

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

Název zprávy:	Závěrečná zpráva projektu
Název části:	Část 2 ze dvou částí Dodatky
Období:	1.1.2005-31.12.2005

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

Odpovědný řešitel:	Ing. Radan Kasal
Spoluřešitelé:	Ing. Luděk Benda
	Ing. Tomáš Nagy
	Ing. Petr Půlpán
	Radek Valeš
	RNDr. Miroslav Wasserbauer
	Ing. Vítězslav Života
	Tibor Stiliz
Datum vydání:	31.1.2006

Obsah

Dodatek A. – Detailní návrh IS	1
A.1 Sekvenční diagramy v případech užití	1
A.1.1 Výběr relevantních bodů z BS 7799.....	1
A.1.2 Určení bezpečnostních parametrů	2
A.1.3 Vytvoření obrazů.....	3
A.1.4 Detekce.....	4
A.1.5 Generování výstupu.....	4
A.1.6 Implementace nefunkčních požadavků	5
A.2 Návrh podsystémů	6
A.2.1 Datová vrstva.....	11
A.2.1.1 Podsystém SysKoDb	11
A.2.2 Střední vrstva.....	12
A.2.2.1 Podsystém SysKoCore	12
A.2.2.2 Podsystém SysKoAsServer	12
A.2.2.3 Podsystém SysKoServer.....	13
A.2.3 Aplikační vrstva	13
A.2.3.1 Podsystém SysKoConsole	13
A.2.3.2 Podsystém SysKoAsClient.....	13
A.2.3.3 Podsystém SysKoApp	13
A.3 Návrhové třídy.....	13
A.3.1 Datová vrstva.....	14
A.3.1.1 Podsystém SysKoDb	14
A.3.2 Střední vrstva.....	23
A.3.2.1 Podsystém SysKoCore	23

A.3.2.2	Podsystem SysKoAsServer	28
A.3.2.3	Podsystem SysKoAsClient	36
A.3.3	Aplikační vrstva	43
A.3.3.1	Podsystem SysKoServer	43
A.3.3.2	Podsystem SysKoConsole	44
A.3.3.3	Podsystem SysKoApp	45
A.4	Návrh databáze	45
A.5	Plán testů softwarových jednotek	52
A.5.1.1	Softwarové jednotky	52
A.5.1.2	Testy funkcí	55
A.6	Vyhodnocení návrhového modelu	55
Dodatek B. - Implementace IS		56
B.1	Implementační model	56
B.2	Tvorba databáze	57
B.3	Kód servisní vrstvy	58
B.4	Testy servisní vrstvy	58
B.5	Kód aplikační vrstvy	58
B.6	Integrace servisní a aplikační vrstvy	58
B.7	Testy aplikační vrstvy	58
B.8	Kvalifikační testy	59
B.8.1	Kvalifikační požadavky	59
B.8.2	Seznam kvalifikačních testů	60
B.9	Vyhodnocení implementace	65
B.10	Protokol o kvalifikačním testování software	65
Dodatek C. – Kvalifikační testování systému		67
C.1	Plán kvalifikačního testování systému	67
C.1.1	Kvalifikační požadavky	67

C.1.2	Seznam kvalifikačních kritérií.....	67
C.2	Testovací data.....	69
C.3	Kvalifikační testování.....	69
C.4	Vyhodnocení integrace a testů systému.....	70
C.5	Protokol o kvalifikačním testování systému	70
Dodatek D. – Instalace a akceptace systému.....		73
D.1	Instalační program	73
D.2	Plán zavádění IS	74
D.3	Instalace, akceptační přezkoumání, kompletace.....	75
D.4	Protokol o převzetí IS.....	75
Dodatek E. – Výstupní dokumentace		77
E.1	Systémová příručka IS.....	77
E.2	Uživatelská příručka IS	77
E.3	Školící a učební testy.....	77

