Imrich Dufinec

Základy riadenia bezpečnosti podniku

Bezpečnosť podniku

Dodávatelia

Zákazníci

Zamestnanci

Spoločnosť a verejnosť

Aktionári

Parciálne zložky bezpečnosti podniku

Sú dané bezpečnostnou politikou podniku

(ktorá vyjadruje):

1. **Čo má byť chránené**
2. **Prečo to má byť chránené**
3. **Ako to má byť chránené**
4. **Čo treba urobiť, ak dôjde k zlyhaniu**

Parciálne zložky bezpečnosti podniku

1 z 2

- Fyzická bezpečnosť podniku
- Ekonomická bezpečnosť podniku
- Environmentálna bezpečnosť podniku
- Bezpečnosť a ochrana zdravia pri práci
- Bezpečnosť infraštruktúry podniku
- Bezpečnosť produkcie podniku

Parciálne zložky bezpečnosti podniku

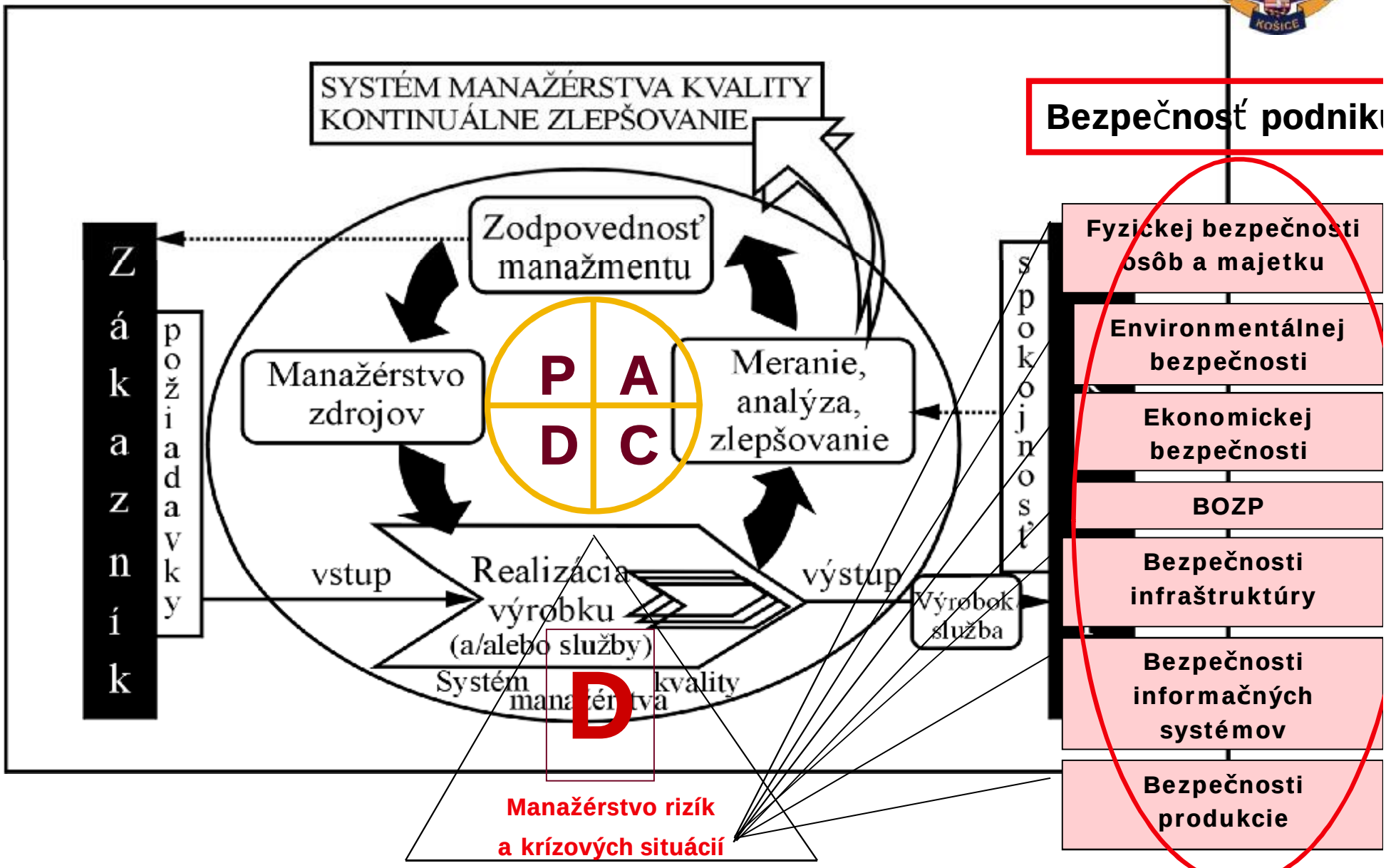
2 z 2

- Bezpečnosť osobných údajov podniku
- Bezpečnosť vnútorného poriadku podniku
- Bezpečnosť utajovaných skutočností podniku
- Bezpečnosť informačných systémov podniku

1. **Funguje samostatne, ako súčasť IT**
2. **Zahŕňa predchádzajúce tri zložky, ak sú aktuálne**
3. **Zahŕňa všetky zložky, ak sú aktuálne**

ISO 27001

Generický Manažérsky Systém



Modely bezpečnosti podniku

- Model ignorovanej bezpečnosti
- Model minimálnej technologickej bezpečnosti
- Model formálnej bezpečnosti
- Model odtrhnutej bezpečnosti
- Model utopenej bezpečnosti
- Model agilnej bezpečnosti
- Model outsorcovanej bezpečnosti
- Model rozsiahlej inštitucionálnej bezpečnosti

Model ignorovanej bezpečnosti

- **Bezpečnostná politika nie deklarovaná**
- **Bezpečnosť je ignorovaná**

- Podporované iba základné funkcie smerom jadru podnikania
- Za IT procesov zodpovedá majiteľ procesov, neformálne a podvedome ako CIO
- Totálna absencia bezpečnosti IT
- Ochrana aktív (hmotných i nehmotných) iba spontánne, bez aplikácie bezpečnostných nástrojov
- Prvé zmeny nastávajú, ak dôjde k incidentu

Modely bezpečnosti podniku

- Model ignorovanej bezpečnosti
- Model minimálnej technologickej bezpečnosti
- Model formálnej bezpečnosti
- Model odtrhnutej bezpečnosti
- Model utopenej bezpečnosti
- Model agilnej bezpečnosti
- Model outsorcovanej bezpečnosti
- Model rozsiahlej inštitucionálnej bezpečnosti

Model minimálnej technologickej bezpečnosti

- Minimálna bezpečnosť IT venovaná iba hlavnému procesu tvoriaceho pridanú hodnotu
- Bezpečnostná politika existuje podvedomé alebo formálne, ak to vyžadujú okolnosti
- Bezpečnosť je chápaná ako technologická súčasť procesu a málokedy prekročí tento rámec
- Riadením bezpečností nie je poverená žiadna osoba na plný úväzok, napriek širokej palete IT. Podnik je vystavený rizikám a incidentom.

Modely bezpečnosti podniku

- Model ignorovanej bezpečnosti
- Model minimálnej technologickej bezpečnosti
- Model formálnej bezpečnosti
- Model odtrhnutej bezpečnosti
- Model utopenej bezpečnosti
- Model agilnej bezpečnosti
- Model outsorcovanej bezpečnosti
- Model rozsiahlej inštitucionálnej bezpečnosti

Model formálnej bezpečnosti

- Vzniká na základoch modelu minimálnej bezpečnosti IT, alebo je s ním stotožnený ale s plnším vedomím potreby bezpečnosti
- Funkcia bezpečnosti je chápaná viac uvedomelo a inštitucionálne. Politika existuje, hoci je obmedzená
- Bezpečnosť je chápaná naďalej ako technologická súčasť procesu ale často prekračuje tento rámec
- Riadením bezpečností na danom úseku (CSO) je poverená osoba bez úväzku, ako kumulácia s CIO, napriek širokej palete IT. Podnik je stále vystavený rizikám a incidentom.

Modely bezpečnosti podniku

- Model ignorovanej bezpečnosti
- Model minimálnej technologickej bezpečnosti
- Model formálnej bezpečnosti
- Model odtrhnutej bezpečnosti
- Model utopenej bezpečnosti
- Model agilnej bezpečnosti
- Model outsorcovanej bezpečnosti
- Model rozsiahlej inštitucionálnej bezpečnosti

Model odtrhnutej bezpečnosti

- Formálne i vecné postavenie CSO inštitucionálne uznané ale je odtrhnuté od IT
- Odtrhnutie CSO od IT vyvoláva konflikt úrovne znalosti pri prudko sa rozvíjajúcej IT
- Konflikt znalosti spochybňuje bezpečnostnú politiku a opatrenia na zlepšovanie bezpečnosti
- Konflikt možno riešiť rozširovaním útvaru CSO o špecialistov (na výpočtovú techniku, na BOZP na fyzickú ochranu, na kvalitu, a pod.)
- Ďalšie zmierňovanie konfliktov sa uskutočňuje posilnením pozície CSO a samostatnou rozpočtovou kapitolou podniku

Modely bezpečnosti podniku

- Model ignorovanej bezpečnosti
- Model minimálnej technologickej bezpečnosti
- Model formálnej bezpečnosti
- Model odtrhnutej bezpečnosti
- Model utopenej bezpečnosti
- Model agilnej bezpečnosti
- Model outsorcovanej bezpečnosti
- Model rozsiahlej inštitucionálnej bezpečnosti

Model utopenej bezpečnosti

- Tiché skrytie CSO pod krídla jedného z najaktuálnejších CIO (napr. počítače a siete)
- Aktuálny CIO, ktorý po skúsenostiach ako manažér procesov a IT preberie zodpovednosť za rozvoj jej bezpečnosti (napr. počítače a siete – informačná bezpečnosť, alebo technický kontrolór a manažér kvality – bezpečnosti produkcie)
- Napriek konfliktu záujmov (porucha kontrolných mechanizmov) sa vylúči odtrhnutie ako väčšie zlo

Modely bezpečnosti podniku

- Model ignorovanej bezpečnosti
- Model minimálnej technologickej bezpečnosti
- Model formálnej bezpečnosti
- Model odtrhnutej bezpečnosti
- Model utopenej bezpečnosti
- Model agilnej bezpečnosti
- Model outsorcovanej bezpečnosti
- Model rozsiahlej inštitucionálnej bezpečnosti

Model agilnej bezpečnosti

- Vnútorná bezpečnosť procesov prostredníctvom prepracovaných postupov IT
- Manažéri procesov (CIO) tvoria Security Board, podriadený generálnemu riaditeľovi (CEO)
- Na čele Security Board stojí formálne jeden z nich ako CSO
- Do Security Board môžu byť menovaní ďalší podnikoví experti a externí odborníci
- Security Board plní funkciu legislatívnu, kontrolnú a riadiacu. Má všetky znaky a podobu IMS
- Bezpečnostná politika je súčasťou celkovej politiky

Modely bezpečnosti podniku

- Model ignorovanej bezpečnosti
- Model minimálnej technologickej bezpečnosti
- Model formálnej bezpečnosti
- Model odtrhnutej bezpečnosti
- Model utopenej bezpečnosti
- Model agilnej bezpečnosti
- Model outsorcovanej bezpečnosti
- Model rozsiahlej inštitucionálnej bezpečnosti

Model outsorcovanej bezpečnosti

- Model predpokladá nákup takých technológií, v ktorých je bezpečnosť IT inherentná.
- V podniku je menovaná funkcia koordinátora „bezpečného nákupu“, ktorý ako CSO je podriadený generálnemu riaditeľovi (CEO)
- Bezpečnostný manažér (CSO) je vo svojej pozícii podobne ako v modeli odtrhnutej bezpečnosti
- Zmiernenie odtrhnutia sa rieši internou spoluprácou s jednotlivými CIO a koordináciou externých expertov
- Jeden z prípadov outsorcovanej bezpečnosti je „nákup“ služieb externej SBS

Modely bezpečnosti podniku

- Model ignorovanej bezpečnosti
- Model minimálnej technologickej bezpečnosti
- Model formálnej bezpečnosti
- Model odtrhnutej bezpečnosti
- Model utopenej bezpečnosti
- Model agilnej bezpečnosti
- Model outsorcovanej bezpečnosti
- Model rozsiahlej inštitucionálnej bezpečnosti

Model rozsiahlej inštitucionálnej bezpečnosti

- Model rozvinutej formálnej bezpečnosti s rozvinutým bezpečnostným útvarom a CSO, alebo
- Model agilnej bezpečnosti so samostatnými relatívne dobre rozvinutými bezpečnosťami IT
- Bezpečnosť je plne formalizovaná
- Bezpečnostná politika je všeobecne záväzná a tvorí základ všetkých realizovaných IT
- Dobre zabezpečená osobná bezpečnosť je samozrejmosťou

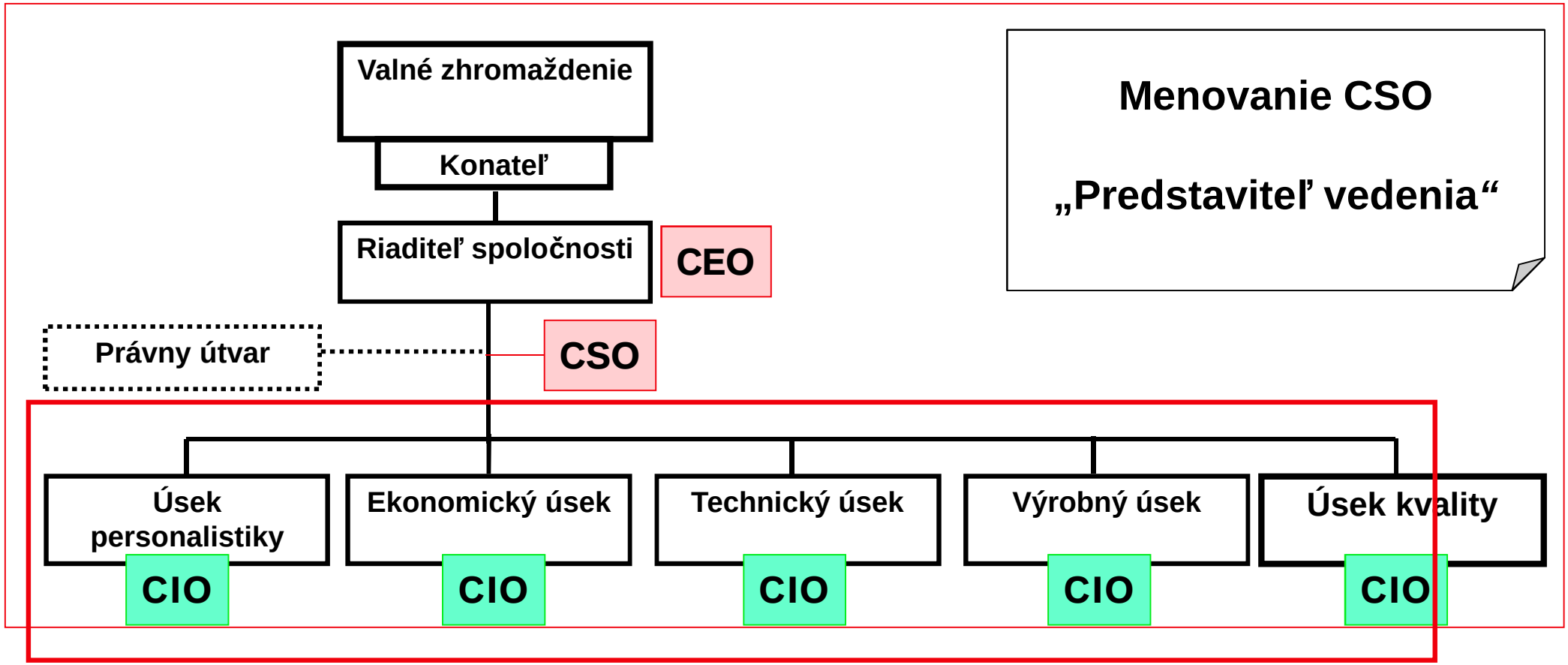
Predstaviteľ bezpečnosti podniku

- Manažment menuje samostatnú osobu funkciou predstaviteľa vedenia na plný úväzok (CSO), ktorý má hlavnú zodpovednosť a inštitucionálnu právomoc vo veciach bezpečnosti v celom podniku:

  - vypracovávať, zavádzať a udržiavať všetky procesy podniku s akcentom na BMS v rámci jednotlivých IT a celého podniku,
  - oboznamovať vrcholový manažment s výkonnosťou obmedzeného BMS a s akoukoľvek potrebou zlepšenia týchto procesov,
  - zvyšovať povedomie bezpečnosti zamestnancov svojho okruhu a jeho (vnútorných) zákazníkov v celej organizácii.

