ACTEMIUM

SAFETY LIFECYCLE FOR THE PROCESS INDUSTRY

História bezpečnosti v priemysle

Bratislava 05/2023

ACTEMIUM

„Úspech je schopnosť kráčať od jedného nezdaru k druhému a nestratiť nadšenie.“

Winston Churchill

Vystihuje najväčšiu prednosť počítačov, ktoré sú nekonečne vytrvalé, môžu zlyhať stotisíc krát bez stopy sklamania, ľudia toho nie sú schopní.

Ing. Martin Gálik

vedúci obchodného oddelenia

TÜV Functional Safety Engineer SIS,
TÜV FSENG 2082/09

Čo je bezpečnosť?

Je veľa definícií bezpečnosti. Každý má svoj vlastný pocit bezpečnosti. Definícia používaná v odbornej literatúre (ISO/IEC Guide 51:1999, 3.1):

Freedom from unacceptable risk

Bezpečnosť je: „nezávislosť od neprijateľného rizika“, kde riziko je kombinácia frekvencie výskytu poruchy a následkov/závažnosti tejto poruchy s vplyvom na stratu na životoch, na životné prostredie a na ekonomickú stratu (cena poškodenia technológie, či strata produkcie výroby).

Čo je bezpečnosť?

Functional safety – je súčasťou celkovej bezpečnosti zastrešujúc stroje, zariadenia, aparáty, kontrolné systémy, ktoré závisia na správnej funkcii E/E/PE bezpečnostného systému a ďalších opatrení na zníženie rizík. [STN EN 61508]

Safety – produkty a služby, ktoré udržujú spotrebiteľa mimo nebezpečenstva.

Security – služby spojené osobou/človekom

Kým začneme

Tímová práca a terminológia

Oblasť priemyselnej bezpečnosti od analýzy rizík, cez zhodnotenie/redukciu rizika až po validáciu životného cyklu prístrojových bezpečnostných systémov si vyžaduje tímové úsilie s pracovníkmi so znalosťami a zručnosťami z rôznych odborov (procesný inžinier, chemický, technológ, strojár, HSE, „functional safety“ inžinier, požiarny technik, atď.).

Čo je bezpečnostný systém?

Bezpečnostný systém je prevádzkovo bezpečný ak náhodné chyby, chyby so spoločnou príčinou alebo systematické chyby nevedú k zlyhaniu bezpečnostného systému a nemajú vplyv:

- na zranenie a smrť osôb
- na zásah do životného prostredia
- na ekonomické straty na zariadení a produkcie

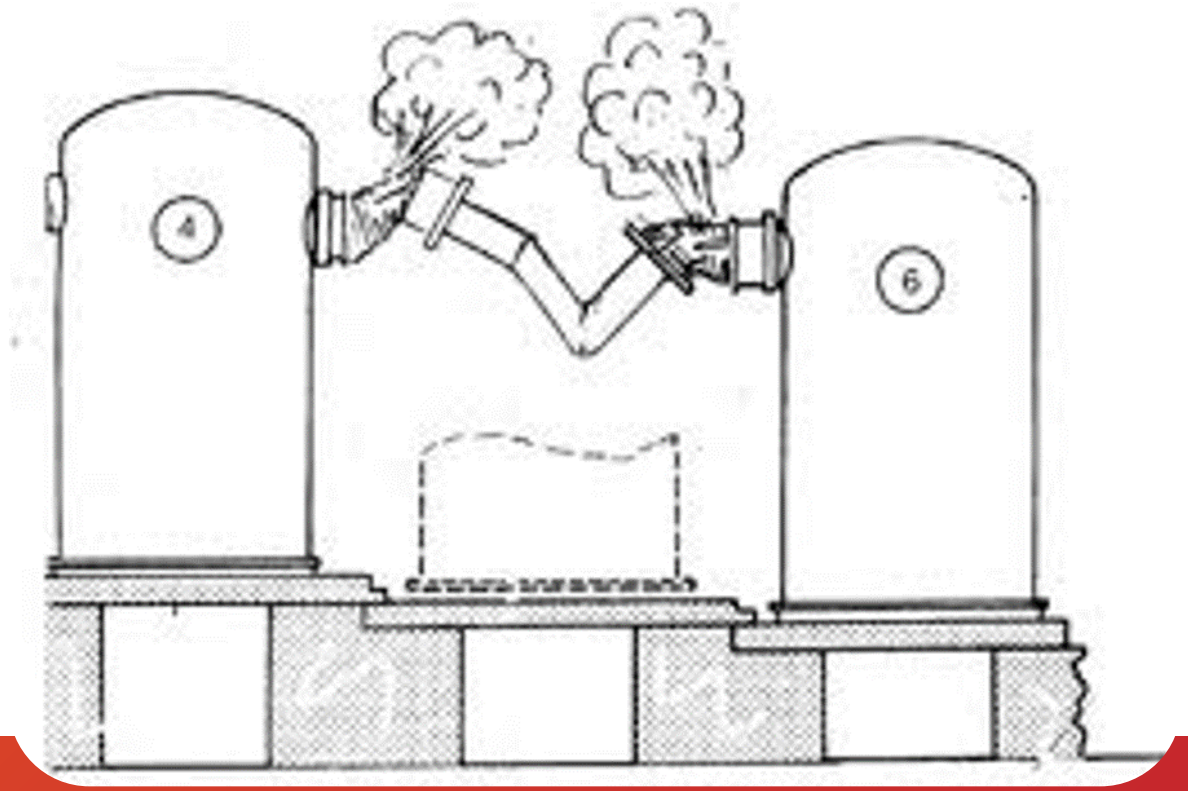
STN EN 61508:2010 – Bezpečnostný systém je nezávislý elektrický/elektronický/elektronicky programovateľný systém, ktorý privedie proces do bezpečného stavu, ak proces je proces mimo kontroly. Bezpečnostný systém musí byť nezávislý od všetkých rizík, preto riadiaci systém a bezpečnostný systém musia byť oddelené.