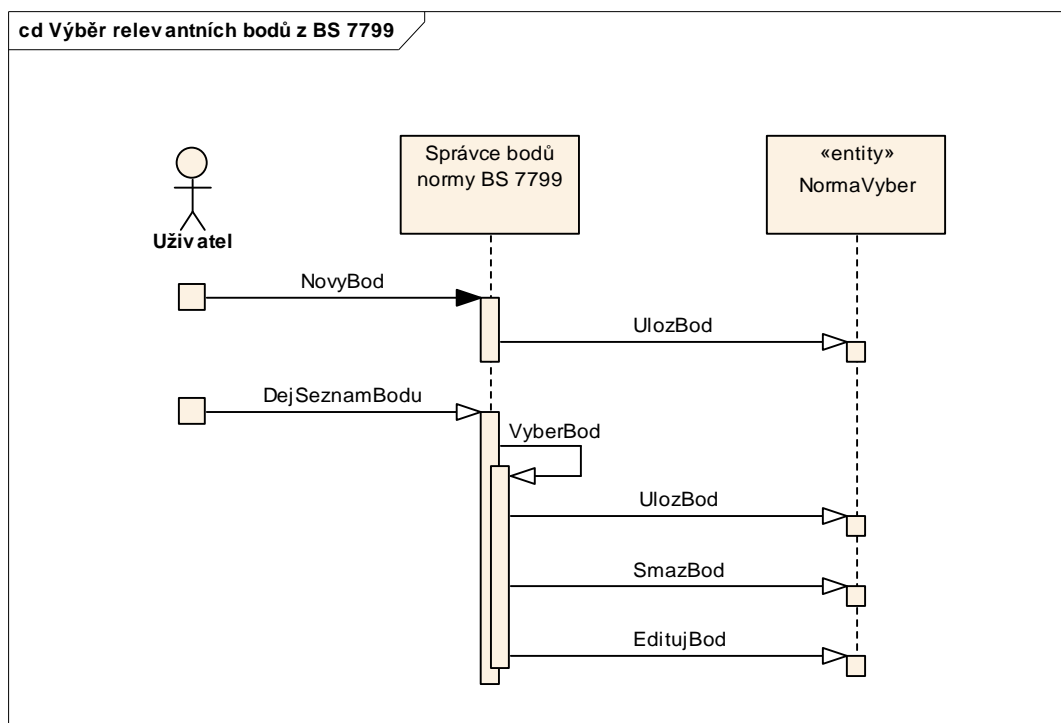
1. – Detailní návrh IS

1.1 Sekvenční diagramy v případech užití

Kapitola obsahuje konečnou verzi sekvenčních diagramů, které modelují funkcionalitu případů užití. Diagramy jsou pokračováním analytického modelu, který byl vypracováván v předchozím období.

1.1.1 Výběr relevantních bodů z BS 7799

Diagram ukazuje výměnu zpráv mezi objekty, které zabezpečují funkce pro práci s body normy BS7799. Zde budou obsaženy definice hodnot bezpečnostní politiky, které může systém kontroly sledovat.



