

Název projektu:	<b>System automatizované kontroly a detekce změn bezpečnostního nastavení informačních systémů založený na specifikaci bezpečnostní politiky podle standardu BS7799</b>
Číslo projektu:	<b>1F43D/007/030</b>

Název zprávy:	<b>Roční zpráva</b>
Název části:	<b>Část 2 ze dvou částí Dodatky</b>
Období:	<b>1.4.2004-31.12.2004</b>

Poskytovatel:	<b>Ministerstvo dopravy ČR</b>
Příjemce:	<b>WAK System, spol. s r.o.</b>
Adresa příjemce	<b>Petržilkova 2564/21, 158 00 Praha 5 - Stodůlky</b>

Odpovědný řešitel:	<b>Ing. Radan Kasal</b>
Spoluřešitelé:	<b>Ing. Luděk Benda</b>
	<b>Ing. Tomáš Nagy</b>
	<b>Ing. Petr Půlpán</b>
	<b>Radek Valeš</b>
	<b>RNDr. Miroslav Wasserbauer</b>
	<b>Ing. Vítězslav Života</b>

Datum vydání:	<b>31.1.2005</b>
---------------	------------------



# Dodatek A. - Analýza domény IS

## A.1 Shromážděné podklady k doméně

### A.1.1 Literatura k doméně

Literatura k doméně obsahuje popis jednotlivých komponent domény včetně detailů. V seznamu literatury jsou to položky:

- Tripwire, Inc., firemní WWW stránky [online] [3],
- Bezpečnost informačních systémů [10],
- Analytická zpráva projektu Plán rozvoje pro zavádění služeb inteligentních dopravních systémů s vazbou na výkon státní správy [online] [12],
- MSDN for Visual Studio .NET [CD] [15],
- .NET Framework programování aplikací [16].

### A.1.2 Legislativa k doméně

Legislativa k doméně obsahuje zákonné normy a legislativní předpisy se vztahem k řešení projektu. V seznamu literatury jsou to položky:

- BS ISO/IEC 17799:2000 Překlad a interpretace normy pro české prostředí [1],
- BS 7799-2:2002 Překlad a interpretace normy pro české prostředí [2],
- 365/2000 Sb. Zákon ze dne 14.zář 2000 [8],
- Věstník MI, ročník 1, částka 1 [9],
- Bezpečnost informačních systémů [10].

### A.1.3 Standardy k doméně

Standardy k doméně je literatura, která obsahuje prostředky sloužící jak k popisu řešení, tak i k formální úpravě výstupní dokumentace. V seznamu literatury jsou to položky:

- Standard ISVS 005/02.01 pro náležitosti životního cyklu informačního systému [4],
- Informační technologie - Procesy v životním cyklu softwaru [5],

- Unified Modeling Language Specification, UML™ Resource Page [online] [6],
- UML a unifikovaný proces vývoje aplikací [7],
- Myslíme v jazyku UML [13],
- Systémové inženýrství – Procesy životního cyklu systému [14],
- ČSN ISO 5966 [18],

Normy diplomových prací - FF UP [19].

## **A.1.4 Rešerše vybraných podkladů**

V této kapitole se popisuje obsah nejdůležitějších podkladů.

### **A.1.4.1 BS ISO/IEC 17799:2000<sup>[1]</sup>:**

Překlad britské normy, která obsahuje seznam obecných opatření pro zajištění bezpečnosti informačních systémů. Norma je základem pro certifikaci informačních systémů podle mezinárodní normy ISO 17799.

### **A.1.4.2 BS 7799-2:2002<sup>[2]</sup>**

Překlad druhé části britské normy BS 7799-2:2002. Slouží jako konkrétní podklad pro vytvoření bezpečnostního auditu informačního systému. Seznam opatření je rozdělen do 10 oblastí, které poskytují doporučení a návod pro zavedení nejlepších opatření.

### **A.1.4.3 Myslíme v jazyku UML<sup>[13]</sup>:**

Příručka pro modelování obecných systémů, jejich analýzy pomocí diagramů jazyka UML a zpracování standardizované dokumentace. Obsahuje postup formální analýzy a vyjádření jednotlivých kroků v UML formátu.

### **A.1.4.4 MSDN for Visual Studio .NET [CD]<sup>[15]</sup>**

Originální dokumentace pro informační systémy založené na platformě Windows, obsahuje všechny informace potřebné k popisu systému.

### **A.1.4.5 .NET Framework programování aplikací<sup>[16]</sup>**

Podrobný popis programovacího prostředí .NET, prostředí a postup tvorby aplikací.

### **A.1.4.6 The Unified Software Development Process<sup>[17]</sup>:**

Originální podrobný popis standardu UML v nejnovější verzi. Obsahuje obecný postup analýzy projektu, tvorbu dokumentace a návrh softwarového řešení.

## A.2 Analýza současného stavu řešení v doméně

### A.2.1 Přehled současných řešení

Pro klasifikaci řešení v doméně bylo stávající řešení rozděleno na šest kategorií podle zadání projektu. Jsou to:

- nastavování a kontrola přístupových práv,
- kontrola přístupu do systému,
- kontrola integrity souborů a klíčů,
- detekce změn v běžících službách systému,
- analýza systémového logu a upozornění na typ události,
- nastavení dané bezpečnostní politiky podle standardu BS 7799.

#### A.2.1.1 Nastavování a kontrola přístupových práv.

Práci s přístupovými právy řeší v první řadě operační systém jako takový, může se lišit podle verze OS. Obecně se správa zabezpečení nachází v systémech platformy Windows v ovládacích panelech, ke kterým má přístup administrátor systému. Pod názvem Uživatelé a hesla (u Windows 2000, u dalších systémů platformy Windows stejný nebo podobný název). Zde lze pak jednotlivým uživatelům nebo jejich skupinám přiřazovat potřebná přístupová práva k různým částem systému.

Pro tuto práci lze najít i některé další programy (i volně šiřitelné programy), ale nástroje OS lze považovat jako dostačující.

#### A.2.1.2 Kontrola přístupu do systému.

Přístup do systému se kontroluje pomocí některého typu firewallu nebo software s podobným zaměřením. Od verze Windows XP je součástí systému, u předchozích verzí je nutné použít instalaci jiného produktu. Jako příklad je možné jmenovat Sygate Personal Firewall od firmy Sygate.

Principem je zamezení přístupu do systému nepovolaným účastníkům a dále monitorování pokusů o přístup (i neúspěšných) s možností je povolovat či zakazovat. Také lze nastavit např. filtrování na určitý typ IP adres hlavně při přístupu z veřejné sítě a další možnosti pro zabezpečení.

#### A.2.1.3 Kontrola integrity souborů a klíčů.

Kontrola integrity se obecně provádí některým z nástrojů, které mohou generovat kontrolní součet souboru a porovnávat ho s ověřeným vzorem.

Jako jednoduchý příklad takového software je zvolen SecExMD5+ firmy Bytefusion Ltd. Slouží hlavně ke generování kontrolního součtu vybraného souboru podle třech standardů, které jsou používány nejčastěji. Jsou to MD5, SHA-1 a RIPEMD-160. Každý pokus třetí strany manipulovat s daným souborem trvale změní jeho kontrolní součet, takže při zpětném porovnání je vnější zásah snadno rozpoznatelný.

Pro správu a kontrolu registrů je ve Windows integrovaný nástroj regedit, z ostatních volně dostupných lze jmenovat Registry Monitor ze serveru [www.sysinternals.com](http://www.sysinternals.com).

Kontrolou integrity registrů je míněno konzistentnost jejich obsahu a množství v jednotlivých složkách.

#### **A.2.1.4 Detekce změn v běžících službách systému.**

K monitorování běžících procesů systému slouží buď ve Windows zabudovaný Správce úloh nebo další volně dostupný nebo komerční software. Jako příklad lze jmenovat Process Explorer ze serveru [www.sysinternals.com](http://www.sysinternals.com).

Detekce změn se bude sledovat jako změny v množství spuštěných služeb, změny názvu, změny stavu, apod.

#### **A.2.1.5 Analýza systémového logu a upozornění na typ události.**

Pro prohlížení systémového logu slouží ve Windows zabudovaný Prohlížeč událostí. Z dalších software lze jmenovat PsLogList ze serveru [www.sysinternals.com](http://www.sysinternals.com). Jejich funkce spočívá ve sběru systémových událostí a jejich ukládání do příslušného logu, jejich zobrazení a možnosti prohlížení se tříděním a filtrací.

Analýza a upozornění bude probíhat s ohledem na nastavené typy událostí, které budou detekovány a automaticky jak předávány uživateli dohodnutým způsobem, tak i zaznamenávány.

#### **A.2.1.6 Nastavení dané bezpečnostní politiky podle standardu BS 7799.**

Nastavení se provádí podle požadavků normy BS 7799, dále jen [2] a existují softwarové produkty, které dovolují nastavit bezpečnostní politiku. Jako příklad lze jmenovat komerční software Tripwire for servers firmy Tripwire, který umožňuje nastavit bezpečnostní politiku systému. Dále má mnoho možností kontroly a monitorování systému, umožňuje monitorovat stav systémových souborů a porovnávat je s předem definovaným korektním stavem. Na platformě Windows dokáže monitorovat přidané, smazané a změněné klíče registrů a jejich hodnoty, identifikovat zdroj změn, dokáže monitorovat přidané, smazané a změněné soubory a další související data. Dovoluje nastavit i bezpečnostní politiku, chybí přímá podpora normy [2].

Pro kontrolu systému podle normy [2] existují softwarová řešení, která kontrolují splnění daných požadavků formou bezpečnostního auditu. Podporují i tvorbu dokumentace tohoto auditu. Součástí bývá znalostní databáze možných krizových situací a reakcí na ně. Příkladem může být software COBRA BS 7799 Consultant.

Norma [2] obsahuje obecný soupis požadavků pro ustanovení, provozování a monitoring ISMS. Pro správnou funkci bezpečného systému odpovídající této normě je třeba jednotlivé body aplikovat do výsledného produktu vytvořením takové bezpečnostní politiky, která odpovídá odstavci 4 normy [2] a následně i odstavcům 5, 6 a 7.

## A.2.2 Závěry ke stavu řešení

V doméně existují řešení, která částečně řeší jednotlivé požadavky projektu. Pro naše účely bude pak optimální takový produkt, který splňuje všechny tyto požadavky najednou. Nejlépe se požadavkům přibližuje software Tripwire for servers firmy Tripwire (viz bod 6. v části A.2.1).

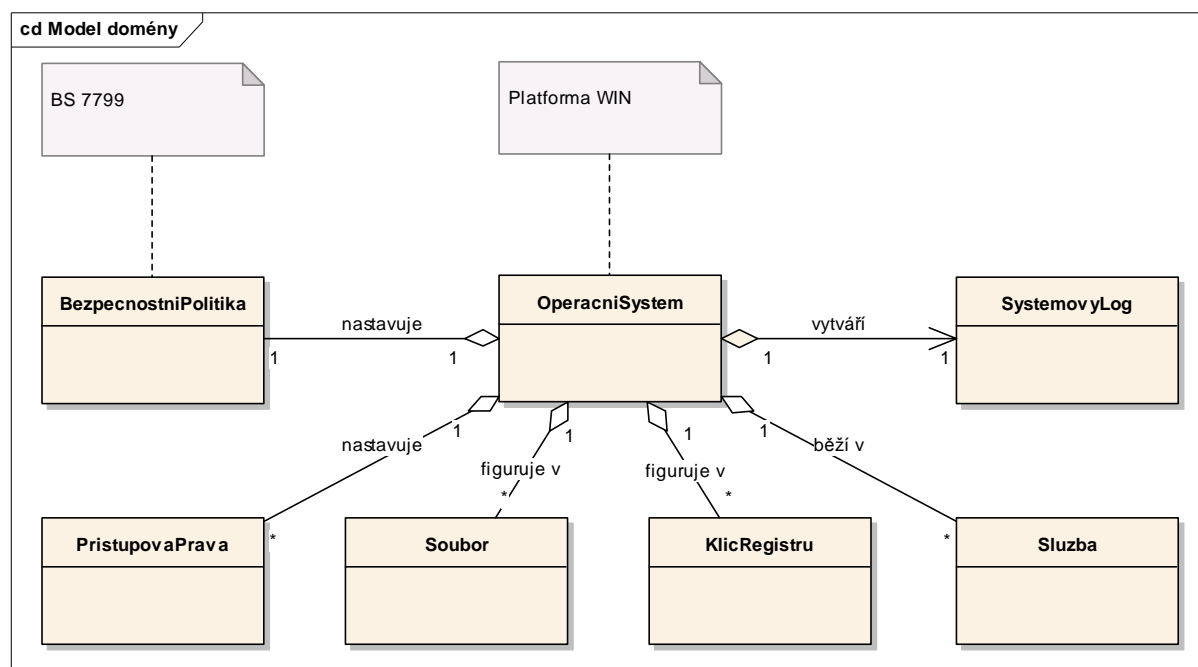
Kompletnímu souboru požadavků projektu nevyhovuje žádné softwarové řešení, které bylo v rámci projektu zkoumáno.

## A.3 Model domény

Pro statický model domény je třeba určit hlavní třídy, tj. části systému, kterých se bude řešení týkat. V první fázi se jedná o nastavení bezpečnostních parametrů systému podle předem definované **bezpečnostní politiky**. Ta bude určena standardem [2].

Bezpečnostní parametry systému jsou vlastnosti jednotlivých součástí systému, jež ovlivňují bezpečnost systému. Mezi takové součásti systému počítáme **služby** systému (především běžící), systémové **soubory**, případně další důležité nesystémové soubory, **klíče registru** a veškerá **přístupová práva** (práva uživatelů, skupiny uživatelů, práva na jednotlivé soubory i adresáře, atd.). Veškeré důležité události systému se pak uchovávají v **systémovém a bezpečnostním logu**.

Podle tohoto popisu lze vytvořit základní statický model domény. Jeho obrázek je uveden.



Obr. 1 Statický model domény

## A.4 Procesy v doméně

Seznam základních procesů v doméně vyplývá z Obr.1:

- Nastavovat
- Běžet
- Vytvářet
- Figurovat

Zde je pak popis, který popisuje chování domény, a tím i smysl jednotlivých procesů.

Bezpečnostní politika založená na BS 7799 obsahuje bezpečnostní parametry, které **nastavují** OS. Služby systému **běží** v rámci OS. Ten obsahuje systémové a další soubory a dále pak klíče registru (**figuruje v** OS). Přístupová práva nastavují OS z hlediska omezení přístupů k určitým jeho částem. OS pak **vytváří** všechny systémové výstupy, tj. chyby, nepravdivosti a další informace do systémového a dalších logů.

## A.5 Třídy domény

Stručný popis jednotlivých tříd statického modelu domény.

- **Bezpečnostní politika:** souhrn všech bezpečnostních parametrů, které nastavují systém. Podle nich je stanovena míra zabezpečení dalších součástí systému proti chybám, proti působení škodlivého software a dalším podobným vlivům.

- **Služba:** jde především o vybrané běžící služby systému. Ty mají přímý vliv na stabilitu a správnou funkci systému.
- **Soubor:** jedná se především o systémové soubory a dále pak o další vybrané sledované soubory. Sledovat se budou především změny v souborech, změny ve výskytu souborů samotných a také jejich integrita.
- **Klíč registru:** jedná se o vybrané klíče registru. Sledovat se budou jednak změny jejich nastavení, případně absence. Integritu jako takovou hlídá samotný OS a v případě potřeby obnovuje stav ze záložní sady klíčů.
- **Přístupová práva:** sledování práv skupin i jednotlivých uživatelů. Práva se týkají vybraných souborů, adresářů, služeb systému a registrů.
- **Systémový log:** soubory obsahující výsledky běžících služeb, výsledky spuštěného software, zaznamenané chyby systému i aplikací, atd.



## Dodatek B. - Systémové požadavky IS

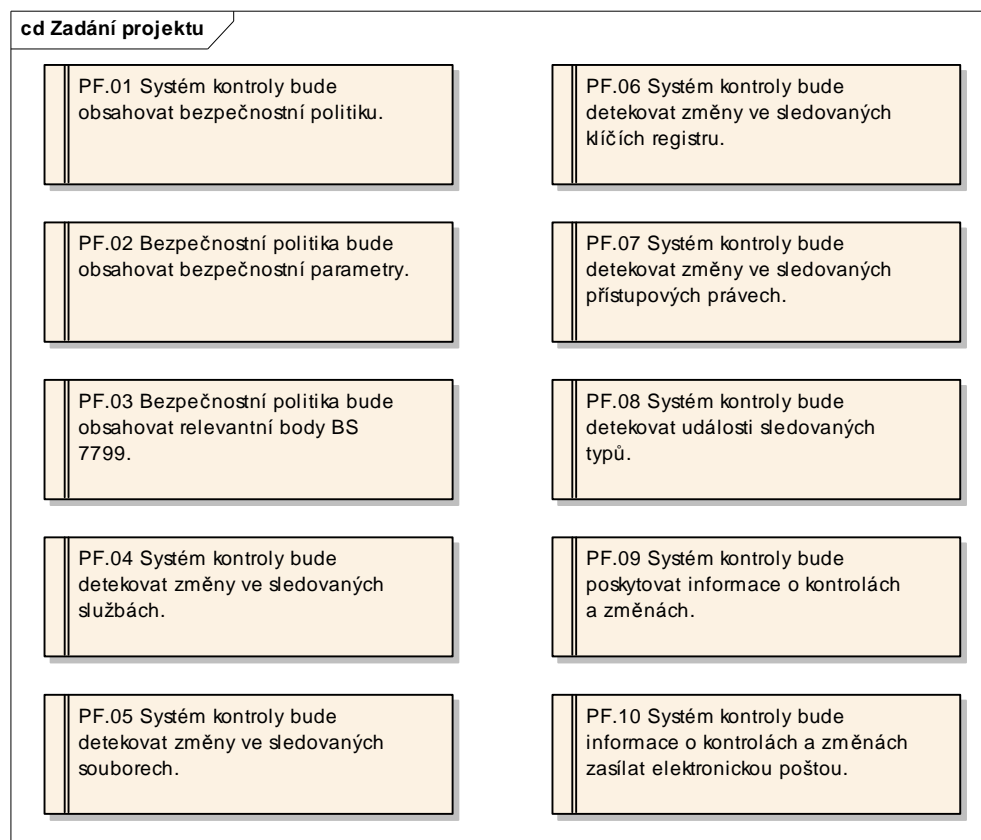
Požadavky projektu se dělí do dvou kategorií - funkční, které mají přímý vliv na funkce systému kontroly a nefunkční (doplňkové), které určují hranice výsledného řešení.

### B.1 Funkční požadavky

Funkční požadavky se dále dělí na požadavky, které vznikly na základě zadání projektu, a požadavky, které je přirozeně doplňují na základě další analýzy.

#### B.1.1 Zadání projektu

Seznam funkčních požadavků vyplývajících ze zadání.



Obr. 2 Zadání projektu

**PF.01 Systém kontroly bude obsahovat bezpečnostní politiku.**

Bezpečnostní politika je souhrn obecných zásad stanovených bezpečnostním správcem a seznam bezpečnostních parametrů.

Vazba	Případ užití	Požadavek
Realizace	Výběr relevantních bodů z BS 7799	PF.01 Systém kontroly bude obsahovat bezpečnostní politiku.
Realizace	Vytvoření bezpečnostní politiky	PF.01 Systém kontroly bude obsahovat bezpečnostní politiku.
Realizace	Určení bezpečnostních parametrů	PF.01 Systém kontroly bude obsahovat bezpečnostní politiku.

**Tab. 1 Vazby PF.01 Systém kontroly bude obsahovat bezpečnostní politiku.**

**PF.02 Bezpečnostní politika bude obsahovat bezpečnostní parametry.**

Bezpečnostní parametry reprezentují seznam všech elementů operačního systému, u kterých se sledují jejich změny a jsou definována jejich správná nastavení.

Vazba	Případ užití	Cíl
Realizace	Určení bezpečnostních parametrů	PF.02 Bezpečnostní politika bude obsahovat bezpečnostní parametry.

**Tab. 2 Vazby PF.02 Bezpečnostní politika bude obsahovat bezpečnostní parametry.**

**PF.03 Bezpečnostní politika bude obsahovat relevantní body BS 7799.**

Bezpečnostní správce vybere z normy BS 7799 body, které mají vztah k systému kontroly a uvede je jako součást bezpečnostní politiky.

Vazba	Případ užití	Požadavek
Realizace	Výběr relevantních bodů z BS 7799	PF.03 Bezpečnostní politika bude obsahovat relevantní body BS 7799.

**Tab. 3 Vazby PF.03 Bezpečnostní politika bude obsahovat relevantní body BS 7799.**

**PF.04 Systém kontroly bude detekovat změny ve sledovaných službách.**

Automaticky nebo na vyžádání se porovnají obrazy služeb a jejich aktuální stav. Porovnání se týká zejména počtu, stavu, jména a nastavení. Při změně bude vytvořen záznam v příslušné tabulce a podle nastavení systému vydáno upozornění.

Vazba	Případ užití	Požadavek
Realizace	Detekce změn v běžících službách	PF.04 Systém kontroly bude detekovat změny ve sledovaných službách.

**Tab. 4 Vazby PF.04 Systém kontroly bude detekovat změny ve sledovaných službách.**

**PF.05 Systém kontroly bude detekovat změny ve sledovaných souborech.**

Automaticky nebo na vyžádání se porovnají obrazy souborů a jejich aktuální stav. Porovnání se týká zejména integrity (kontrolní součet), stavu a jména. Při změně bude vytvořen záznam v příslušné tabulce a podle nastavení systému vydáno upozornění.

Vazba	Případ užití	Požadavek
Realizace	Detekce změn v souborech	PF.05 Systém kontroly bude detekovat změny ve sledovaných souborech.

Tab. 5 Vazby PF.05 Systém kontroly bude detekovat změny ve sledovaných souborech.

**PF.06 Systém kontroly bude detekovat změny ve sledovaných klíích registru.**

Automaticky nebo na vyžádání se porovnají obrazy klíčů registru a jejich aktuální stav. Porovnání se týká zejména počtu, jména a nastavení. Při změně bude vytvořen záznam v příslušné tabulce a podle nastavení systému vydáno upozornění.

Vazba	Případ užití	Požadavek
Realizace	Detekce změn v klíích registru	PF.06 Systém kontroly bude detekovat změny ve sledovaných klíích registru.

Tab. 6 Vazby PF.06 Systém kontroly bude detekovat změny ve sledovaných klíích registru.

**PF.07 Systém kontroly bude detekovat změny ve sledovaných přístupových právech.**

Automaticky nebo na vyžádání se porovnají obrazy přístupových práv a jejich aktuální stav. Porovnání se týká zejména počtu uživatelů, jmen a nastavení práv. Při změně bude vytvořen záznam v příslušné tabulce a podle nastavení systému vydáno upozornění.

Vazba	Případ užití	Požadavek
Realizace	Detekce změn v přístupových právech	PF.07 Systém kontroly bude detekovat změny ve sledovaných přístupových právech.

Tab. 7 Vazby PF.07 Systém kontroly bude detekovat změny ve sledovaných přístupových právech.

**PF.08 Systém kontroly bude detekovat události sledovaných typů.**

Podle seznamu podmínek pro vyhledání událostí bude sledován výskyt událostí těchto typů. Při výskytu bude vytvořen záznam v příslušné tabulce a podle nastavení systému vydáno upozornění.