Zákon č. 128/2015 - Bezpečnostný riadiaci systém obsahuje potrebné opatrenia najmä v oblasti organizačnej štruktúry podniku vrátane potrebných zamestnancov, identifikácie a hodnotenia závažných nebezpečenstiev, riadenia prevádzky, riadenia zmien, havarijného plánovania, kontroly plnenia cieľov a princípov programu, ako aj na systematické hodnotenie aktuálnosti a účinnosti programu i bezpečnostného riadiaceho systému vrátane vykonávania interného auditu

ACTEMIUM

Flixborough, UK 1974 - z kamprolaktánovej produkčnej jednotky sa uvoľnil cyclohexán v neohraničenom, parovo-výbušnom mraku, 28 mŕtvych

História, známe nehody



Seveso, Taliansko, 1976 - obsah reaktora s 2,4,5-trichloropenalu (TCP) spustil exotermickú reťazovú reakciu, ktorej výsledkom bol vyzdvihnutý roztrhnutý disk, 4000 zranených

ACTEMIUM

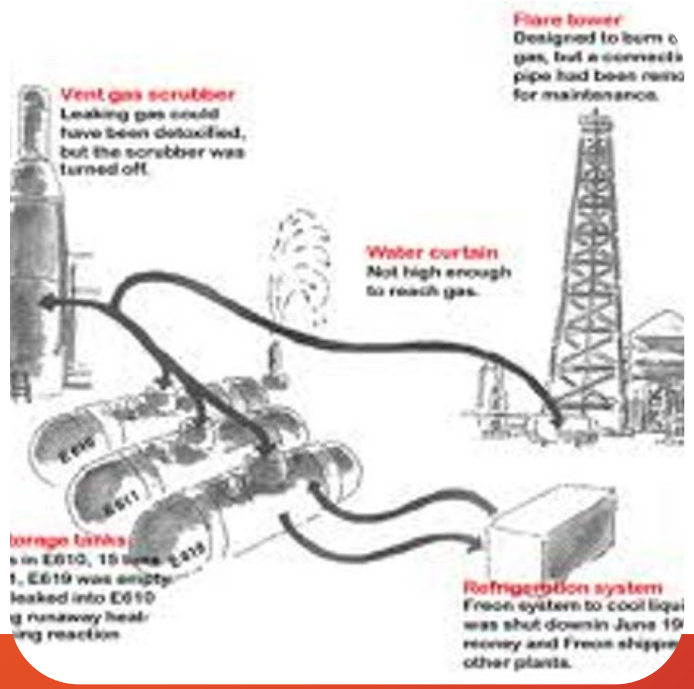
História, známe nehody

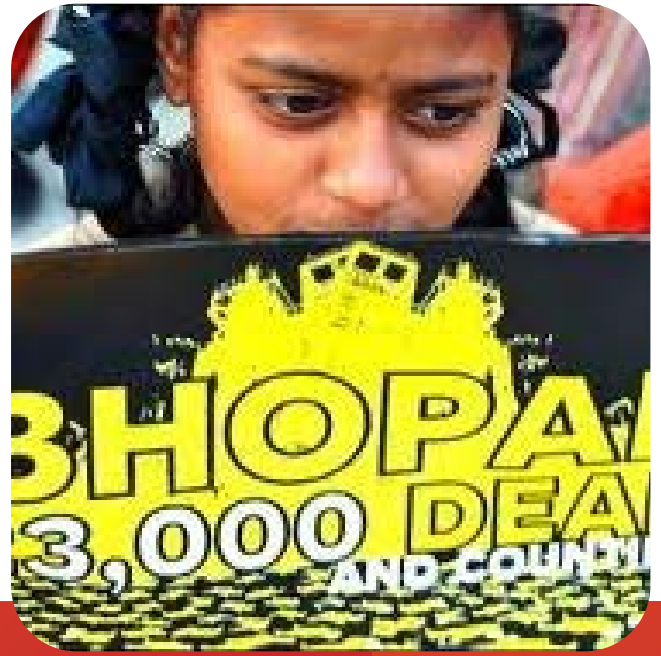
Šaľa, Slovensko, 1982 – pri eliminácii netesnosti na prírube pomocou furmanitu prišlo k úniku syntézneho plynu min. 96 % vodíka a následnej explózii. Zahynulo 6 osôb.

ACTEMIUM

Bhopal, India, 1984 - objavil sa únik kyanidu počas vstrekovania vody do metyl-isocyanatového zásobníka, 2500 smrteľných zranení a ďalších 170,000 zranení

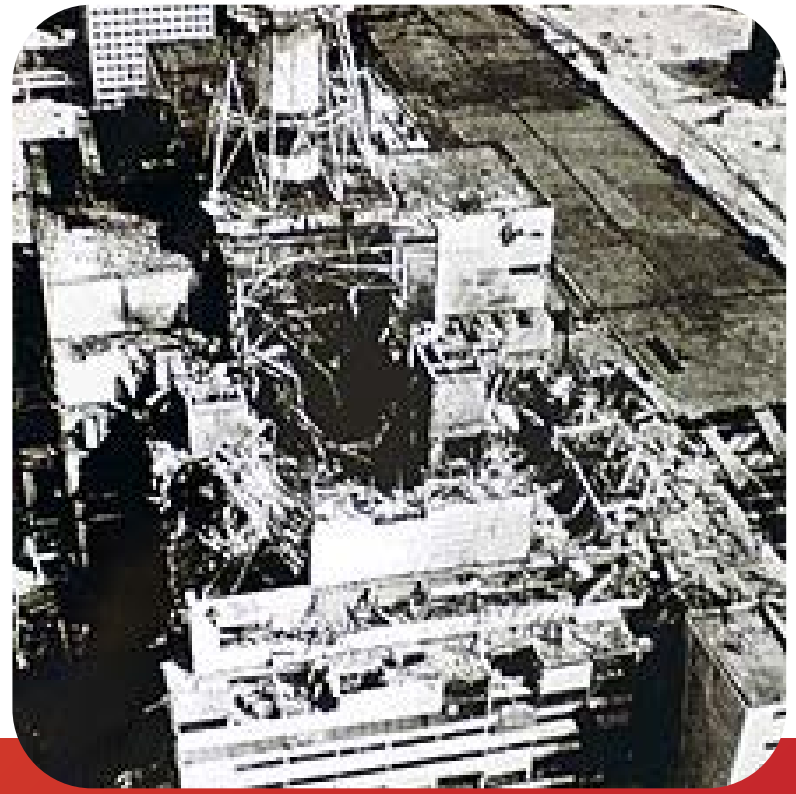
História, známe nehody





Černobyľ, Ukrajina, 1986 – v priebehu experimentu a testu nového bezpečnostného systému vtedy došlo k prehriatiu a následne k explózii reaktora RMBK-1000, presídlenie 200 000 ľudí, priame úmrtia 31, odhady sa pohybujú od stovky po tisíc