Obr. 1 Sekvenční diagram pro výběr bodů BS 7799

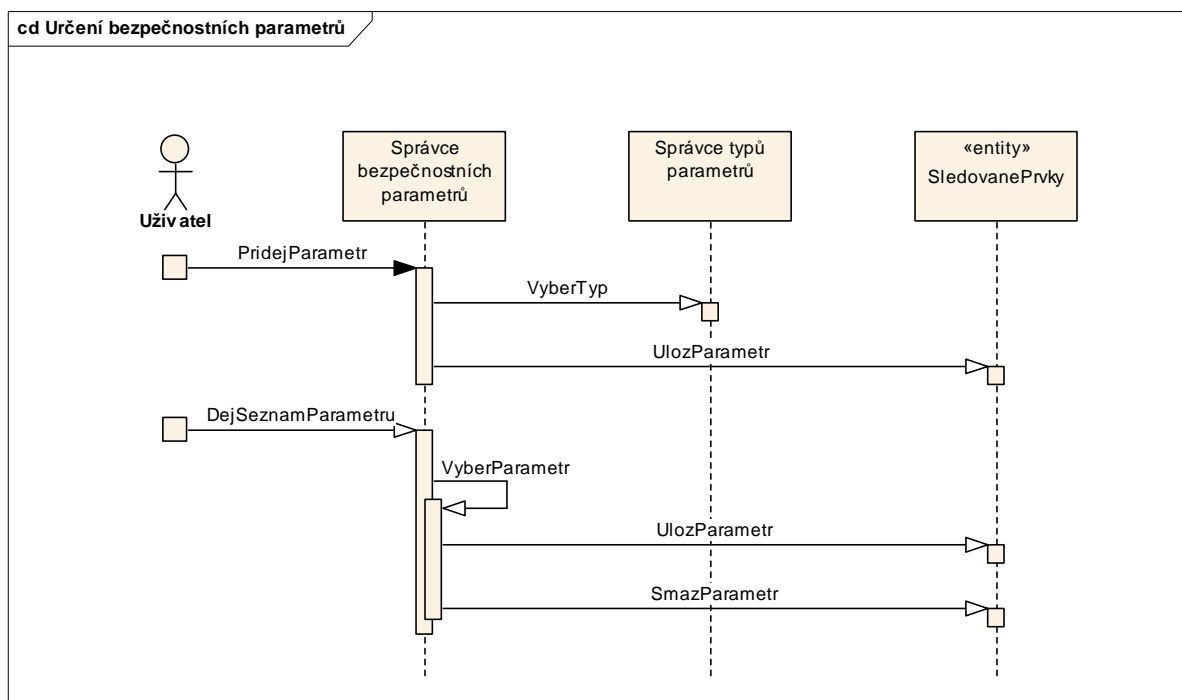
Zpráva	Z objektu	Do objektu	Popis
NovyBod	Uživatel	Správce bodů normy BS 7799	Zápis nového bodu normy BS 7799
DejSeznamBodu	Uživatel	Správce bodů normy BS 7799	Seznam bodů normy BS 7799 uložených v systému kontroly
VyberBod	Správce bodů normy BS 7799	Správce bodů normy BS 7799	Umožňuje vybrat bod normy BS 7799

Zpráva	Z objektu	Do objektu	Popis
UlozBod	Správce bodů normy BS 7799	NormaVyber	Uložení bodu normy BS 7799
SmazBod	Správce bodů normy BS 7799	NormaVyber	Vymazání bodu normy BS 7799
EditujBod	Správce bodů normy BS 7799	NormaVyber	Oprava nastavení bodu normy BS 7799

Tab. 1 Zprávy výběru relevantních bodů BS 7799

1.1.2 Určení bezpečnostních parametrů

Diagram ukazuje výměnu zpráv mezi objekty, které zabezpečují funkce nastavování bezpečnostních parametrů.



Obr. 2 Sekvenční diagram pro určení bezpečnostních parametrů

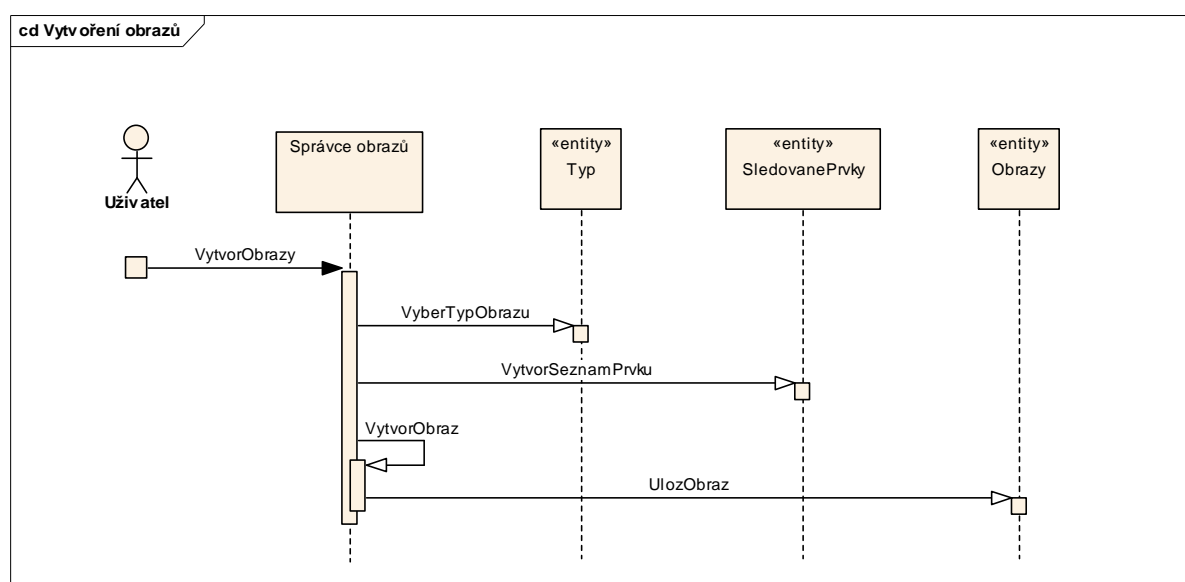
Spojení	Z objektu	Do objektu	Popis
PridejParametr	Uživatel	Správce bezpečnostních parametrů	Zápis nového bezpečnostního parametru
VyberTyp	Správce bezpečnostních parametrů	Správce typů parametrů	Umožňuje vybrat typ bezpečnostního parametru
UlozParametr	Správce bezpečnostních parametrů	SledovanePrvky	Uložení bezpečnostního parametru
DejSeznamParametru	Uživatel	Správce bezpečnostních parametrů	Seznam bezpečnostních parametrů systému kontroly