Predstaviteľ bezpečnosti podniku

- Manažment menuje samostatnú osobu funkciou, ako predstaviteľ vedenia na plný úväzok, ktorý má hlavnú zodpovednosť a inštitucionálnu právomoc vo veciach bezpečnosti v celom podniku:



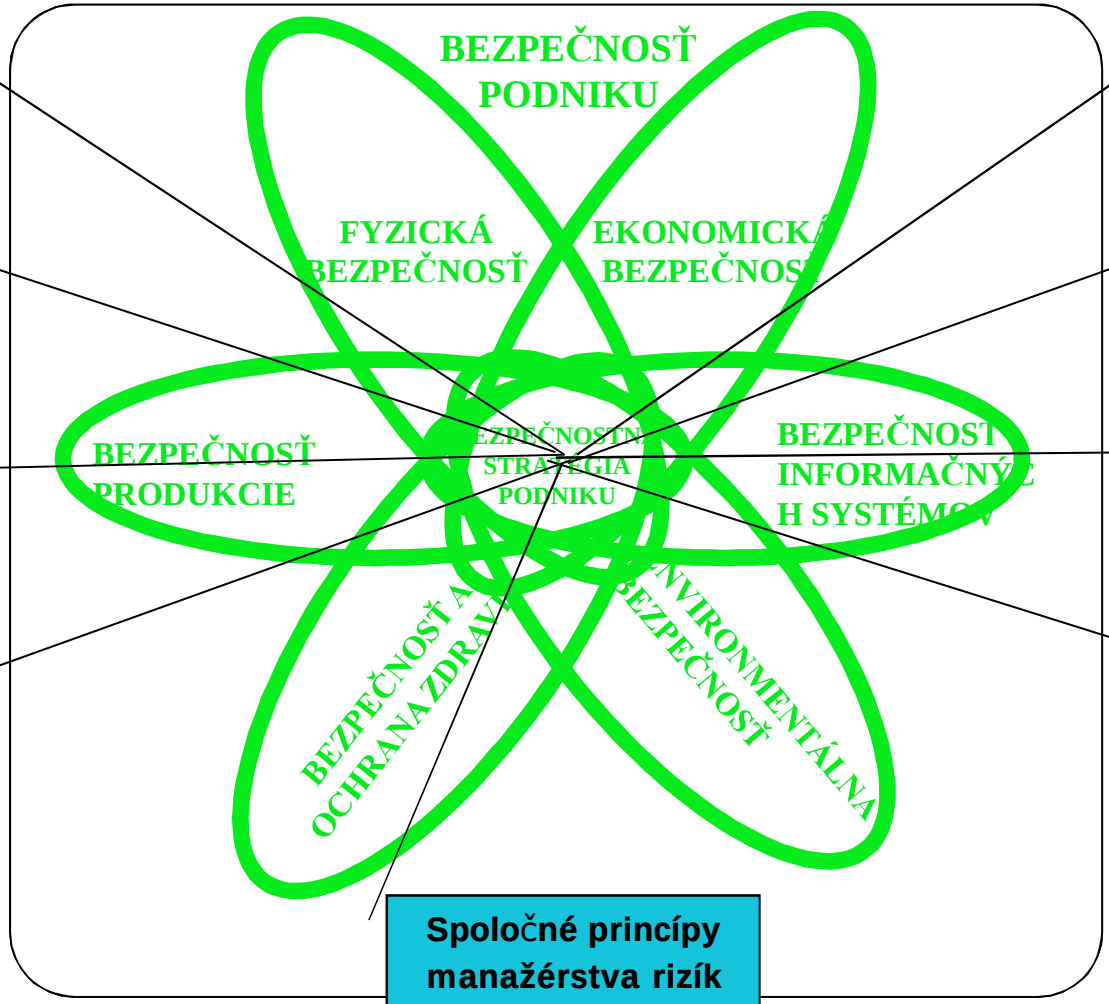
Oblasť integrácie

Spoločný systém riadenej dokumentácie

Spoločná príručka

Spoločný audit

Spoločné riadenie efektívnosti



Spoločné princípy manažérstva rizík

Spoločná politika Q, E, S, (F)

Spoločné plánovanie

Spoločný manažment realizácie

Spoločné meranie, analýza a zlepšovanie

Riziko

Pod rizikami sa rozumejú všetky budúce udalosti (finančné a nefinančné), ako aj všetky možné vývoje vo vnútri alebo navonok podniku, ktoré sa môžu, vzhľadom k dosahovaným podnikovým cieľom, uskutočniť s negatívnym alebo pozitívnym, ***v každom prípade však neistým výsledkom.***

Prečo manažérstvo rizík

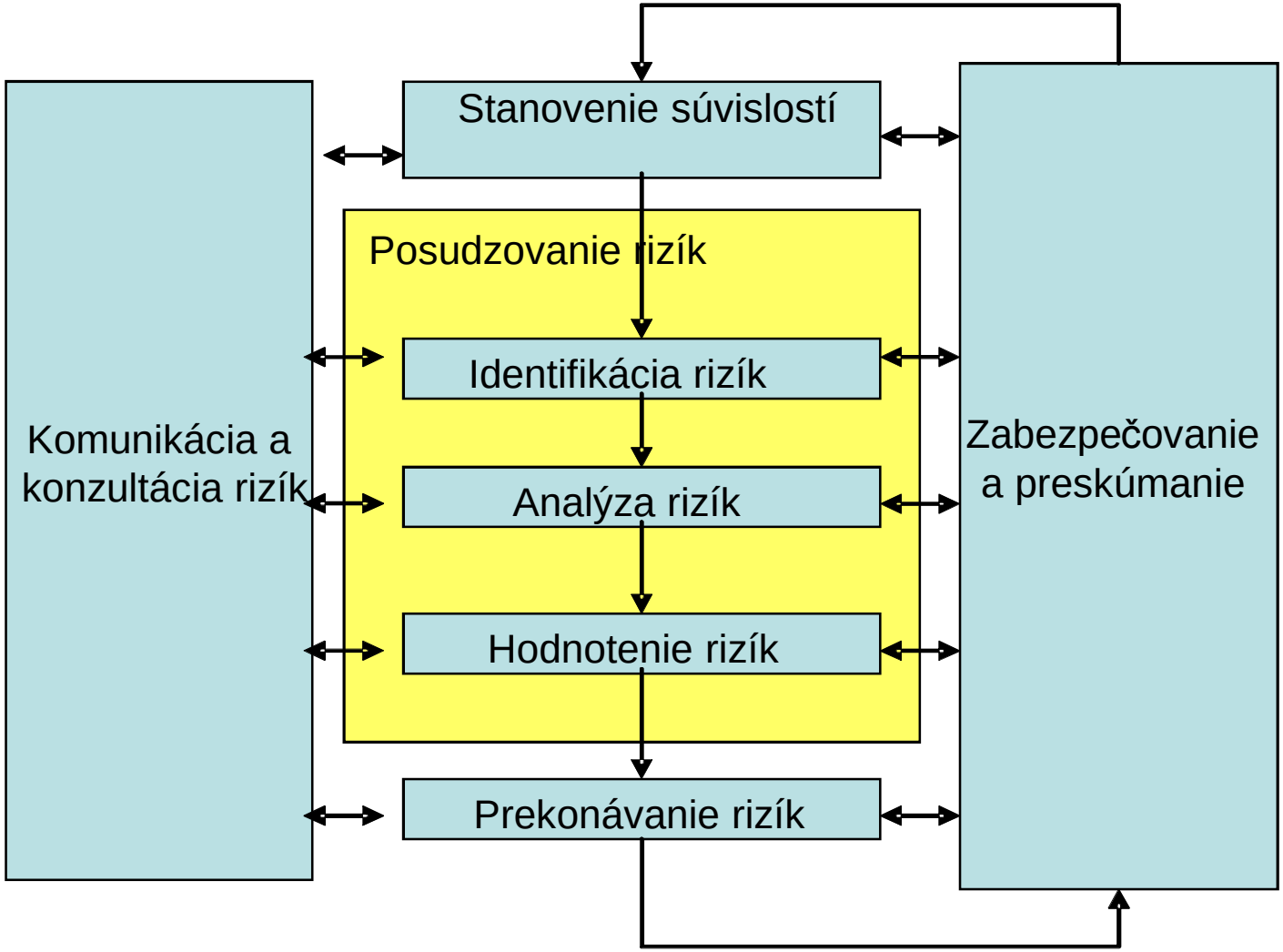
- Konkrétne povedomie rizík podniku je všeobecne nízke.
- Hodnotenie rizík je poväčšine iba podvedomé, intuitívne.
- Vo svete podnikania je posudzovanie rizík vývoja podniku, založené na náhode a intuícií, neúnosné.
- Aby bolo možné zabezpečovať čo najväčšiu úspešnosť podniku, musia byť všetky relevantné rozhodnutia podniku založené na báze čísel, údajov a faktov.
- Riziko vyjadruje pravdepodobnosť vzniku neistého javu s neistými dôsledkami, založenú na posúdení a hodnotení faktov, ktoré vyžadujú primerané riadenie.

Manažérstvo rizík

S cieľom zostať na trhu úspešným, je potrebné:

- **Rizikám predchádzať**
- **Riziká zmenšovať alebo**
- **Riziká prenášať na tretiu osobu.**

Manažérstvo rizík
ISO 31000:2009



Identifikácia rizík

- Cieľom IR je zostaviť zoznam (katalóg) možných ohrození , ktoré môžu podstatne ovplyvniť činnosť a výsledky podniku.
- Všetky riziká sa nedajú identifikovať a tie, ktoré identifikované boli, treba roztriediť na významné a nevýznamné riziká.
- Zoznam rizík bude závisieť od typu a veľkosti organizácie, od jej činností a procesov, ako aj od prostredia, v ktorom organizácia pôsobí.

Dve kategórie rizík

Podľa iniciácie možno hovoriť o dvoch kategóriách rizík:

1. Externé riziká:
vznikajú pod vplyvom vývoja životného prostredia, podnikateľského prostredia a pod vplyvom ich fluktuácie.

2. Interné riziká:
vznikajú pod vplyvom manažmentu, sú závislé od úrovne manažérskeho systému.

Sú náročné na požiadavky manažérskych nástrojov ale sú ovládateľnejšie než externé riziká.

Trhové riziká

- Trh je východiskom analýzy podnikateľských rizík.
- Zmeny trhu dokážu natrvalo ohroziť alebo úplne zničiť na riziká nepripravený podnik.
- Čím je citlivosť podniku a okolia na trhové zmeny väčšia, tým je trhové riziko vyššie.
- Čím je riziko vyššie, tým je jeho manažérstvo naliehavejšie.

Personálne riziká

- Nedostatok kvalifikovaného personálu.
- Výpadok dôležitých jednotlivcov, manažérov a odborníkov.
- Chýbajúce rezervy a manažérstvo náhradných ľudských zdrojov.
- Riziko nemocí a nehôd.
- Fluktuácia v dôsledku blízkej konkurencie.

Hospodárske riziká

- Materiálne zdroje, zásobovanie a logistika.
- Nestabilita cien nakupovaných vstupov.
- Finančné riziká.
- Riziká spojené s produktom alebo sortimentom.
- Riziká spojené so zákazníkom a konkurenciou.

Technické riziká

- Riziká vlastnej podnikateľskej činnosti a výkonov.
- Riziká výrobných procesov a riziká použiteľných zdrojov.
- Riziká, ovplyvňujúce kvalitu a kvantitu výkonov:
  - Materiálové vstupy,
  - Personálne vstupy.

Právne riziká

Tieto riziká ovplyvňujú všetky oblasti podnikania

- Právne riziká konformity sú spojené s celou dokumentáciou činnosti, od príkazov a zákazov, cez popisy dokumentovaných postupov jednotlivých procesov, až po právne povedomie personálnej práce.
- Neznalosť práva neospravedlňuje.

Majetkové riziká

- Pri majetkových deliktoch sa jedná o:
  - Klasickú krádež hmotného majetku,
  - Krádež duševného majetku (know-how, údaje, informácie).

Administratívne riziká

- Riziká plánovania,
- Riziká organizačné,
- Riziká správne.

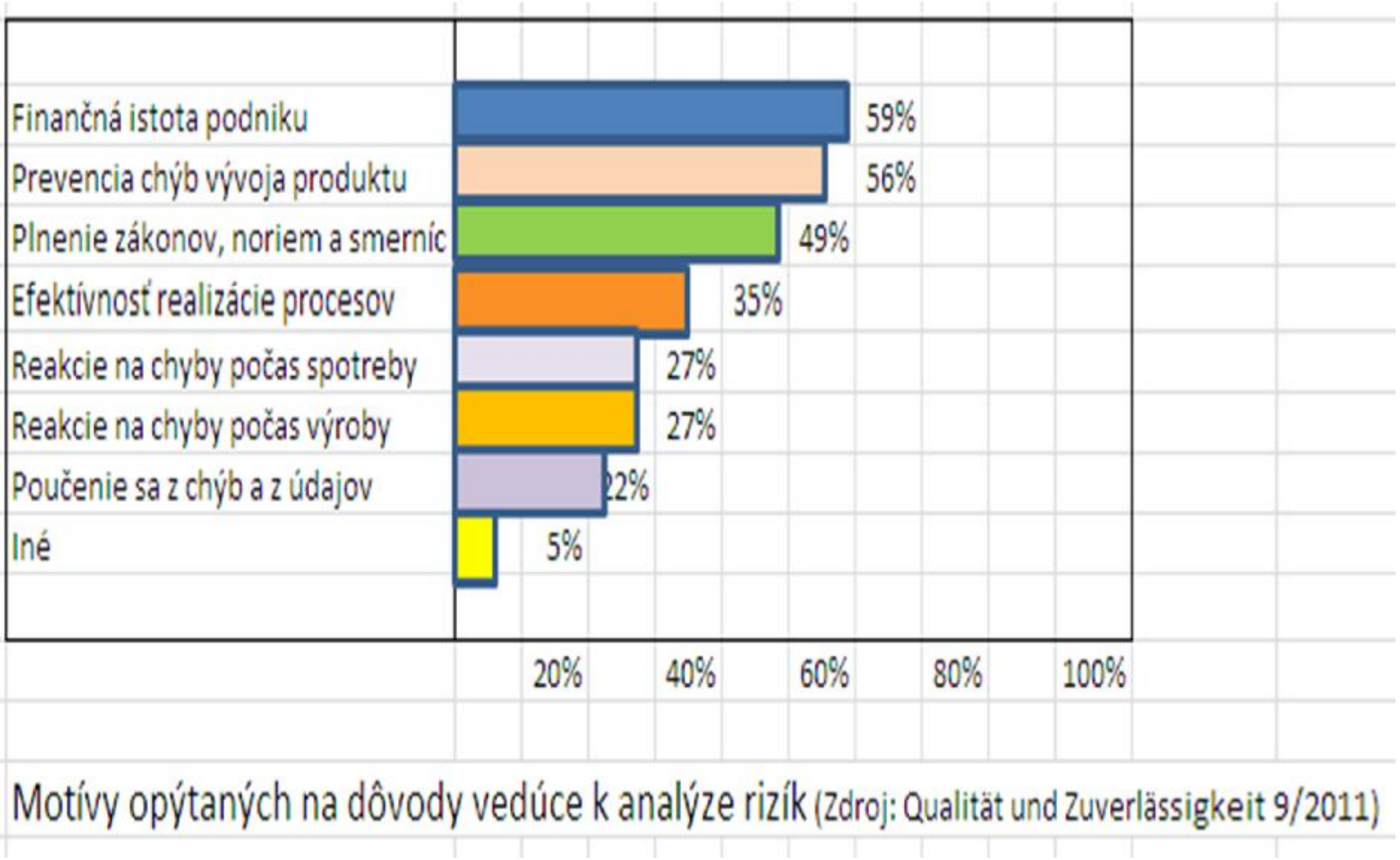
Riziká politické a spoločenské

- Makroekonomické rizika hospodárskej politiky štátu.