História, známe nehody



Piper Alpha, North Sea, 1988 – výbuch a následný požiar ropy a plynu, 167 mŕtvych, 61 prežilo

História, známe nehody

ACTEMIUM

Toulouse, Francúzsko, 2001 – výbuch hnojiva, ekvivalent 20-40 ton TNT, 31 mŕtvych, 2442 zranených

História, známe nehody

ACTEMIUM

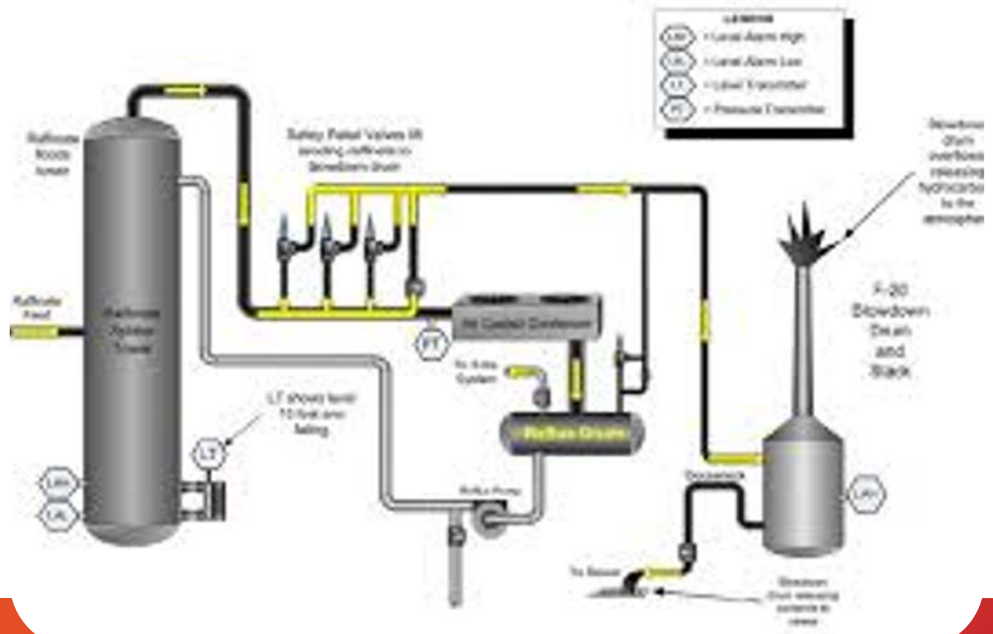
História, známe nehody

Geleen, Holandsko, 2003 – únik plynu v priemyselnej zóne, 24 mŕtvych, 132 zranených

ACTEMIUM

Texas City, USA, 2005 – pravdepodobná chyba štiepnej destilačnej kolóny, 15 mŕtvych, 170 zranených

História, známe nehody



ACTEMIUM

História, známe nehody

Jilin City, Čína, 2005, vysoká hladina benzénu a nitrobenzénu sa po explózii vyliala do rieky, 6 mŕtvych, 80 km znečistená rieka

ACTEMIUM

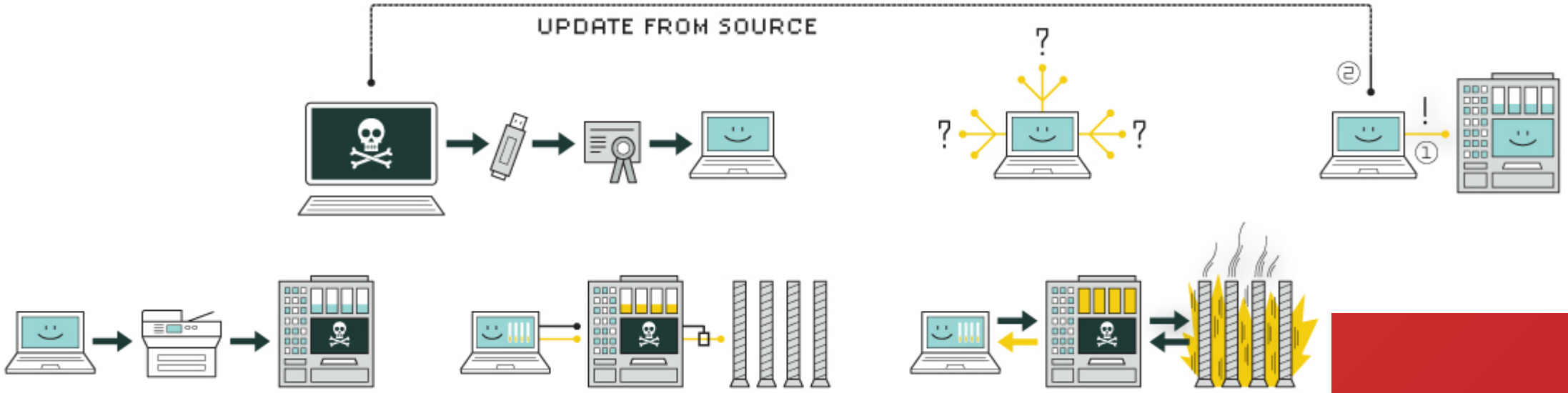
História, známe nehody

Deepwater Horizon, Mexický záliv, 2010 – explózia, z doteraz nezistených príčin, 11 mŕtvych, ropná škvrna 10 000 km^2

ACTEMIUM

História, známe nehody

STUXNET - je počítačový červ, údajne vyvinutý a spustený Spojenými štátmi a Izraelom, ktorý sa špecificky zameriava na programovateľné logické riadiace jednotky (PLC). Je považovaný za prvú kybernetickú zbraň použitú vo svete kvôli schopnosti spôsobiť fyzické zničenie a je zároveň aj prvým známym škodlivým softvérom určeným na infikovanie priemyselných riadiacich systémov (ICS).