Spojení	Z objektu	Do objektu	Popis
VyberParametr	Správce bezpečnostních parametrů	Správce bezpečnostních parametrů	Umožňuje vybrat bezpečnostní parametr
SmazParametr	Správce bezpečnostních parametrů	SledovanePrvky	Mazání bezpečnostního parametru

Tab. 2 Zprávy určení bezpečnostních parametrů

1.1.3 Vytvoření obrazů

Diagram ukazuje výměnu zpráv mezi objekty, které zabezpečují funkce vytvoření obrazů sledovaných částí OS.



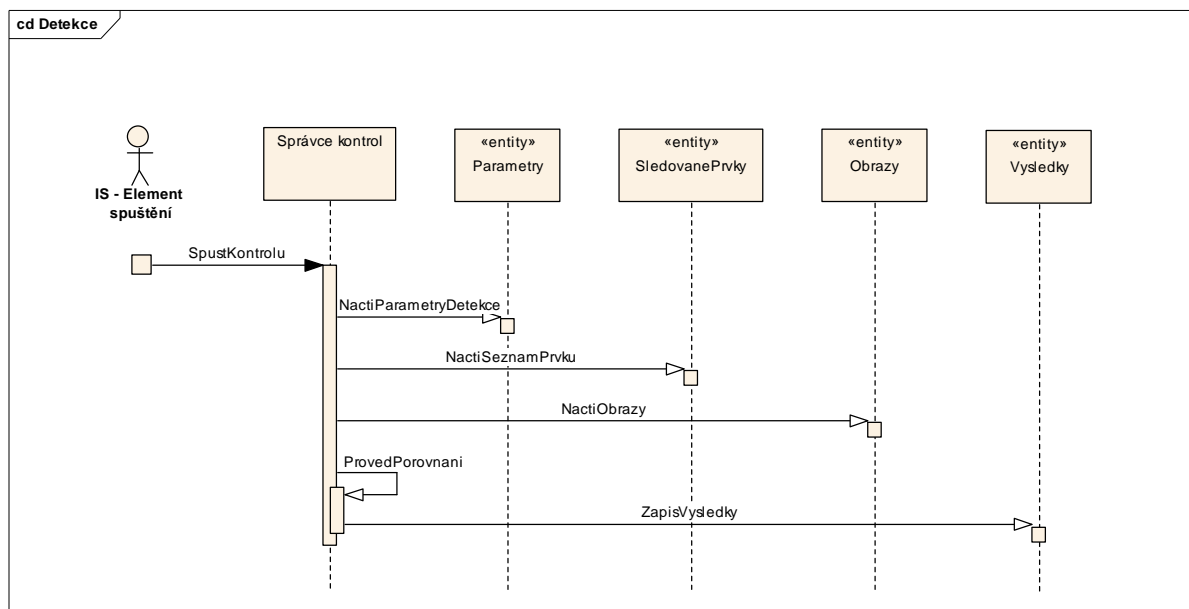
Obr. 3 Sekvenční diagram pro vytvoření obrazů