Prírodné riziká a katastrofy

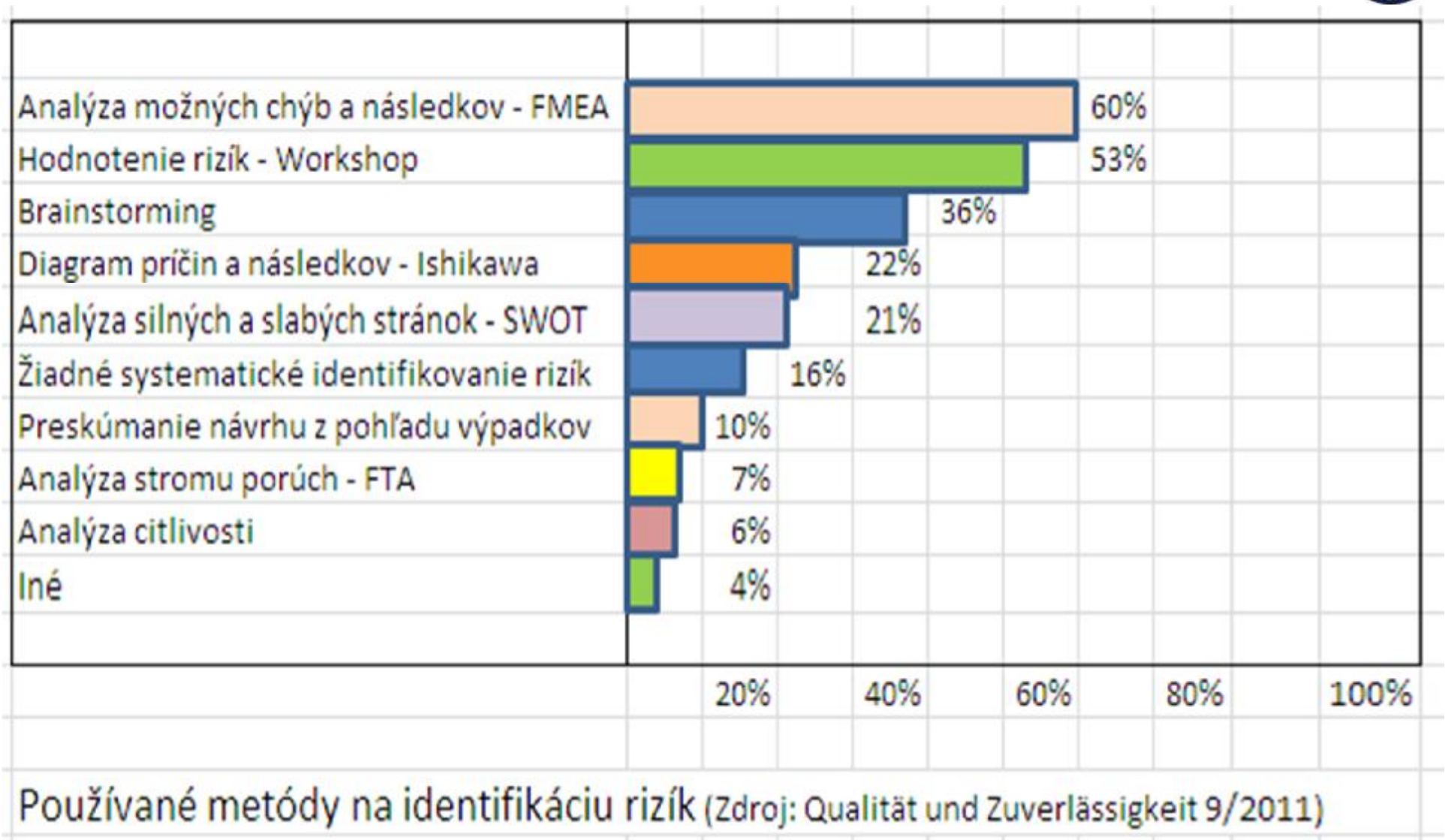
- Bežné udalosti,
- Búrky, povodne
- Krupobitie,
- Zosuvy pôdy,
- Požiare z bleskov,
- Lavíny,
- Periodicky sa opakujúce zle počasie,
- ....

Dôvody analýzy rizík



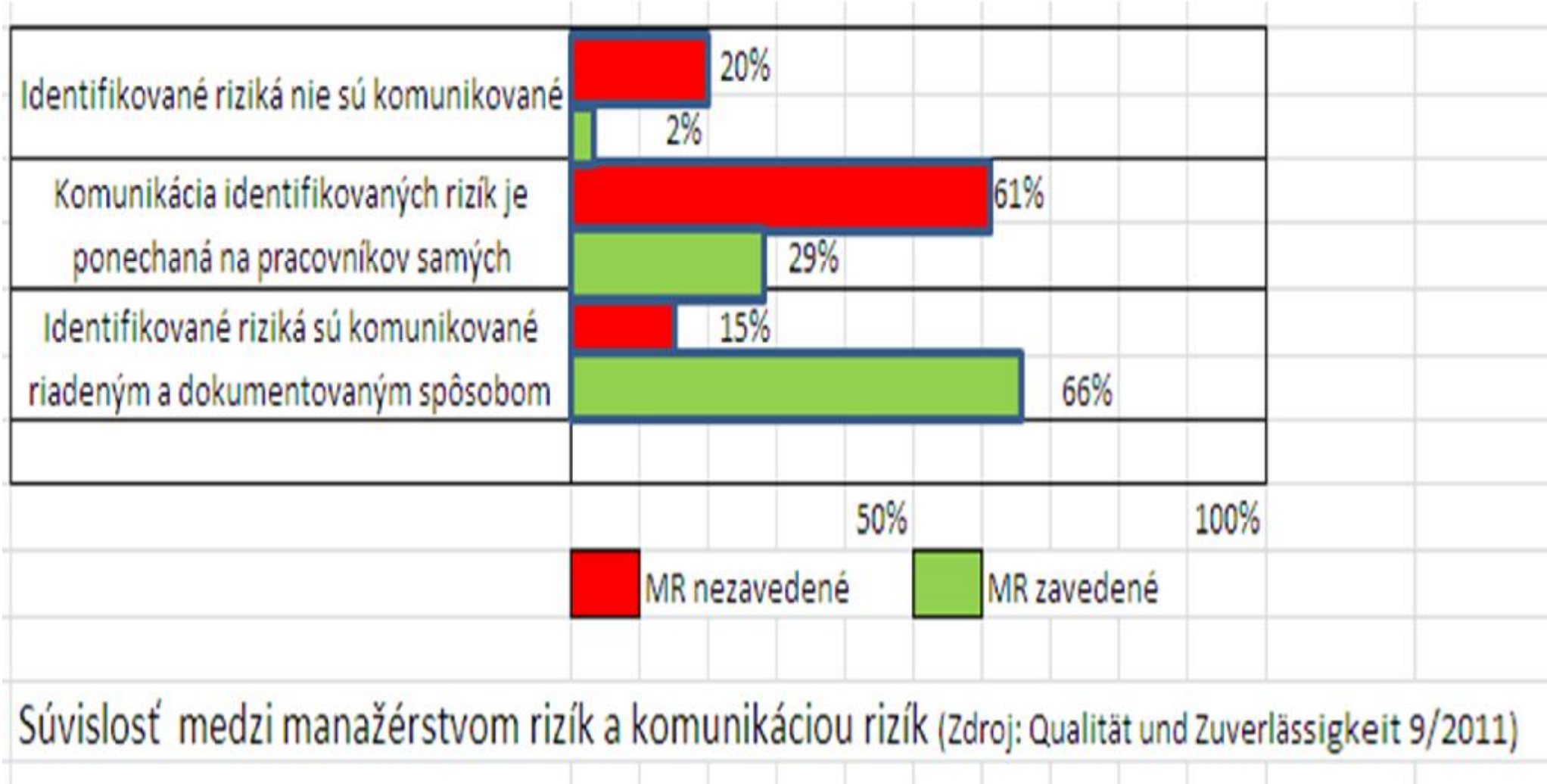
Motívy opýtaných na dôvody vedúce k analýze rizík (Zdroj: Qualität und Zuverlässigkeit 9/2011)

Metódy identifikácie rizík



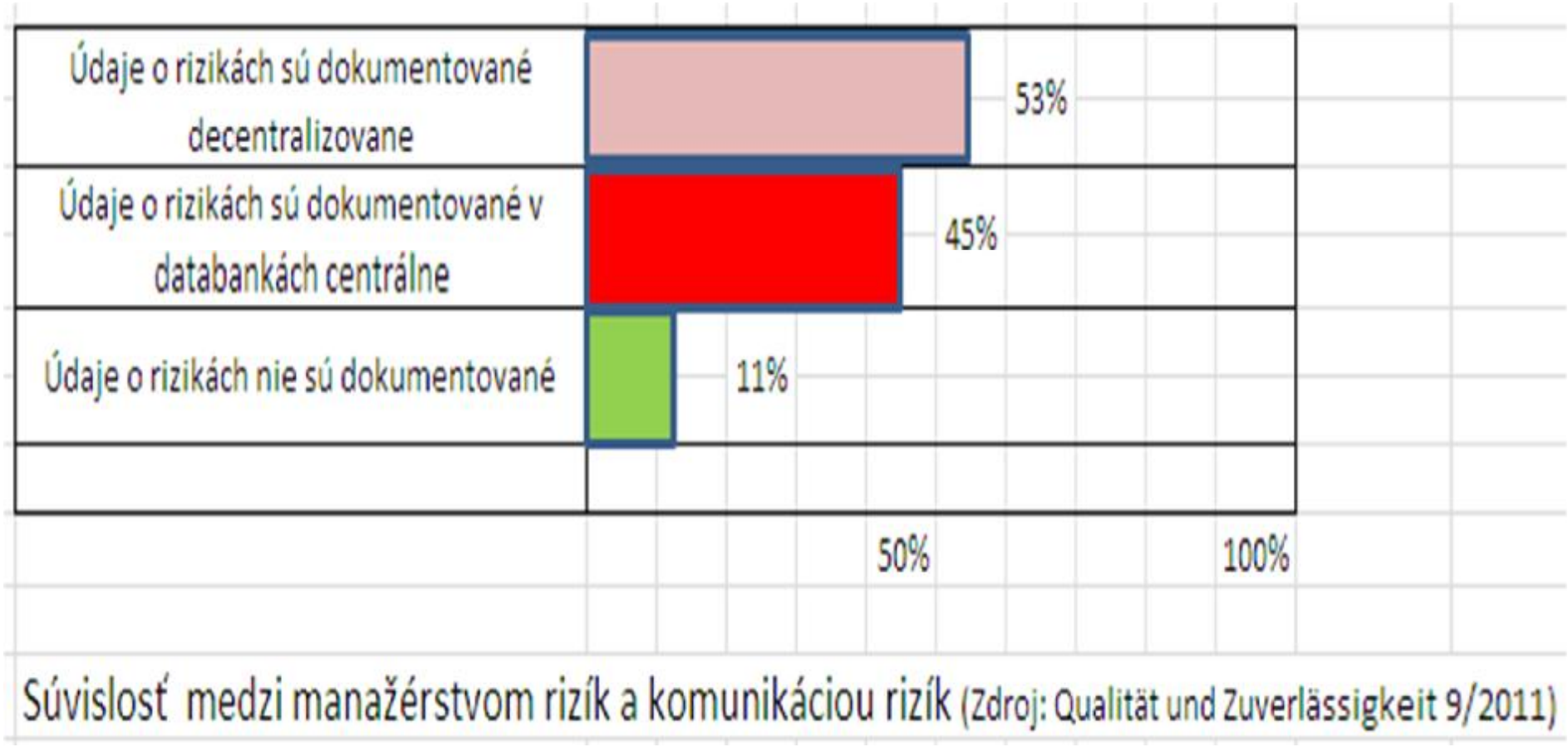
Používané metódy na identifikáciu rizík (Zdroj: Qualität und Zuverlässigkeit 9/2011)

Manažérstvo a komunikácia rizík



Súvislosť medzi manažérstvom rizík a komunikáciou rizík (Zdroj: Qualität und Zuverlässigkeit 9/2011)

Forma dokumentovania rizík



Súvislosť medzi manažérstvom rizík a komunikáciou rizík (Zdroj: Qualität und Zuverlässigkeit 9/2011)

Riziko

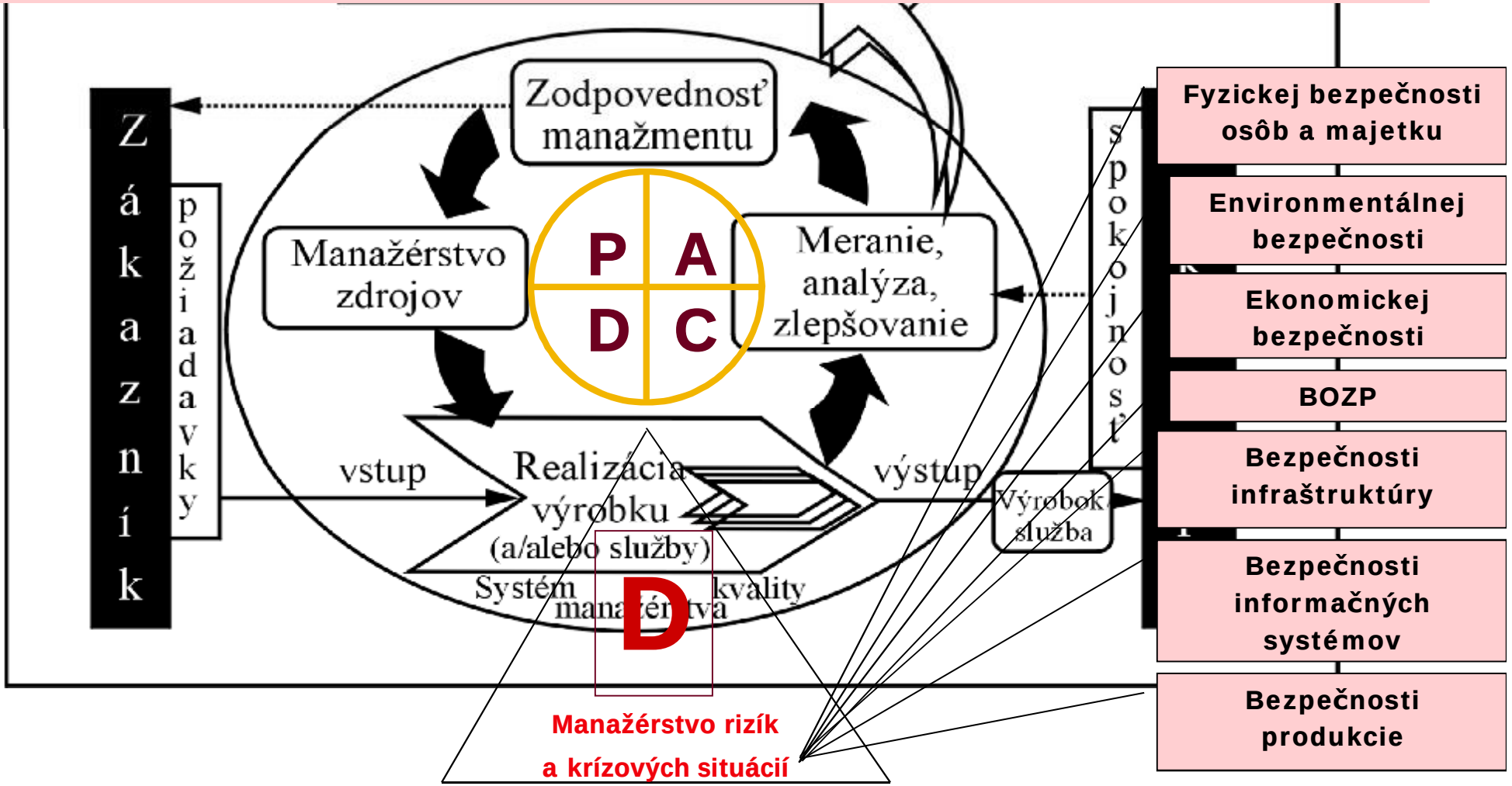
Manažérstvo kvality

ISO 9001:2008

„očakáva“ manažovanie rizík podľa ISO 31000

Riziká sú integrálnou súčasťou každej podnikateľskej činnosti

Bezpečnostné manažérstvo



Manažérstvo rizík

Riziko

je funkciou pravdepodobnosti vzniku (negatívnej) udalosti (P)

a veľkosti jej následkov (D)

R = P x D

Manažérstvo rizík ako súčasť procesu realizácie produktu

je znižovanie úrovne rizika minimálne na hodnotu akceptovateľného rizika.