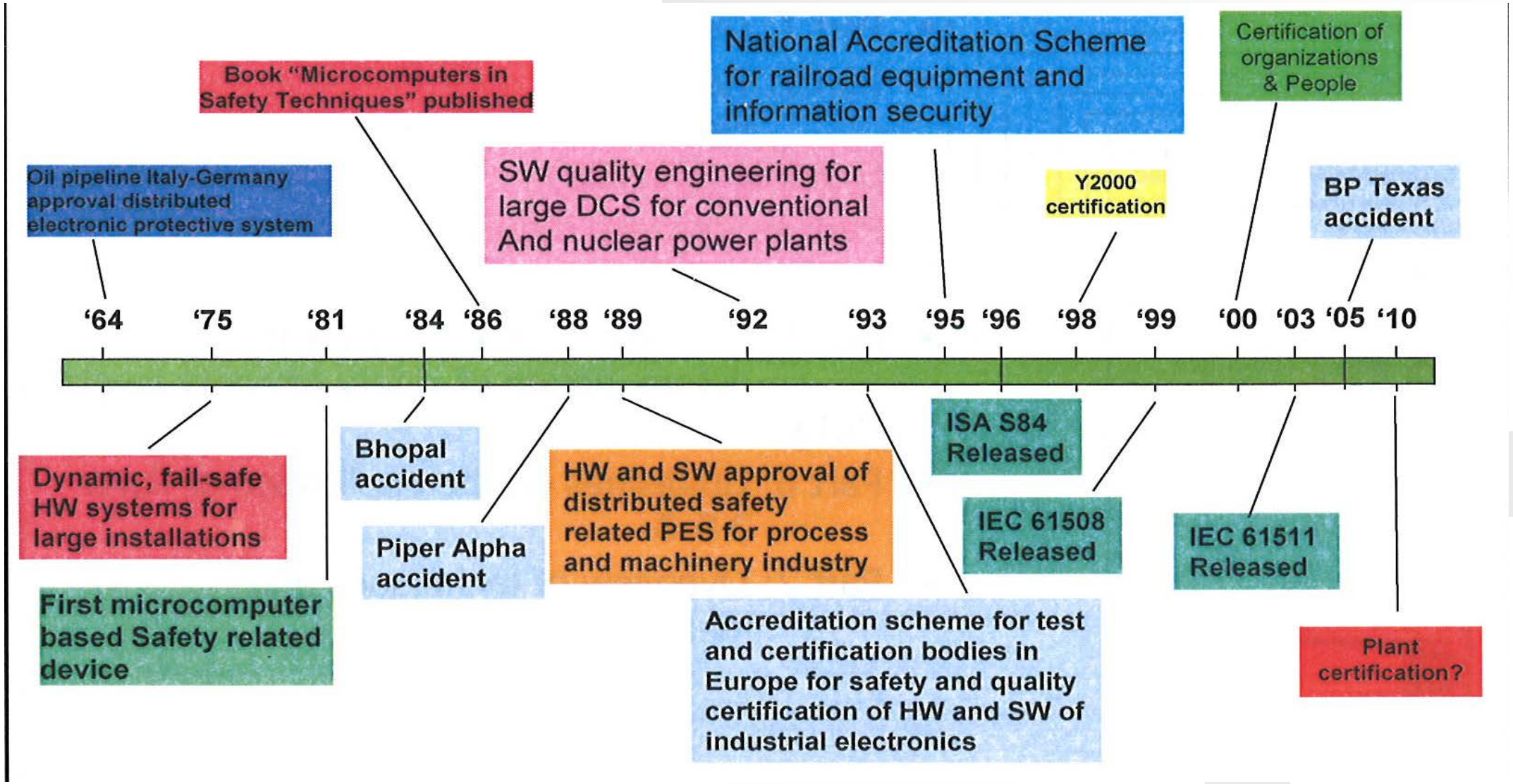
HISTÓRIA

Kvôli týmto nehodám vybudovali priemyselne najvyspelejšie štáty Európy systém nariadení pre nebezpečné prevádzky. Nemecko presadzovalo "The Hazardous Incident Ordinance (1980)" a Európske spoločenstvo vytvorilo "The Major Accident Hazards Directive (1982). Okolo roku 1980 sa začali používať generálne odporúčania pre bezpečnosť, ktoré sa volali AK-triedy, na základe nemeckej normy DIN19250 (Evolution of Basic Safety Systems). DIN V 19251 (Safety requirement for instrument and control system used in Safety application).

HISTÓRIA

V roku 1988 zahájila spoločnosť Instrument Society of America (ISA) osem rokov trvajúcu cestu k vypracovaniu normy na tvorbu prístrojových systémov pre použitie v procesnom priemysle, určených na zaistenie bezpečnosti (Safety Instrumented Systems – SIS) ANSI/ISA 84.01-1996. V roku 1997 bola táto norma s názvom „Aplikácia prístrojových bezpečnostných systémov v procesnom priemysle“, po doporučení spoločnosťou ISA, prijatá Úradom pre normalizáciu v USA (American National Standards Institute – ANSI) ako štátna norma. Štátne úrady USA, zodpovedajúce za politiku v oblasti ochrany životného prostredia Environmental Protection Agency (EPA), bezpečnosti a ochrany zdravia pri práci (Occuppational Safety and Health Administration (OSHA) ju napokon uznali ako uznávanú a prijatú priemyselnú prax. Každý bezpečnostný prístrojový systém projektovaný v USA po marci 1997 musí vyhovovať požiadavkám tejto normy.

HISTÓRIA


Book "Microcomputers in Safety Techniques" published
National Accreditation Scheme for railroad equipment and information security
Certification of organizations & People
Oil pipeline Italy-Germany approval distributed electronic protective system
SW quality engineering for large DCS for conventional And nuclear power plants
Y2000 certification
BP Texas accident
'64 '75 '81 '84 '86 '88 '89 '92 '93 '95 '96 '98 '99 '00 '03 '05 '10
Dynamic, fail-safe HW systems for large installations
Bhopal accident
ISA S84 Released
HW and SW approval of distributed safety related PES for process and machinery industry
IEC 61508 Released
IEC 61511 Released
First microcomputer based Safety related device
Piper Alpha accident
Accreditation scheme for test and certification bodies in Europe for safety and quality certification of HW and SW of industrial electronics
Plant certification?