Vazba	Případ užití	Požadavek
Realizace	Detekce událostí podle nastavení	PF.08 Systém kontroly bude detekovat události sledovaných typů.

Tab. 8 Vazby PF.08 Systém kontroly bude detekovat události sledovaných typů.

**PF.09 Systém kontroly bude poskytovat informace o kontrolách a změnách.**

Systém kontroly bude upozorňovat uživatele na stanovené výstupy kontrol a změn. Množství a typ výstupů bude možné ovlivnit v nastavení systému kontroly.

Vazba	Případ užití	Požadavek
Realizace	Vytvoření výstupu podle nastavení	PF.09 Systém kontroly bude poskytovat informace o kontrolách a změnách.

**Tab. 9 Vazby PF.09 Systém kontroly bude poskytovat informace o kontrolách a změnách.**

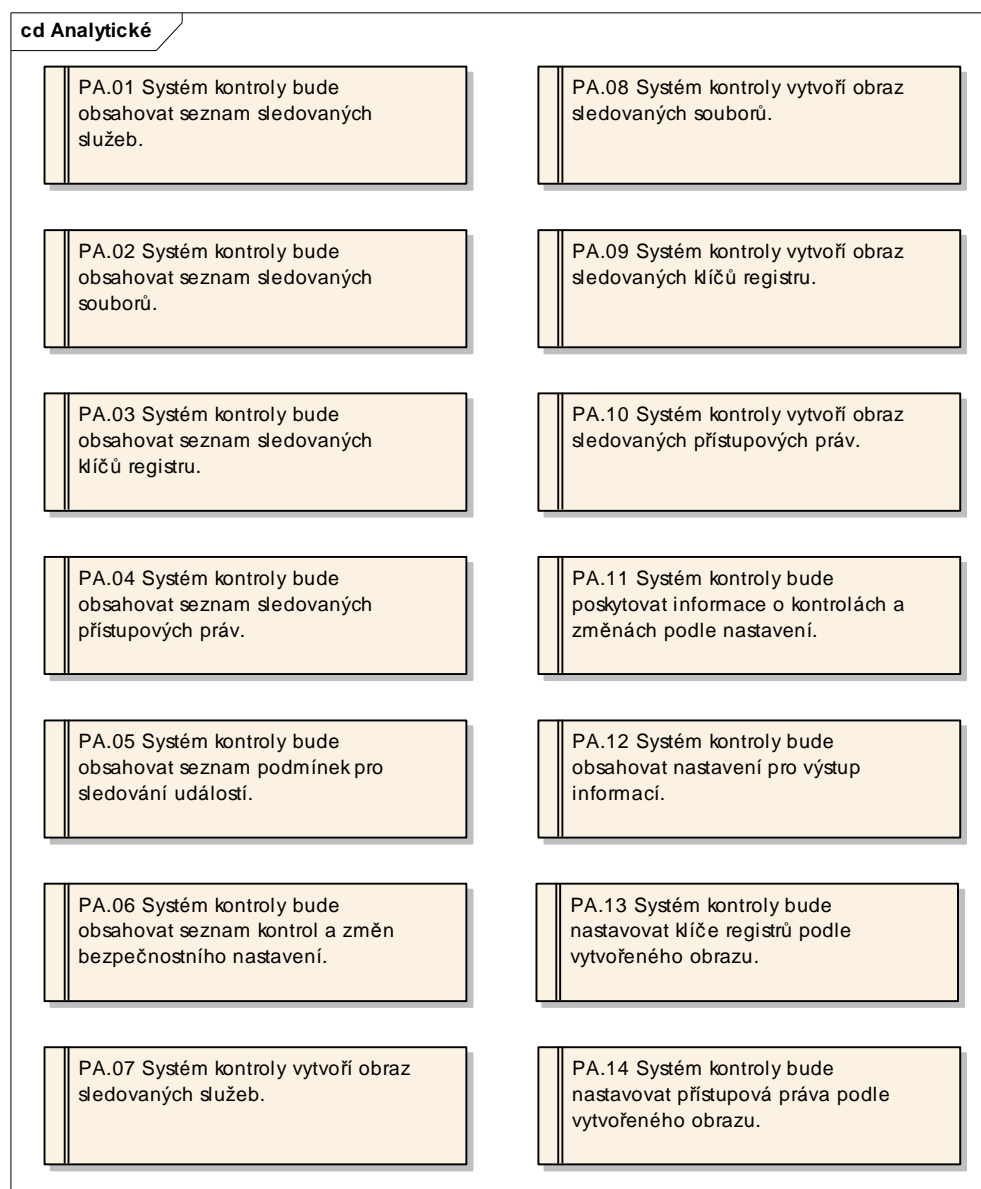
**PF.10 Systém kontroly bude informace o kontrolách a změnách zasílat elektronickou poštou.**

Všechny záznamy generované funkcí PFF.13 se budou podle nastavení předávat do poštovního klienta a následně zasílány na dané adresy.

Vazba	Případ užití	Požadavek
Realizace	Nastavení výstupu	PF.10 Systém kontroly bude informace o kontrolách a změnách zasílat elektronickou poštou.
Realizace	Vytvoření výstupu podle nastavení	PF.10 Systém kontroly bude informace o kontrolách a změnách zasílat elektronickou poštou.

**Tab. 10 Vazby PF.10 Systém kontroly bude informace o kontrolách a změnách zasílat elektronickou poštou.**

## B.1.2 Analytické



Obr. 3 Analytické

### PA.01 Systém kontroly bude obsahovat seznam sledovaných služeb.

Správce systému kontroly určí služby, které se budou sledovat. Každý záznam obsahuje parametry, které určují správné nastavení.

Vazba	Případ užití	Požadavek
Realizace	Stanovení seznamu sledovaných služeb	PA.01 Systém kontroly bude obsahovat seznam sledovaných služeb.

Tab. 11 Vazby PA.01 Systém kontroly bude obsahovat seznam sledovaných služeb.

**PA.02 Systém kontroly bude obsahovat seznam sledovaných souborů.**

Správce systému kontroly určí soubory, které se budou sledovat. Každý záznam obsahuje parametry, které se budou ověřovat (např. kontrolní součet kvůli integritě).

Vazba	Případ užití	Požadavek
Realizace	Stanovení seznamu sledovaných souborů	PA.02 Systém kontroly bude obsahovat seznam sledovaných souborů.

Tab. 12 Vazby PA.02 Systém kontroly bude obsahovat seznam sledovaných souborů.

**PA.03 Systém kontroly bude obsahovat seznam sledovaných klíčů registru.**

Správce systému kontroly určí klíče registru, které se budou sledovat. Každý záznam obsahuje parametry, které určují správné nastavení.

Vazba	Případ užití	Požadavek
Realizace	Stanovení seznamu sledovaných klíčů registru	PA.03 Systém kontroly bude obsahovat seznam sledovaných klíčů registru.

Tab. 13 Vazby PA.03 Systém kontroly bude obsahovat seznam sledovaných klíčů registru.

**PA.04 Systém kontroly bude obsahovat seznam sledovaných přístupových práv.**

Správce systému kontroly určí nastavení přístupových práv, které se budou sledovat. Každý záznam obsahuje parametry, které určují správné nastavení.

Vazba	Případ užití	Požadavek
Realizace	Stanovení seznamu sledovaných přístupových práv	PA.04 Systém kontroly bude obsahovat seznam sledovaných přístupových práv.

Tab. 14 Vazby PA.04 Systém kontroly bude obsahovat seznam sledovaných přístupových práv.

**PA.05 Systém kontroly bude obsahovat seznam podmínek pro sledování událostí.**

Správce systému kontroly určí podmínky pro sledované události, které se budou sledovat.

Vazba	Případ užití	Požadavek
Realizace	Stanovení podmínek pro sledování událostí	PA.05 Systém kontroly bude obsahovat seznam podmínek pro sledování událostí.

Tab. 15 Vazby PA.05 Systém kontroly bude obsahovat seznam podmínek pro sledování událostí.

**PA.06 Systém kontroly bude obsahovat seznam kontrol a změn bezpečnostního nastavení.**

Každý výsledek kontroly a každá změna v bezpečnostním nastavení budou zaznamenány do databáze s popisem této události a dalšími potřebnými identifikačními prvky.

Vazba	Případ užití	Požadavek
Realizace	Vytvoření výstupu podle nastavení	PA.06 Systém kontroly bude obsahovat seznam kontrol a změn bezpečnostního nastavení.

Tab. 16 Vazby PA.06 Systém kontroly bude obsahovat seznam kontrol a změn bezpečnostního nastavení.

**PA.07 Systém kontroly vytvoří obraz sledovaných služeb.**

Podle seznamu sledovaných služeb budou načteny výchozí (korektní) parametry. S nimi se pak srovnávají provozní parametry.

Vazba	Případ užití	Požadavek
Realizace	Vytvoření obrazu běžících služeb OS	PA.07 Systém kontroly vytvoří obraz sledovaných služeb.
Realizace	Nastavení parametrů systému kontroly	PA.07 Systém kontroly vytvoří obraz sledovaných služeb.

Tab. 17 Vazby PA.07 Systém kontroly vytvoří obraz sledovaných služeb.

**PA.08 Systém kontroly vytvoří obraz sledovaných souborů.**

Podle seznamu sledovaných souborů budou načteny a vytvořeny výchozí (korektní) parametry. S nimi se pak srovnávají aktuální parametry souborů.

Vazba	Případ užití	Požadavek
Realizace	Vytvoření obrazu souborů OS	PA.08 Systém kontroly vytvoří obraz sledovaných souborů.
Realizace	Nastavení parametrů systému kontroly	PA.08 Systém kontroly vytvoří obraz sledovaných souborů.

Tab. 18 Vazby PA.08 Systém kontroly vytvoří obraz sledovaných souborů.

**PA.09 Systém kontroly vytvoří obraz sledovaných klíčů registru.**

Podle seznamu sledovaných klíčů registrů budou načteny výchozí (korektní) parametry. S nimi se pak srovnávají provozní parametry.

Vazba	Případ užití	Požadavek
Realizace	Nastavení parametrů systému kontroly	PA.09 Systém kontroly vytvoří obraz sledovaných klíčů registru.
Realizace	Vytvoření obrazu klíčů registru OS	PA.09 Systém kontroly vytvoří obraz sledovaných klíčů registru.

Tab. 19 Vazby PA.09 Systém kontroly vytvoří obraz sledovaných klíčů registru.

**PA.10 Systém kontroly vytvoří obraz sledovaných přístupových práv.**

Obraz stávajícího nastavení přístupových práv se uloží při inicializaci systému.

Vazba	Případ užití	Požadavek
Realizace	Vytvoření obrazu přístupových práv	PA.10 Systém kontroly vytvoří obraz sledovaných přístupových práv.
Realizace	Nastavení parametrů systému kontroly	PA.10 Systém kontroly vytvoří obraz sledovaných přístupových práv.

Tab. 20 Vazby PA.10 Systém kontroly vytvoří obraz sledovaných přístupových práv.

**PA.11 Systém kontroly bude poskytovat informace o kontrolách a změnách podle nastavení.**

Výstupy budou poskytovány v množství a typech určených nastavením systému kontroly. Upozornění uživatelů na stanovené výstupy kontrol a změn bude možné změnit.

Vazba	Zdroj	Požadavek
Realizace	Vytvoření výstupu podle nastavení	PA.11 Systém kontroly bude poskytovat informace o kontrolách a změnách podle nastavení.

Tab. 21 Vazby PA.11 Systém kontroly bude poskytovat informace o kontrolách a změnách podle nastavení.

**PA.12 Systém kontroly bude obsahovat nastavení pro výstup informací.**

K dispozici bude několik variant výstupu výsledných údajů s možností uživatelské změny.

Vazba	Případ užití	Požadavek
Realizace	Nastavení výstupu	PA.12 Systém kontroly bude obsahovat nastavení pro výstup informací.

Tab. 22 Vazby PA.12 Systém kontroly bude obsahovat nastavení pro výstup informací.

**PA.13 Systém kontroly bude nastavovat klíče registrů podle vytvořeného obrazu.**

Podle vytvořených obrazů klíčů registru bude na vyžádání provedeno nastavení registrů systému

Vazba	Případ užití	Požadavek
Realizace	Nastavení klíčů registru	PA.13 Systém kontroly bude nastavovat klíče registrů podle vytvořeného obrazu.

Tab. 23 Vazby PA.13 Systém kontroly bude nastavovat klíče registrů podle vytvořeného obrazu.

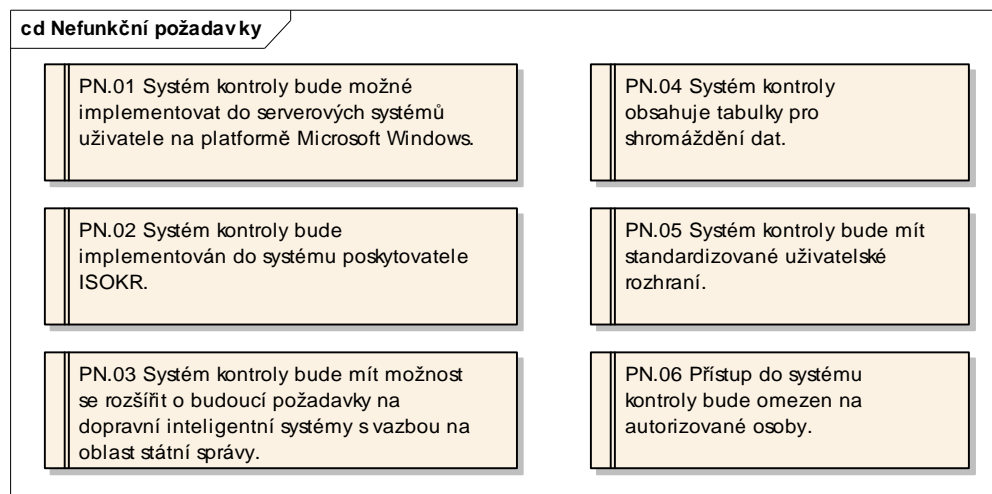
**PA.14 Systém kontroly bude nastavovat přístupová práva podle vytvořeného obrazu.**

Podle vytvořených obrazů přístupových práv bude na vyžádání provedeno nastavení registrů systému

Vazba	Případ užití	Požadavek
Realizace	Nastavení přístupových práv	PA.14 Systém kontroly bude nastavovat přístupová práva podle vytvořeného obrazu.

Tab. 24 Vazby PA.14 Systém kontroly bude nastavovat přístupová práva podle vytvořeného obrazu.

## B.2 Nefunkční požadavky



Obr. 4 Nefunkční požadavky

### **PN.01 Systém kontroly bude možné implementovat do serverových systémů uživatele na platformě Microsoft Windows.**

Požadavek ze zadání projektu. Týká se verze Microsoft Windows NT 4.0, Microsoft Windows 2000, Microsoft Windows XP a Microsoft Windows 2003 Server.

### **PN.02 Systém kontroly bude implementován do systému poskytovatele ISOKR.**

Jako pilotní implementace bude systém kontroly použit v systému ISOKR na Ministerstvu dopravy ČR. ISOKR běží na serveru s operačním systémem Windows NT 4.0.

### **PN.03 Systém kontroly bude mít možnost se rozšířit o budoucí požadavky na dopravní inteligentní systémy s vazbou na oblast státní správy.**

Systém kontroly je závislý na normě BS 7799<sup>[1],[2]</sup>, která určuje hlavní rysy bezpečnosti a spolehlivosti. První část normy byla přijata jako mezinárodní standard ISO 17799, takže tvorba systému kontroly je založena na předpokladu, že legislativní požadavky na podobné systémy (tedy i inteligentní systémy dopravy) budou splňovat požadavky této normy. Samozřejmě může později dojít k odchylkám, resp. dalším specifikacím, a proto je systém koncipován jako otevřený z hlediska úprav vstupních požadavků vycházejících z BS 7799<sup>[2]</sup>.

### **PN.04 Systém kontroly obsahuje tabulky pro shromáždění dat.**

Data budou shromažďována v databázi relačního typu.

### **PN.05 Systém kontroly bude mít standardizované uživatelské rozhraní.**

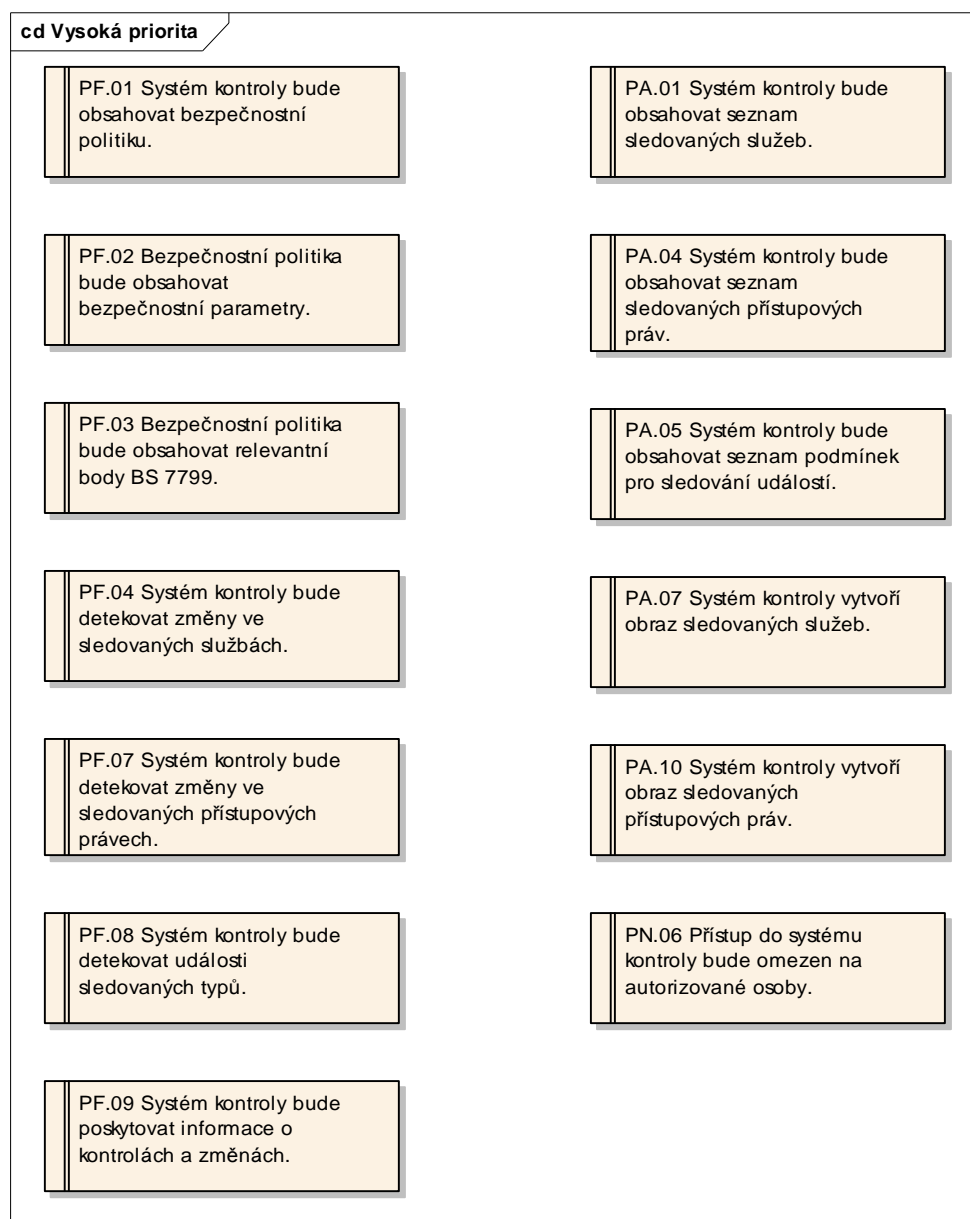
Rozhraní systému kontroly se bude skládat ze standardizovaných softwarových prvků používaných v systémech platformy Windows.

**PN.06 Přístup do systému kontroly bude omezen na autorizované osoby.**

Přístup do systému kontroly bude omezen standardními postupy při autorizaci a autentizaci osob.

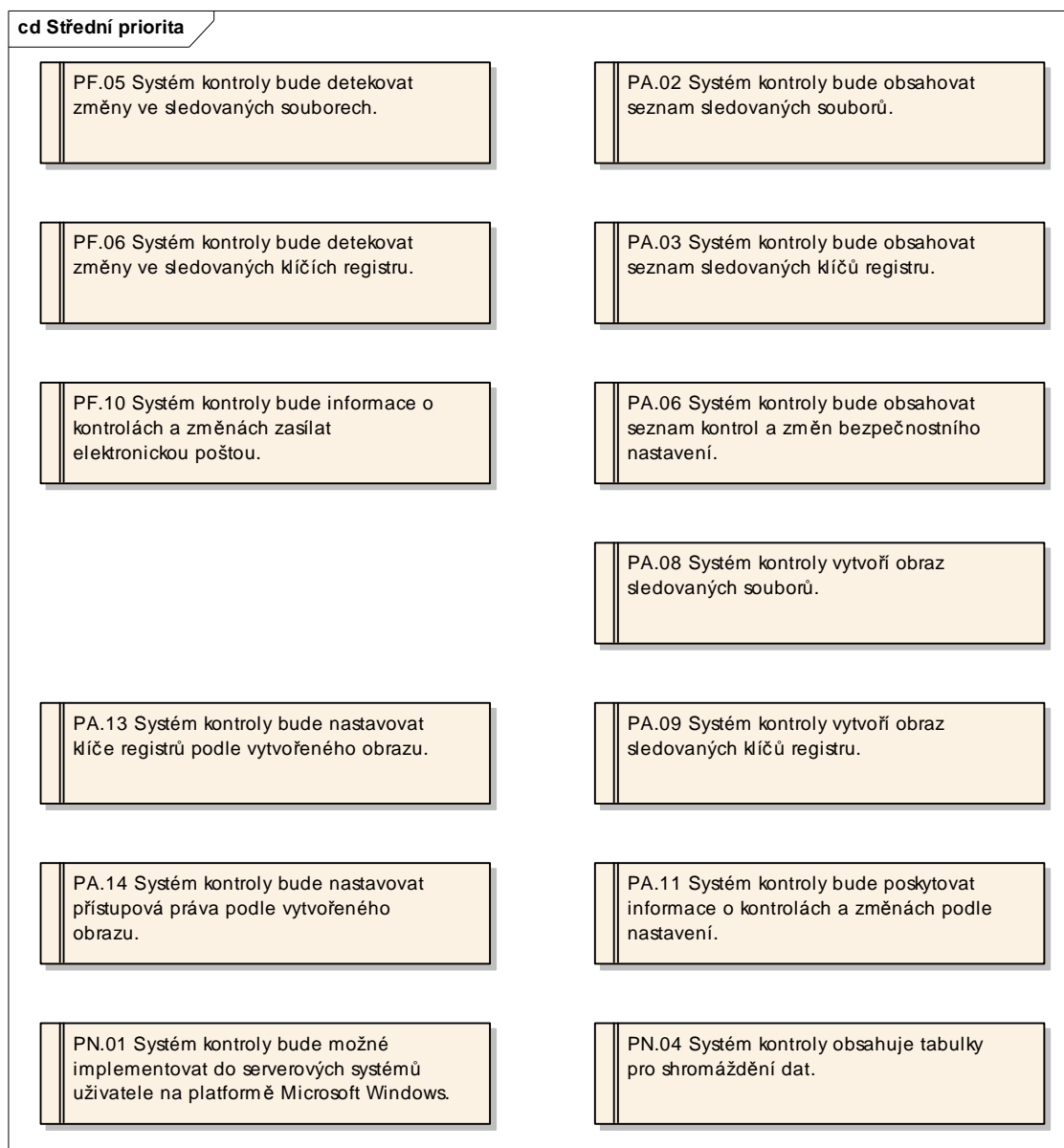
## B.3 Priority požadavků

Požadavky předchozích kapitol byly rozděleny na základě nutnosti implementace do tří kategorií priorit.