Manažérstvo rizík

- Definovanie systému a bezpečnostnej politiky
- Analýza možných rizík
- Prekonávanie existujúcich rizík
- Udržiavanie rizík v akceptovateľných medziach
- Postupné znižovanie rizík

Realizácia produktu podniku

Kapitola 7 podľa ISO 9001:2008

7.1 Plánovanie produktu

7.2 Komunikácia so zákazníkom

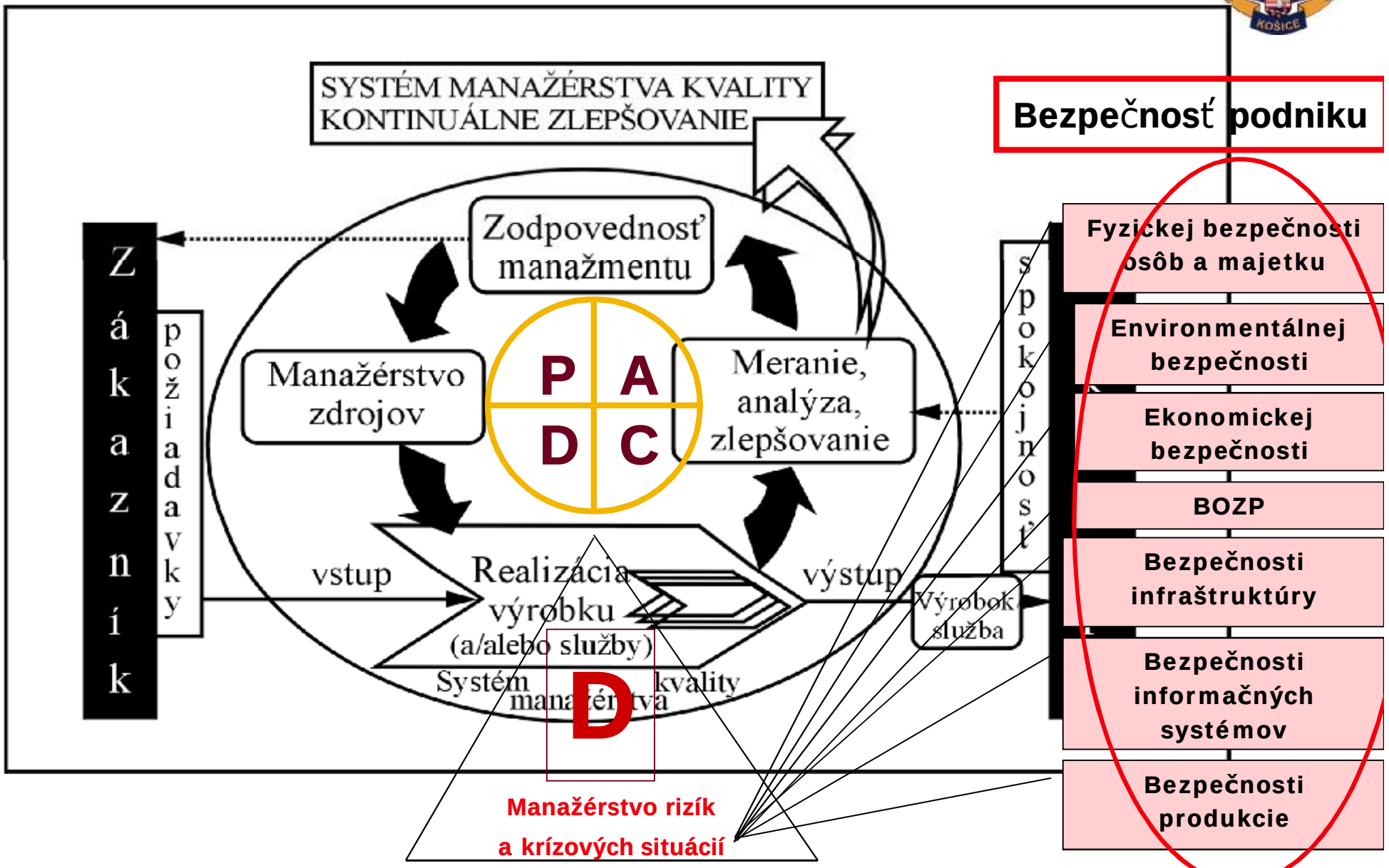
7.3 Návrh a vývoj

7.4 Nakupovanie

7.5 Výroba a poskytovanie služieb

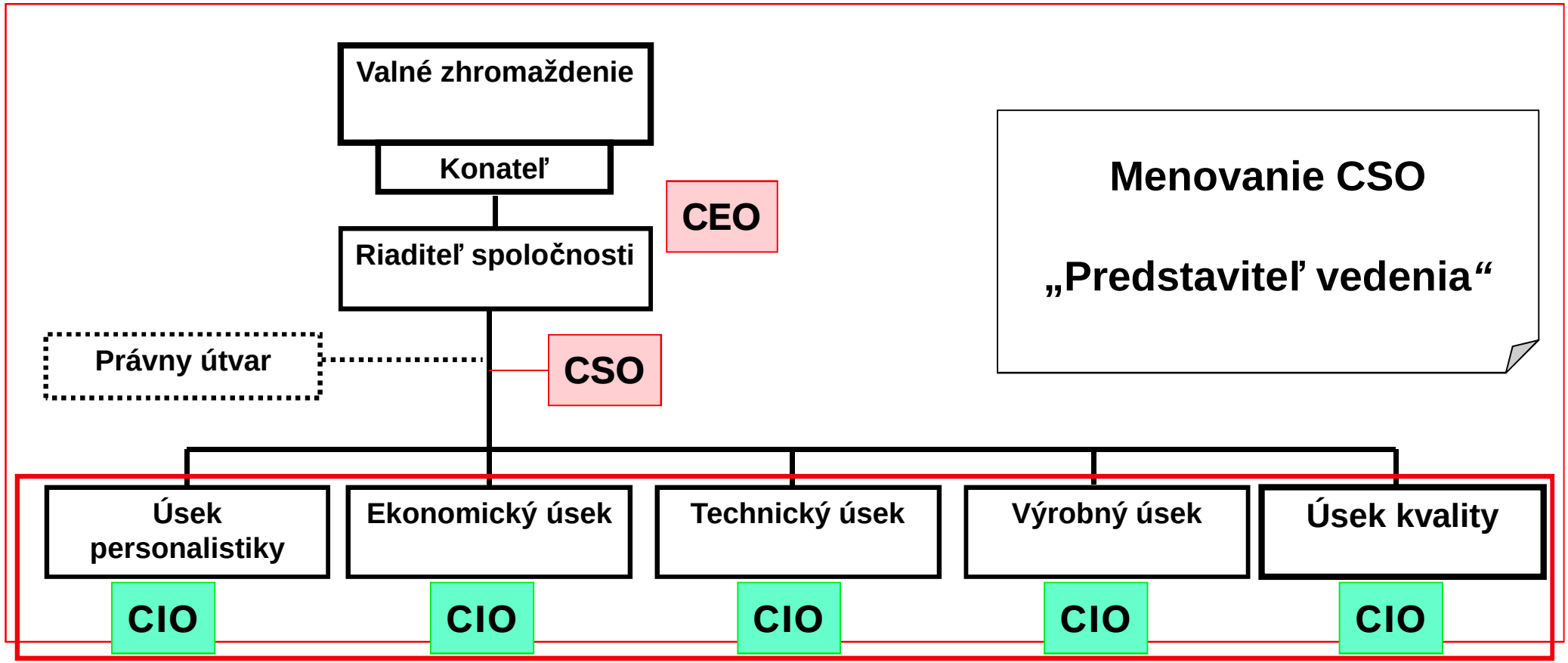
7.6 Riadenie meracích a monitorovacích zariadení

Generický Manažérsky Systém

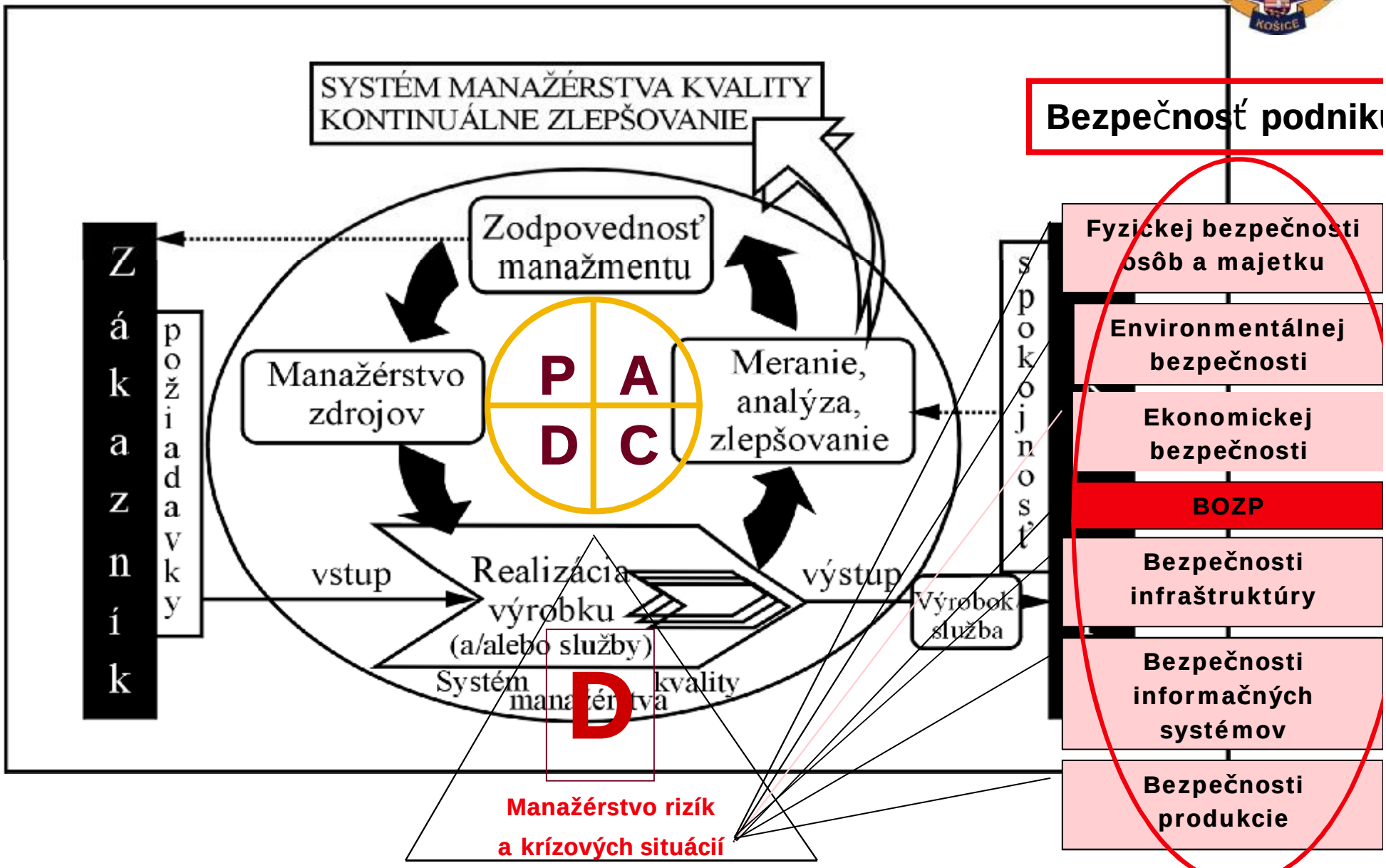


Organizácia bezpečnosti podniku

- Manažment menuje samostatnú osobu funkciou predstaviteľa vedenia na plný úväzok, ktorý má hlavnú zodpovednosť a inštitucionálnu právomoc vo veciach rizík a celého bezpečnostného manažérskeho systému, vhodne vybraného typu, v celom podniku:



Generický Manažérsky Systém



Čo je BOZP?

Bezpečnosť a ochrana zdravia pri práci.