Z identifikácie nebezpečenstva a z analýzy rizík cez špecifikáciu k návrhu bezpečnostného systému

Špecifikácia bezpečnostných požiadaviek bezpečnostného systému musí byť založená na analýze nebezpečenstiev a rizík, ktorá je prevažne založená na základe:

- identifikácie nebezpečenstiev
- analýzy nebezpečenstiev (následky)
- analýzy rizík
- riadení rizík
- prijateľného rizika
- znižovania rizík prostredníctvom existujúcich ochranných vrstiev
- znižovania rizík prostredníctvom dodatočných bezpečnostných vrstiev

TECHNIKY ZNIŽOVANIA A REDUKCIE RIZIKA

Existujú mnohé techniky pre podporu identifikácie nebezpečenstva a rizika. Neexistuje však záväzná technika, pomocou ktorej sa môže urobiť všetko, riziková štúdia používa rôzne metódy a techniky. Známe metódy zisťovania nebezpečenstva a rizika:

- Checklists
- What if study
- Failure mode and effect analysis (FMEA)
- Hazard and operability analysis (HAZOP)
- Dynamic flowgraph methodology (DFM)

Techniky pre analýzu rizík:

- Event tree analysis (ETA)
- Fault tree analysis (FTA)
- Cause consequence analysis

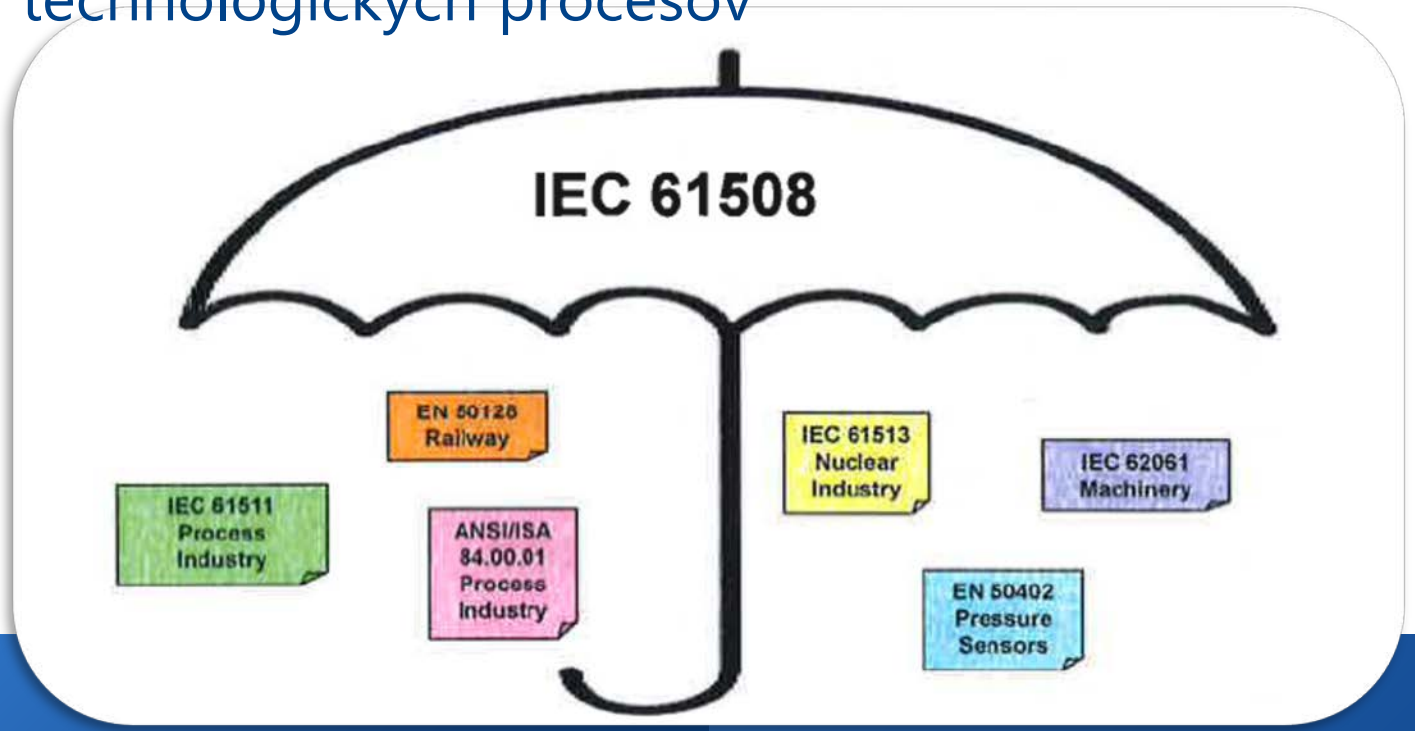
Techniky na zníženie rizika:

- Event tree analysis (ETA)
- Layer of protection analysis (LOPA, a variation on ETA)