Spojení	Z objektu	Do objektu	Popis
VytvorObrazy	Uživatel	Správce obrazů	Vytvoření obrazů sledovaných prvků
VyberTypObrazu	Správce obrazů	Typ	Výběr okruhu sledovaných prvků
VytvorObraz	Správce obrazů	Správce obrazů	Generování vybraného obrazu
VytvorSeznamPrvku	Správce obrazů	SledovanePrvky	Stanovení seznamu prvků pro generování obrazů
UlozObraz	Správce obrazů	Obrazy	Uložení obrazů do databáze

Tab. 3 Zprávy vytvoření obrazů

1.1.4 Detekce

Diagram ukazuje výměnu zpráv mezi objekty, které zabezpečují funkce pro detekování změn v OS.



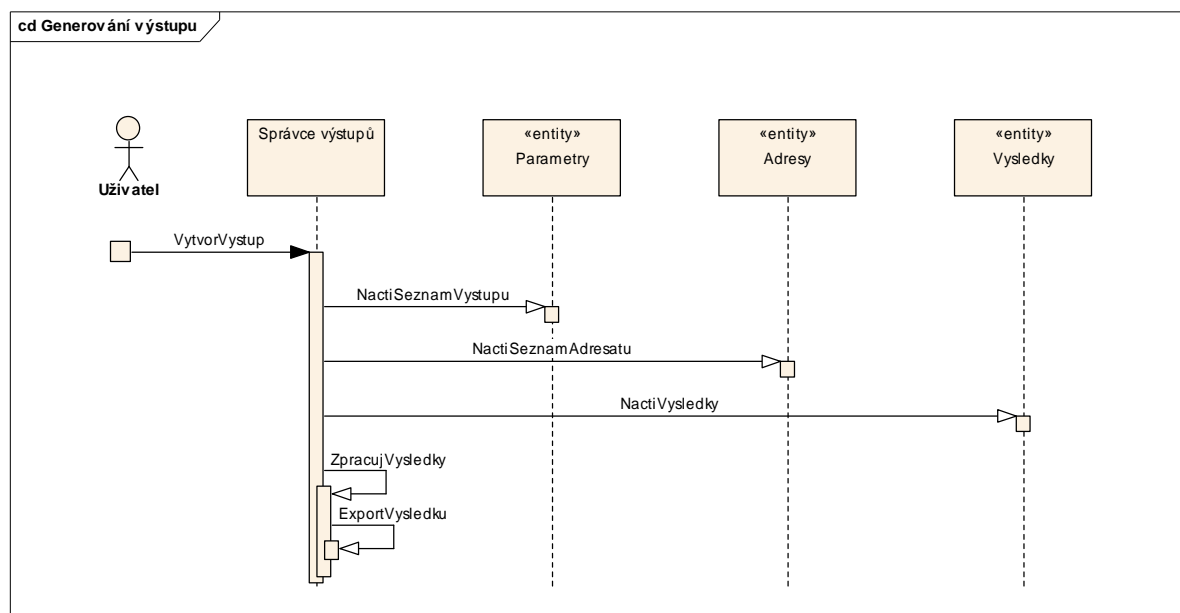
Obr. 4 Sekvenční diagram pro detekci

Spojení	Z objektu	Do objektu	Popis
SpustKontroly	IS – Element spuštění	Správce kontrol	Spuštění porovnávání výsledků s uloženými obrazy
NactiParametryDetekce	Správce kontrol	Parametry	Načtení parametrů, podle kterých se bude detekce provádět
NactiSeznamPrvku	Správce kontrol	SledovanePrvky	Načtení seznamu sledovaných prvků
NactiObrazy	Správce kontrol	Obrazy	Načtení uložených obrazů
ProvedPorovnavani	Správce kontrol	Správce kontrol	Porovnání výsledků detekce a uložených obrazů
ZapisVysledky	Správce kontrol	Vysledky	Zápis výsledků porovnání

Tab. 4 Zprávy detekce

1.1.5 Generování výstupu

Diagram ukazuje výměnu zpráv mezi objekty, které zabezpečují funkce pro výstup výsledků systému kontroly.