- BOZP nie je len protiúrazová prevencia.
- BOZP rieši – pracovné prostredie, pracovné podmienky, pracovné vzťahy, stres, záťaž a ostatné faktory ovplyvňujúce pohodu pri práci.
- BOZP je integrálnou súčasťou bezpečnosti podniku

Systém riadenia BOZP

Je to časť celkového systému riadenia, ktorá umožňuje efektívne riadenie rizík BOZP súvisiacich s činnosťou organizácie

OHSAS 18001/18002

Systém akceptovateľný certifikačnými orgánmi ako náhrada za neschválenú normu ISO (plánovaný rad ISO 18000)

- **OHSAS 18001/18002**

bol vyvinutý z britského štandardu BS 8800 za podpory nasledujúcich partnerov:

1. **Štandardizačných orgánov z :** **Veľkej Británie, Írska, Južnej Afriky, Malayzie, Španielska**
2. **Skúšobných a certifikačných orgánov:** **BSI, BVQI, Quality Austria, DNV, LRQA, NQA, SFS, STS, ISMO Ltd., ICS**

- **OHSAS 18001/18002**

bol vyvinutý za účelom preverovania a certifikácie organizácií. Existujú národné normy OHSAS, napr. STN OHSAS 18001/18002

4.1 Všeobecné požiadavky

4.2 Politika bezpečnosti a ochrany zdravia pri práci (BOZP)

4.3 Plánovanie

4.3.1 Posudzovanie rizík a havarijná pripravenosť,
4.3.2 Právne a iné požiadavky
4.3.3 Ciele
4.3.4 Program realizácie BOZP

4.4 Realizácia a organizačné zabezpečenie

4.4.1 Organizačná štruktúra a zodpovednosť
4.4.2 Vzdelávanie, odborná spôsobilosť, motivácia
4.4.3 Operatívne riadenie a komunikácia
4.4.4 Dokumentácia
4.4.5 Riadenie dokumentácie a záznamov
4.4.6 Riadenie procesov
4.4.7 Prevencia úrazov, havárií a prijímanie opatrení

4.5 Kontrolná činnosť a opatrenia

4.5.1 Meranie a kontrola
4.5.2 Vyšetrovanie úrazov, havárií a kontrola prijatých opatrení
4.5.3 Riadenie predpisov
4.5.4 Audit

4.6 Preskúmanie manažmentom

Právny základ prvkov systému riadenia BOZP
V Slovenskej republike

POLITIKA BOZP

Zákon 124/2006 Z.z.,
„Zamestnávateľ je povinný:-
*-- Písomne vypracovať koncepciu **politiky BOZP**, ktorá bude obsahovať zásadné zámery, ktoré sa majú dosiahnuť v oblasti BOZP a **program jej realizácie**, obsahujúci najmä postup, prostriedky a spôsob jej vykonania, pravidelne ho vyhodnocovať a podľa potreby aktualizovať.“*

DOKUMENTÁCIA

Zákon NR SR .124/2006

„zamestnávateľ je povinný

*- viesť a uchovávať predpísanú **dokumentáciu,** záznamy o evidencii*

- vydávať pravidlá a pokyny na zaistenie BOZP,

-

POSUDZOVANIE RIZÍK

Zákon 124/2006

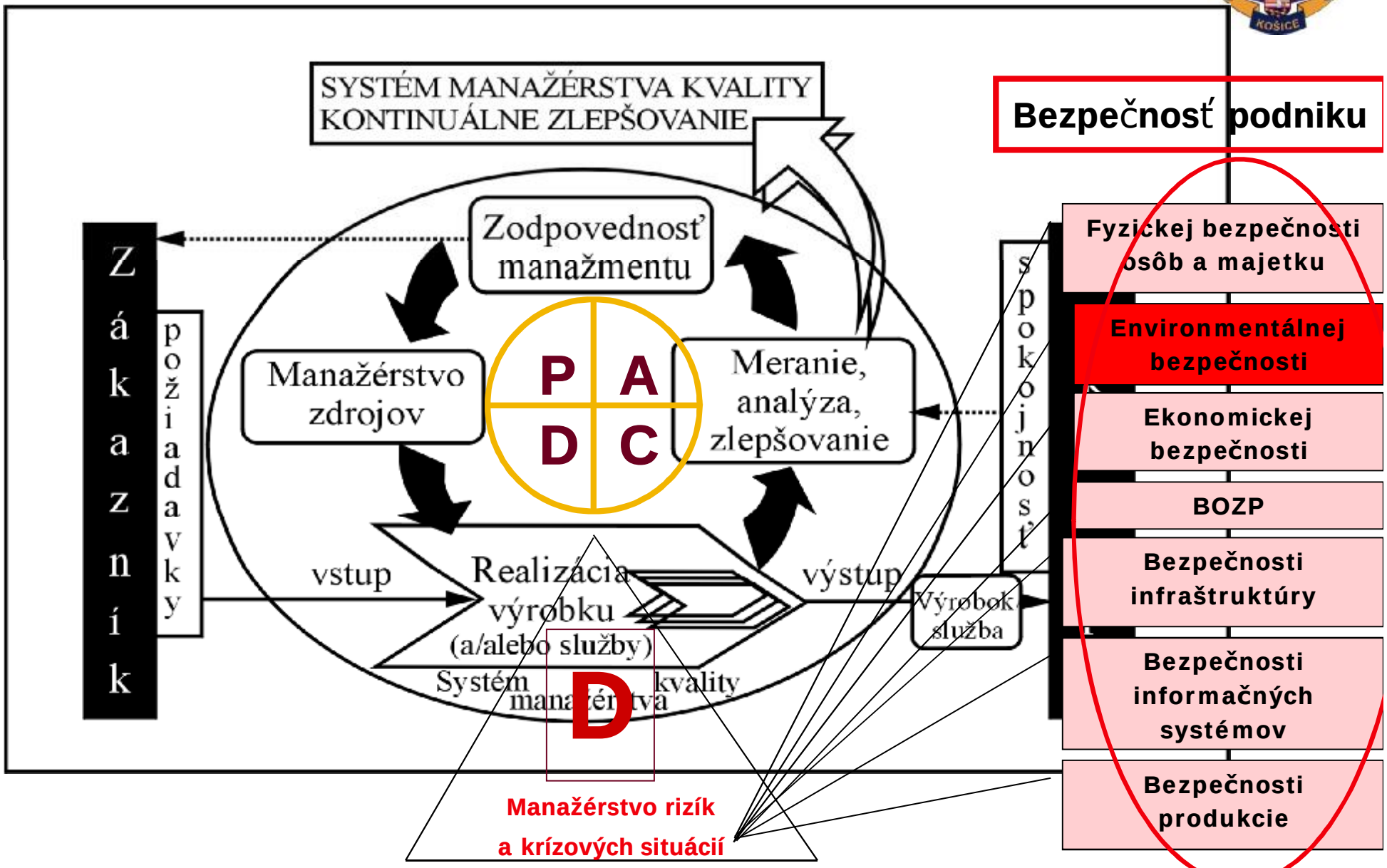
„zamestnávateľ je povinný zisťovať nebezpečenstvá a ohrozenia, posudzovať riziko aj vrátane osobitných skupín zamestnancov a vypracovať písomný dokument o posúdení rizika“