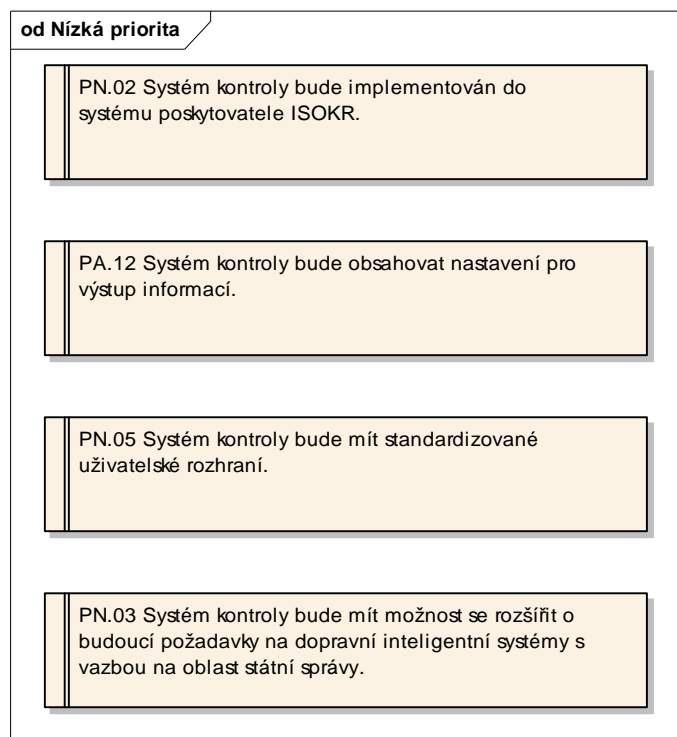


Obr. 5 Vysoká priorita

Vysokou prioritu mají požadavky, které se týkají bezpečnostního nastavení, přístupových práv a přístupů obecně, sledování služeb systému a výskytu událostí stanovených typů.

**Obr. 6 Střední priorita**

Střední prioritu mají ostatní funkční požadavky a nefunkční požadavky týkající se konkrétních omezení systému.

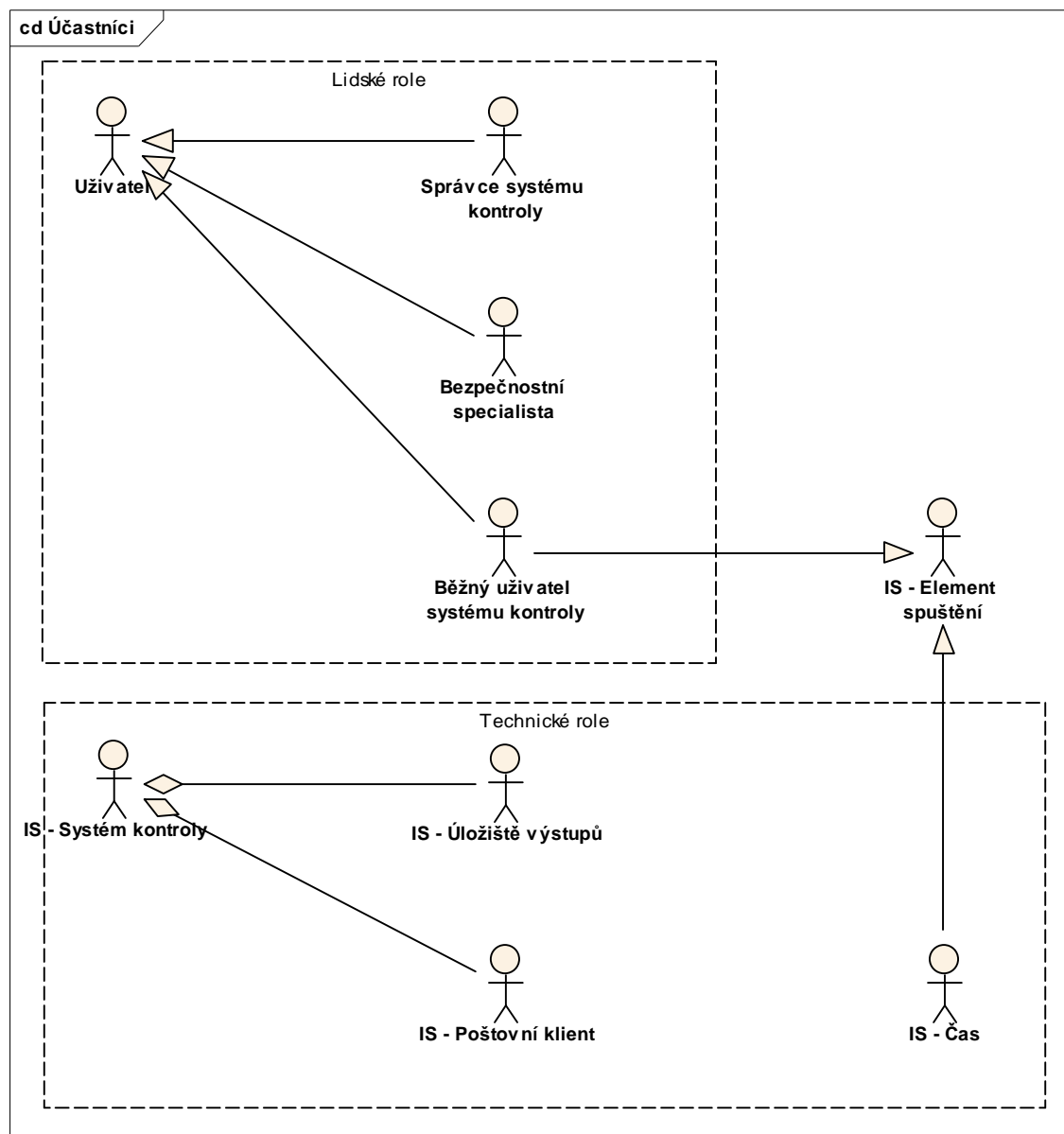


**Obr. 7 Nízká priorita**

Nízkou prioritu mají ostatní nefunkční požadavky.

## B.4 Budoucí uživatelé a jejich role

Kapitola obsahuje budoucí uživatele systému kontroly, jejich vazby na součásti systému i vazby mezi sebou.



Obr. 8 Účastníci

Role jsou rozdělené na dvě skupiny. Lidské obsahují lidské účastníky a technické všechny ostatní.

### Uživatel

Obecný zástupce uživatelů - lidský faktor.

### **Bezpečnostní specialista**

Uživatel se speciálními právy v systému kontroly, nastavuje bezpečnostní politiku a je odpovědný za její správnost.

### **Správce systému kontroly**

Uživatel s nejvyššími právy v systému kontroly, nastavuje systém a má odpovědnost za jeho provoz.

### **Běžný uživatel systému kontroly**

Uživatel s běžnými právy v systému kontroly, provozuje systém a odebírá výstupy.

### **Uživatel systému kontroly**

Uživatel s běžnými právy v systému kontroly, provozuje systém a odebírá výstupy.

### **IS - Element spuštění**

Obecný element, který způsobuje spuštění služeb systému kontroly.

### **IS - Systém kontroly**

Vlastní zástupce systému kontroly.

### **IS - Čas**

Zástupce časového okamžiku (automatizované spuštění).

### **IS - Úložiště výstupů**

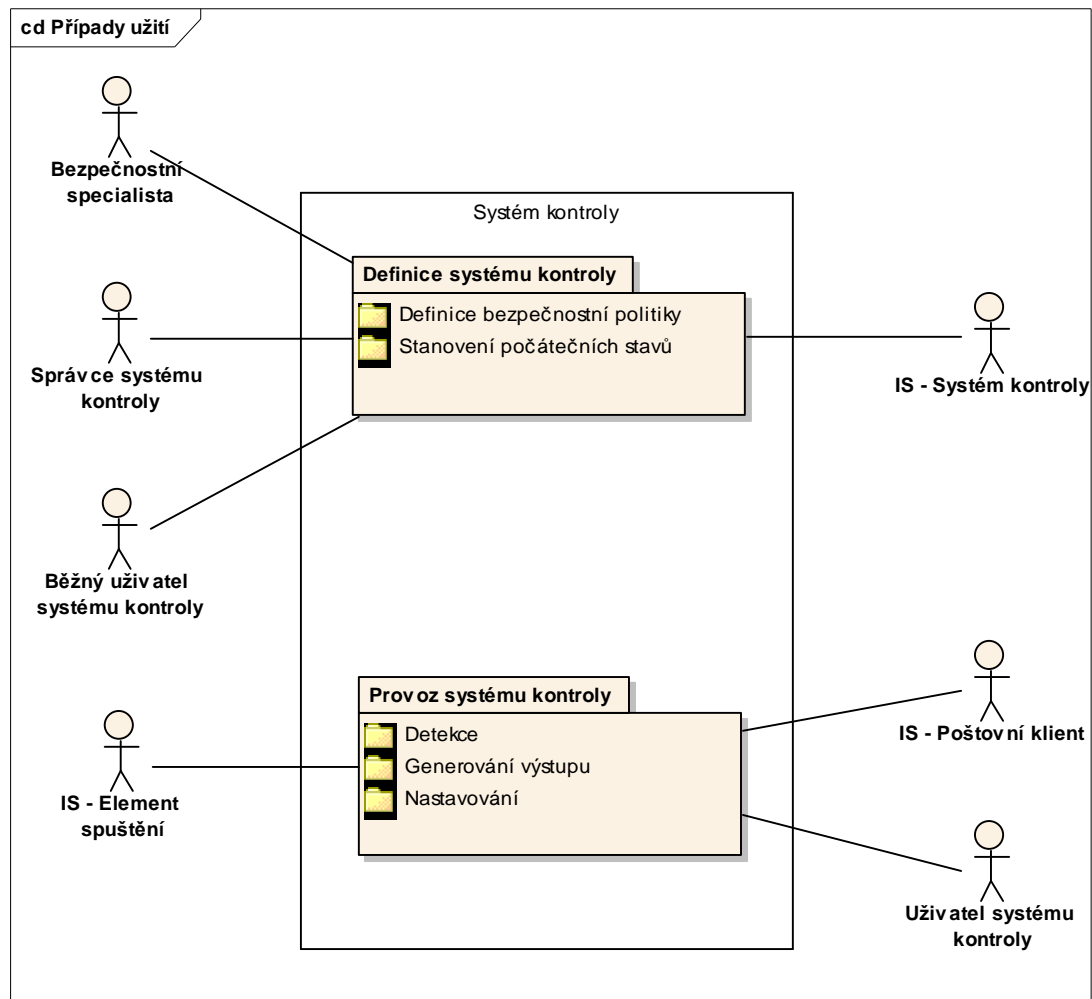
Součást systému kontroly, místo pro ukládání výstupů systému.

### **IS - Poštovní klient**

Zástupce pro zasílání výsledků e-mailem.

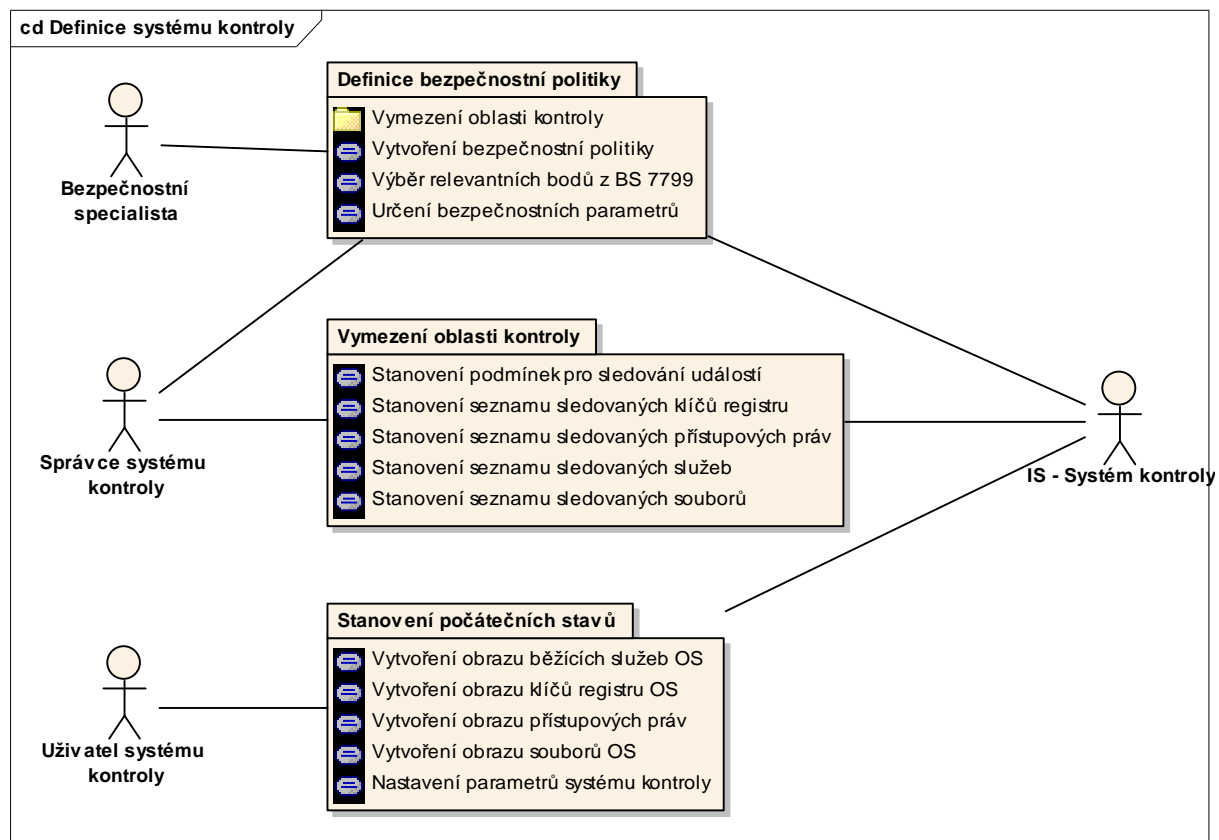
## B.5 Případy užití

Kapitola obsahuje konečné verze případů užití včetně pracovních postupů (scénářů) a vazeb mezi případy užití a dalšími součástmi analýzy, především požadavky.



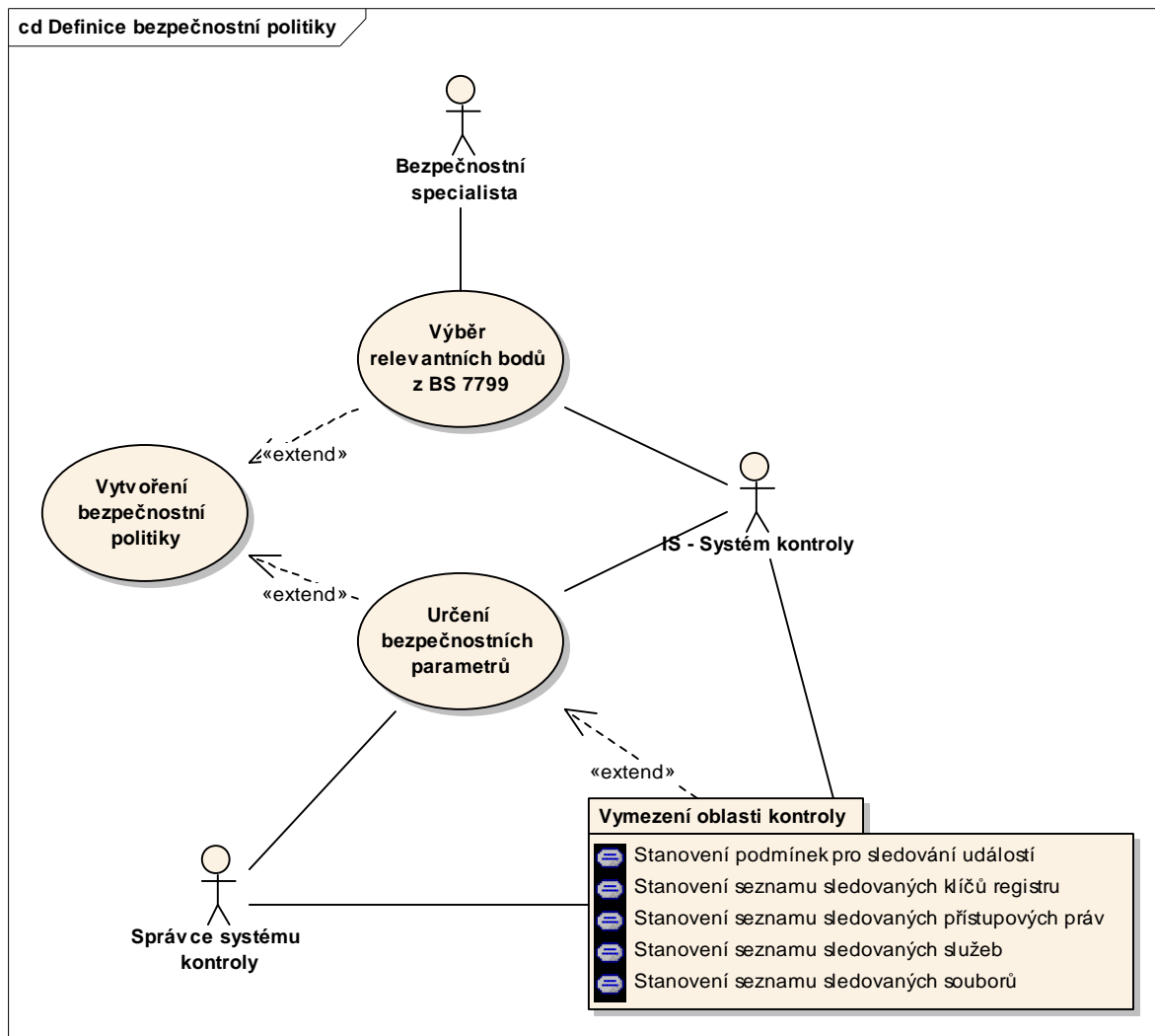
Obr. 9 : Případy užití

## B.5.1.1.1 Definice systému kontroly



Obr. 10 Definice systému kontroly

## Definice bezpečnostní politiky



Obr. 11 Definice bezpečnostní politiky

### Vytvoření bezpečnostní politiky

#### *Systémové požadavky*

§ PF.01 Systém kontroly bude obsahovat bezpečnostní politiku.

#### *Podmínky*

§ *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Je připravena struktura pro zadání bezpečnostní politiky

§ *Nutné Následná podmínka.* Případ užití - výstup 1.  
Je vytvořena bezpečnostní politika

#### *Pracovní postupy (scénáře)*

SC.01 Vytvoření bezpečnostní politiky {Hlavní}.

1. Výběr relevantních bodů z BS 7799 (SC.02)
2. Určení bezpečnostních parametrů (SC.03)

#### Výběr relevantních bodů z BS 7799

##### *Systémové požadavky*

- § PF.01 Systém kontroly bude obsahovat bezpečnostní politiku.
- § PF.03 Bezpečnostní politika bude obsahovat relevantní body BS 7799.

##### *Podmínky*

- § *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Je k dispozici norma BS 7799.
- § *Nutné Vstupní podmínka.* Příklad užití - vstup 2.  
Je k dispozici tabulka pro zápis bodů z BS 7799.
- § *Očekávané Vstupní podmínka.* Příklad užití - vstup 3.  
Bezpečnostní politika nemá definovaný seznam bodů z BS 7799.
- § *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Bezpečnostní politika obsahuje vybraný seznam bodů z BS 7799.

##### *Pracovní postupy (scénáře)*

#### SC.02 Výběr relevantních bodů z BS 7799 {Hlavní}

1. Příklad užití začíná volbou "Přidat bod" (není ještě zadán žádný bod).
2. Uživatel zadá název bodu a další určené údaje pro jeho identifikaci.
3. KDYŽ chce uživatel zadat jeden bod, pak
  - 3.1 Uživatel zvolí "Přidat bod".
  - 3.2 Uživatel zadá název bodu a další určené údaje pro jeho identifikaci.
  - 3.3 Uživatel zvolí "Uložit bod".
4. KDYŽ chce uživatel zadat opravit bod, pak
  - 4.1 Uživatel zvolí "Opravit bod".
  - 4.2 Uživatel vybere bod ze seznamu.
  - 4.3 Uživatel opraví žádané údaje.
  - 4.4 Uživatel zvolí "Uložit bod".
5. KDYŽ chce uživatel smazat bod, pak
  - 5.1 Uživatel zvolí "Smazat bod".
  - 5.2 Uživatel vybere bod ze seznamu.
  - 5.3 Uživatel potvrdí svou volbu.

#### Určení bezpečnostních parametrů

##### *Systémové požadavky*

§ PF.01 Systém kontroly bude obsahovat bezpečnostní politiku.

§ PF.02 Bezpečnostní politika bude obsahovat bezpečnostní parametry.

### **Podmínky**

§ *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Existuje tabulka pro zápis bezpečnostních parametrů v rámci bezpečnostní politiky.

§ *Očekávané Vstupní podmínka.* Příklad užití - vstup 2.  
Seznam bezpečnostních parametrů není zadán nebo není aktualizovaný.

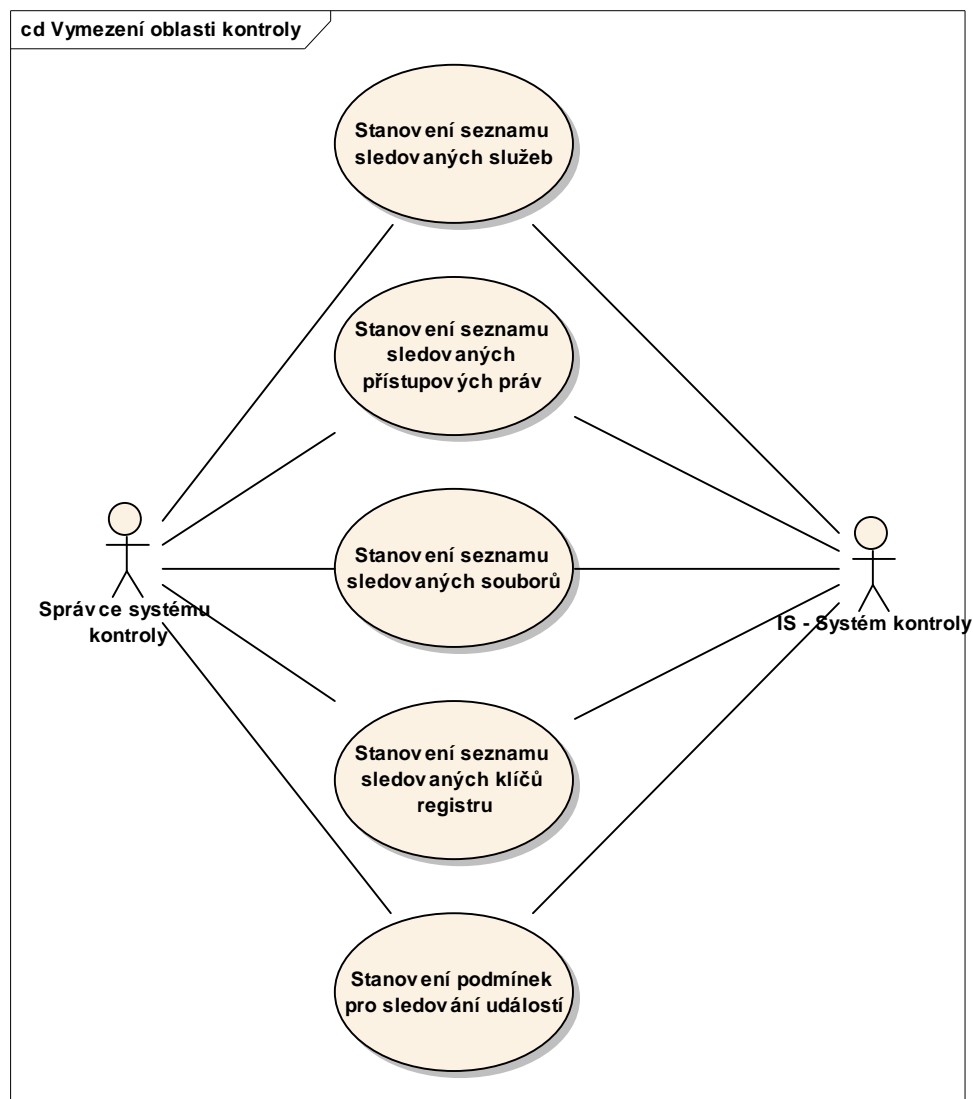
§ *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Bezpečnostní politika obsahuje seznam bezpečnostních parametrů.