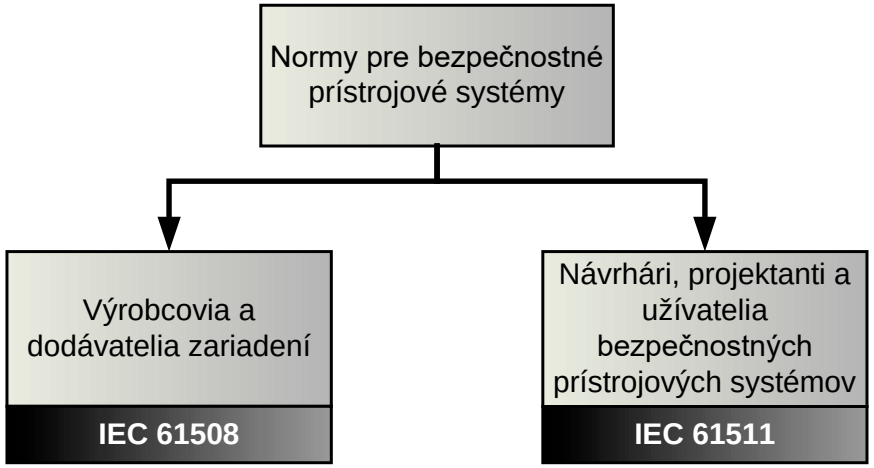
LEGISLATÍVA

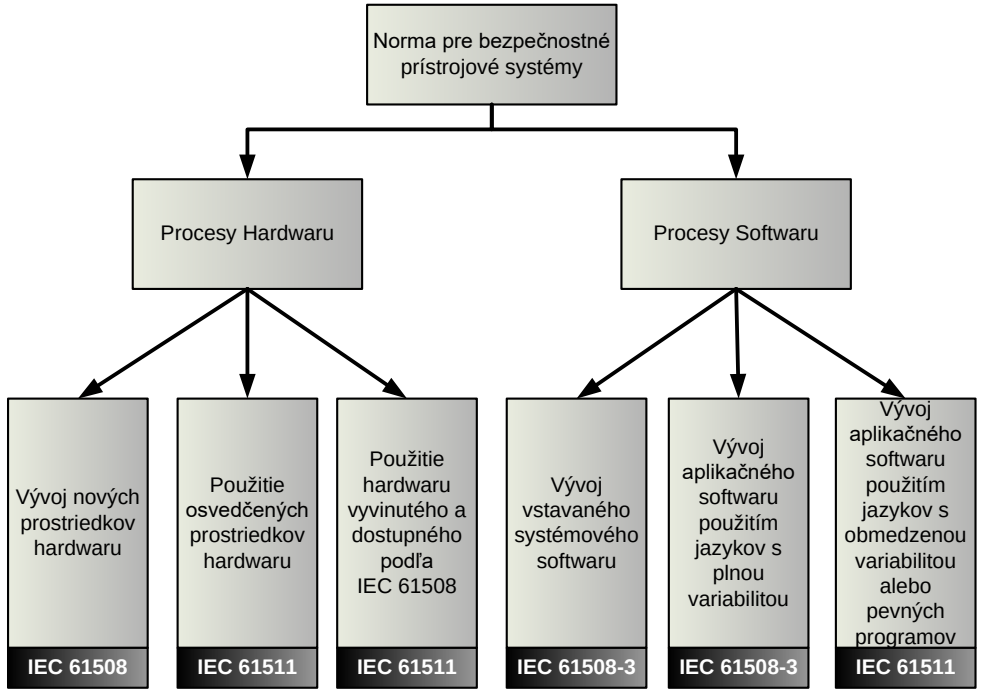
IEC 61508 – Funkčná bezpečnosť elektrických/elektronických/programovateľných elektronických bezpečnostných systémov

IEC 61511 = ANSI/ISA 84.00.01 - Funkčná bezpečnosť. Bezpečnostné riadiace systémy spojitých technologických procesov