VZDELÁVANIE ZAMESTNANCOV

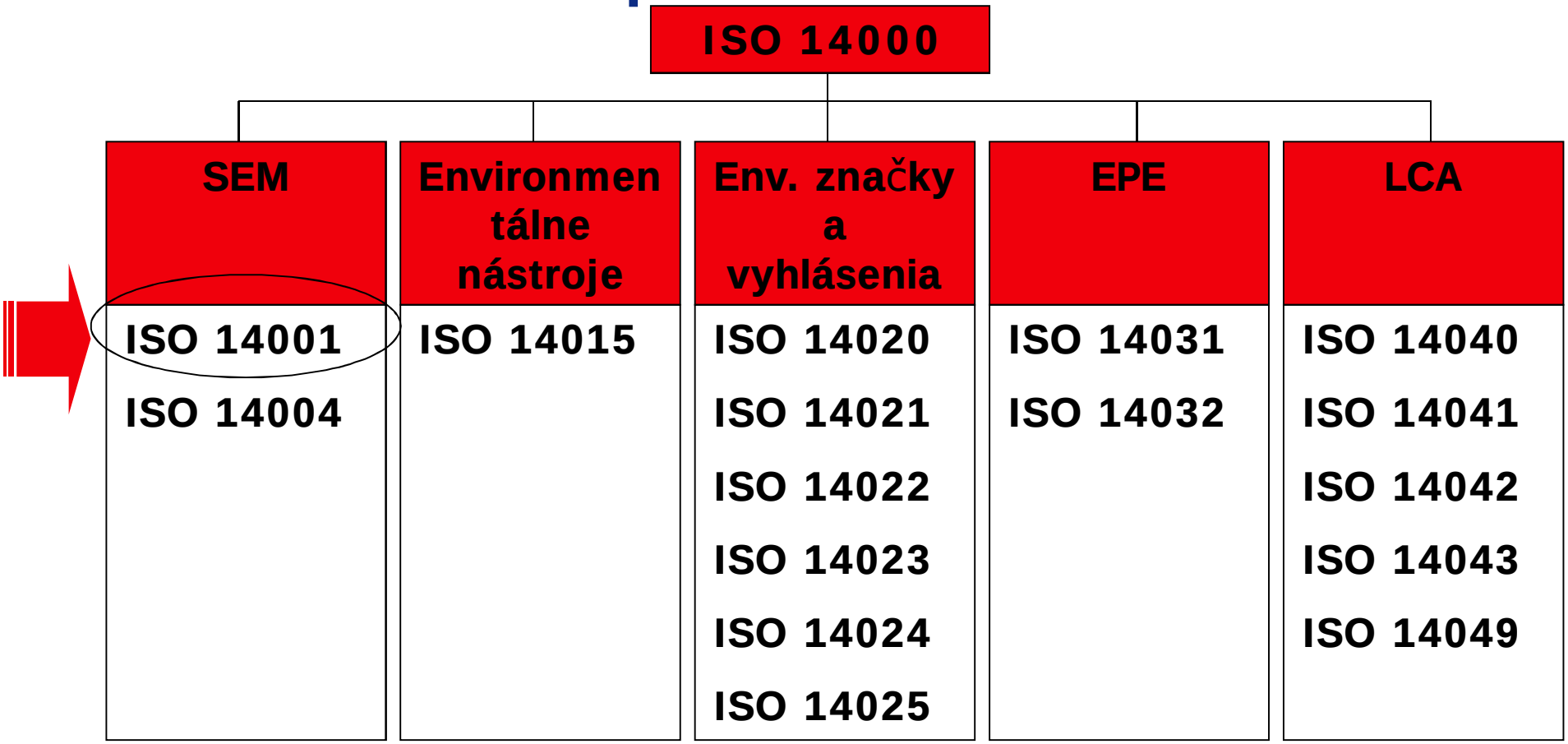
VYŠETROVANIE ÚRAZOV

HAVARIJNE OPATRENIA

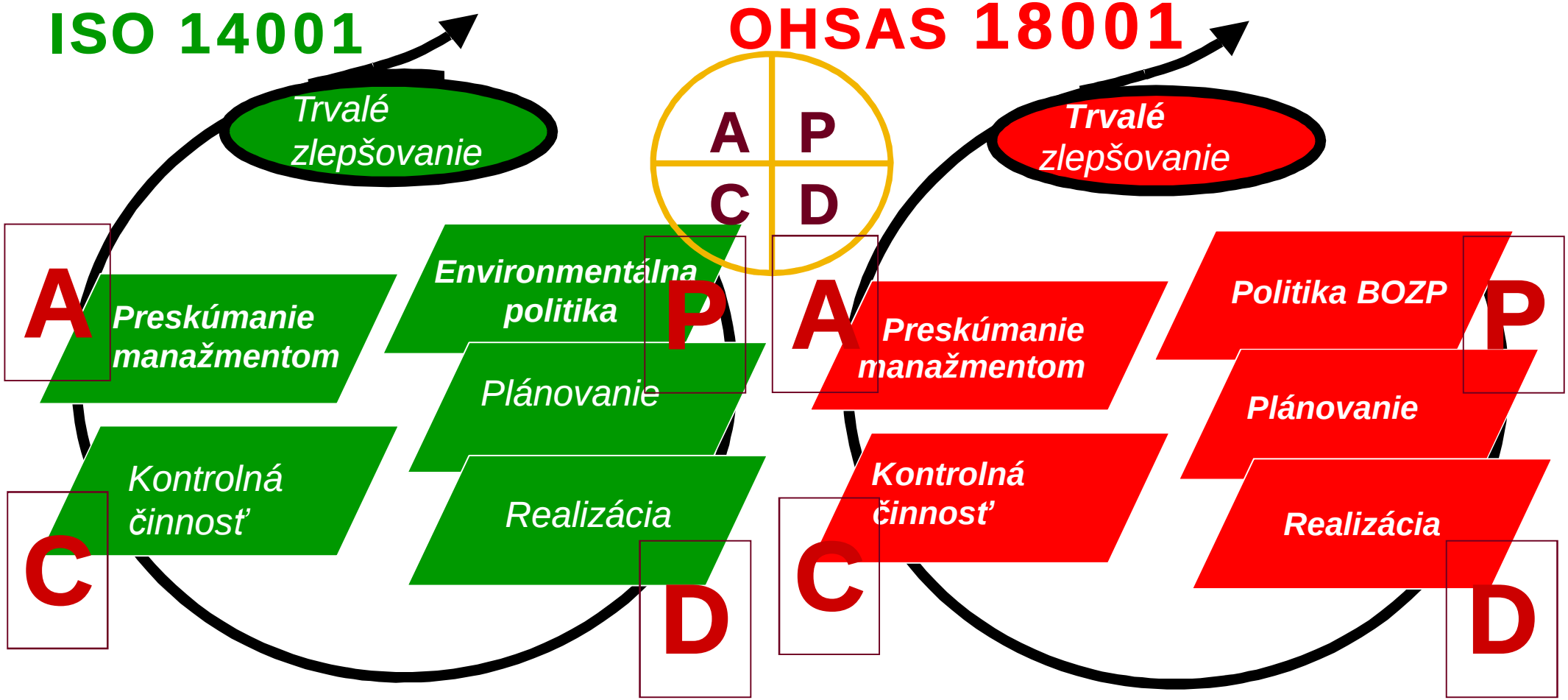
Generický Manažérsky Systém

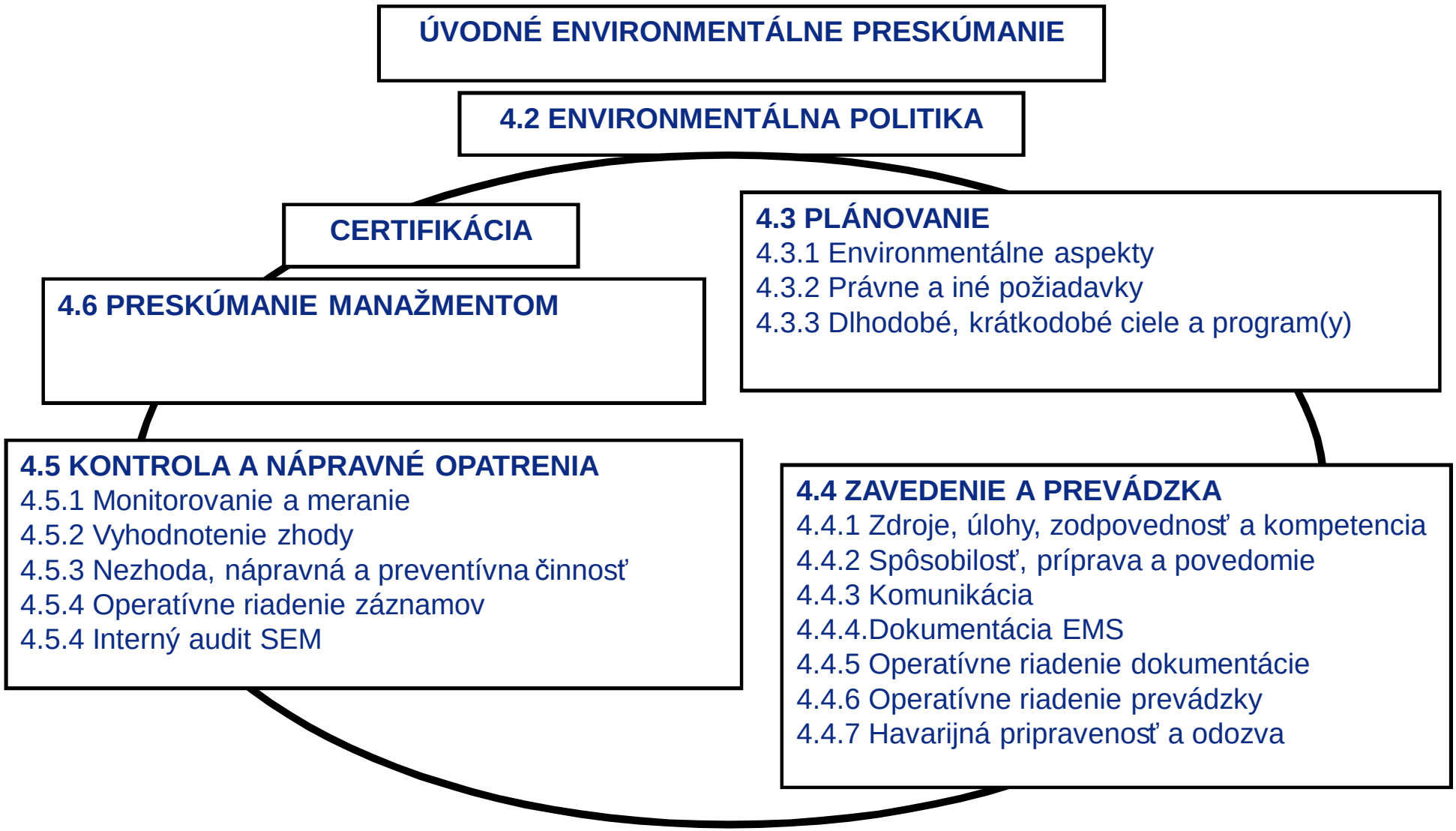


Systémy environmentálneho manažérstva podľa ISO EN 14001

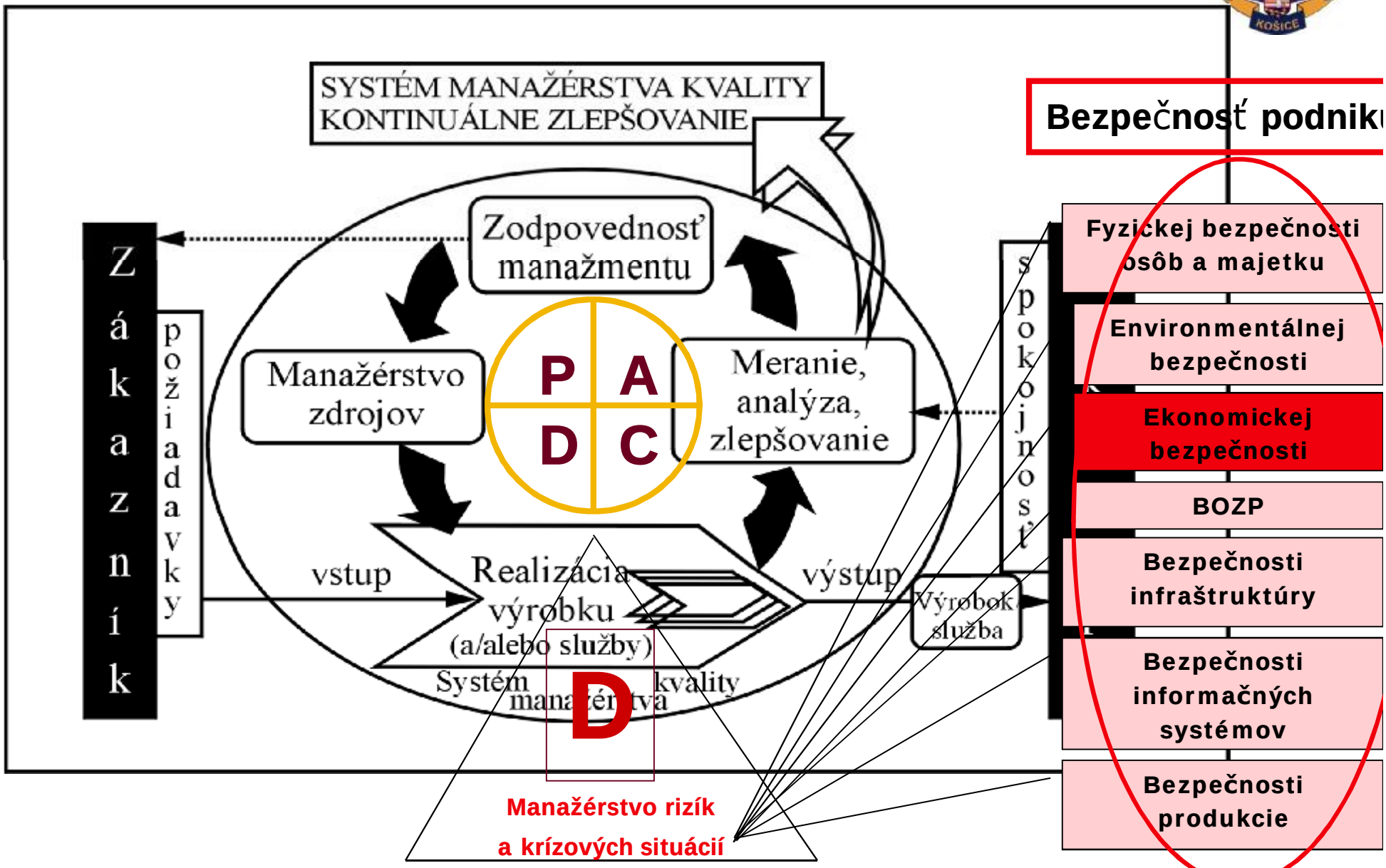


Porovnanie medzi OHSAS 18001 a ISO 14001




ÚVODNÉ ENVIRONMENTÁLNE PRESKÚMANIE
4.2 ENVIRONMENTÁLNA POLITIKA
4.3 PLÁNOVANIE
4.3.1 Environmentálne aspekty
4.3.2 Právne a iné požiadavky
4.3.3 Dlhodobé, krátkodobé ciele a program(y)
4.4 ZAVEDENIE A PREVÁDZKA
4.4.1 Zdroje, úlohy, zodpovednosť a kompetencia
4.4.2 Spôsobilosť, príprava a povedomie
4.4.3 Komunikácia
4.4.4.Dokumentácia EMS
4.4.5 Operatívne riadenie dokumentácie
4.4.6 Operatívne riadenie prevádzky
4.4.7 Havarijná pripravenosť a odozva
4.5 KONTROLA A NÁPRAVNÉ OPATRENIA
4.5.1 Monitorovanie a meranie
4.5.2 Vyhodnotenie zhody
4.5.3 Nezhoda, nápravná a preventívna činnosť
4.5.4 Operatívne riadenie záznamov
4.5.4 Interný audit SEM
4.6 PRESKÚMANIE MANAŽMENTOM
CERTIFIKÁCIA

Generický Manažérsky Systém



Tri najdôležitejšie dokumenty riadenia podniku

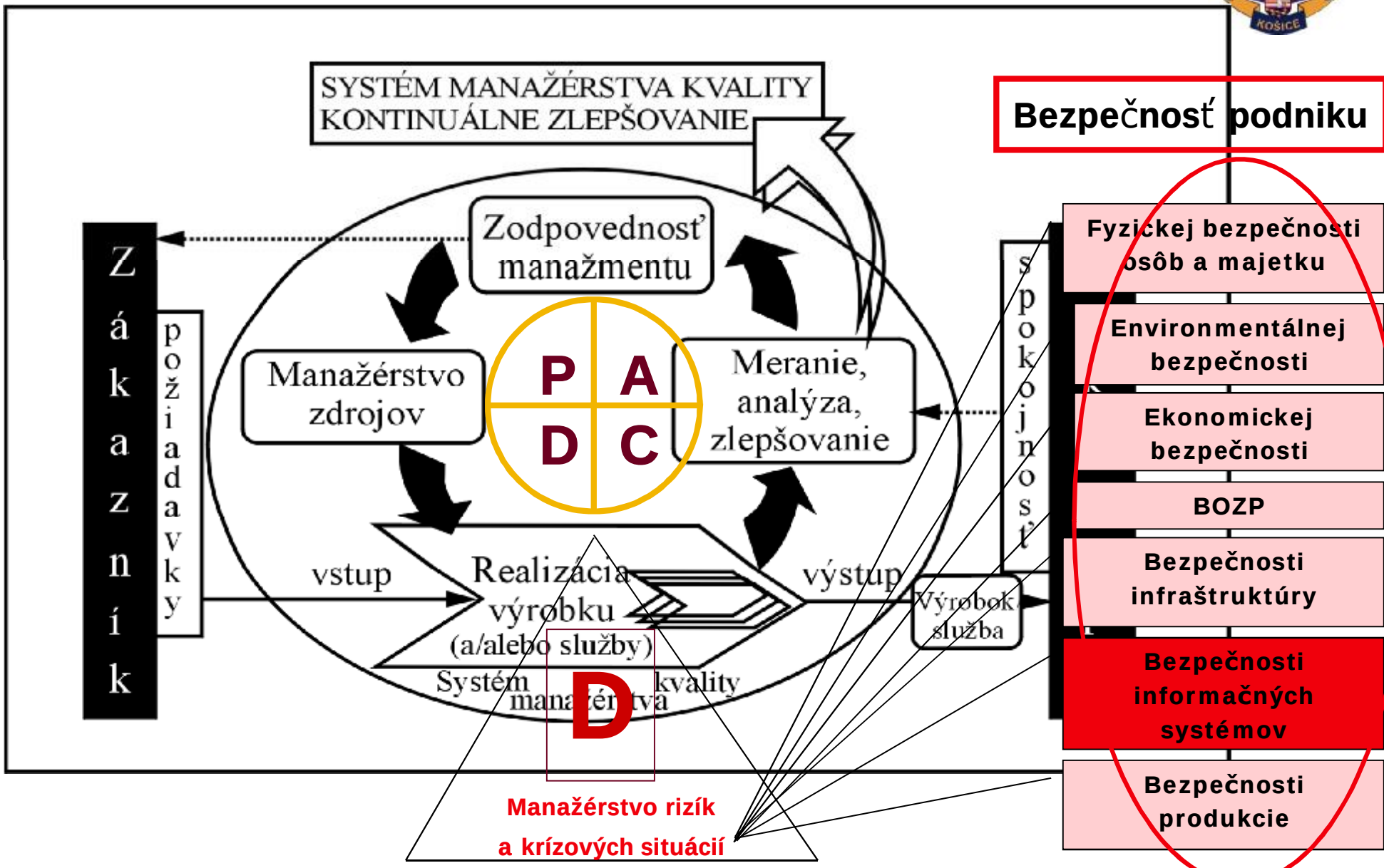
1. Majetková súvaha
2. Výsledovka
3. Finančný tok (cash flow)

- **Hovorí o okamžitom stave aktív a pasív (fotografický stav)**
- **Hovorí o hospodárení (zisk-strata)**
- **Je to „živina“ podniku (ak zastane finančný tok, podnik zbankrotuje)**

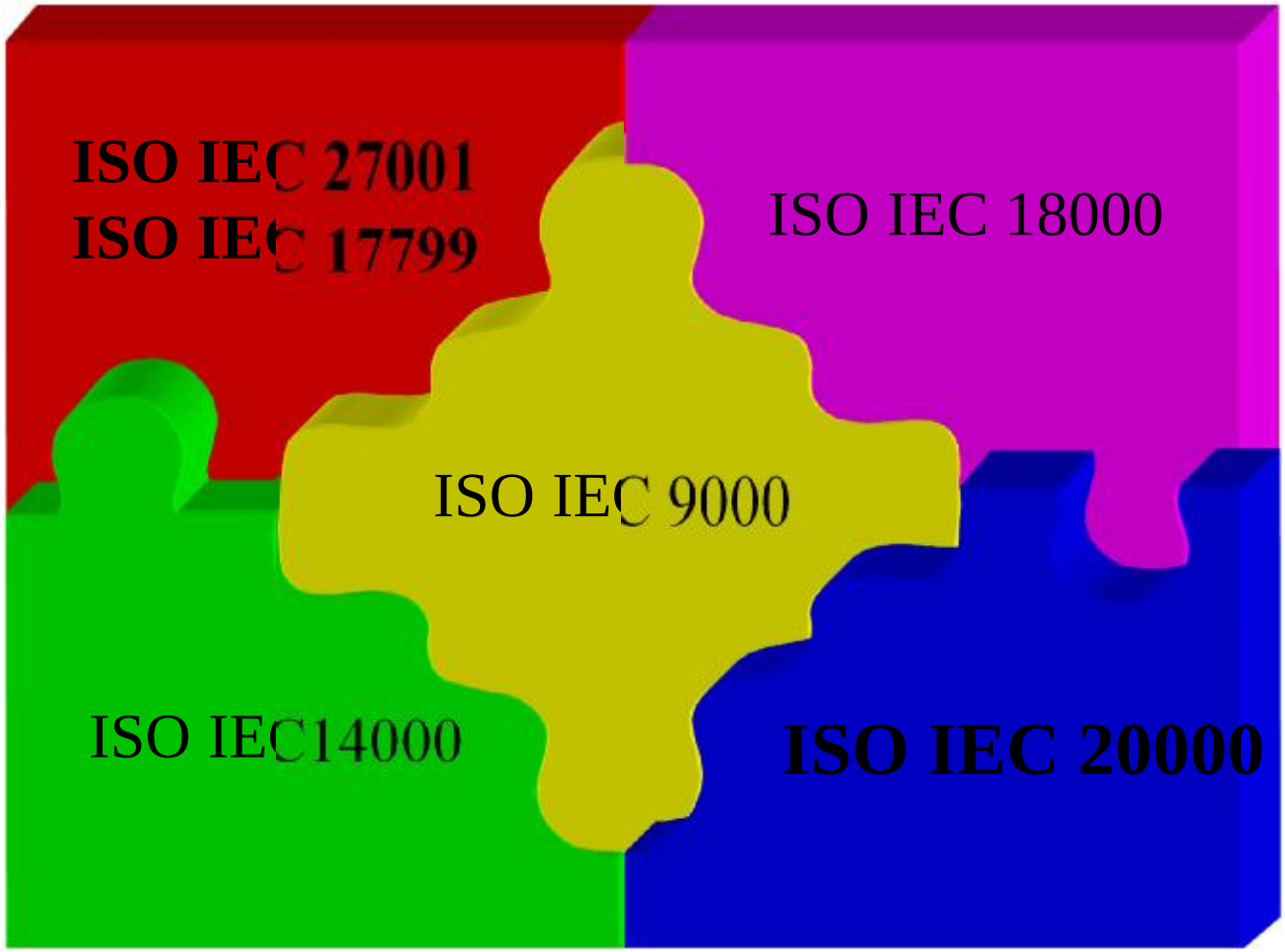
Najzávažnejšie riziká podnikania

- Nízka vymožiteľnosť práva
  - Ochrana zamestnancov
  - Mafiánske spôsoby
  - Preťaženosť súdov
- Neefektívnosť bakrotov
  - Riadený bankrot
  - Donútený bankrot
- Vysoká miera korupcie
  - Medzi podnikateľmi
  - Medzi obyvateľstvom
  - Medzi štátnymi úradníkmi
  - Kartelové dohody
  - Monopolné správanie sa
  - Pyramídové podnikanie
  - Iné neduhy podnikateľského sveta