### **Pracovní postupy (scénáře)**

#### SC.03 Určení bezpečnostních parametrů {Hlavní}.

1. Příklad užití začíná volbou "Přidat parametr" (není ještě zadán žádný parametr). Parametry rozumíme soubor, klíč registru, služba nebo uživatelská práva.
2. Uživatel zadá název parametru a další určené údaje pro jeho identifikaci.
3. KDYŽ chce uživatel zadat jeden parametr, pak
  - 3.1 Uživatel zvolí "Přidat parametr".
  - 3.2 Uživatel zadá název parametru a další určené údaje pro jeho identifikaci.
  - 3.3 Uživatel zvolí "Uložit parametr".
4. KDYŽ chce uživatel zadat opravit parametr, pak
  - 4.1 Uživatel zvolí "Opravit parametr".
  - 4.2 Uživatel vybere parametr ze seznamu.
  - 4.3 Uživatel opraví žádané údaje.
  - 4.4 Uživatel zvolí "Uložit parametr".
5. KDYŽ chce uživatel smazat parametr, pak
  - 5.1 Uživatel zvolí "Smazat parametr".
  - 5.2 Uživatel vybere parametr ze seznamu.
  - 5.3 Uživatel potvrdí svou volbu.

### Vymezení oblasti kontroly



Obr. 12 Vymezení oblasti kontroly

#### Stanovení podmínek pro sledování událostí

##### *Systémové požadavky*

§ PA.05 Systém kontroly bude obsahovat seznam podmínek pro sledování událostí.

##### *Podmínky*

- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje tabulka pro zadání podmínek.
- § *Očekávané Vstupní podmínka.* Případ užití - vstup 2.  
Seznam podmínek pro sledování událostí není zadáný nebo není aktuální.
- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Seznam podmínek je zadání. Vlastnosti pro sledování jsou nastaveny.

### ***Pracovní postupy (scénáře)***

#### **SC.12 Stanovení podmínek pro sledování událostí {Hlavní}**.

1. Příklad užití začíná volbou "Přidat podmínku" (nejsou ještě zadány žádné podmínky).
2. Uživatel zadá podmínku.
3. KDYŽ chce uživatel zadat jednu podmínku, pak
  - 3.1 Uživatel zvolí "Přidat podmínku".
  - 3.2 Uživatel zadá podmínku a případné operátory.
  - 3.3 Uživatel zvolí "Uložit podmínku".
4. KDYŽ chce uživatel smazat podmínku, pak
  - 4.1 Uživatel zvolí "Smazat podmínku".
  - 4.2 Uživatel vybere podmínku ze seznamu.
  - 4.3 Uživatel potvrdí svou volbu.

#### **Stanovení seznamu sledovaných klíčů registru**

##### ***Systémové požadavky***

- § PA.03 Systém kontroly bude obsahovat seznam sledovaných klíčů registru.

##### ***Podmínky***

- § *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Existuje tabulka pro zadání seznamu vybraných klíčů registru.
- § *Očekávané Vstupní podmínka.* Příklad užití - vstup 2.  
Seznam sledovaných klíčů registru není zadáný nebo není aktuální.
- § *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Seznam sledovaných klíčů registru je zadán a je aktuální. Vlastnosti pro sledování jsou nastaveny.

### ***Pracovní postupy (scénáře)***

#### **SC.04 Stanovení seznamu sledovaných klíčů registru {Hlavní}**.

1. Příklad užití začíná volbou "Přidat klíč registru" (není ještě zadán žádný klíč registru).
2. Uživatel zadá název klíče registru a další určené údaje pro jeho identifikaci.
3. KDYŽ chce uživatel zadat jeden klíč registru, pak
  - 3.1 Uživatel zvolí "Přidat klíč registru".
  - 3.2 Uživatel zadá název klíč registru a další určené údaje pro jeho identifikaci.
  - 3.3 Uživatel zvolí "Uložit klíč registru".
4. KDYŽ chce uživatel zadat opravit klíč registru, pak
  - 4.1 Uživatel zvolí "Opravit klíč registru".
  - 4.2 Uživatel vybere klíč registru ze seznamu.
  - 4.3 Uživatel opraví žádané údaje.
  - 4.4 Uživatel zvolí "Uložit klíč registru".
5. KDYŽ chce uživatel smazat klíč registru, pak
  - 5.1 Uživatel zvolí "Smazat klíč registru".

5.2 Uživatel vybere klíč registru ze seznamu.

5.3 Uživatel potvrdí svou volbu.

#### Stanovení seznamu sledovaných přístupových práv

##### *Systémové požadavky*

§ PA.04 Systém kontroly bude obsahovat seznam sledovaných přístupových práv.

##### *Podmínky*

§ *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Existuje tabulka pro zadání seznamu vybraných přístupových práv.

§ *Očekávané Vstupní podmínka.* Příklad užití - vstup 2.  
Seznam sledovaných přístupových práv není zadáný nebo není aktuální.

§ *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Seznam sledovaných přístupových práv je zadán a je aktuální. Vlastnosti pro sledování jsou nastaveny.

##### *Pracovní postupy (scénáře)*

#### SC.06 Stanovení seznamu sledovaných přístupových práv {Hlavní}.

1. Příklad užití začíná volbou "Přidat práva" (nejsou ještě zadána žádná práva).
2. Uživatel zadá název práva a další určené údaje pro jeho identifikaci.
3. KDYŽ chce uživatel zadat jedno právo, pak
  - 3.1 Uživatel zvolí "Přidat práva".
  - 3.2 Uživatel zadá název práva a další určené údaje pro jeho identifikaci.
  - 3.3 Uživatel zvolí "Uložit práva".
4. KDYŽ chce uživatel zadat opravit práva, pak
  - 4.1 Uživatel zvolí "Opravit práva".
  - 4.2 Uživatel vybere práva ze seznamu.
  - 4.3 Uživatel opraví žádané údaje.
  - 4.4 Uživatel zvolí "Uložit práva".
5. KDYŽ chce uživatel smazat práva, pak
  - 5.1 Uživatel zvolí "Smazat práva".
  - 5.2 Uživatel vybere práva ze seznamu.
  - 5.3 Uživatel potvrdí svou volbu.

#### Stanovení seznamu sledovaných služeb

##### *Systémové požadavky*

§ PA.01 Systém kontroly bude obsahovat seznam sledovaných služeb.

##### *Podmínky*

§ *Nutné Vstupní podmínka.* Příklad užití - vstup 1.

Existuje tabulka pro zadání seznamu vybraných služeb.

§ *Očekávané Vstupní podmínka.* Případ užití - vstup 2.  
Seznam sledovaných služeb není zadáný nebo není aktuální.

§ *Nutné Následná podmínka.* Případ užití - výstup 1.  
Seznam sledovaných služeb je zadán a je aktuální. Vlastnosti pro sledování jsou nastaveny.

### ***Pracovní postupy (scénáře)***

#### **SC.08 Stanovení seznamu sledovaných služeb {Hlavní}.**

1. Případ užití začíná volbou "Přidat službu" (není ještě zadána žádná služba).
2. Uživatel zadá název služby a další určené údaje pro její identifikaci.
3. KDYŽ chce uživatel zadat jednu službu, pak
  - 3.1 Uživatel zvolí "Přidat službu".
  - 3.2 Uživatel zadá název služby a další určené údaje pro její identifikaci.
  - 3.3 Uživatel zvolí "Uložit službu".
4. KDYŽ chce uživatel zadat opravit službu, pak
  - 4.1 Uživatel zvolí "Opravit službu".
  - 4.2 Uživatel vybere službu ze seznamu.
  - 4.3 Uživatel opraví žádané údaje.
  - 4.4 Uživatel zvolí "Uložit službu".
5. KDYŽ chce uživatel smazat službu, pak
  - 5.1 Uživatel zvolí "Smazat službu".
  - 5.2 Uživatel vybere službu ze seznamu.
  - 5.3 Uživatel potvrdí svou volbu.

#### **Stanovení seznamu sledovaných souborů**

### ***Systémové požadavky***

§ PA.02 Systém kontroly bude obsahovat seznam sledovaných souborů.

### ***Podmínky***

§ *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje tabulka pro zadání seznamu vybraných souborů.

§ *Očekávané Vstupní podmínka.* Případ užití - vstup 2.  
Seznam sledovaných souborů není zadáný nebo není aktuální.

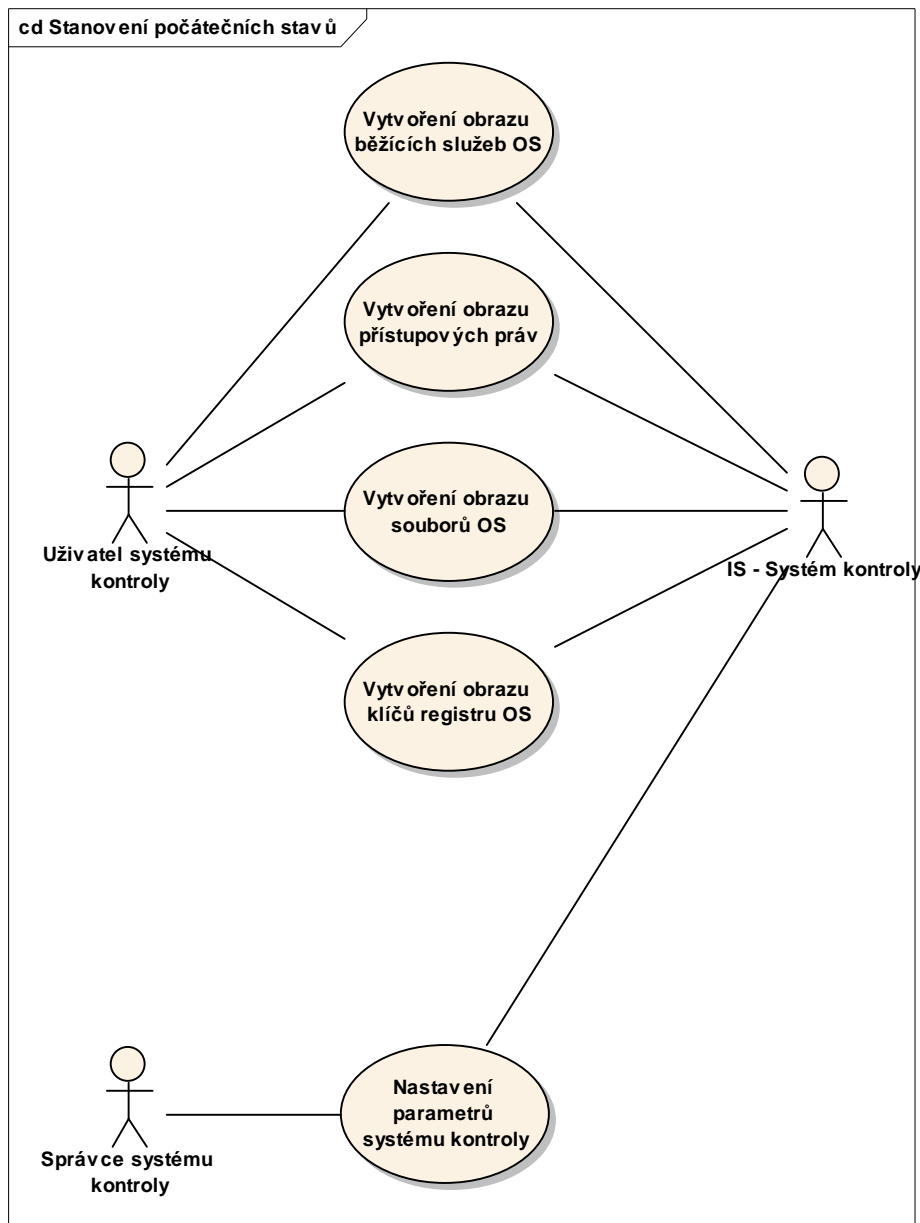
§ *Nutné Následná podmínka.* Případ užití - výstup 1.  
Seznam sledovaných souborů je zadán a je aktuální. Vlastnosti pro sledování jsou nastaveny.

### ***Pracovní postupy (scénáře)***

#### **SC.10 Stanovení seznamu sledovaných souborů {Hlavní}.**

1. Příklad užití začíná volbou "Přidat soubor" (není ještě zadán žádný soubor).
2. Uživatel zadá název souboru a další určené údaje pro jeho identifikaci.
3. KDYŽ chce uživatel zadat jeden soubor, pak
  - 3.1 Uživatel zvolí "Přidat soubor".
  - 3.2 Uživatel zadá název souboru a další určené údaje pro jeho identifikaci.
  - 3.3 Uživatel zvolí "Uložit soubor".
4. KDYŽ chce uživatel zadat opravit soubor, pak
  - 4.1 Uživatel zvolí "Opravit soubor".
  - 4.2 Uživatel vybere soubor ze seznamu.
  - 4.3 Uživatel opraví žádané údaje.
  - 4.4 Uživatel zvolí "Uložit soubor".
5. KDYŽ chce uživatel smazat soubor, pak
  - 5.1 Uživatel zvolí "Smazat soubor".
  - 5.2 Uživatel vybere soubor ze seznamu.
  - 5.3 Uživatel potvrdí svou volbu.

### Stanovení počátečních stavů



Obr. 13 Stanovení počátečních stavů

#### Vytvoření obrazu běžících služeb OS

#### *Systémové požadavky*

§ PA.07 Systém kontroly vytvoří obraz sledovaných služeb.

#### *Podmínky*

- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje aktualizovaný seznam sledovaných služeb.
- § *Očekávané Vstupní podmínka.* Případ užití - vstup 2.  
Atributy pro sledování jednotlivých služeb jsou nastaveny.

- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Byl vytvořen korektní obraz sledovaných služeb podle daného nastavení.

### ***Pracovní postupy (scénáře)***

#### **SC.13 Vytvoření obrazu běžících služeb OS {Hlavní}.**

1. Případ užití začíná volbou "Vytvořit obrazy služeb".
2. Systém pro každou určenou službu ze seznamu vytvoří (vybere nebo vypočítá) sadu atributů podle aktuálního stavu.
3. Systém vytvořenou sadu atributů uloží do části obrazy.

#### **Vytvoření obrazu klíčů registru OS**

### ***Systémové požadavky***

- § PA.09 Systém kontroly vytvoří obraz sledovaných klíčů registru.

### ***Podmínky***

- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje aktualizovaný seznam sledovaných klíčů registru.
- § *Očekávané Konečná podmínka.* Případ užití - vstup 2.  
Atributy pro sledování jednotlivých klíčů registru jsou nastaveny.
- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Byl vytvořen korektní obraz sledovaných klíčů registru podle daného nastavení.

### ***Pracovní postupy (scénáře)***

#### **SC.14 Vytvoření obrazu klíčů registru OS {Hlavní}.**

1. Případ užití začíná volbou "Vytvořit obrazy klíčů registru".
2. Systém pro každý určený klíč registru ze seznamu vytvoří (vybere nebo vypočítá) sadu atributů podle aktuálního stavu.
3. Systém vytvořenou sadu atributů uloží do části obrazy.

#### **Vytvoření obrazu přístupových práv**

### ***Systémové požadavky***

- § PA.10 Systém kontroly vytvoří obraz sledovaných přístupových práv.

### ***Podmínky***

- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje aktualizovaný seznam sledovaných přístupových práv.
- § *Očekávané Vstupní podmínka.* Případ užití - vstup 2.

Atributy pro sledování přístupových práv jsou nastaveny.

- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Byl vytvořen korektní obraz sledovaných přístupových práv podle daného nastavení.

### ***Pracovní postupy (scénáře)***

#### **SC.15 Vytvoření obrazu přístupových práv** {Hlavní}.

1. Případ užití začíná volbou "Vytvořit obrazy přístupových práv".
2. Systém pro každé přístupové právo ze seznamu vytvoří (vybere nebo vypočítá) sadu atributů podle aktuálního stavu.
3. Systém vytvořenou sadu atributů uloží do části obrazy.

#### **Vytvoření obrazu souborů OS**

### ***Systémové požadavky***

- § PA.08 Systém kontroly vytvoří obraz sledovaných souborů.

### ***Podmínky***

- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje aktualizovaný seznam sledovaných souborů.
- § *Očekávané Vstupní podmínka.* Případ užití - vstup 2.  
Atributy pro sledování jednotlivých souborů jsou nastaveny.
- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Byl vytvořen korektní obraz sledovaných souborů podle daného nastavení.

### ***Pracovní postupy (scénáře)***

#### **SC.16 Vytvoření obrazu souborů OS** {Hlavní}.

1. Případ užití začíná volbou "Vytvořit obrazy souborů".
2. Systém pro každý určený soubor ze seznamu vytvoří (vybere nebo vypočítá) sadu atributů podle aktuálního stavu.
3. Systém vytvořenou sadu atributů uloží do části obrazy.

#### **Nastavení parametrů systému kontroly**

### ***Systémové požadavky***

- § PA.07 Systém kontroly vytvoří obraz sledovaných služeb.
- § PA.08 Systém kontroly vytvoří obraz sledovaných souborů.
- § PA.09 Systém kontroly vytvoří obraz sledovaných klíčů registru.

§ PA.10 Systém kontroly vytvoří obraz sledovaných přístupových práv.

### ***Podmínky***

§ *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje tabulka pro uložení parametrů systému kontroly.

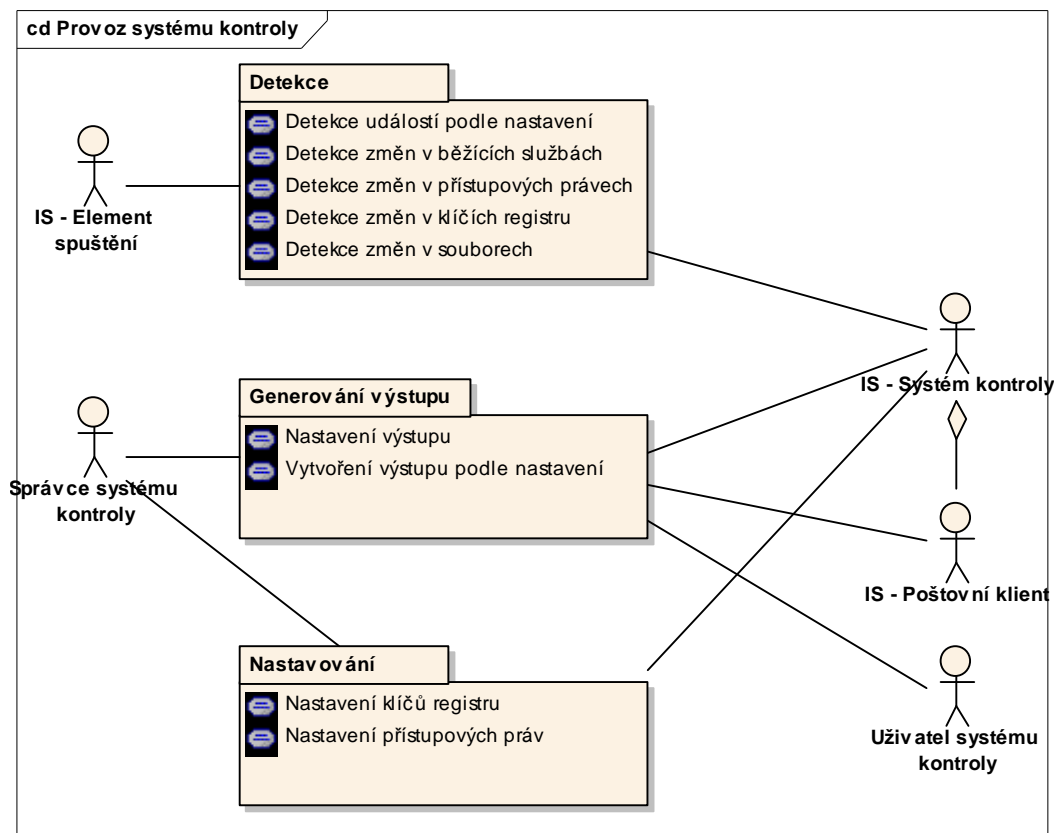
§ *Nutné Následná podmínka.* Případ užití - výstup 1.  
Systém kontroly je nastaven pro vytvoření obrazů sledovaných částí systému.

### ***Pracovní postupy (scénáře)***

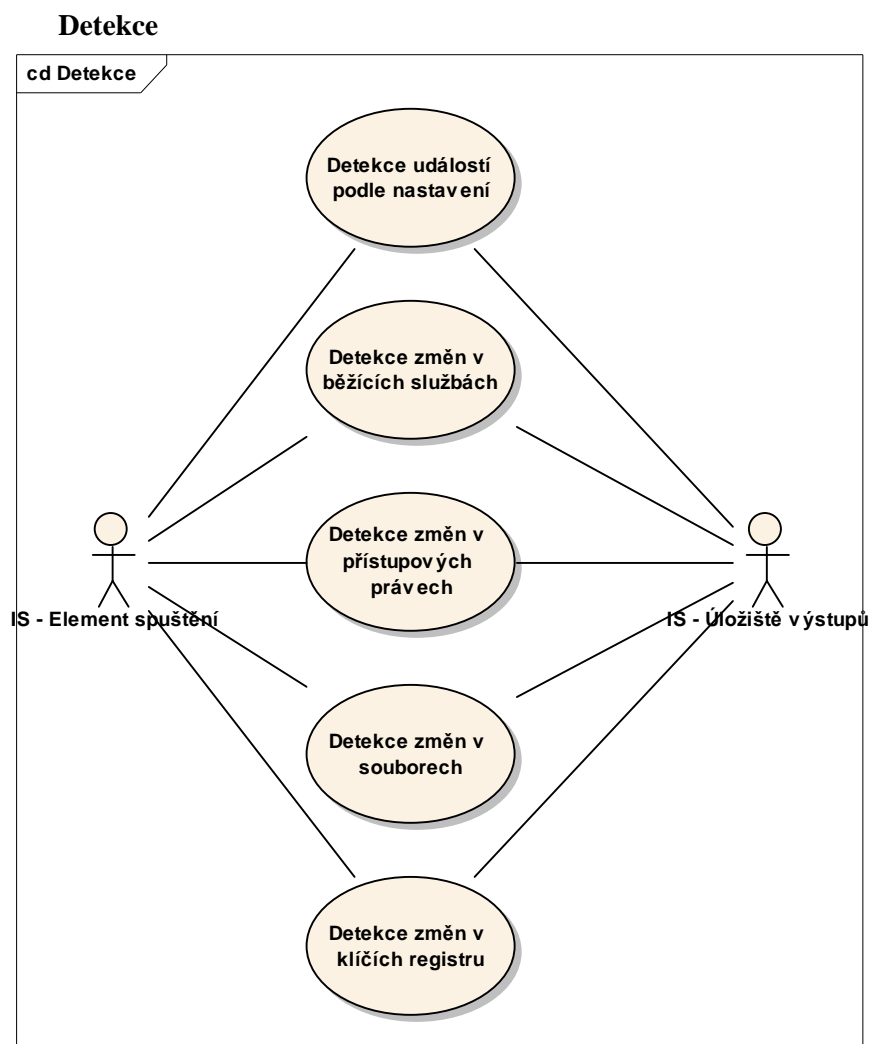
SC.17 Nastavení parametrů systému kontroly {Hlavní}.