Obr. 5 Sekvenční diagram pro generování výstupu

Spojení	Z objektu	Do objektu	Popis
VytvorVystup	Uživatel	Správce výstupů	Vytvoření výstupu
NactiSeznamVystupu	Správce výstupů	Parametry	Načtení seznamu všech typů výstupu, které je třeba vytvořit
NactiSeznamAdresatu	Správce výstupů	Adresy	Načtení seznamu všech adresátů výstupu
NactiVysledky	Správce výstupů	Vysledky	Načtení všech příslušných výsledků
ZpracujVysledky	Správce výstupů	Správce výstupů	Vytvoření formátovaných výstupů
ExportVysledku	Správce výstupů	Správce výstupů	Předání výstupů adresátům

Tab. 5 Zprávy generování výstupu

1.1.6 Implementace nefunkčních požadavků

Nefunkční (doplňkové) požadavky jsou realizovány podle následujícího popisu.

ID	Požadavek	Realizace
PN.01	Systém kontroly bude možné implementovat do serverových systémů uživatele na platformě Microsoft Windows.	Pro realizaci systému kontroly jsou použity funkce API systému Windows.
PN.02	Systém kontroly bude implementován do systému poskytovatele ISOKR.	Systém kontroly je kompatibilní s OS Windows systému ISOKR.

PN.03	Systém kontroly bude mít možnost se rozšířit o budoucí požadavky na dopravní inteligentní systémy s vazbou na oblast státní správy.	Systém lze nastavit podle požadavků uživatele pro sledování požadovaných částí OS modifikací konfiguračních souborů. Systém lze dále rozšiřovat pomocí grafických prvků, výstupních sestav a rozšiřováním funkčnosti.
PN.04	Systém kontroly obsahuje tabulky pro shromáždění dat.	Datové tabulky jsou součástí implementace systému kontroly.
PN.05	Systém kontroly bude mít standardizované uživatelské rozhraní.	Grafická část rozhraní je provedena podle standardů používaných v programech pro OS Windows. Konfigurační soubory a výstupní sestavy odpovídají standardu XML verze 1.0.
PN.06	Přístup do systému kontroly bude omezen na autorizované osoby.	Po spuštění systému kontroly je uživatel identifikován.