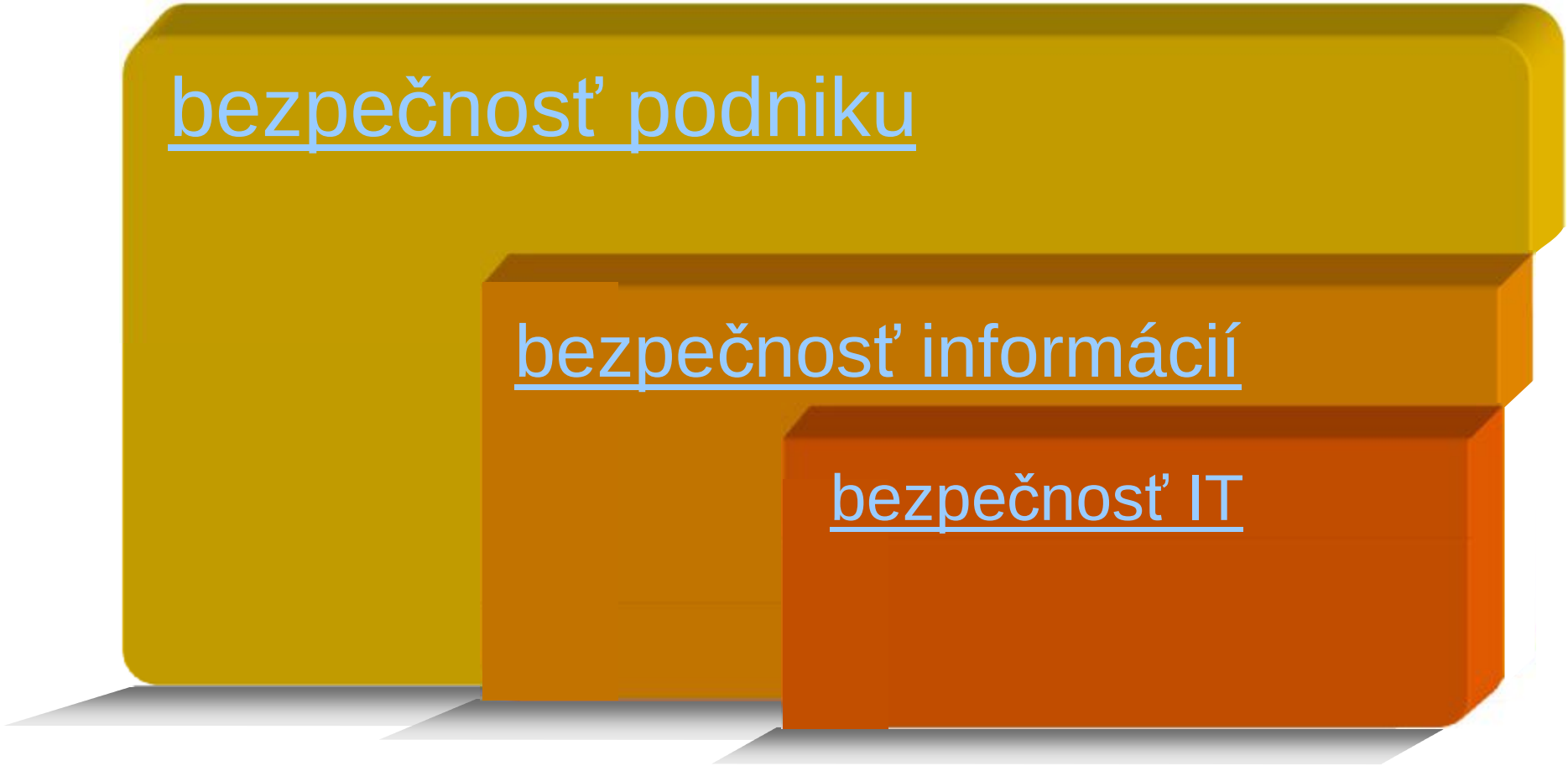
Generický Manažérsky Systém



Riešenie v kontexte ostatných štandardov



Zaradenie bezpečnosti IT



Desatoro bezpečnostných opatrení

1. Definovať opatrenia/procesy
2. Stanoviť zodpovedností
3. Formalizovať postupy
4. Schváliť vedením organizácie

Plánuj **P**

5. Vyškoliť pracovníkov
6. Zaviesť opatrenia

Vykonaj **D**

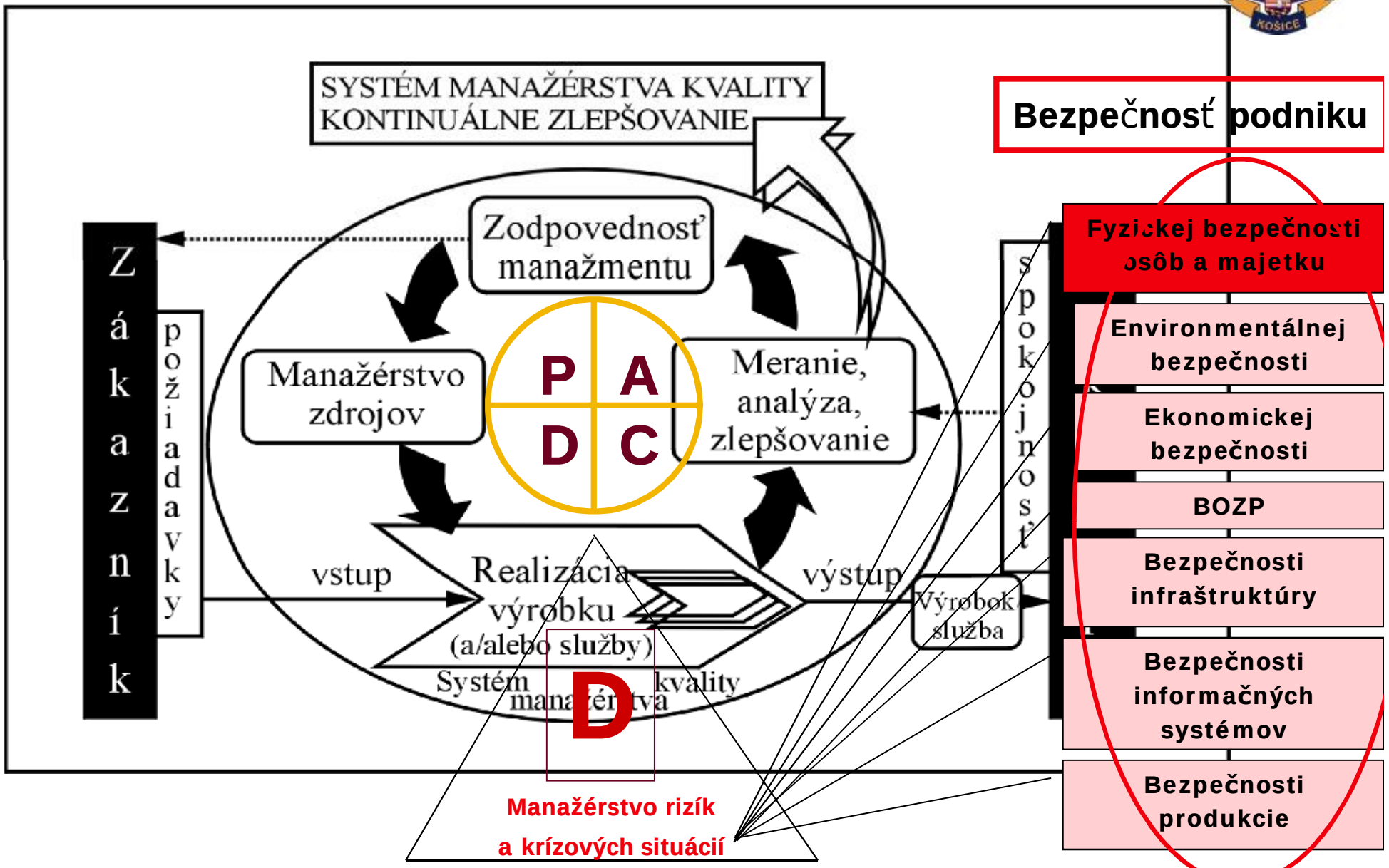
7. Merať účinnosť opatrení
8. Kontrolovať súlad s politikou
9. Vyhodnocovať incidenty

Kontroluj **C**

10. Zlepšovať opatrenia

Aktualizuj **A**

Generický Manažérsky Systém



Druhy ochrany podniku

(Mach, 2010).

Medzi základné druhy ochrany objektov patrí:

- klasická
- režimová
- technická
- fyzická

Využívanie mechanických zábranných prostriedkov na zamedzenie vniku do objektu ochrany

Druhy ochrany podniku

(Mach, 2010).

Medzi základné druhy ochrany objektov patrí:

- klasická
- režimová
- technická
- fyzická

Systém poriadku a režimu,

Zabezpečenie systému a režimu

Kontrola systému a režimu

Druhy ochrany podniku

(Mach, 2010).

Medzi základné druhy ochrany objekto

- klasická
- režimová
- technická
- fyzická

Snímanie a detekovanie neobvyklých javov technickými prostriedkami:

- Požiare
- Vniknutie do zabezpečovaného priestoru

Druhy ochrany podniku

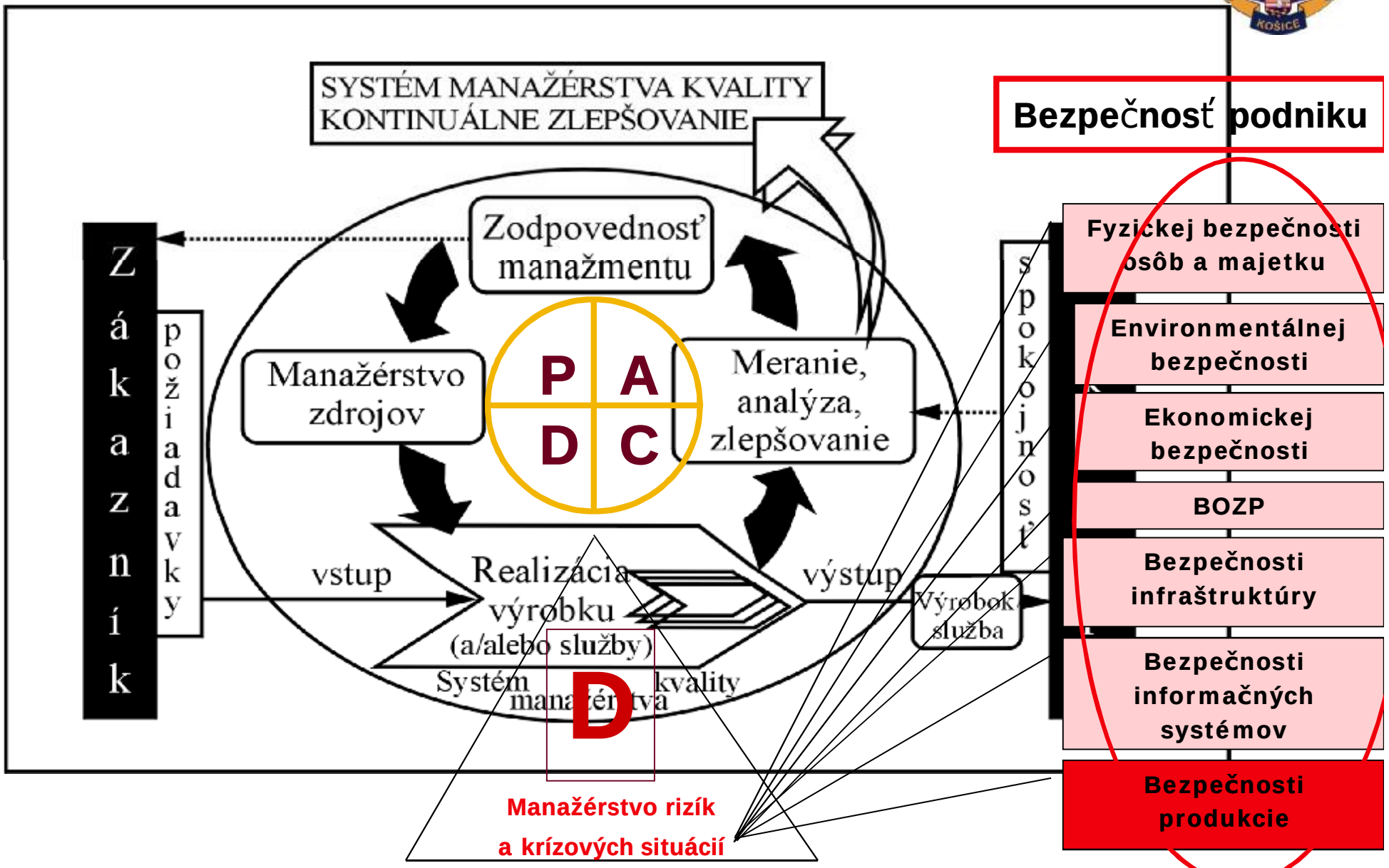
(Mach, 2010).

Medzi základné druhy ochrany objektov patrí:

- klasická
- režimová
- technická
- fyzická

Spočíva v bezprostrednom strážení objektu, priestoru, predmetov a iných chránených záujmov podniku fyzickými osobami.

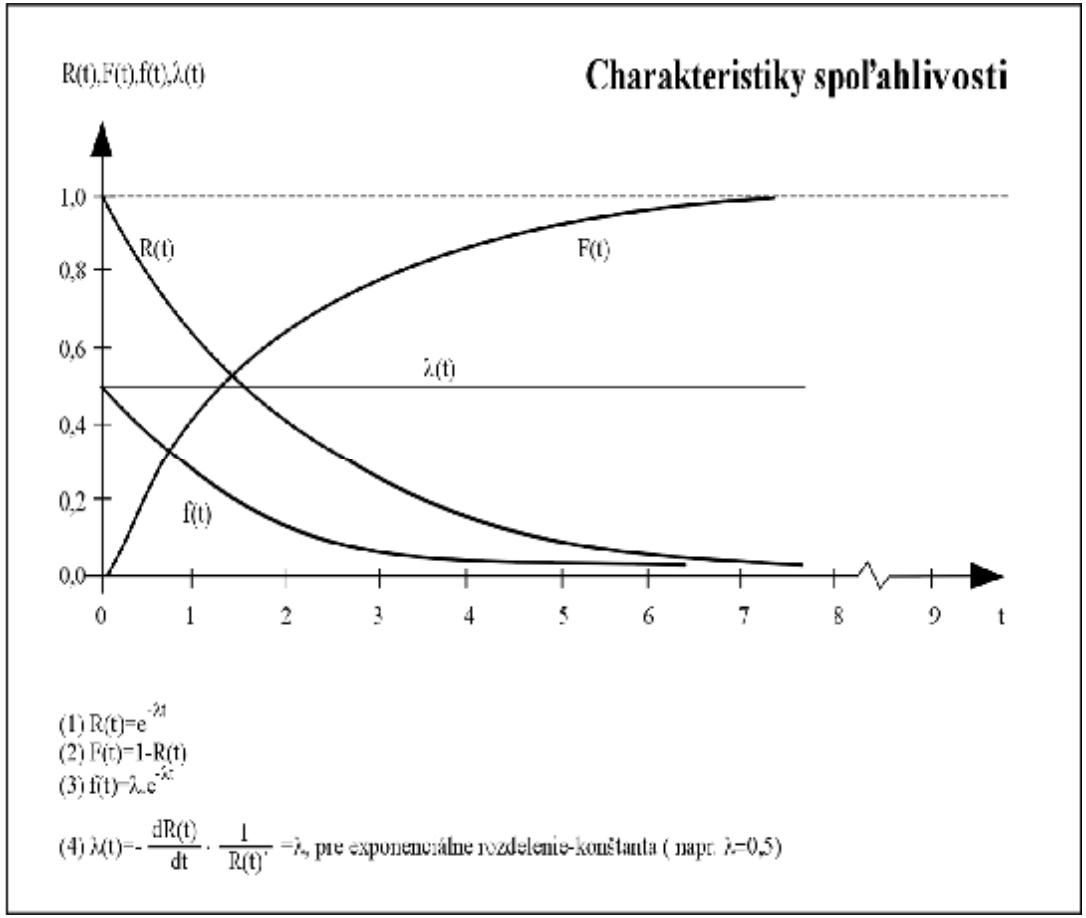
Generický Manažérsky Systém



Charakteristiky spoľahlivosti

- Pravdepodobnosť poruchy **F**(t)
- Intenzita porúch **λ**(t)
- Hustota porúch **f**(t),
- Bezporuchovosť

  R(t) = 1 – F(t)



Spoľahlivosť v systéme

Výber materiálov, dielov a skupín

- Kartotéka materiálov, príslušné normy domáce i zahraničné
- Kartotéka a normy normovaných a typizovaných súčiastok
- Smernice a predpisy o bezpečnosti a ochrane
- Kartotéka dodávateľov a výsledky odberateľských auditov systému manažérstva kvality

Spoľahlivosť v systéme

Konštrukčné postupy

- redundancia, potreba zdvojenej poistnej funkcie voči poruche
- chrana voči zlyhaniu niektorej z požiadaviek prevádzkových podmienok
- spustenie do prevádzky a návod na obsluhu
- poistné riešenie v prípade poruchy alebo nebezpečenstva
- udržiavateľnosť a výbava náhradnými dielmi

Spoľahlivosť v systéme

Skúšky spoľahlivosti a analýza porúch

- Počas skúšok určujeme typ funkcie rozdelenia *F(t)* skúšaných výrobkov a odhadujeme parametre spoľahlivosti na základe štatistických výsledkov.
- Závery skúšok spoľahlivosti treba ukončiť metódami štatistickej indukcie, t.j. štatistickým odhadom parametrov, stanovením intervalu spoľahlivosti a testovaním hypotéz o spoľahlivosti

Spoľahlivosť v systéme

Spätné informácie

- V teórii spoľahlivosti platí téza „Najlepšie skúšky sú skúšky zákazníka“. Táto téza neznamená, že výrobca prenáša všetky náklady spojené so skúšaním a overovaním na zákazníka, ale znamená, že výrobca ani pri najlepšej vôli nedokáže vystihnúť všetky okolnosti a podmienky, za ktorých výrobok plní svoje funkcie.
- Spätné informácie o prevádzke výrobku sú veľmi dôležité a táto spätná väzba uzatvára aj špirálu kvality.
- O aký druh informácií ide, o tom rozhoduje konštruktér a za zber informácií zodpovedá servis.