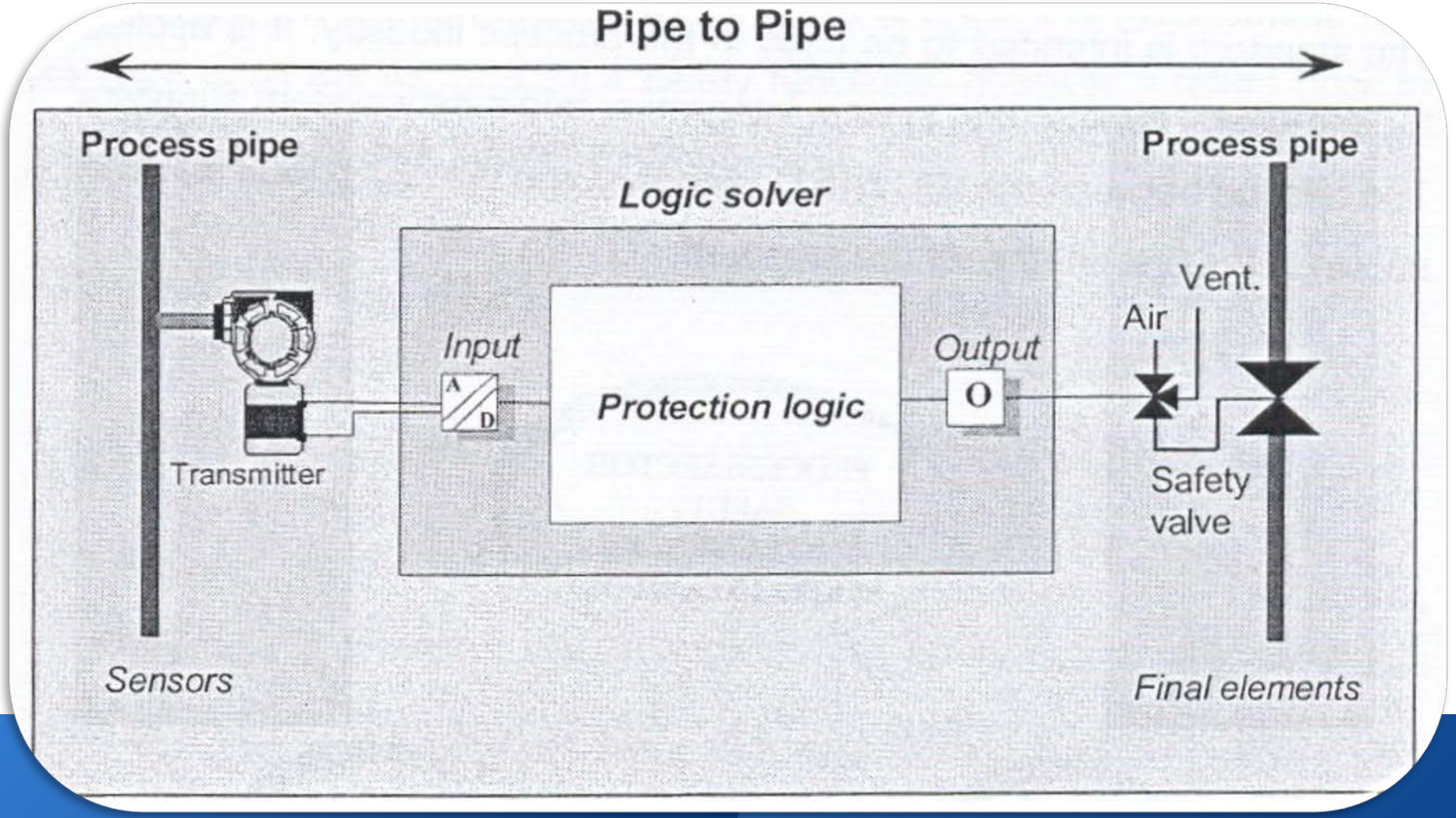


VZŤAH MEDZI STN EN 61508 – 61511

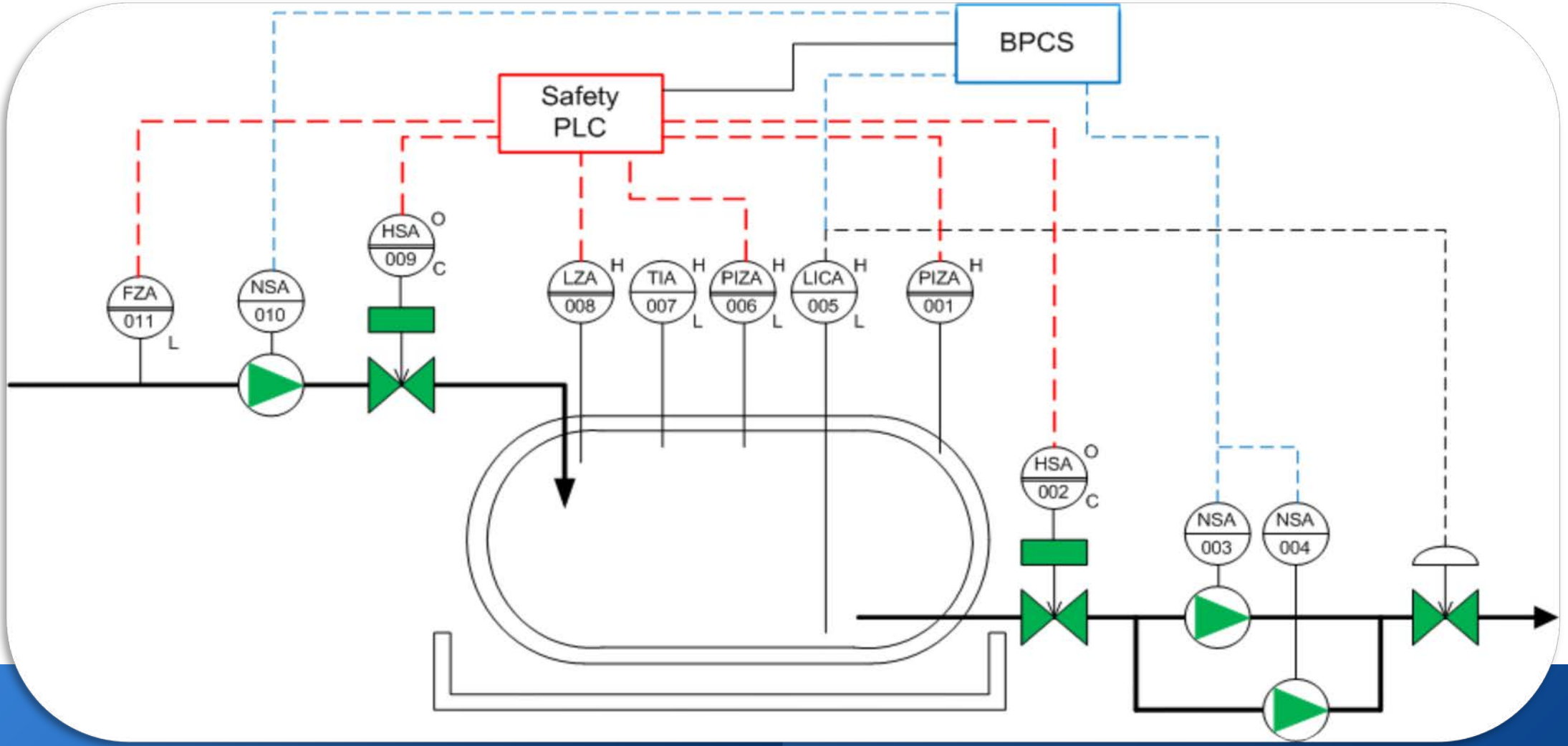




BEZPEČNOSTNÝ OBVOD SIF



ČO JE PRIEMYSELNÁ/FUNKČNÁ BEZPEČNOSŤ?

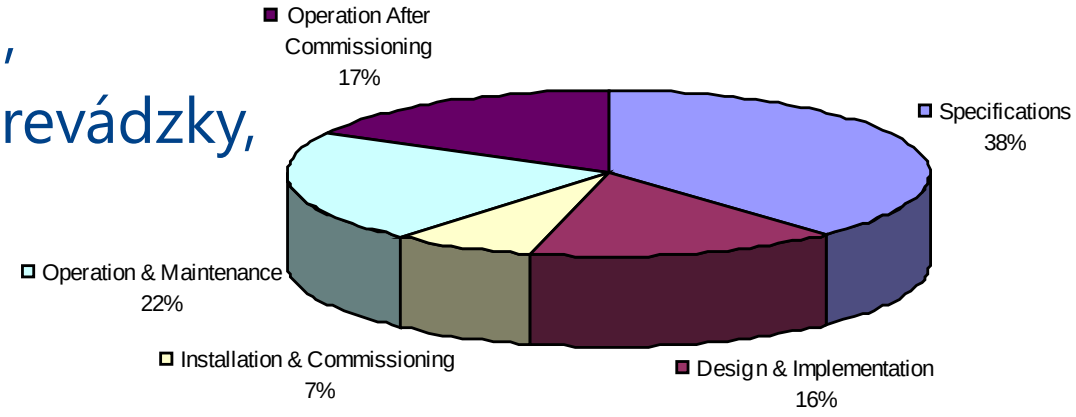


Príklady využitia zásad dobrej inžinierskej praxe v oblasti priemyselnej (funkčnej) bezpečnosti

NÁVRH SIS – ŠTATISTIKA CHÝB

Počas celého životného cyklu je nutné odstraňovať prvotné príčiny možných zlyhaní prístrojových systémov. Bola urobená analýza príčin závažných priemyselných havárií. Táto analýza vychádzala z piatich definovaných fáz životného cyklu SIS:

- špecifikácia,
- vyprojektovanie a implementácia,
- inštalácia a uvedenie do trvalej prevádzky,
- prevádzkovanie a údržba,
- zmeny v technickom prevedení po uvedení do trvalej prevádzky.



„NEDOBRÉ“ INŽINIERSKE PRAKTIKY

Pri tvorbe riešení SIS je nutné vyvarovať sa „nedobrých“ inžinierskych praktík, ako napríklad:

Pokiaľ nie je niečo výslovne prikázané alebo zakázané v normách, netreba sa s tým vôbec zapodievať!

Projektovanie SIS takým spôsobom, že sú síce rešpektované bezpečnostné požiadavky, avšak nedbá sa na požiadavku ekonomickosti riešenia!