Tab. 6 Realizace nefunkčních požadavků

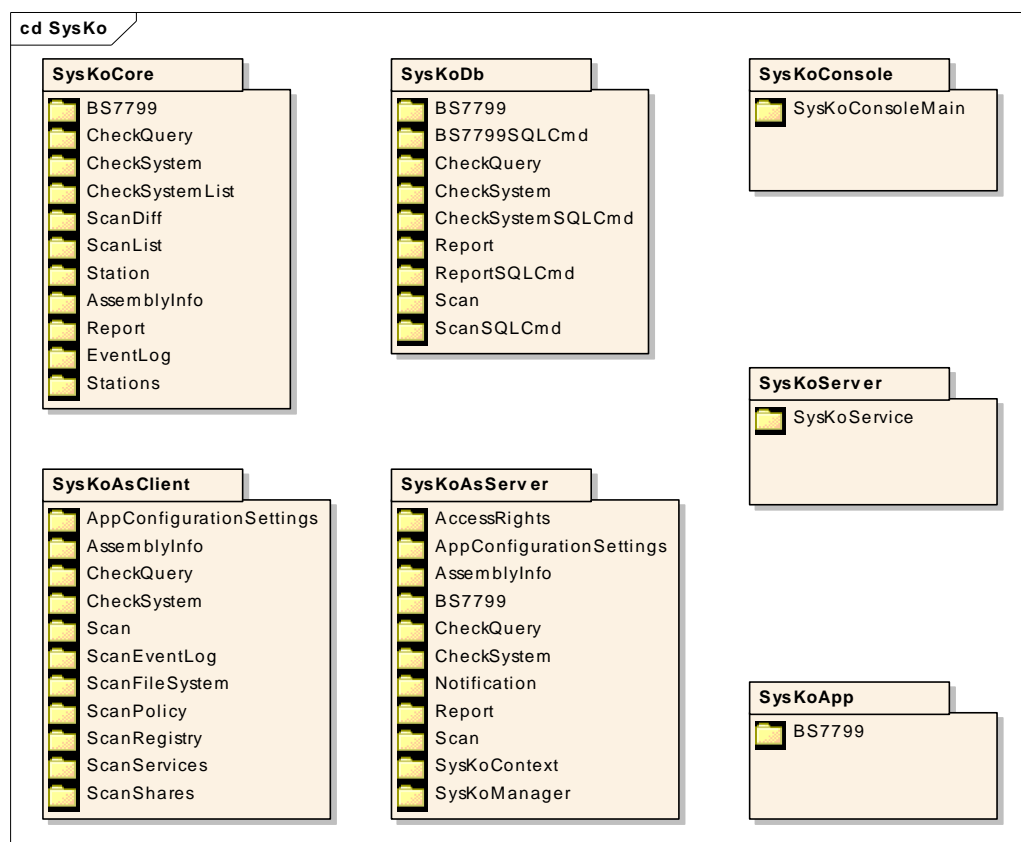
1.2 Návrh podsystémů

Celý systém kontroly (pro další použití zkráceně SysKo) byl rozdělen do 7 podsystémů podle umístění v jednotlivých vrstvách a podle použití.

Datová vrstva obsahuje podsystém SysKodb.

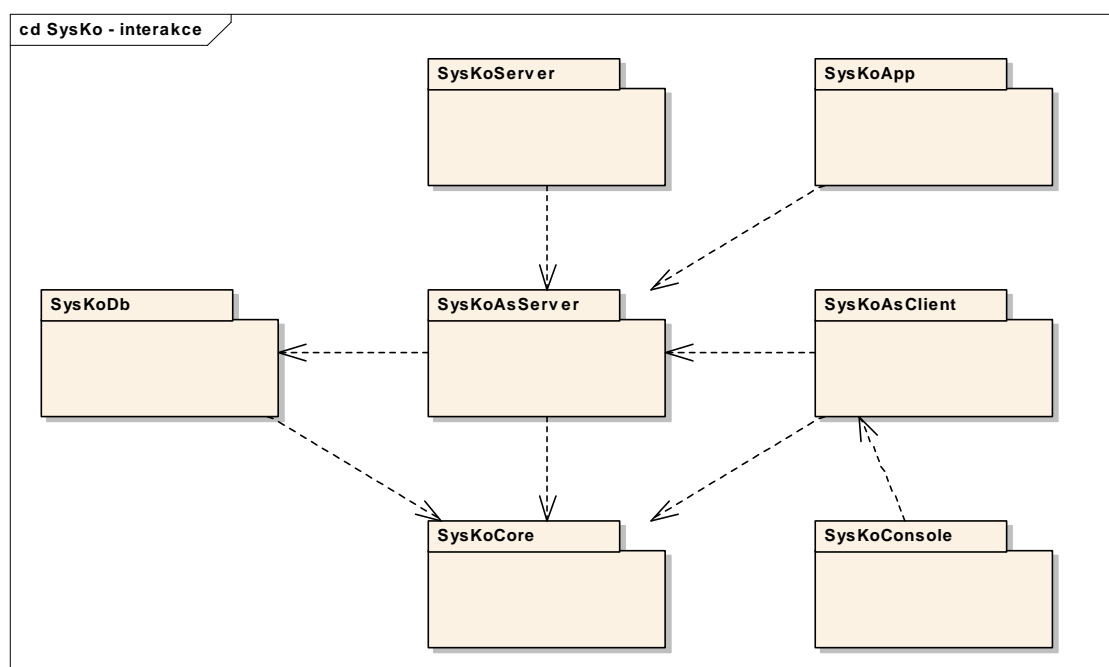
Střední vrstva obsahuje podsystém SysKoServer, SysKoAsServer a SysKoCore.