Spoľahlivosť v systéme

Hodnotenie výrobkov

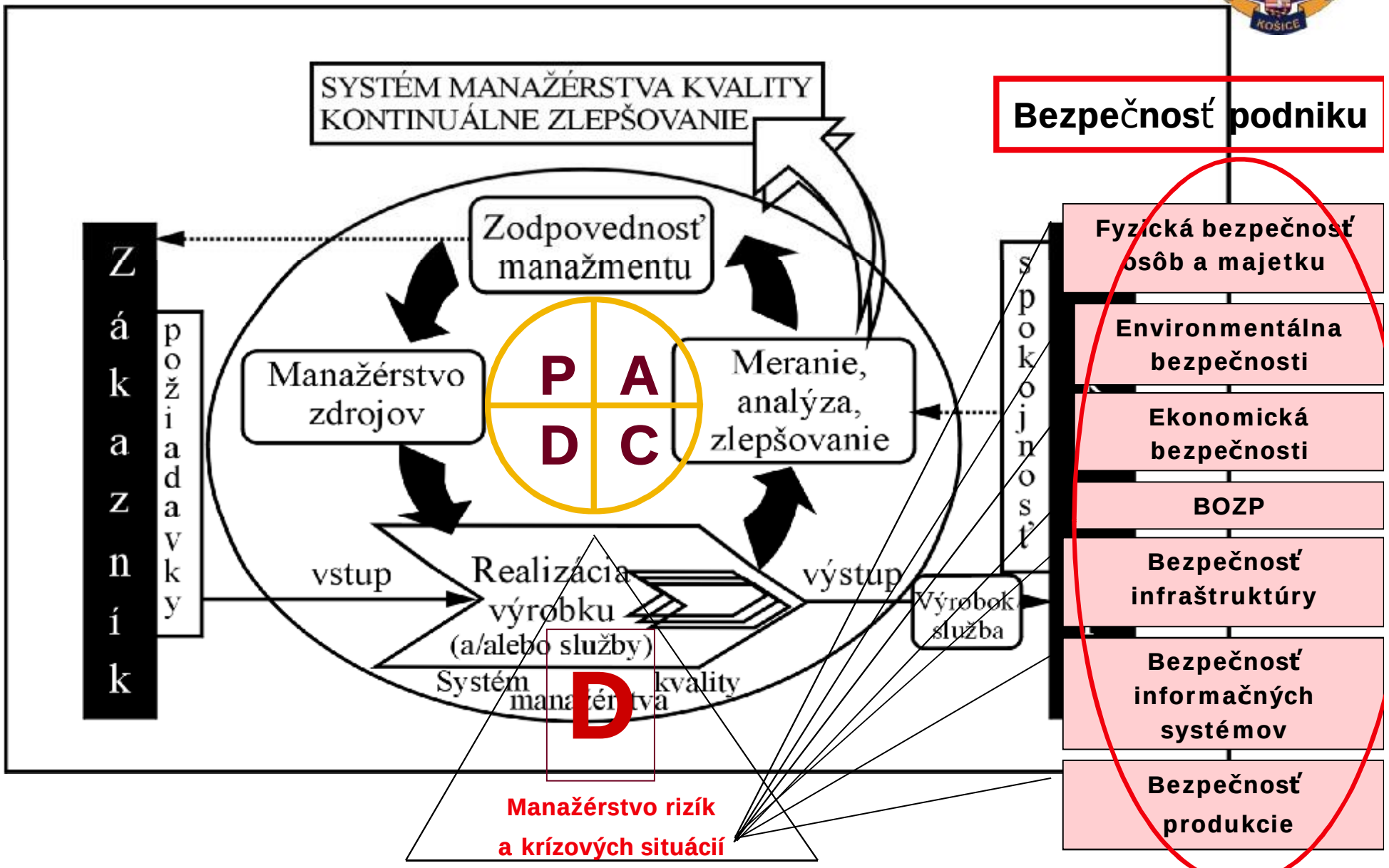
- Podstata hodnotenia výrobkov je v porovnávaní skutočného výrobku s predstavou akéhosi optima kvality, alebo s normou. Do úvahy sa berú všetky parametre, vrátane parametrov spoľahlivosti.
- Ak máme stanovené ukazovatele jednotlivých hodnotených vlastností , môžeme si vypočítať súhrnný ukazovateľ kvality

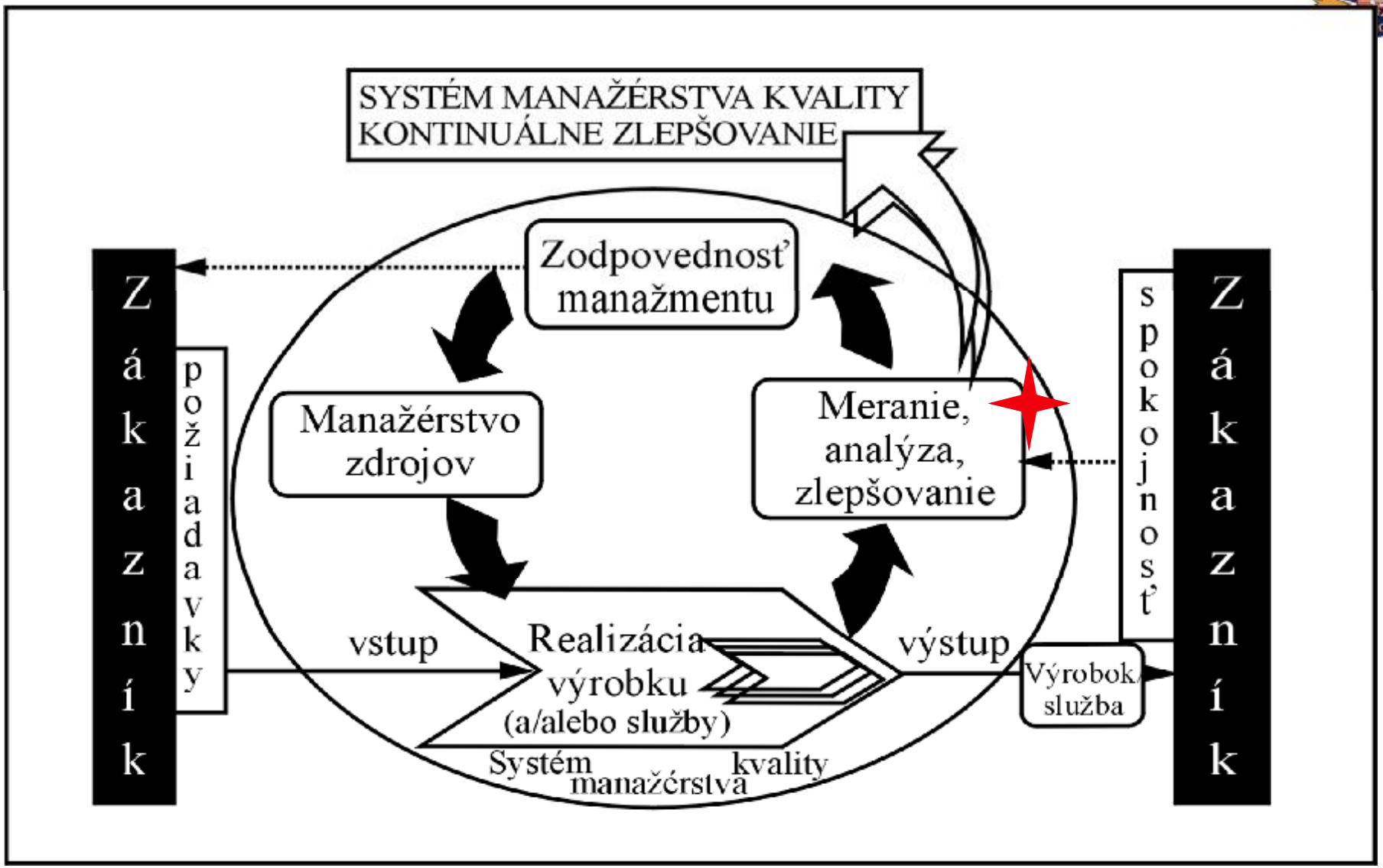
$$Q_\Sigma = \Sigma\, q_i \,.\, Q_i$$

kde Q_i – jednotlivý ukazovateľ (napr. spoľahlivosť, bezpečnosť, presnosť, výkonnosť,...)

q_i - váha i-tej vlastnosti, pričom $\Sigma\, q_i = 1$

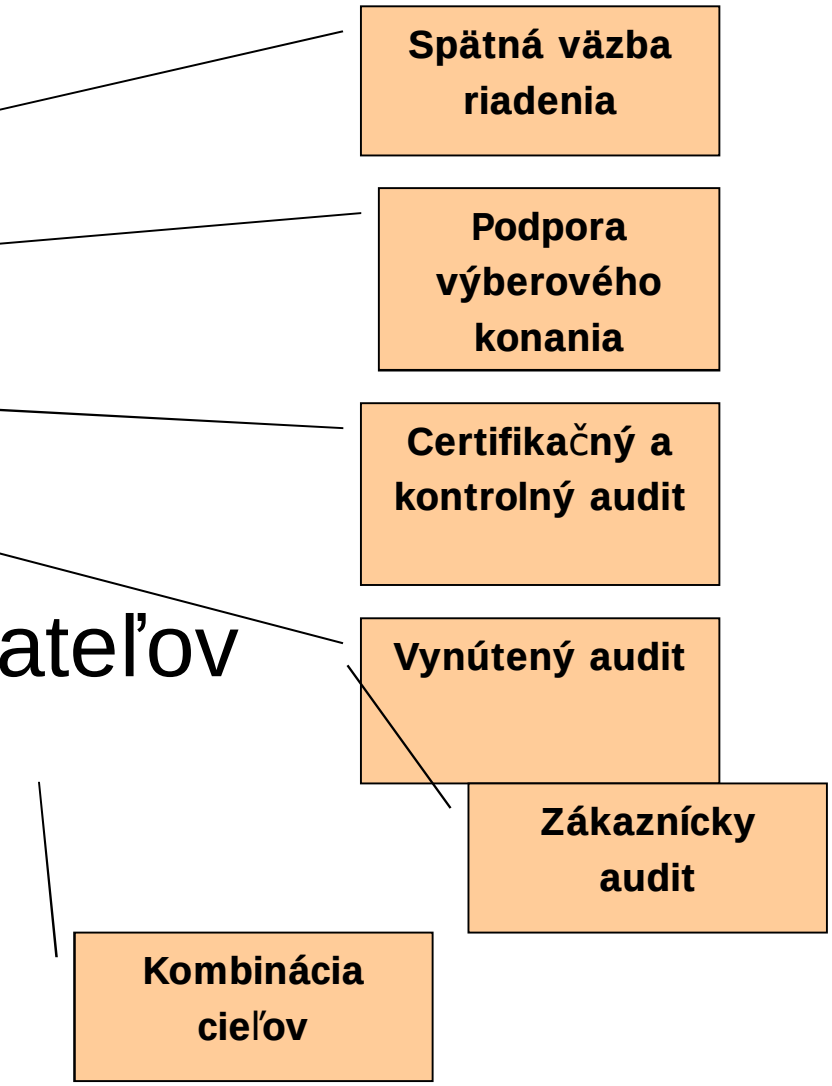
Generický Manažérsky Systém




SYSTÉM MANAŽÉRSTVA KVALITY
KONTINUÁLNE ZLEPŠOVANIE
Zákazník
požiadavky
Zodpovednosť manažmentu
Manažérstvo zdrojov
Meranie, analýza, zlepšovanie
spokojnosť
Zákazník
vstup
Realizácia výrobku (a/alebo služby)
výstup
Výrobok/ služba
Systém manažérstva kvality

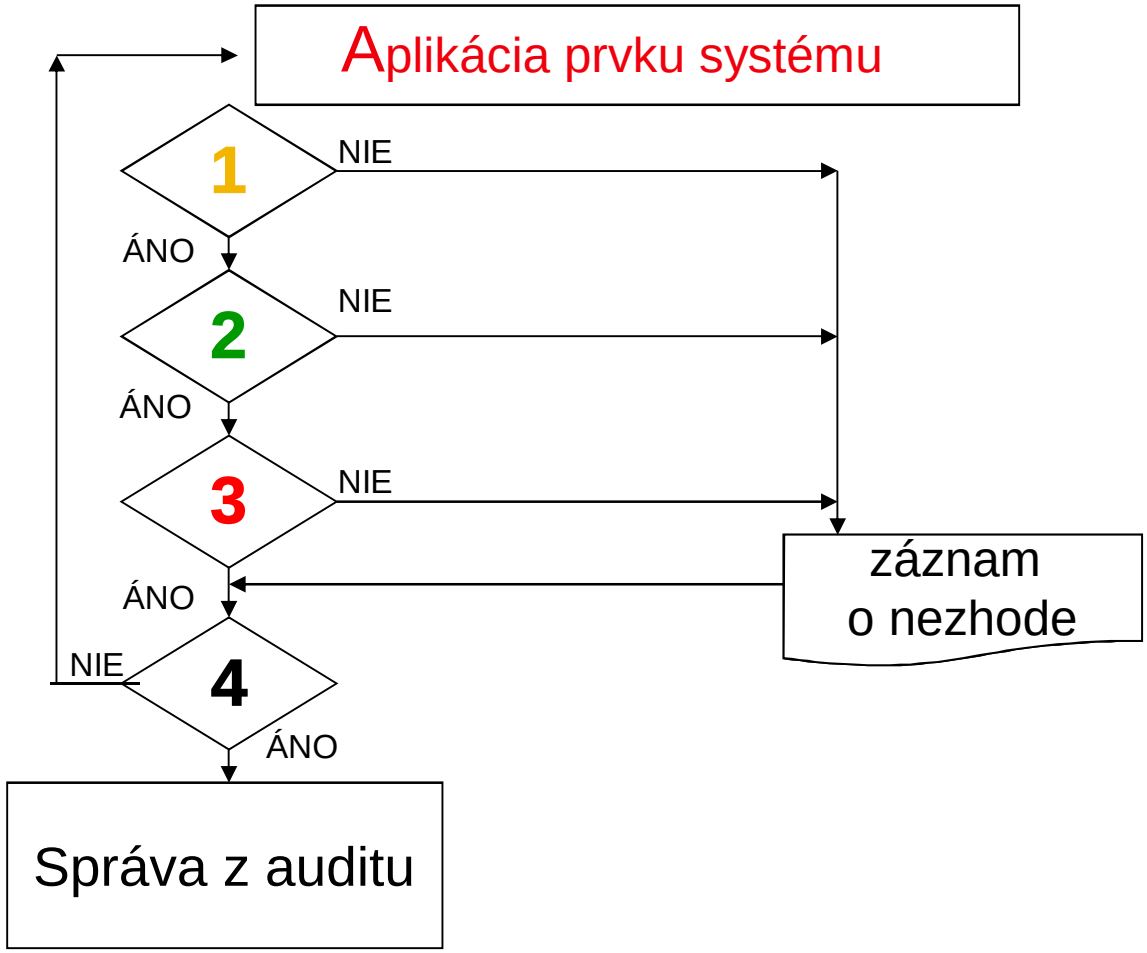
Ciele auditu

- Priority manažmentu
- Komerčné záujmy
- Požiadavky systému
- Požiadavky zákazníka
- Potreby hodnotenia dodávateľov
- Iné požiadavky a potreby



Proces auditovania (logika)

1. Existencia dokumentácie
2. Prijateľnosť
3. Zhoda a prax
4. Kompletnosť



Koniec