1. Případ užití začíná volbou "Nastavit parametry sledování".
2. Uživatel zadá nebo změní hodnoty parametrů.
3. Uživatel zvolí volbu "Uložit nastavení".

## B.5.1.1.2 Provoz systému kontroly



Obr. 14 Provoz systému kontroly



Obr. 15 : Detekce

**Detekce událostí podle nastavení*****Systémové požadavky***

§ PF.08 Systém kontroly bude detekovat události sledovaných typů.

***Podmínky***

- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Element spuštění dá pokyn k provedení kontroly.
- § *Nutné Vstupní podmínka.* Případ užití - vstup 2.  
Existuje seznam podmínek pro vyhledání událostí.
- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Vznikl záznam popisující výsledek kontroly.

***Pracovní postupy (scénáře)***

### SC.18 Detekce událostí podle nastavení {Hlavní}.

1. Příklad užití začíná volbou "Detekovat události".
2. Element spuštění dá pokyn k provedení detekce podle zadaných podmínek.
3. Výsledek je uložen do výstupního úložiště dat.

#### *Detekce změn v běžících službách*

##### *Systémové požadavky*

- § PF.04 Systém kontroly bude detekovat změny ve sledovaných službách.

##### *Podmínky*

- § *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Element spuštění dá pokyn k provedení kontroly.
- § *Nutné Vstupní podmínka.* Příklad užití - vstup 2.  
Existuje korektní obraz sledovaných služeb.
- § *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Vznikl záznam popisující výsledek kontroly.
- § *Alternativní Následná podmínka.* Příklad užití - výstup 2.  
Je vytvořen nový obraz sledovaných služeb v závislosti na nastavení.

##### *Pracovní postupy (scénáře)*

### SC.19 Detekce změn v běžících službách {Hlavní}.

1. Příklad užití začíná volbou "Detekovat změny ve službách".
2. Element spuštění dá pokyn k provedení detekce změn.
3. Systém porovnáním obrazu služeb se stávajícím stavem vytvoří výsledné záznamy.
4. Výsledek je uložen do výstupního úložiště dat.
5. KDYŽ je nastaveno vytvoření nového obrazu
  - 5.1. Spustí se SC.13 Vytvoření obrazu běžících služeb OS.

#### *Detekce změn v přístupových právech*

##### *Systémové požadavky*

- § PF.07 Systém kontroly bude detekovat změny ve sledovaných přístupových právech.

##### *Podmínky*

- § *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Element spuštění dá pokyn k provedení kontroly.

- § *Nutné Vstupní podmínka.* Příklad užití - vstup 2.  
Existuje korektní obraz sledovaných přístupových práv.
- § *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Vznikl záznam popisující výsledek kontroly.
- § *Alternativní Následná podmínka.* Příklad užití - výstup 2.  
Je vytvořen nový obraz sledovaných přístupových práv v závislosti na nastavení.

### ***Pracovní postupy (scénáře)***

#### **SC.20 Detekce změn v přístupových právech** {Hlavní}.

1. Příklad užití začíná volbou "Detekovat změny v přístupových právech".
2. Element spuštění dá pokyn k provedení detekce změn.
3. Systém porovnáním obrazu přístupových práv se stávajícím stavem vytvoří výsledné záznamy.
4. Výsledek je uložen do výstupního úložiště dat.
5. KDYŽ je nastaveno vytvoření nového obrazu
  - 5.1. Spustí se SC.15 Vytvoření obrazu přístupových práv.

#### **Detekce změn v klíčích registru**

### ***Systémové požadavky***

- § PF.06 Systém kontroly bude detekovat změny ve sledovaných klíčích registru.

### ***Podmínky***

- § *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Element spuštění dá pokyn k provedení kontroly.
- § *Nutné Vstupní podmínka.* Příklad užití - vstup 2.  
Existuje korektní obraz sledovaných klíčů registru.
- § *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Vznikl záznam popisující výsledek kontroly.
- § *Alternativní Následná podmínka.* Příklad užití - výstup 2.  
Je vytvořen nový obraz sledovaných klíčů registru v závislosti na nastavení.

### ***Pracovní postupy (scénáře)***

#### **SC.21 Detekce změn v klíčích registru** {Hlavní}.

1. Příklad užití začíná volbou "Detekovat změny v klíčích registru".
2. Element spuštění dá pokyn k provedení detekce změn.
3. Systém porovnáním obrazu klíčů registru se stávajícím stavem vytvoří výsledné záznamy.
4. Výsledek je uložen do výstupního úložiště dat.

5. KDYŽ je nastaveno vytvoření nového obrazu
  - 5.1. Spustí se SC.14 Vytvoření obrazu klíčů registru OS

### Detekce změn v souborech

#### *Systémové požadavky*

- § PF.05 Systém kontroly bude detekovat změny ve sledovaných souborech.

#### *Podmínky*

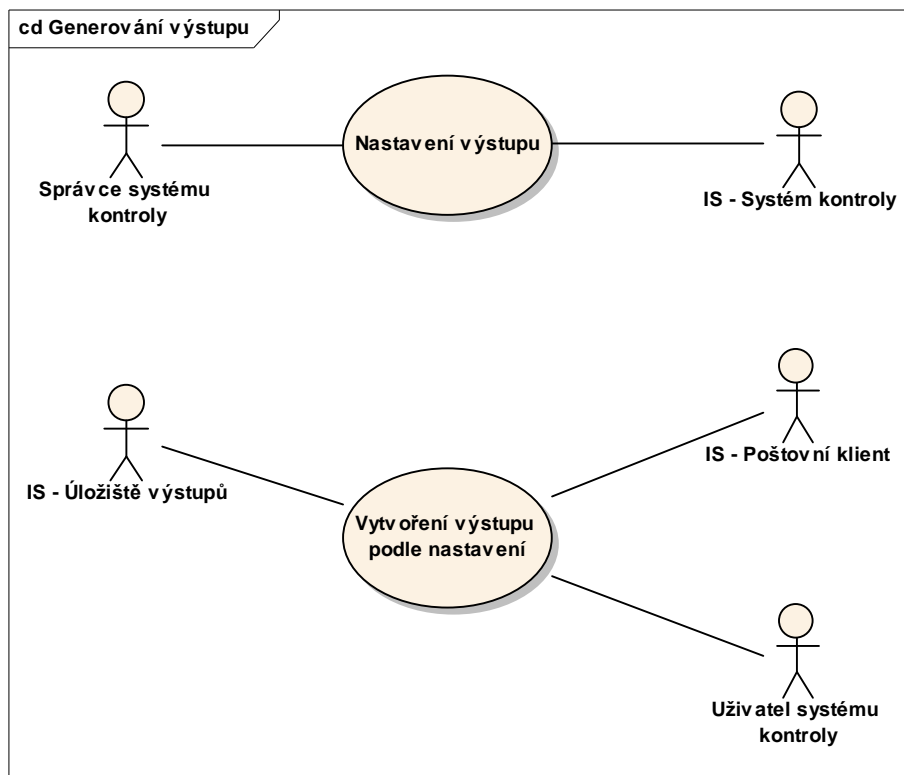
- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Element spuštění dá pokyn k provedení kontroly.
- § *Nutné Vstupní podmínka.* Případ užití - vstup 2.  
Existuje korektní obraz sledovaných souborů.
- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Vznikl záznam popisující výsledek kontroly.
- § *Alternativní Následná podmínka.* Případ užití - výstup 2.  
Je vytvořen nový obraz sledovaných souborů v závislosti na nastavení.

#### *Pracovní postupy (scénáře)*

##### SC.22 Detekce změn v souborech {Hlavní}.

1. Případ užití začíná volbou "Detekovat změny v souborech".
2. Element spuštění dá pokyn k provedení detekce změn.
3. Systém porovnáním obrazu souborů se stávajícím stavem vytvoří výsledné záznamy.
4. Výsledek je uložen do výstupního úložiště dat.
5. KDYŽ je nastaveno vytvoření nového obrazu
  - 5.1. Spustí se SC.16 Vytvoření obrazu souborů OS.

## Generování výstupu



Obr. 16 Generování výstupu

### Nastavení výstupu

#### *Systémové požadavky*

- § PA.12 Systém kontroly bude obsahovat nastavení pro výstup informací.
- § PF.10 Systém kontroly bude informace o kontrolách a změnách zasílat elektronickou poštou.

#### *Podmínky*

- § *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Existuje tabulka pro nastavení výstupu ze systému kontroly.
- § *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Systém kontroly je nastaven pro vytvoření výstupů.

#### *Pracovní postupy (scénáře)*

SC.23 Nastavení výstupu {Hlavní}.

1. Příklad užití začíná volbou "Nastavit parametry výstupu".
2. Uživatel zadá nebo změní hodnoty parametrů.
3. Uživatel zvolí volbu "Uložit nastavení".

### Vytvoření výstupu podle nastavení

#### *Systémové požadavky*

- § PA.06 Systém kontroly bude obsahovat seznam kontrol a změn bezpečnostního nastavení.
- § PA.11 Systém kontroly bude poskytovat informace o kontrolách a změnách podle nastavení.
- § PF.09 Systém kontroly bude poskytovat informace o kontrolách a změnách.
- § PF.10 Systém kontroly bude informace o kontrolách a změnách zasílat elektronickou poštou.

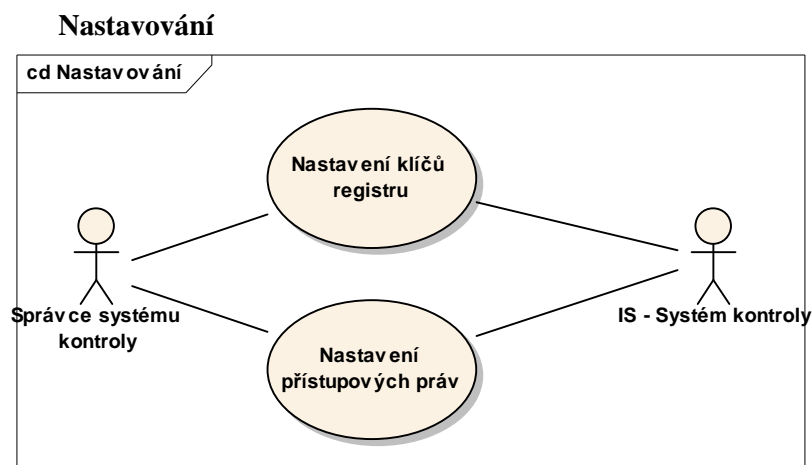
#### *Podmínky*

- § *Nutné Vstupní podmínka.* Příklad užití - vstup 1.  
Existují záznamy v úložišti záznamů.
- § *Očekávané Vstupní podmínka.* Příklad užití - vstup 2.  
Výstupy jsou nastaveny.
- § *Nutné Následná podmínka.* Příklad užití - výstup 1.  
Byl vytvořen naformátovaný výstup.
- § *Nutné Následná podmínka.* Příklad užití - výstup 2.  
Výstup byl zaslán všem adresátům.

#### *Pracovní postupy (scénáře)*

##### SC.24 Vytvoření výstupu podle nastavení {Hlavní}.

1. Příklad užití začíná volbou "Vytvořit výstup".
2. Systém vytvoří formátovaný výstup ze zjištěných dat.
3. KDYŽ je nastaven formát výstupu text
  - 3.1. Textový dokument systém uloží na místo podle nastavení.
4. KDYŽ je nastaven formát výstupu XML
  - 4.1. Systém vytvoří z formátovaného výstupu XML dokument.
  - 4.2. XML dokument uloží na místo podle nastavení.
5. KDYŽ je nastaven formát výstupu e-mail
  - 5.1. Systém zjistí platné adresáty výstupu.
  - 5.2. Systém zašle na zjištěné adresy výstup podle nastavení.
6. KDYŽ je nastaven formát výstupu ve formě upozornění
  - 6.1. Systém vyše na obrazovku upozornění na vznik výstupu.
  - 6.2. Dokument je uložen podle nastavení.



Obr. 17 Nastavování

**Nastavení klíčů registru*****Podmínky***

- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje správný obraz klíčů registru.
- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Klíče registru jsou nastaveny podle zvoleného obrazu.

***Pracovní postupy (scénáře)*****SC.19 Nastavení klíčů registru** {Hlavní}.

1. Případ užití začíná volbou "Nastavit klíče registrů".
2. Uživatel vybere obraz registrů, kterým nahradí stávající stav registrů.
3. Uživatel spustí nastavení volbou "Spustit nastavení".
4. Uživatel musí potvrdit dotaz na správnost akce.

**Nastavení přístupových práv*****Podmínky***

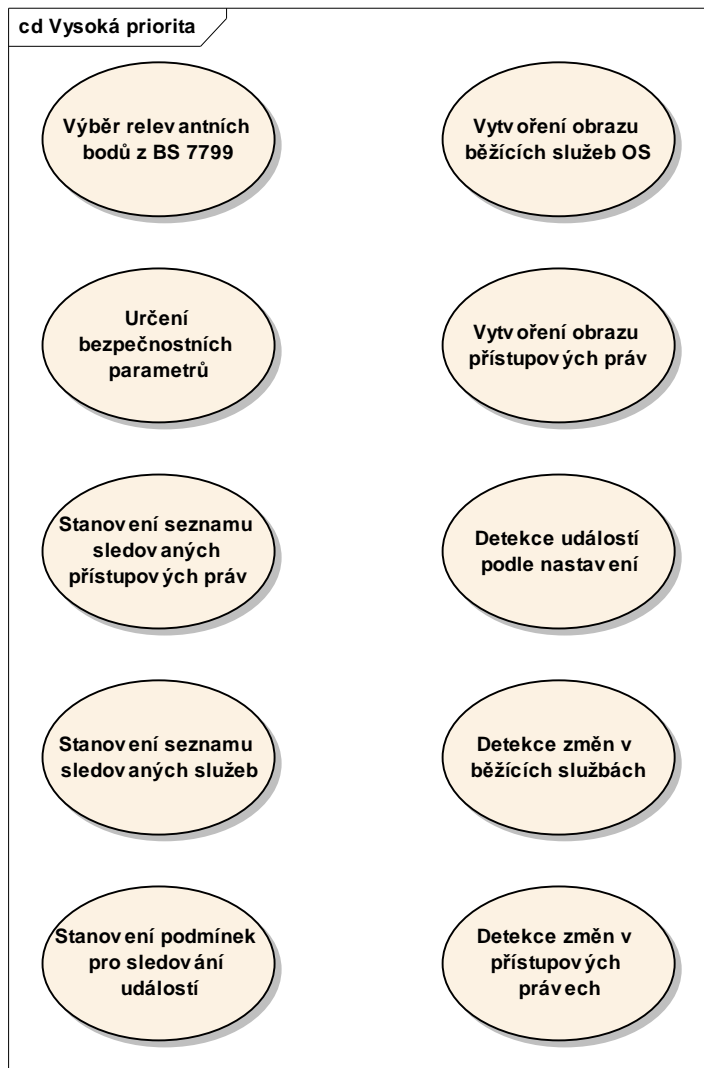
- § *Nutné Vstupní podmínka.* Případ užití - vstup 1.  
Existuje správný obraz přístupových práv.
- § *Nutné Následná podmínka.* Případ užití - výstup 1.  
Přístupová práva jsou nastavena podle zvoleného obrazu.

***Pracovní postupy (scénáře)***

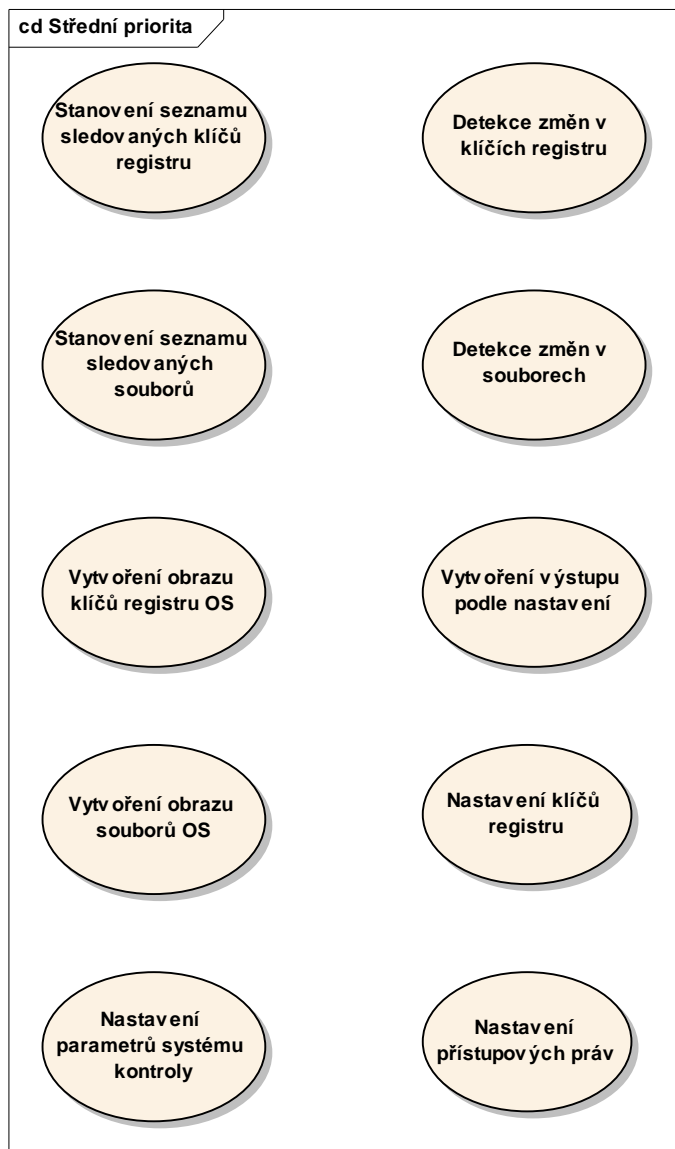
SC.20 Nastavení přístupových práv {Hlavní}.

1. Příklad užití začíná volbou "Nastavit přístupová práva".
2. Uživatel vybere obraz přístupových práv, kterým nahradí stávající přístupová práva.
3. Uživatel spustí nastavení volbou "Spustit nastavení".
4. Uživatel musí potvrdit dotaz na správnost akce.

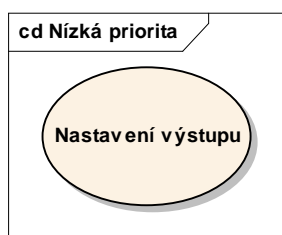
## B.6 Priority případů užití



Obr. 18 Vysoká priorita



Obr. 19 Střední priorita



Obr. 20 Nízká priorita

## B.7 Systémové požadavky

### Vyhodnocení

Jednotlivé oblasti případů užití na sebe časově navazují a případy užití, které obsahují, splňují kompletně systémové požadavky. Každý případ užití lze odděleně otestovat při splnění vstupních požadavků.

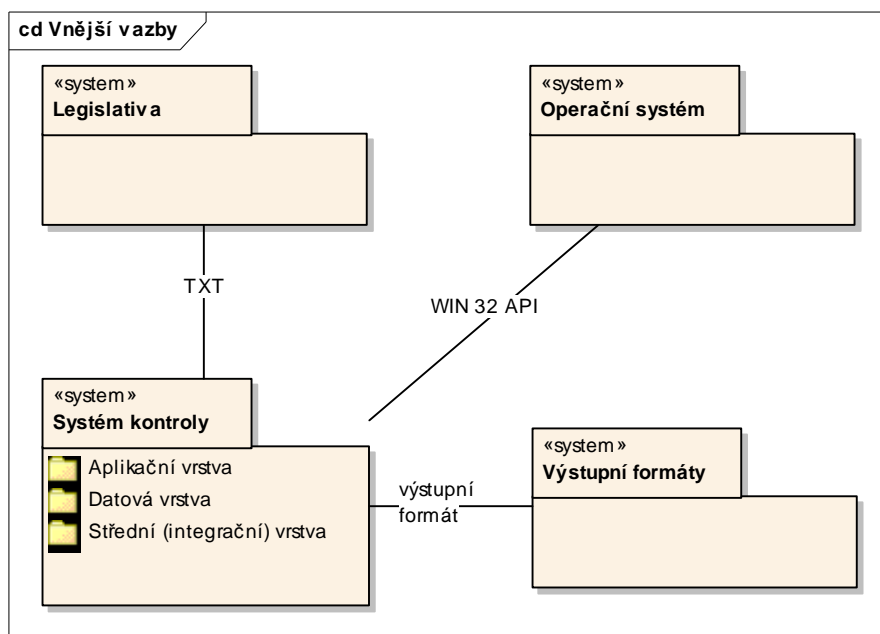
Z hlediska proveditelnosti není známo žádné kritické místo v návrhu systému kontroly, v provozování ani údržbě.



## Dodatek C. - Úvodní studie

### C.1 Spolupracující systémy

Při architektonické analýze bylo nejdříve zjištěno budoucí funkční okolí systému kontroly. Systém kontroly bude komunikovat s danými normami (BS 7799), se serverovým operačním systémem a s blíže neurčeným systémem nebo systémy pro výstup informací. Tento popis znázorňuje následující schéma.

