všechny, do jednoho, nefunkční, a to v důsledku úpravy, kterou mohl provést jen odborník [2].

Je také nutné říci, že hlavní příčinou nehody v rafinerii Grangemouth nebyla chyba operátora, jak zněl oficiální závěr vyšetřování. Posouzeno s odstupem času jí spíše bylo závažné selhání při údržbě a kontrole zařízení a nedodržení standardních postupů. Postupným odebráním bezpečnostních prvků byla bezpečnost zařízení ponechána pouze na ostražitosti operátora bez upozornění výstražným hlášením. Operátorovo přehlédnutí bylo pouze otázkou času.

Závěr

Selhání lidské obsluhy a jeho někdy až nebetyčným důsledkům se v průmyslové praxi

nelze vyhnout. Proto je účelné vynaložit určitou dobu a prostředky za účelem předem odhalit a minimalizovat možné příčiny selhání člověka při obsluze dané provozní jednotky včetně jejího řídicího systému. Běžnými kvalitativními metodami analýzy vlivu lidského činitele na řízenou provozní jednotku či zařízení (i těmi, které jsou doporučeny v české legislativě) lze potenciální selhání lidského činitele zjistit jen velmi obtížně. Nijak přínosné by v této oblasti nebylo ani použití kvantitativních metod. Řešení zde nabízí zevrubná analýza rizik metodou HAZOP/Human HAZOP v těsné součinnosti s operátory a pracovníky údržby dané jednotky [10].

Poděkování:

Tento článek vznikl za podpory projektu MŠMT 1M06047 - CQR.

Literatura:

[1] WHITTINGHAM, R. B.: *The blame machine: Why human error causes accidents.* Oxford, Elsevier Butterworth-Heinemann, 2004.

[2] KLETZ, T.: *An Engineer's View of Human Error.* Butterworth-Heinemann, 1991.

[3] KUCHARSKÝ, M.: *Řízení abnormálních situací.* Automa, 2009, roč. 15, č. 4, s. 14–17.

[4] ERRINGTON, D. V. et al.: *Effective Alarm Management Practices.* ASM Consortium Guidelines, ASM, May 2007.

[5] ANDOW, P. et al.: *Alarm Flood Analysis Report.* Honeywell HPS, ASM Consortium, 2007.

[6] NOCHUR, A. et al.: *Alarm Performance Metrics.* In: IFAC Workshop on On-line Fault Detection and Supervision in the Chemical Process Industries (CHEMFAS-4), 2001.

[7] EEMUA: *Alarm Systems, A Guide to Design, Management, and Procurement.* EEMUA Publication, No. 191, London, 1999.

[8] ANDOW, P.: *Alarm Management and Safety Related Issues.* Honeywell Hi-Spec Solutions, Honeywell International Inc., ASM Consortium, 2002.

[9] HOŠŤÁLKOVÁ, E. – STLUKA, P.: *Racionalizace alarmů pro zvýšení efektivity a bezpečnosti chemických provozů.* In: Sborník Aprochem 2009, Milovy, ČSVTS, 2009.

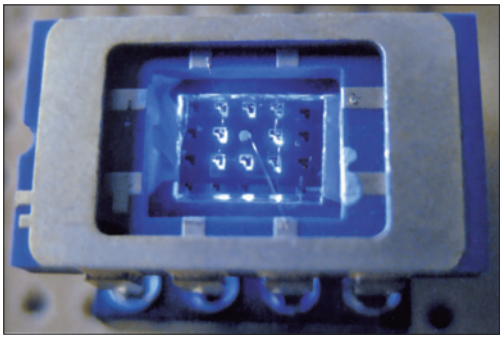
[10] KOTEK, L.: *Použití metody Human HAZOP při redukci chyb operátorů.* Automa, 2009, roč. 15, č. 11, s. 58–59.

Ing. Luboš Kotek, Ph.D.,
Fakulta strojního inženýrství VUT v Brně
(kotek.l@fme.vutbr.cz),
Ing. Eva Hošťálková,
Honeywell Prague Laboratory,
Honeywell spol. s r. o.
(eva.hostalkova@honeywell.com)

Článek vznikl na základě příspěvků Kotek, L. – Babinec, F: Analýza vlivu lidského činitele na bezpečný provoz rozsáhlých technologií a Hošťálková, E. – Stluka, P.: Racionalizace alarmů pro zvýšení efektivity a bezpečnosti chemických provozů přednesených na konferenci Aprochem 2009, Milovy, duben 2009.