Zameranie sa výlučne na dosiahnutie predpísanej úrovne SIL, avšak nie na prevenciu zbytočných výpadkov prevádzky chráneného technologického zariadenia!

V žiadnych technických normách sa podrobne nehovorí o „availability“ (dostupnosti, užitočnosti, spoľahlivosti) daného riešenia SIS. Avšak je veľmi dôležitá pre koncového užívateľa. „Availability“ je často meraná v percentách. Je to skôr horšia cesta ako ju špecifikovať, pretože sa nedá špecifikovať očakávané číslo porúch v časovom intervale. Keď zoberieme prevádzku, kde je výpadok raz za rok a potrebuje 8 hodín na nábeh a porovnáme to s prevádzkou, kde je výpadok raz za mesiac a nábeh trvá 1 hodinu, obidve majú „availability“ okolo 99,9 %.

„DOBRÉ“ INŽINIERSKE PRAKTIKY

Spojenie „Safety-Availability“ by malo byť súčasťou každého návrhu SIS. Pre všeobecné názorné vysvetlenie môžeme predstaviť dva príklady:

- máme super drahé auto so všetkými bezpečnostnými funkciami ako sú ABS, airbagy, špeciálne bezpečnostné pásy, výstuže karosérie, keď však nenaštartuje motor
- opačný príklad je, že máme staré, ošarpané auto, ktoré je funkčné a ide mu motor, avšak nefungujú mu brzdy

Bezpečnú prevádzku výrobného procesu nie je možné dosiahnuť izolovane od ekonomických dopadov. Stratégia zníženia rizika prevádzky musí tiež vziať do úvahy **obchodné potreby vlastníka/prevádzkovateľa procesu**. Všetci pracovníci (od manažmentu cez operátora až po údržbu) prevádzkovanej procesnej jednotky musia mať za cieľ nie len výrobnú cenu, kvalitu výrobkov, ale **hlavne pomer ceny a výkonu**. Vyvažovanie bezpečnostných a výrobných cieľov je veľmi náročné, hlavne keď návrh, implementácia a manažment bezpečnostného prístrojového systému nie je schopné adekvátne reagovať na prevádzkové potreby výrobného procesu.

SUMMERS, Angela E, Ph.D., P.E., President, Avoid Bad Engineering Practices in Safety Instrumented System Design, SIS-Tech Solution, LLC, Published INTECH, November 1999

„DOBRÉ“ INŽINIERSKE PRAKTIKY

Vhodnosť vybraných komponentov musí byť preukázaná dokumentáciou výrobcu (HW, SW časť) – *certifikát nezávislej organizácie (TUV, EXIDA, ...)*

- **Návrh rozhrania SIS**
  - Minimalizovať zásah operátora
    - Premostenie (MOS, OOS, SOS) SIF funkcie (HW/SW) musí byť chránené proti neoprávnenému použitiu (heslo, kľúč, ...)
  - Všetky dôležité informácie o stave SIS musí mať operátor k dispozícii
- **Technické požiadavky na údržbu**
    - dodržiavať výrobcom predpísaný spôsob testovania za účelom potvrdenia funkčnosti zariadenia pre deklarovaný SIL

ACTEMIUM

„DOBRÉ“ INŽINIERSKE PRAKTIKY

Application Area	**Safety Instrumented Systems**
ID-No.	**#2082/ 09**
Certificate Owner	**Martin Gálik** Slovak Republic
Course Provider	HIMA Paul Hildebrandt GmbH
Training Contents	Process Safety Risk / Layers of Protection International Safety Standards, Regulations, Enforcement Safety Integrity Level (SIL) Assignment Methodologies Safety Requirement Specifications (SRS) Development Safety Integrity Level (SIL) Verification Methodologies Management of Functional Safety SIS Design and Good Engineering Practices
Initial Issue Date	October 2009
Expiry Date	October 2029

ACTEMIUM

„DOBRÉ“ INŽINIERSKE PRAKTIKY

Certifikačné spoločnosti pre oblasť priemyselnej bezpečnosti

TÜV Rheinland – Functional Safety program

Functional Safety Technician

Functional Safety Engineer

Functional Safety Expert

TÜV SÜD – Functional Safety Certification program

“Functional Safety Engineer” corresponding to Level 1

“Functional Safety Professional” corresponding to Level 2

“Functional Safety Expert” corresponding to Level 3

ACTEMIUM

„DOBRÉ“ INŽINIERSKE PRAKTIKY

Range of Functional Safety Services for Machinery

- Moderation and support regarding risk evaluation according to EN ISO 14121-1
- Technical assistance in setting up and authoring safety concepts to reduce risk potentials
- Validation of single safety functions according to EN ISO 13849-2 and EN 62061
- Safety-related assessment of safety systems according to EN ISO 13849-1 and EN 62062

ProCS s.r.o.

Location Kráľovská 824/8, 927 01 Šaľa, Slovakia

Has been audited for Functional Safety Management (FSM) compliance following IEC61508 and/or IEC61511 and has been verified as applying an FSM system consistent with a Systematic Safety Integrity of 3 (Systematic Capability = SC3).

IEC61511 lifecycle phases assessed:

- Phase 1: Hazard and Risk Assessment
  Limited to: SIS only. Participation and hosting, not chairing.
- Phase 2: Allocation of Safety Functions to Protection Layers
  Limited to: SIS only. Participation and hosting, not chairing.
- Phase 3: Safety Requirements Specification for the Safety Instrumented System
  Limited to: SIS only.
- Phase 4: Design and Engineering of the Safety Instrumented System
- Phase 5: Installation, Commissioning and Validation
  Limited to: Installation and Commissioning of SIS only.
- Phase 6: Operation and Maintenance
  Limited to: SIS Maintenance only.
- Phase 7: Modification
  Limited to: SIS only.

Spoločnosť ProCS, s.r.o. ako prvá inžinierska spoločnosť na Slovensku prešla auditom na Function Safety Management v zmysle EN 61511, ktorým dosiahla Systematic Capability declaration SC3 pre aplikácie v celom životnom cykle bezpečnostnej aplikácie.

ĎAKUJEME ZA POZORNOSŤ

ProCS, s.r.o.
Kráľovská ulica 8/824
927 01 Šaľa
Tel.: +421 31 7731111

info@actemium.sk
www.actemium.sk
linkedin.com/company/actemium-slovakia