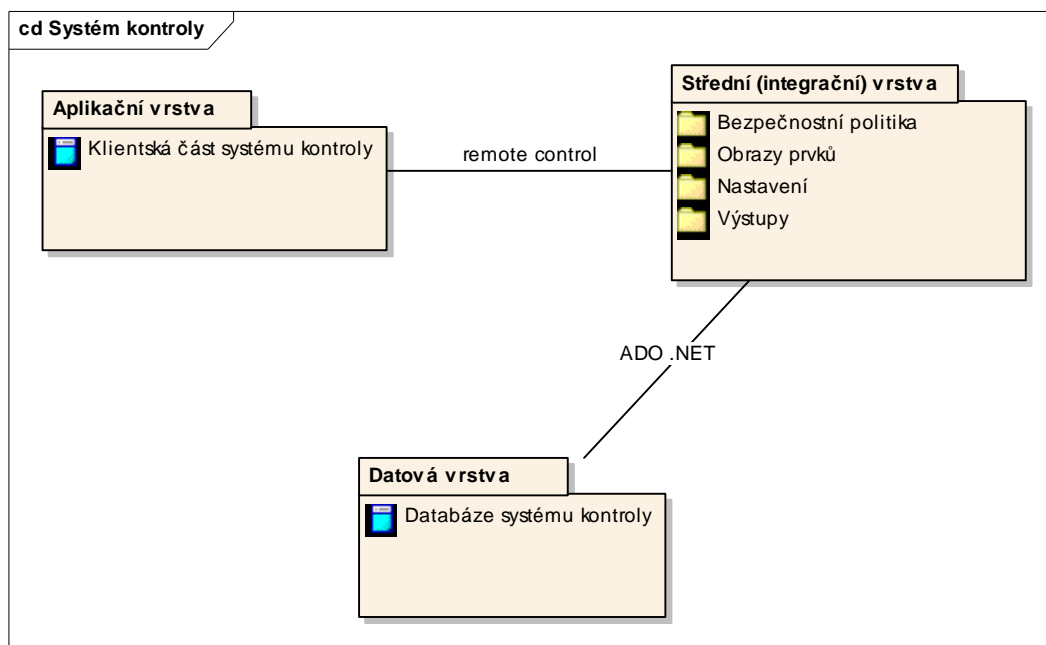


Obr. 21 Spolupracující systémy

### C.2 Vrstvy a analytické balíčky

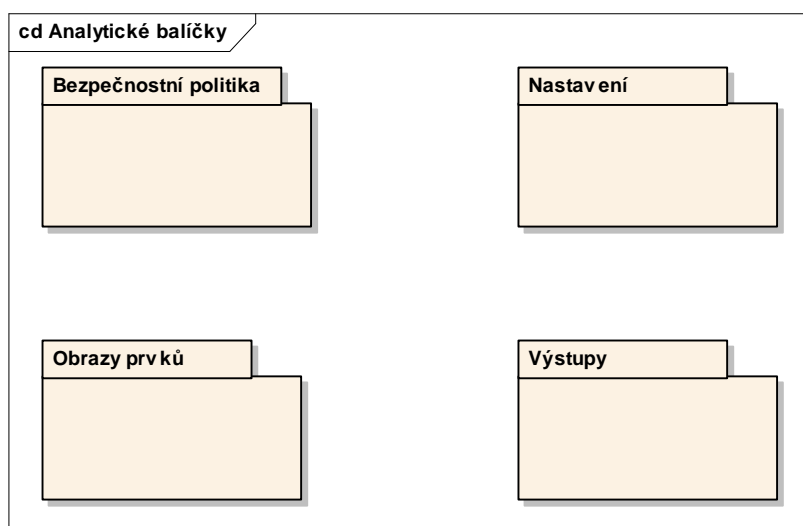
Systém kontroly musí mít balíček služeb na testovaném serveru, datové úložiště a možnost ovládní z vstupní konzoly. Z tohoto předpokladu vychází i architektonická analýza, která tudíž předpokládá klasickou třívrstvou architekturu. Hlavní část systému se tak soustřeďuje do střední vrstvy, která obsahuje i základní analytické balíčky.

Následující obrázek schématicky danou architekturu zobrazuje.



Obr. 22 Architektura systému kontroly

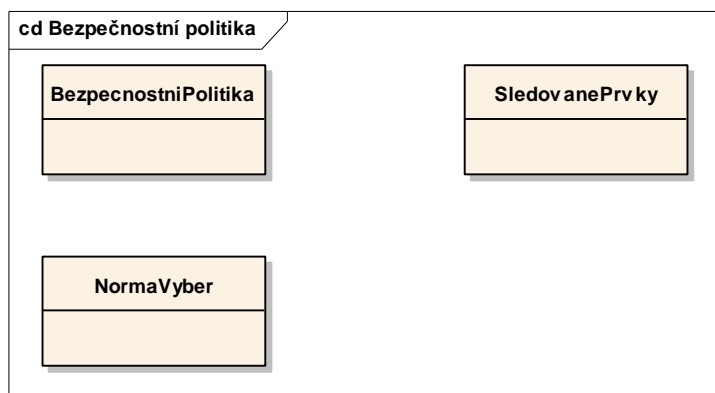
Znázorněné analytické balíčky budou dále zpřesňovány a bude analyzován jejich obsah pro určení analytických tříd.



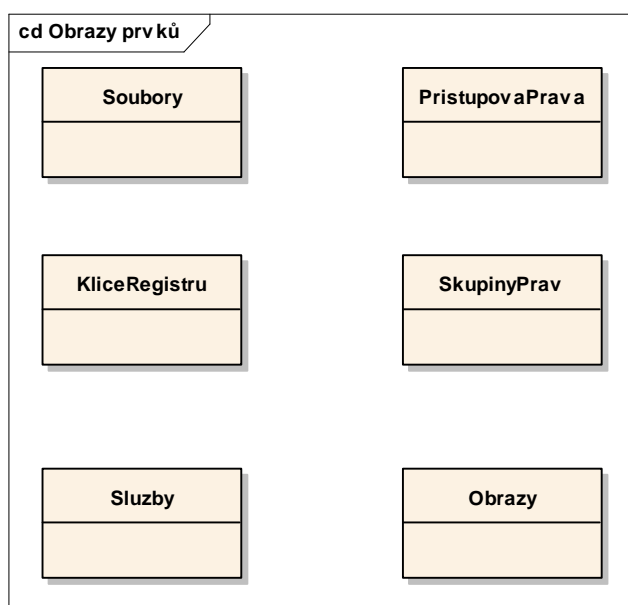
Obr. 23 Analytické balíčky

### C.3 Analytické třídy

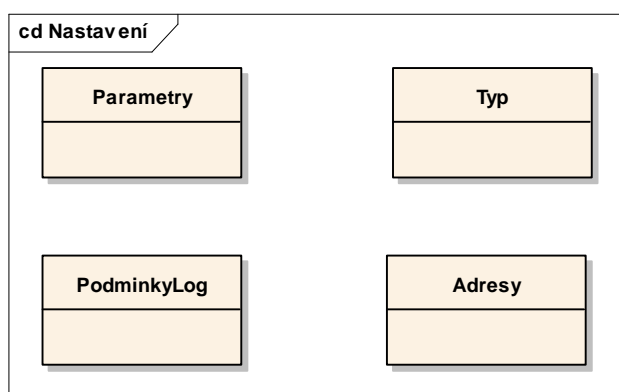
Rozpracováním analytických balíčků z předchozí kapitoly se dospěje k nalezení základních analytických tříd vhodných jako východisko pro podrobnou analýzu vnitřní struktury budoucího systému kontroly. Následují diagramy všech balíčků s analytickými třídami.



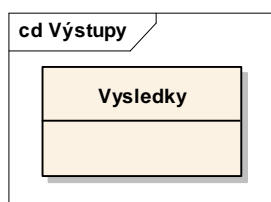
Obr. 24 Balíček Bezpečnostní politika



Obr. 25 Balíček Obrazy prvků



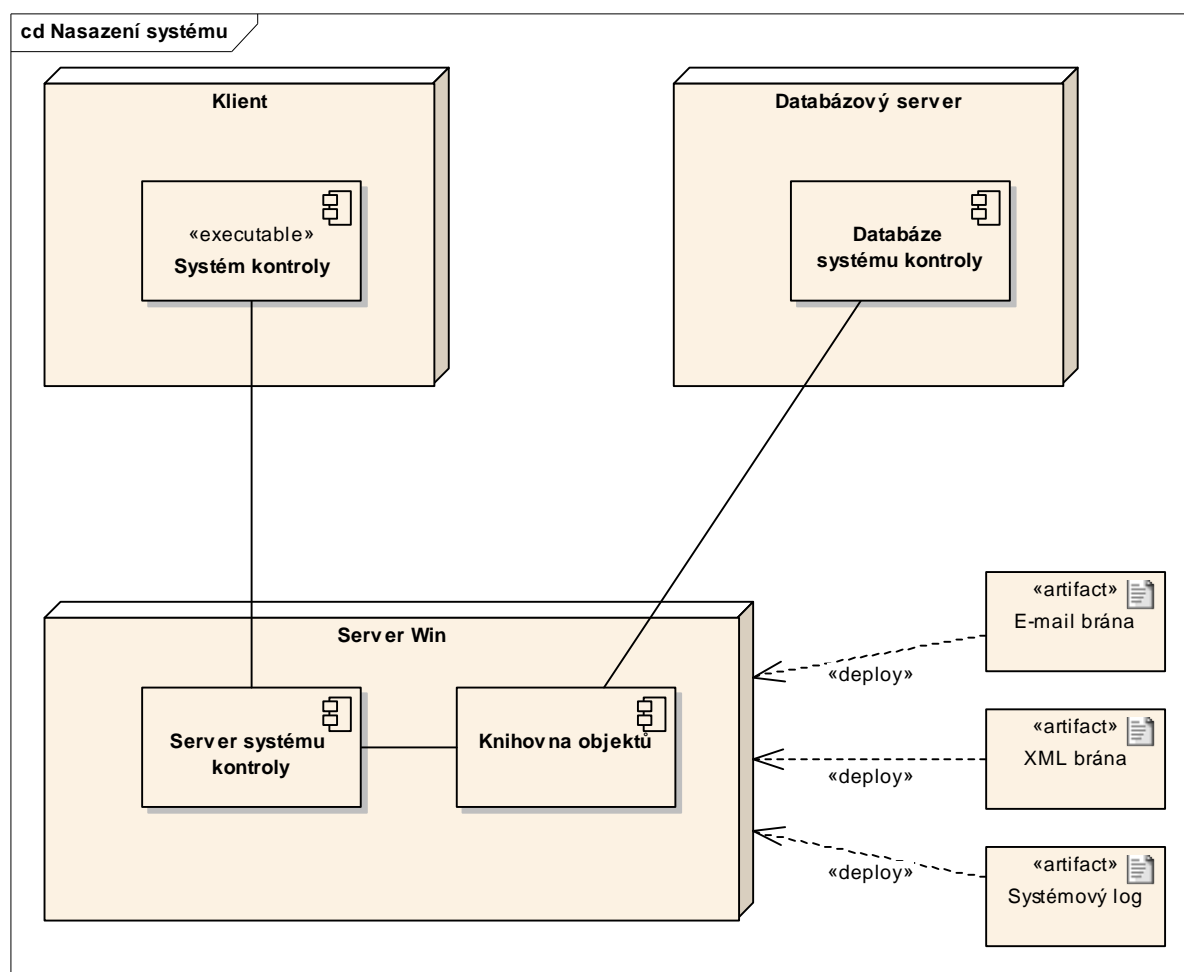
Obr. 26 Balíček Nastavení



Obr. 27 Balíček Výstupy

## C.4 Nasazení systému

Následující obrázek vyjadřuje způsob nasazení systému kontroly na hardware.



Obr. 28 Nasazení systému kontroly

Klientskou část by měl tvořit tzv. tenký klient s minimální náročností na hardware, protože veškeré zásadní operace se budou odehrávat na serveru. Tato část slouží především k zadávání dat a spouštění služeb pomocí vzdáleného přístupu.

Serverovou stranu bude tvořit aplikace obsahující veškeré spouštěné služby. Aplikace bude mít podporu knihovny předem vytvořených objektů.

Databázový server bude tvořit některý ze standardních serverů obsahující relační databázi.

## C.5 Omezující implementační podmínky

### C.5.1 Vývojová technologie

Pro implementaci řešení jsme zvolili aplikační platformu Microsoft .NET Framework.

Jedná se o již ověřenou moderní technologii, u které lze téměř s jistotou předpokládat, že bude podporována v budoucích operačních systémech platformy Microsoft Windows.

Tato technologie je standardizována v rámci ECMA (European Computer Manufacturers Association). Standardy byly přijaty jak pro CLI (Common Language Infrastructure), tak pro programovací jazyk C#, v současné době klíčový programovací jazyk pro danou platformu. Díky této standardizaci již nyní probíhají práce na přenosu .NET Frameworku na jiné platformy, konkrétně pro operační systémy založené na Linuxu.

Aplikační rozhraní CLR provádí kód nad vrstvou API operačního systému v tzv. řízeném prostředí. Kód může být od operačního systému zcela izolován. Při zavádění a běhu kódu je vykonávána řada kontrol, které významně přispívají k větší stabilitě a bezpečnosti aplikace. Vzhledem k tomu, že CLI kód je do strojového kódu překládán až při zavádění, je optimalizován pro konkrétní operační systém a procesor.

Aplikační platforma je nezávislá na programovacím jazyku (pro implementaci našeho řešení byl zvolen C#). To umožňuje v budoucnu zvolit s minimálními časovými a pracovními náklady jiný jazyk, který generuje kód vyhovující CLI.

Aplikace pro platformu .NET jsou snadno instalovatelné a konfigurovatelné.

Další výhodou technologie je možnost spolupráce aplikací s předchozími technologiemi typu ActiveX či COM. To dovoluje využívat hotové komponenty, které implementují funkčnosti, které nejsou dosud v .NET Frameworku obsaženy, případně v odůvodněných případech obejít řízený běhový systém a přistupovat přímo k API.

### C.5.2 Hardwarové požadavky

Jako hardware bude použit serverový model PC, který umožňuje provozování systému Microsoft Windows NT4.0, Microsoft Windows 2000, Microsoft Windows XP Professional nebo Microsoft Windows 2003 Server podle požadavku zadání projektu.

Klientská část bude provozována na běžném modelu PC, který umožňuje komunikaci se serverem.

## C.6 Požadavky na data a databáze

Pro uchování data bude potřeba standardní databáze relačního typu, která je schopna komunikovat se střední vrstvou (v návrhu je komunikační protokol .NET). Předpokládá se Microsoft SQL Server 2000.

## C.7 Vyhodnocení architektury systému

### C.7.1 Přehled možných rizik

Riziko použité technologie – přestože je technologie relativně nová, lze ji považovat za ověřenou díky velkému množství aplikací, které již byly vytvořeny na jejím základě. Případné problémy lze pak eliminovat díky velkému rozšíření, a tím i podpoře od velkého množství vývojových pracovníků. Vývojový tým tuto technologii již ověřil pro implementaci přenosu dat mezi informačními systémy pomocí webových služeb.

Riziko bezpečnosti – bezpečnost bude zajištěna standardní autentizací při přihlášení k serveru, takže odpovídá běžným požadavkům, přístup do databáze bude chráněn speciálním přístupovým právem. Bezpečnost vlastního www serveru proti útoku je závislá na správném nastavení a aplikaci bezpečnostních oprav. Útoky typu DoS lze eliminovat vhodným nastavením firewallu umístěného před www serverem.

Riziko implementace – důležitým předpokladem pro implementování systému bude součinnost poskytovatele a potencionálních uživatelů s vývojovým týmem. Testování a další práce spojené s implementací bude prací nad rámec povinností a bude záležet do velké míry na ochotě uživatelů takovou činnosti provádět. V běžném provozu by neměl systém kontroly znamenat velké časové zatížení obsluhy.

### C.7.2 Zvážení variant řešení

Protože na straně klienta není potřeba provádět žádné náročné operace, je řešení představované tzv. tenkým klientem ideální z hlediska malé náročnosti jak řešení, tak i nároků na technické vybavení klientské stanice. Každá další varianta by zbytečně zvyšovala jak náročnost řešení, tak i možnost chyb a nespolehlivosti.

Výhody použité technologie na straně serveru je podrobně rozebrána v části C.5.1 Vývojová technologie. Zároveň je i vysvětlen rozdíl od jiných použitelných technologií (např. MFC technologie). Samozřejmě jsou použitelné, ale rozdíl v kontrole kódu a jednoduchosti přístupu k potřebným funkcím je značný. Zároveň oddělení aplikace od OS další vrstvou runtime CLR přidává další ochranu před během dalších aplikací v rámci OS.

Použitá technologie přístupu k datovým záznamům (ADO .NET) pak vyplývá z výše uvedených důvodů použití .NET. Samozřejmě v případě potřeby lze tento přístup poměrně jednoduše modifikovat.

### C.7.3 Vhodnost implementačních metod

Při navržené třívrstvé architektuře bude možné umístit nezávisle na sobě klientskou část a serverovou část. Tenkého klienta předpokládáme ve formě internetového prohlížeče, který je standardní součástí systémů platformy Windows. Serverovou část lze umístit podle potřeby informačního oddělení a nezávisle na ní i část databázovou, což je vhodné jak z hlediska variability, tak i z hlediska bezpečnosti.

## **C.7.4 Návaznost na systémové požadavky**

Navrhovaný systém obsahuje řešení všech systémových požadavků.



## **Dodatek D. - Globální návrh IS**

### **D.1 Strukturovaný model případů užití**

Stávající model případů užití byl upraven podle architektonického návrhu, tj. byly upraveny jak případy užití, tak i vazby mezi nimi. Přehled případů užití je uveden, jednotlivé případy užití jsou podrobně popsány v dodatku B – Systémové požadavky IS.

### **D.2 Strukturované scénáře případu užití**

Obecné scénáře navržené v dodatku B byly po upřesnění vlastních případů užití podrobně rozebrány pro další využití při návrhu realizace případů užití. Výsledné scénáře jsou uvedeny v dodatku B – Systémové požadavky IS.

### **D.3 Slovník pojmů pro činnosti a třídy**

Následující odstavec obsahuje stručný popis vytvářeného systému kontroly včetně jeho činnosti. Pomocí analýzy podstatných jmen a sloves se poté vytvoří slovník pojmů pro činnosti a třídy.

Systém kontroly bude vytvořen pro platformu Windows. Bude obsahovat bezpečnostní politiku odvozenou od standardu BS 7799. Součástí bezpečnostní politiky bude seznam bodů z BS 7799, které vybere bezpečnostní správce a mají vztah k domněně řešení, a seznam sledovaných prvků OS, který bude reprezentovat bezpečnostní parametry. Bezpečnostní parametry budou rozlišeny podle typu a budou to soubory (systémové a další vybrané), klíče registrů, služby OS a přístupová práva a skupiny práv. Systém kontroly umožní výstup bezpečnostní politiky do externího souboru. Systém kontroly bude obsahovat korektní obrazy sledovaných prvků OS. Pro soubory to bude jejich existence, atributy, velikost, název, kontrolní součet, datum modifikace a práva přístupu. Pro klíče registrů to bude jejich existence, název, hodnota, typ, umístění a přístupová práva. Pro služby OS to bude jejich název, stav, typ spouštění, cesta k souboru a práva (účet pro přihlášení). Pro přístupová práva a skupiny to bude jméno a členství ve skupinách. Systém kontroly bude obsahovat seznam podmínek vztahující se k systémovému logu. Podle jejich nastavení bude reagovat na vznik událostí. Součástí sledování přístupových práv bude možnost jejich obnovy podle předem vytvořeného schématu (obrazu). Další součástí systému kontroly budou kontroly výše uvedených obrazů proti aktuálnímu stavu podle parametrického nastavení. Výsledky se budou ukládat do seznamu provedených kontrol. Poslední možností bude možnost výstupu daných výsledků do textového souboru, do XML, do e-mailu a do systémového logu také podle zvoleného nastavení.

Z tohoto popisu byla vybrána tato podstatná jména jako kandidáti tříd a jejich atributů:

- bezpečnostní politika

- body z BS 7799
- sledované prvky OS = bezpečnostní parametry
- typ bezpečnostních parametrů
- výstup bezpečnostní politiky
- korektní obraz
- soubory
- klíče registrů
- služby OS
- přístupová práva
- skupiny práv
- existence
- atributy
- velikost
- název
- kontrolní součet
- datum modifikace
- hodnota
- typ
- umístění
- stav
- typ spouštění
- cesta k souboru
- členství ve skupinách
- seznam podmínek pro systémový log
- nastavení
- událost

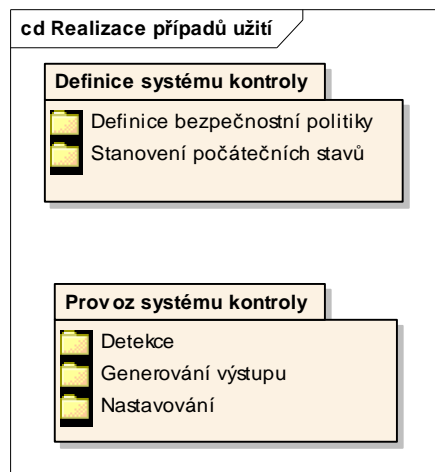
- seznam provedených kontrol = výsledky

Z tohoto popisu byla vybrána tato slovesa a spojení jako kandidáti odpovědností:

- vybrat
- rozlišovat
- umožnit
- reagovat
- ukládat
- sledování přístupových práv
- obnova přístupových práv
- kontrola obrazů proti aktuálnímu stavu
- výstup do XML, textu, e-mailu a systémového logu

## D.4 Realizace případů užití

V této kapitole je rozpracována realizace případů užití do úrovně analytických struktur.

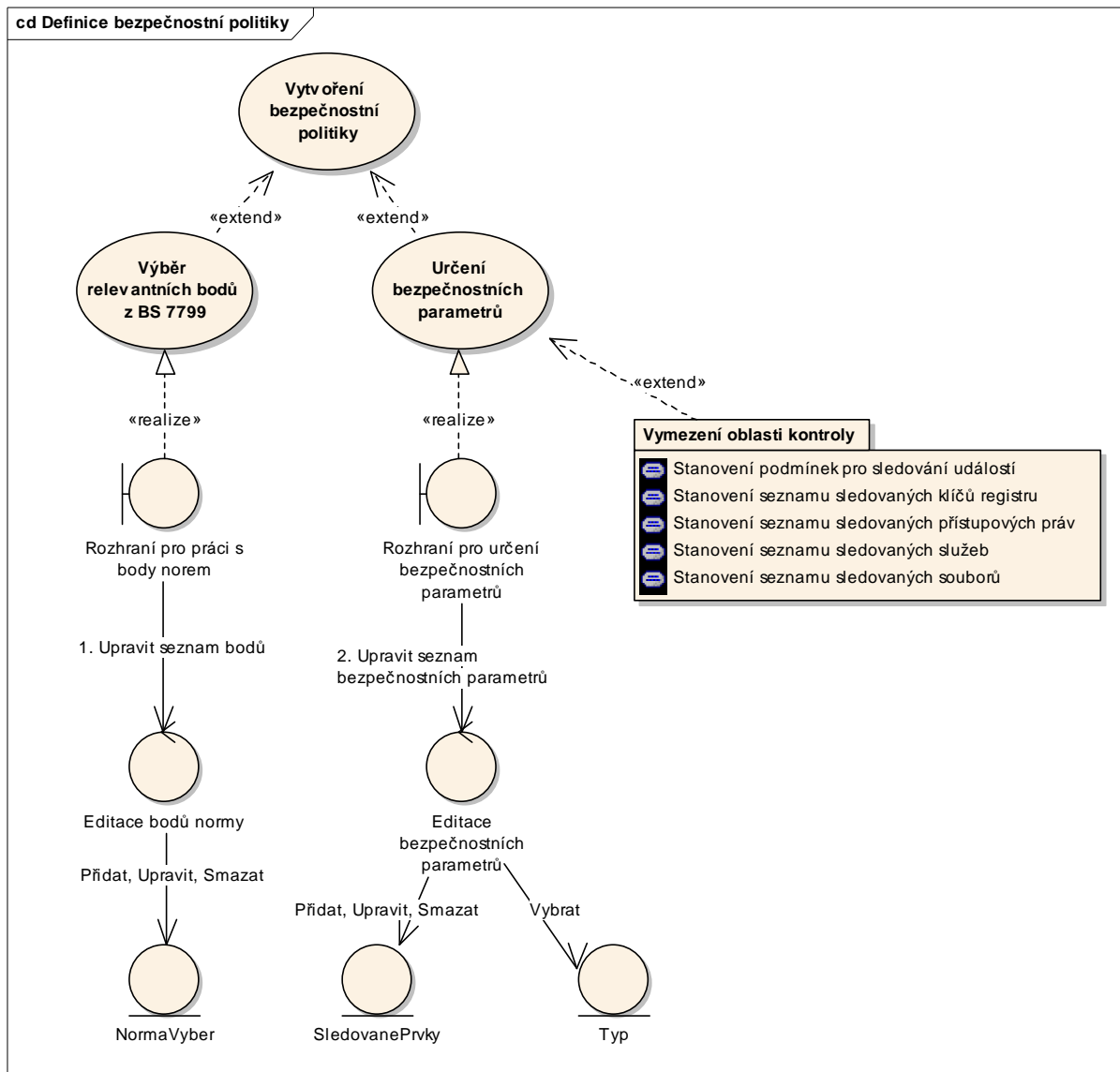


Obr. 29 Realizace případů užití

### D.4.1 Definice systému kontroly

Realizace části systému kontroly, kterým se systém nastavuje a definuje jeho další provoz.