Nový senzor malých koncentrací ozonu na obzoru

Slzící oči, podrážděné sliznice, bolesti hlavy, dráždivý kašel – příliš velká koncentrace ozonu v dýchaném vzduchu ovlivňuje zdraví lidí. Silně oxidující plyn se vyskytuje v ovzduší především v létě jako součást tzv. letního smogu. Ozon emitují také některé moderní kancelářské přístroje, jako laserové tiskárny a kopírky. Evropská komise chce do roku 2010 výrazně snížit povolené koncentrace tohoto zdraví škodlivého plynu v ovzduší – ze současných 120 na 60 ppb (*parts per billion* = $= 1 \cdot 10^{-9}$). Ke sledování malých koncentrací ozonu v oblasti přípustných mezních hodnot budou třeba nová výkonná měřicí zařízení, jakým je např. miniaturní senzor koncentrace ozonu nedávno vyvinutý a vyzkoušený odborníky z Fraunhoferova ústavu pro aplikovanou fyziku tuhých těles IAF (*Institut für Angewandte Festkörperphysik*) ve Freiburgu.



Obr. 1. Nový senzor koncentrace ozonu (foto: Fraunhofer IAF)

Velmi citlivý senzor s rozměry jen 0,25 × × 0,25 mm (*obr. 1*) se pohodlně vejde do každého mobilního telefonu a může měřit koncentraci ozonu s prahovou citlivostí až 40 ppb. Zvláštností nového senzoru je, že pracuje bez nákladné optiky. Ke stanovení koncentrace ozonu používá citlivou vrstvu oxidu inditého (In_2O_3), nanesenou v nepatrné tloušťce jen 15 nm na zadní straně světelné diody (LED) s fialovým světlem. Elektrický odpor této nanovrstvy se mění se stupněm oxidace, úměrně podle koncentrace ozonu v okolním vzduchu. Při zapnutí LED se senzor regeneruje studeným fotochemickým redukčním procesem. To je významný pokrok v porovnání s dosud běžně používanými přístroji pro měření koncentrace ozonu, které se před novým měřením regenerují zahřátím citlivého prvku na teplotu asi 300 °C. Spotřebovávají tudíž mnoho energie a svou velikostí se blíží rozměrům malé chladničky.

U senzorů z Fraunhoferova ústavu IAF se naproti tomu LED jen krátce rozsvítí, neboť elektrický odpor senzoru během asi dvou minut opět klesne na výchozí hodnotu a senzor je připraven k dalšímu měření. Určitým problémem bylo, že působením záření emitovaného světelnou diodou v ultrafialové části spektra vzniká ze vzdušného kyslíku ozon, a mohlo by tudíž dojít ke zkreslení výsledků měření. Proto muselo být frekvenční spektrum záření emitovaného diodou velmi přesně přizpůsobeno fyzikálnímu procesu probíhajícímu ve vrstvě In_2O_3. Princip senzoru, který pracovníci IAF použili, je již 25 let starý, ale až dosud se ho nepodařilo výrobně realizovat. Úspěchu bylo dosaženo teprve nyní, a to díky týmové spolupráci odborníků Technické univerzity v Ilmenau pracujících v oblasti citlivých nanovrstev a expertů z IAF s velkými zkušenostmi s vývojem světelných diod.

Nový senzor koncentrace ozonu při zkouškách prokázal, že použitá konstrukce je jak velmi citlivá na změny koncentrace ozonu, tak mimořádně odolná proti rušivým vlivům. Odborníci z IAF v současné době dále pracují na standardizaci výrobní technologie a na její modifikaci na podmínky sériové výroby. Jakmile se podaří vytvořit metodu nanášení nanovrstvy na zadní stranu světelné diody použitelnou při sériové výrobě, bude k dispozici levný produkt k hromadnému použití. Z jedné křemíkové podložky bude možné vyrobit až několik tisíc senzorů.

[BANZHAF, D.: *Handy gibt Ozónalarm.* Fraunhofer Magazin, 2008, č. 2, s. 18–19.]

Kab.