**Definice bezpečnostní politiky**



**Obr. 30 Definice bezpečnostní politiky**

**Editace bezpečnostních parametrů**

Vazba	Zdroj	Cíl
Asociace Vybrat	Editace bezpečnostních parametrů	Typ
Asociace 2. Upravit seznam bezpečnostních parametrů	Rozhraní pro určení bezpečnostních parametrů	Editace bezpečnostních parametrů
Asociace Přidat, Upravit, Smazat	Editace bezpečnostních parametrů	SledovanePrvky

**Tab. 25 Vazby Editace bezpečnostních parametrů**

**Editace bodů normy**

Vazba	Zdroj	Cíl
Asociace 1. Upravit seznam bodů	Rozhraní pro práci s body norem	Editace bodů normy
Asociace Přidat, Upravit, Smazat	Editace bodů normy	NormaVyber

Tab. 26 Vazby Editace bodů normy

**NormaVyber**

Vazba	Zdroj	Cíl
Asociace Přidat, Upravit, Smazat	Editace bodů normy	NormaVyber

Tab. 27 Vazby NormaVyber

**Rozhraní pro práci s body norem**

Vazba	Zdroj	Cíl
Asociace 1. Upravit seznam bodů	Rozhraní pro práci s body norem	Editace bodů normy
Realizace	Rozhraní pro práci s body norem	Výběr relevantních bodů z BS 7799

Tab. 28 Vazby Rozhraní pro práci s body norem

**Rozhraní pro určení bezpečnostních parametrů**

Vazba	Zdroj	Cíl
Asociace 2. Upravit seznam bezpečnostních parametrů	Rozhraní pro určení bezpečnostních parametrů	Editace bezpečnostních parametrů
Realizace	Rozhraní pro určení bezpečnostních parametrů	Určení bezpečnostních parametrů

Tab. 29 Vazby Rozhraní pro určení bezpečnostních parametrů

**SledovanePrvky**

Vazba	Zdroj	Cíl
Asociace Přidat, Upravit, Smazat	Editace bezpečnostních parametrů	SledovanePrvky

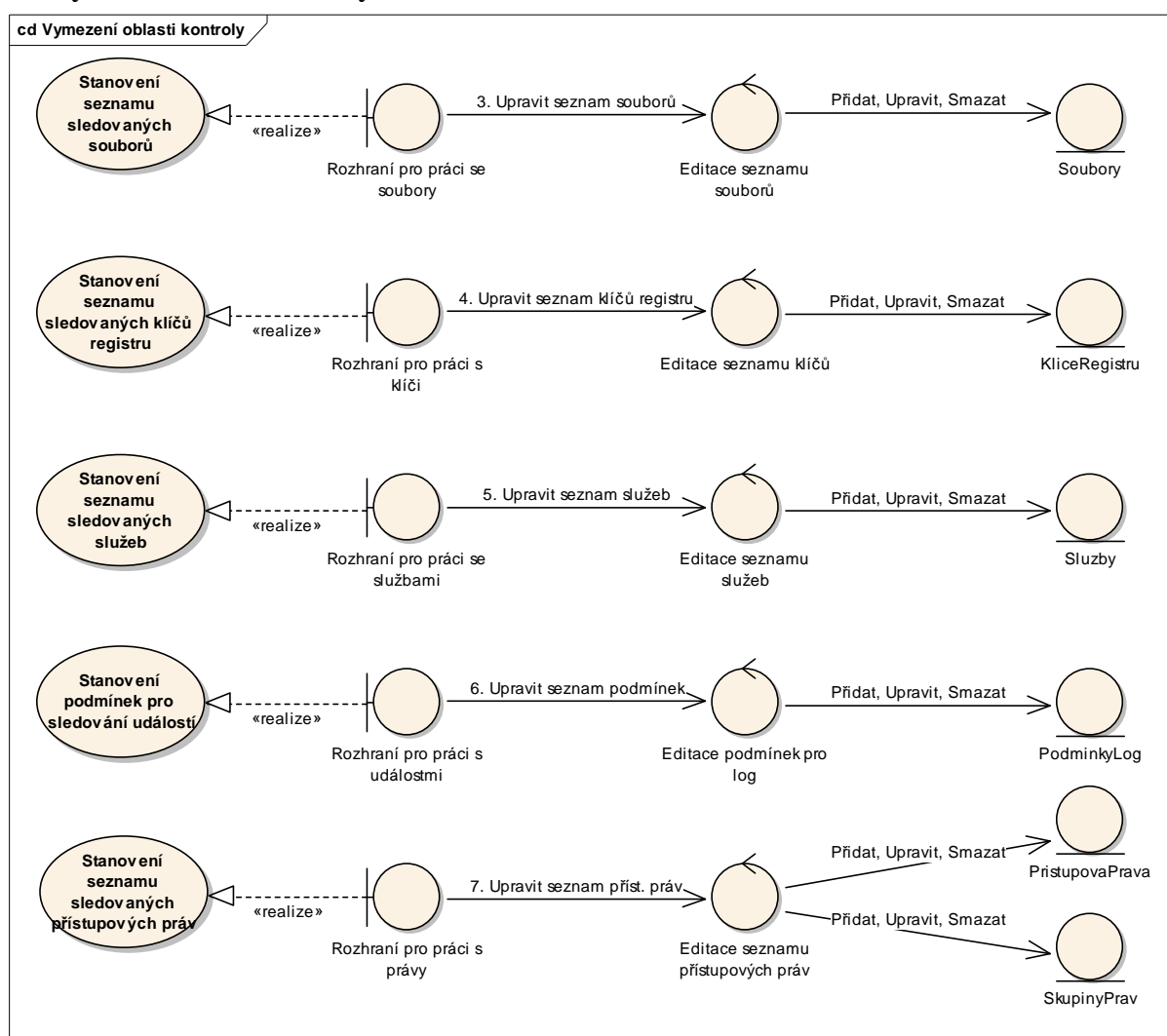
Tab. 30 Vazby SledovanePrvky

## Typ

Vazba	Zdroj	Cíl
Asociace Vybrat	Vytvoření obrazů	Typ
Asociace Vybrat	Editace bezpečnostních parametrů	Typ
Asociace Uložit	Typ	Obrazy

Tab. 31 Vazby Typ

## Vymezení oblasti kontroly



Obr. 31 Vymezení oblasti kontroly

**Editace podmínek pro log**

Vazba	Zdroj	Cíl
Asociace 6. Upravit seznam podmínek	Rozhraní pro práci s událostmi	Editace podmínek pro log
Asociace Přidat, Upravit, Smazat	Editace podmínek pro log	PodminkyLog

Tab. 32 Vazby Editace podmínek pro log

**Editace seznamu klíčů**

Vazba	Zdroj	Cíl
Asociace 4. Upravit seznam klíčů registru	Rozhraní pro práci s klíči	Editace seznamu klíčů
Asociace Přidat, Upravit, Smazat	Editace seznamu klíčů	KliceRegistru

Tab. 33 Vazby Editace seznamu klíčů

**Editace seznamu přístupových práv**

Vazba	Zdroj	Cíl
Asociace 7. Upravit seznam příst. práv	Rozhraní pro práci s právy	Editace seznamu přístupových práv
Asociace Přidat, Upravit, Smazat	Editace seznamu přístupových práv	PristupovaPrava
Asociace Přidat, Upravit, Smazat	Editace seznamu přístupových práv	SkupinyPrav

Tab. 34 Vazby Editace seznamu přístupových práv

**Editace seznamu služeb**

Vazba	Zdroj	Cíl
Asociace 5. Upravit seznam služeb	Rozhraní pro práci se službami	Editace seznamu služeb
Asociace Přidat, Upravit, Smazat	Editace seznamu služeb	Sluzby

Tab. 35 Vazby Editace seznamu služeb

**Editace seznamu souborů**

Vazba	Zdroj	Cíl
-------	-------	-----

Vazba	Zdroj	Cíl
Asociace Přidat, Upravit, Smazat	Editace seznamu souborů	Soubory
Asociace 3. Upravit seznam souborů	Rozhraní pro práci se soubory	Editace seznamu souborů

Tab. 36 Vazby Editace seznamu souborů

**KliceRegistru**

Vazba	Zdroj	Cíl
Asociace Přidat, Upravit, Smazat	Editace seznamu klíčů	KliceRegistru
Asociace Vybrat	KliceRegistru	Nastavení klíčů registru
Asociace Porovnat	Detekce	KliceRegistru

Tab. 37 Vazby KliceRegistru

**PodminkyLog**

Vazba	Zdroj	Cíl
Asociace Porovnat	PodminkyLog	Detekce
Asociace Přidat, Upravit, Smazat	Editace podmínek pro log	PodminkyLog

Tab. 38 VazbyPodminkyLog

**PristupovaPrava**

Vazba	Zdroj	Cíl
Asociace Porovnat	Detekce	PristupovaPrava
Asociace Přidat, Upravit, Smazat	Editace seznamu přístupových práv	PristupovaPrava
Asociace Vybrat	PristupovaPrava	Nastavení přístupových práv

Tab. 39 Vazby PristupovaPrava

**Rozhraní pro práci s klíči**

Vazba	Zdroj	Cíl
Asociace 4. Upravit seznam klíčů registru	Rozhraní pro práci s klíči	Editace seznamu klíčů

Vazba	Zdroj	Cíl
Realizace	Rozhraní pro práci s klíči	Stanovení seznamu sledovaných klíčů registru

Tab. 40 Vazby Rozhraní pro práci s klíči

**Rozhraní pro práci s právy**

Vazba	Zdroj	Cíl
Asociace 7. Upravit seznam příst. práv	Rozhraní pro práci s právy	Editace seznamu přístupových práv
Realizace	Rozhraní pro práci s právy	Stanovení seznamu sledovaných přístupových práv

Tab. 41 Vazby Rozhraní pro práci s právy

**Rozhraní pro práci s událostmi**

Vazba	Zdroj	Cíl
Asociace 6. Upravit seznam podmínek	Rozhraní pro práci s událostmi	Editace podmínek pro log
Realizace	Rozhraní pro práci s událostmi	Stanovení podmínek pro sledování událostí

Tab. 42 Vazby Rozhraní pro práci s událostmi

**Rozhraní pro práci se službami**

Vazba	Zdroj	Cíl
Asociace 5. Upravit seznam služeb	Rozhraní pro práci se službami	Editace seznamu služeb
Realizace	Rozhraní pro práci se službami	Stanovení seznamu sledovaných služeb

Tab. 43 Vazby Rozhraní pro práci se službami

**Rozhraní pro práci se soubory**

Vazba	Zdroj	Cíl
Asociace 3. Upravit seznam souborů	Rozhraní pro práci se soubory	Editace seznamu souborů
Realizace	Rozhraní pro práci se soubory	Stanovení seznamu sledovaných souborů

Tab. 44 Vazby Rozhraní pro práci se soubory

**SkupinyPrav**

Vazba	Zdroj	Cíl
-------	-------	-----

Vazba	Zdroj	Cíl
Asociace Přidat, Upravit, Smazat	Editace seznamu přístupových práv	SkupinyPrav

Tab. 45 Vazby SkupinyPrav

**Sluzby**

Vazba	Zdroj	Cíl
Asociace Porovnat	Detekce	Sluzby
Asociace Přidat, Upravit, Smazat	Editace seznamu služeb	Sluzby

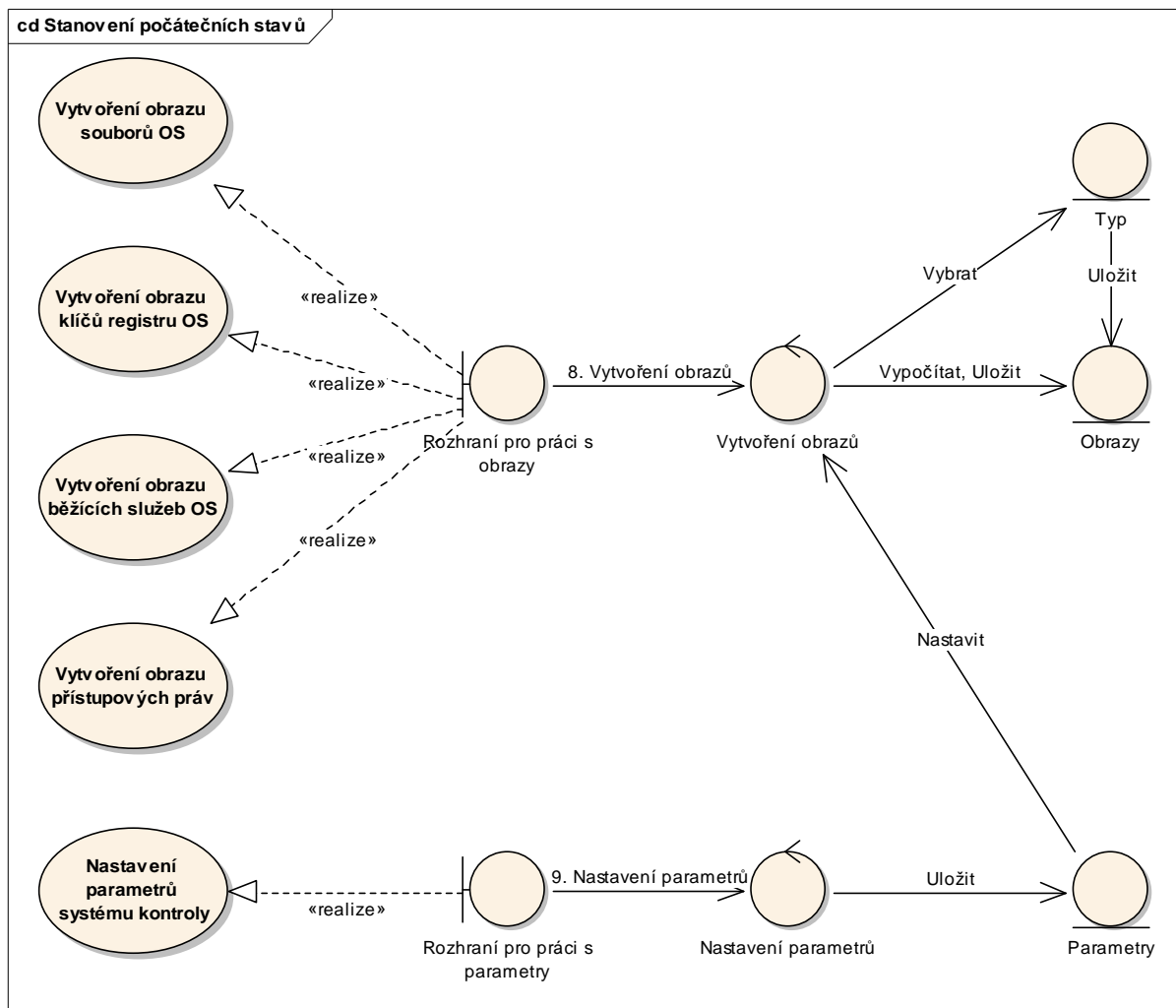
Tab. 46 Vazby Sluzby

**Soubory**

Vazba	Zdroj	Cíl
Asociace Přidat, Upravit, Smazat	Editace seznamu souborů	Soubory
Asociace Porovnat	Detekce	Soubory

Tab. 47 Vazby Soubory

### Stanovení počátečních stavů



Obr. 32 Stanovení počátečních stavů

### Nastavení parametrů

Vazba	Zdroj	Cíl
Asociace Uložit	Nastavení parametrů	Parametry
Asociace 9. Nastavení parametrů	Rozhraní pro práci s parametry	Nastavení parametrů

Tab. 48 Vazby Nastavení parametrů

### Obrazy

Vazba	Zdroj	Cíl
Asociace Vypočítat, Uložit	Vytvoření obrazů	Obrazy

Vazba	Zdroj	Cíl
Asociace Vybrat	Obrazy	Nastavení klíčů registru
Asociace Uložit	Typ	Obrazy
Asociace Vybrat	Obrazy	Nastavení přístupových práv

Tab. 49 Vazby Obrazy

#### Parametry

Vazba	Zdroj	Cíl
Asociace Nastavit	Parametry	Tvorba výstupu
Asociace Uložit	Nastavení parametrů	Parametry
Asociace Nastavit	Vytvoření obrazů	Parametry
Asociace Nastavit	Detekce	Parametry

Tab. 50 Vazby Parametry

#### Rozhraní pro práci s obrazy

Vazba	Zdroj	Cíl
Asociace 8. Vytvoření obrazů	Rozhraní pro práci s obrazy	Vytvoření obrazů
Realizace	Rozhraní pro práci s obrazy	Vytvoření obrazu souborů OS
Realizace	Rozhraní pro práci s obrazy	Vytvoření obrazu běžících služeb OS
Realizace	Rozhraní pro práci s obrazy	Vytvoření obrazu klíčů registru OS
Realizace	Rozhraní pro práci s obrazy	Vytvoření obrazu přístupových práv

Tab. 51 Vazby Rozhraní pro práci s obrazy

#### Rozhraní pro práci s parametry

Vazba	Zdroj	Cíl
Asociace 9. Nastavení parametrů	Rozhraní pro práci s parametry	Nastavení parametrů
Realizace	Rozhraní pro práci s parametry	Nastavení parametrů systému kontroly

Tab. 52 Vazby Rozhraní pro práci s parametry

## Vytvoření obrazů

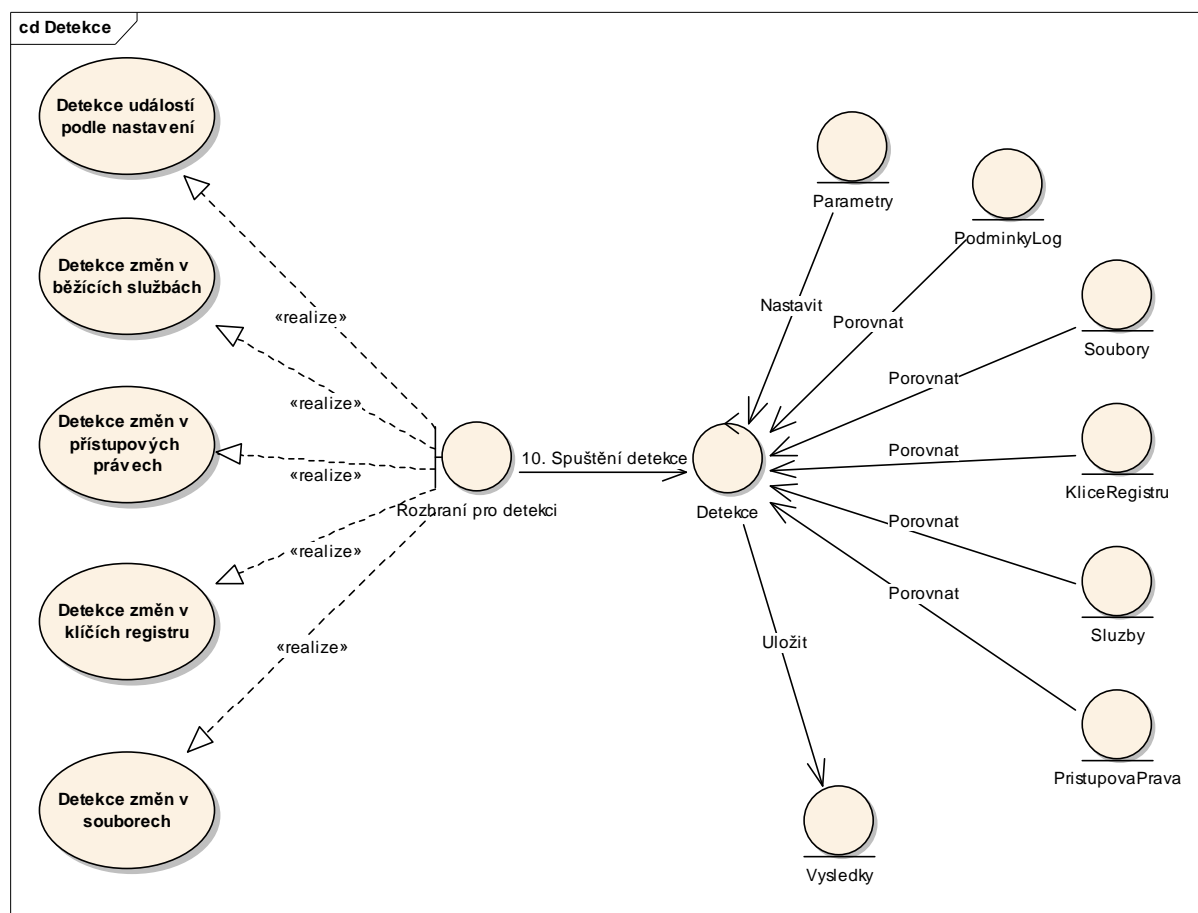
Vazba	Zdroj	Cíl
Asociace Vybrat	Vytvoření obrazů	Typ
Asociace Vypočítat, Uložit	Vytvoření obrazů	Obrazy
Asociace 8. Vytvoření obrazů	Rozhraní pro práci s obrazy	Vytvoření obrazů
Asociace Nastavit	Vytvoření obrazů	Parametry

Tab. 53 Vazby Vytvoření obrazů

## D.4.2 Provoz systému kontroly

Část systému kontroly, který popisuje běžný provoz systému kontroly.

## Detekce



Obr. 33 Detekce

**Detekce**

<b>Vazba</b>	<b>Zdroj</b>	<b>Cíl</b>
Asociace Porovnat	Detekce	Sluzby
Asociace Uložit	Detekce	Vysledky
Asociace Porovnat	PodminkyLog	Detekce
Asociace Porovnat	Detekce	PristupovaPrava
Asociace Nastavit	Detekce	Parametry
Asociace Porovnat	Detekce	Soubory
Asociace 10. Spuštění detekce	Rozhraní pro detekci	Detekce
Asociace Porovnat	Detekce	KliceRegistru

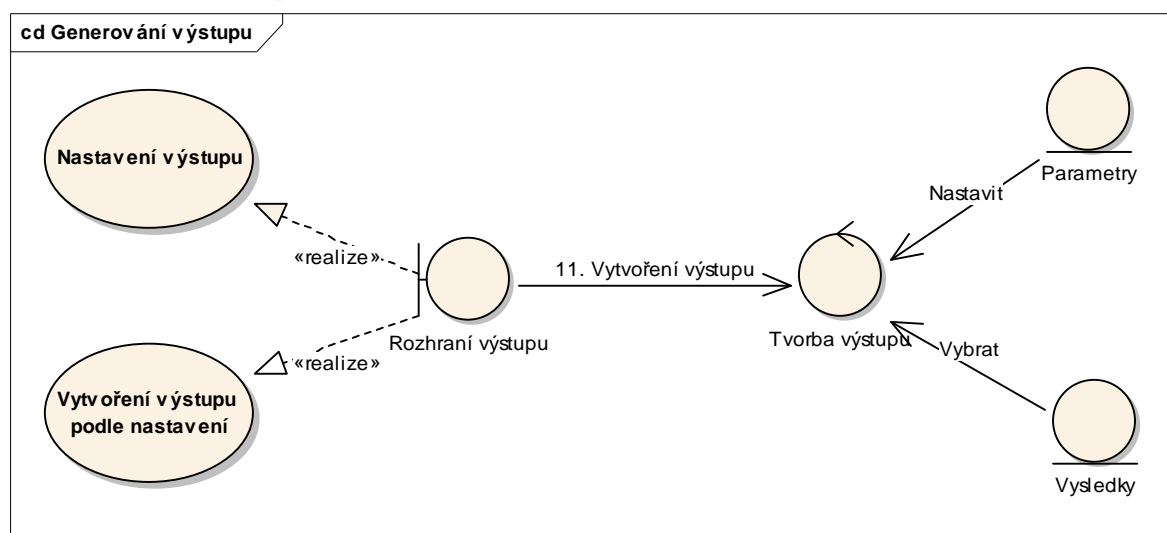
**Tab. 54 VazbyDetekce****Rozhraní pro detekci**

<b>Vazba</b>	<b>Zdroj</b>	<b>Cíl</b>
Asociace 10. Spuštění detekce	Rozhraní pro detekci	Detekce
Realizace	Rozhraní pro detekci	Detekce změn v souborech
Realizace	Rozhraní pro detekci	Detekce změn v běžících službách
Realizace	Rozhraní pro detekci	Detekce změn v klíčích registru
Realizace	Rozhraní pro detekci	Detekce událostí podle nastavení
Realizace	Rozhraní pro detekci	Detekce změn v přístupových právech

**Tab. 55 VazbyRozhraní pro detekci****Vysledky**

<b>Vazba</b>	<b>Zdroj</b>	<b>Cíl</b>
Asociace Uložit	Detekce	Vysledky
Asociace Vybrat	Vysledky	Tvorba výstupu

**Tab. 56 VazbyVysledky**

**Generování výstupu**

Obr. 34 Generování výstupu

**Rozhraní výstupu**

Vazba	Zdroj	Cíl
Asociace 11. Vytvoření výstupu	Rozhraní výstupu	Tvorba výstupu
Realizace	Rozhraní výstupu	Nastavení výstupu
Realizace	Rozhraní výstupu	Vytvoření výstupu podle nastavení

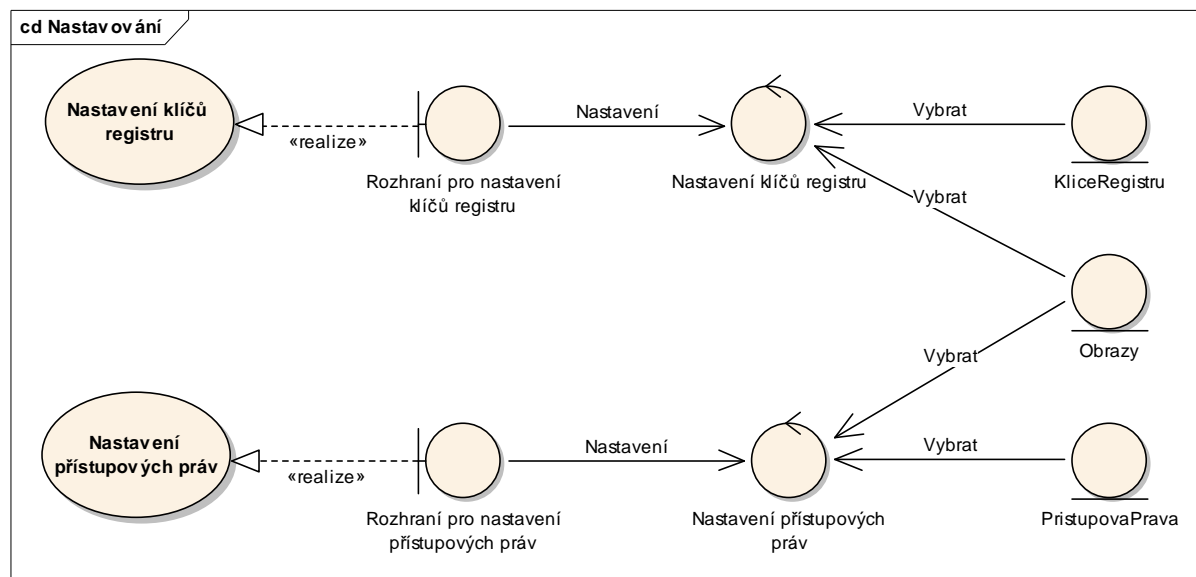
Tab. 57 Vazby Rozhraní výstupu

**Tvorba výstupu**

Vazba	Zdroj	Cíl
Asociace Nastavit	Parametry	Tvorba výstupu
Asociace 11. Vytvoření výstupu	Rozhraní výstupu	Tvorba výstupu
Asociace Vybrat	Vysledky	Tvorba výstupu

Tab. 58 Vazby Tvorba výstupu

## Nastavování



Obr. 35 Nastavování

### Nastavení klíčů registru

Vazba	Zdroj	Cíl
Asociace Vybrat	Obrazy	Nastavení klíčů registru
Asociace Nastavení	Rozhraní pro nastavení klíčů registru	Nastavení klíčů registru
Asociace Vybrat	KliceRegistru	Nastavení klíčů registru

Tab. 59 Vazby Nastavení klíčů registru

### Nastavení přístupových práv

Vazba	Zdroj	Cíl
Asociace Nastavení	Rozhraní pro nastavení přístupových práv	Nastavení přístupových práv
Asociace Vybrat	Obrazy	Nastavení přístupových práv
Asociace Vybrat	PristupovaPrava	Nastavení přístupových práv

Tab. 60 Vazby Nastavení přístupových práv

### Rozhraní pro nastavení klíčů registru

Vazba	Zdroj	Cíl
Asociace Nastavení	Rozhraní pro nastavení klíčů registru	Nastavení klíčů registru
Realizace	Rozhraní pro nastavení klíčů registru	Nastavení klíčů registru

Tab. 61 Vazby Rozhraní pro nastavení klíčů registru

**Rozhraní pro nastavení přístupových práv**

<b>Vazba</b>	<b>Zdroj</b>	<b>Cíl</b>
Asociace Nastavení	Rozhraní pro nastavení přístupových práv	Nastavení přístupových práv
Realizace	Rozhraní pro nastavení přístupových práv	Nastavení přístupových práv

**Tab. 62 Vazby Rozhraní pro nastavení přístupových práv**

## D.5 Prototyp uživatelského rozhraní

Kapitola obsahuje hrubý návrh uživatelského rozhraní pomocí symbolických prvků.

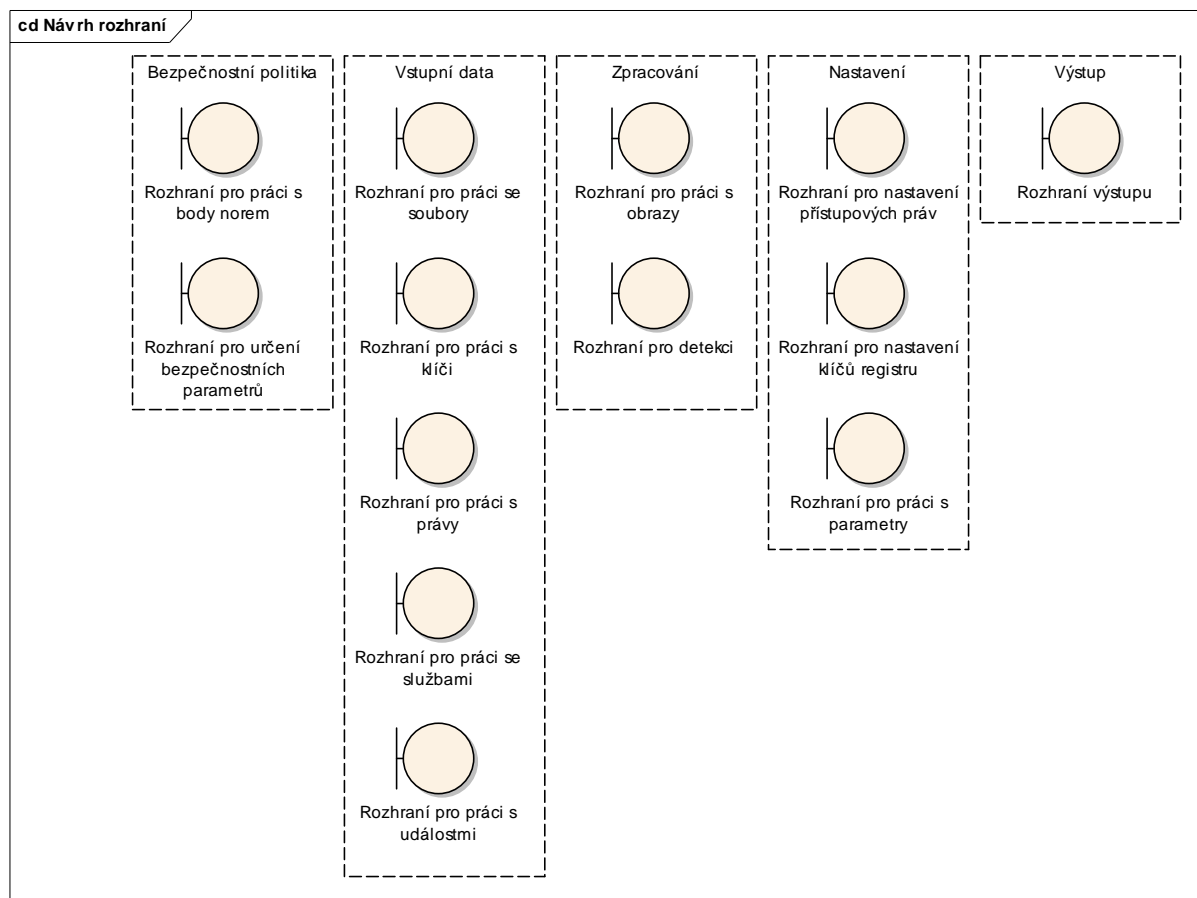
### D.5.1 Požadavky na rozhraní

Požadavky na rozhraní určuje především nefunkční požadavek „PN.01 Systém kontroly bude možné implementovat do serverových systémů uživatele na platformě Microsoft Windows“. Podle něj byly vybrány tyto 4 hlavní body:

- P.01 GRO musí mít standardní ovládací prvky.
- P.02 Hlavní ovládací panel bude ve formě menu.
- P.03 Seznamy dat budou zobrazeny ve formě tabulek.
- P.04 Vstupy dat budou realizovány ve formě oken.

### D.5.2 Hrubý grafický návrh rozhraní

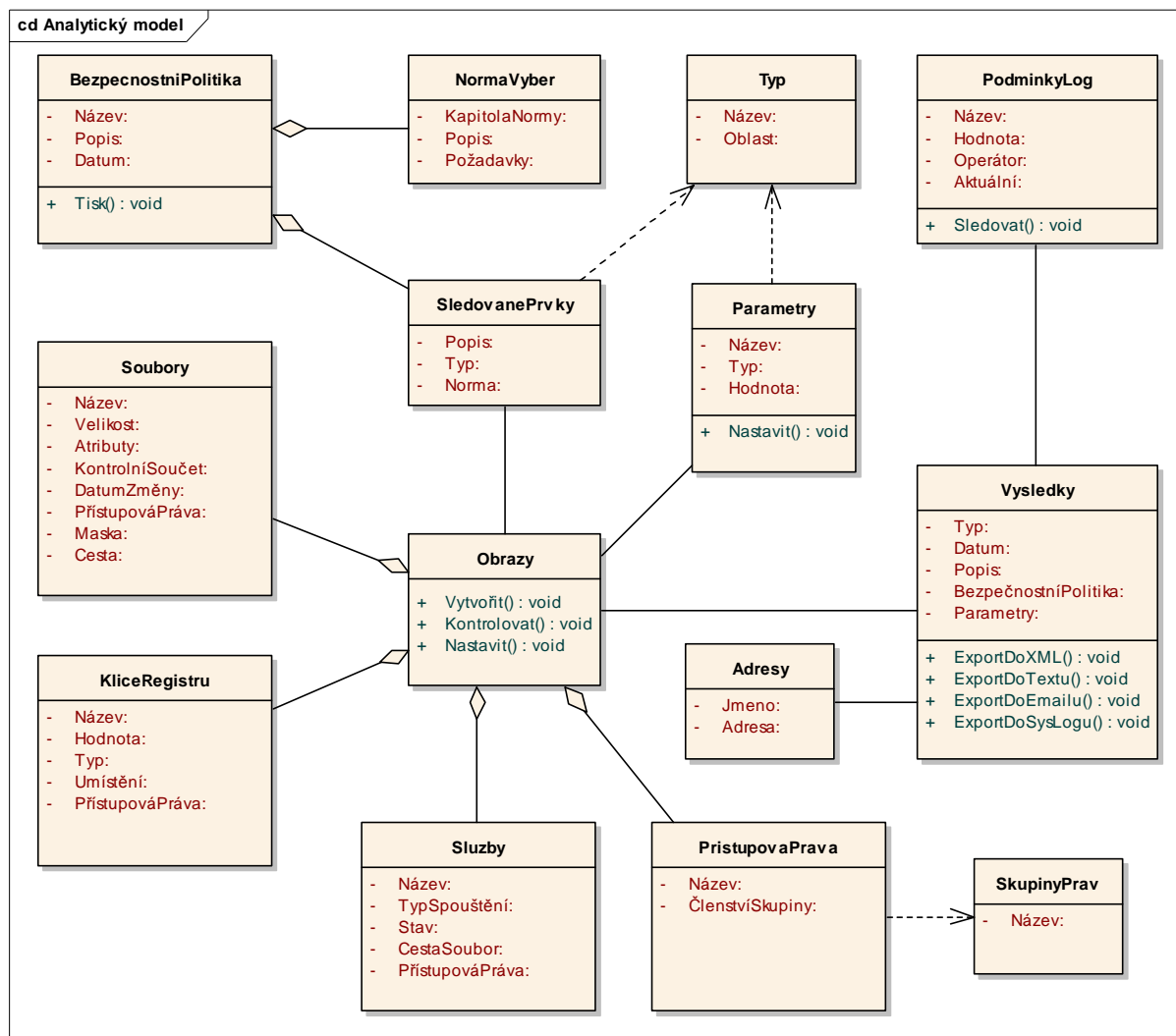
Návrh vychází z rozhraní použitých v realizaci případů užití. Jednotlivá rozhraní byla seskupena do tématických skupin, které mohou v budoucí implementaci ukazovat na položky hlavního menu.



Obr. 36 Návrh rozhraní

## D.6 Detailní diagramy analytických tříd

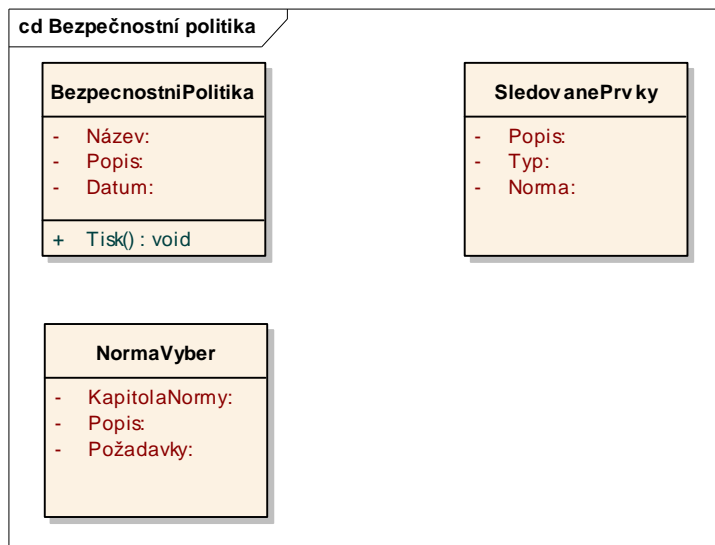
Model představuje analytické třídy návrhového modelu. Zároveň je možné vysledovat návrhy struktury budoucích objektů.



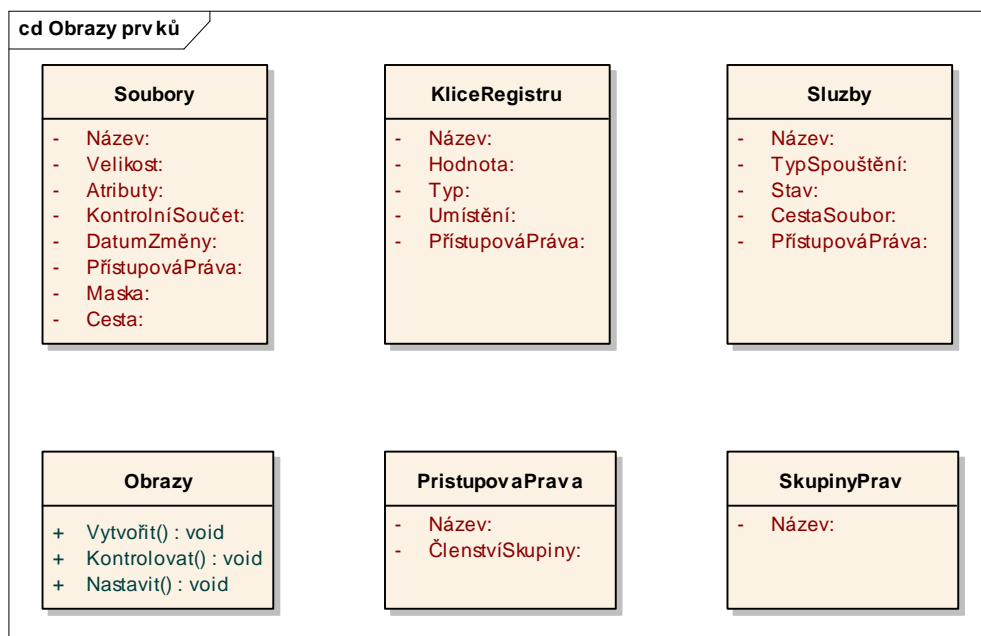
Obr. 37 Analytický model

## D.7 Detailní diagramy analytických balíčků

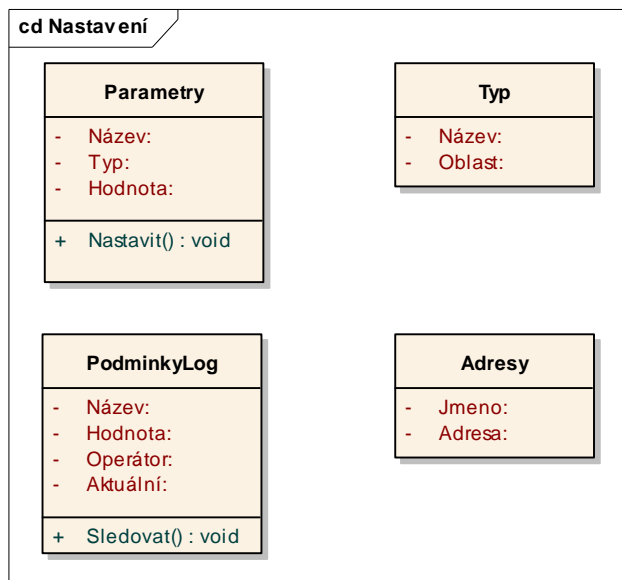
Podle architektonického návrhu a detailů tříd lze nyní specifikovat detaily jednotlivých analytických balíčků.



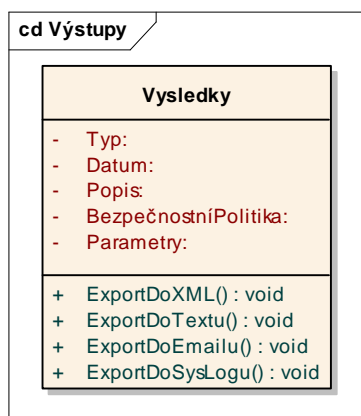
Obr. 38 Detail balíčku Bezpečnostní politika



Obr. 39 Detail balíčku Obrazy prvků



Obr. 40 Detail balíčku Nastavení



Obr. 41 Detail balíčku Výstupy

## **D.8 Vyhodnocení analytického modelu**

Analytický model je logickým pokračováním architektonického návrhu. Rozpracováním obsahu architektonického návrhu balíčků byl vytvořen analytický model s návrhem vnitřních struktur.

Vzniklý model postihuje celé zadání, navrhované struktury a funkce odpovídají požadavkům kladeným na budoucí softwarové řešení.



# Obsah

Dodatek A. - Analýza domény IS.....	1
A.1    Shromážděné podklady k doméně.....	1
A.1.1    Literatura k doméně.....	1
A.1.2    Legislativa k doméně.....	1
A.1.3    Standardy k doméně .....	1
A.1.4    Rešerše vybraných podkladů .....	2
A.2    Analýza současného stavu řešení v doméně.....	3
A.2.1    Přehled současných řešení.....	3
A.2.2    Závěry ke stavu řešení .....	5
A.3    Model domény.....	5
A.4    Procesy v doméně.....	6
A.5    Třídy domény .....	6
Dodatek B. - Systémové požadavky IS .....	9
B.1    Funkční požadavky.....	9
B.1.1    Zadání projektu.....	9
B.1.2    Analytické.....	13
B.2    Nefunkční požadavky .....	17
B.3    Priority požadavků .....	19
B.4    Budoucí uživatelé a jejich role .....	22
B.5    Případy užití .....	24
B.6    Priority případů užití .....	47
B.7    Systémové požadavky .....	49
Dodatek C. - Úvodní studie.....	51
C.1    Spolupracující systémy.....	51

C.2	Vrstvy a analytické balíčky .....	51
C.3	Analytické třídy .....	52
C.4	Nasazení systému .....	54
C.5	Omezující implementační podmínky .....	55
C.5.1	Vývojová technologie.....	55
C.5.2	Hardwarové požadavky.....	55
C.6	Požadavky na data a databáze .....	55
C.7	Vyhodnocení architektury systému .....	56
C.7.1	Přehled možných rizik.....	56
C.7.2	Zvážení variant řešení .....	56
C.7.3	Vhodnost implementačních metod.....	56
C.7.4	Návaznost na systémové požadavky .....	57
Dodatek D. - Globální návrh IS.....		59
D.1	Strukturovaný model případů užití.....	59
D.2	Strukturované scénáře případu užití .....	59
D.3	Slovník pojmů pro činnosti a třídy .....	59
D.4	Realizace případů užití .....	61
D.4.1	Definice systému kontroly.....	61
D.4.2	Provoz systému kontroly .....	71
D.5	Prototyp uživatelského rozhraní .....	76
D.5.1	Požadavky na rozhraní .....	76
D.5.2	Hrubý grafický návrh rozhraní .....	76
D.6	Detailní diagramy analytických tříd .....	77
D.7	Detailní diagramy analytických balíčků .....	79
D.8	Vyhodnocení analytického modelu .....	81