Aplikační vrstva obsahuje podsystém SysKoConsole, SysKoAsClient a SysKoApp.



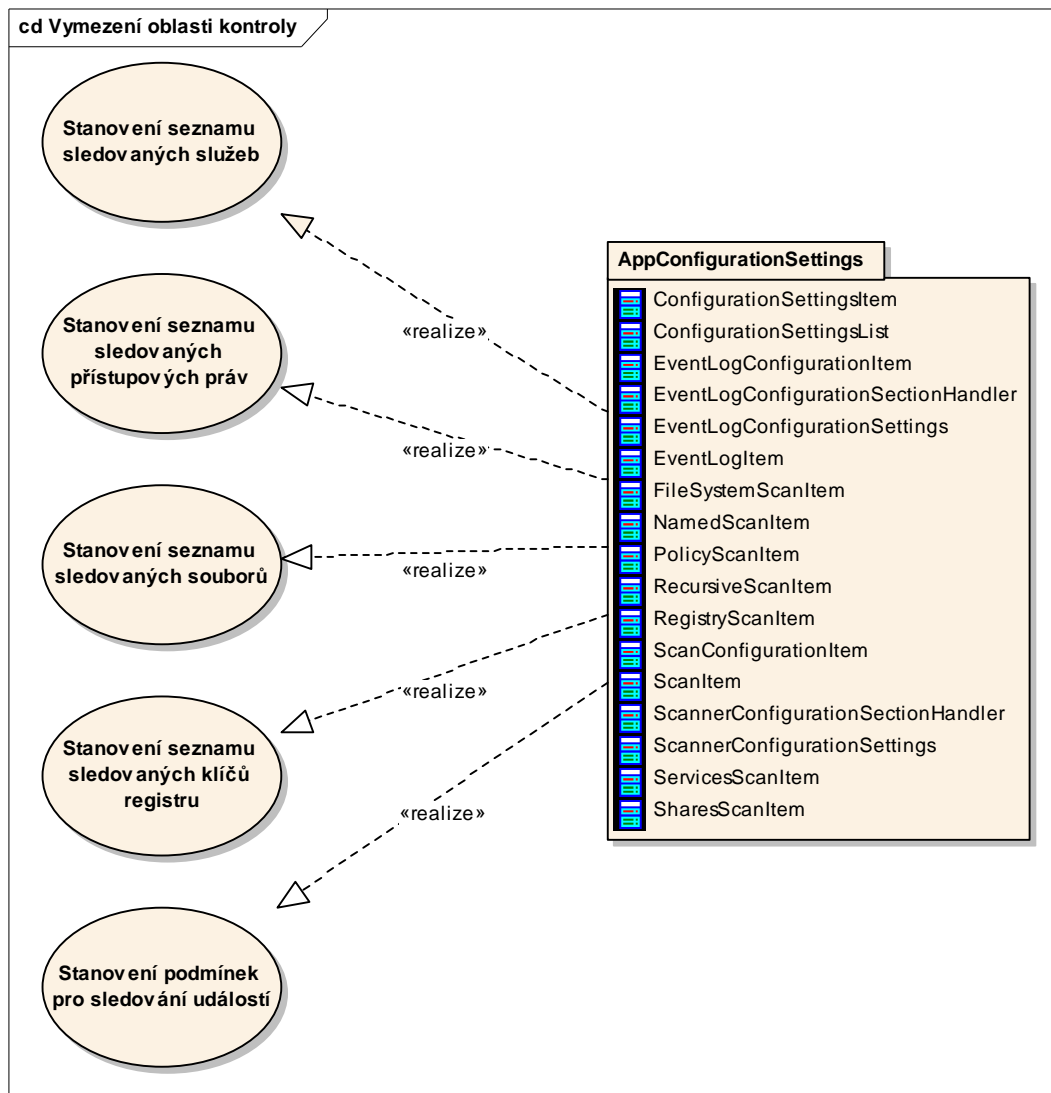
Obr. 6 Podsystemy SysKo

Jejich interakci na nejvyšší úrovni ukazuje následující diagram. V různých navrhovaných podsystémech jsou okruhy návrhových tříd se stejným názvem. Je to způsobeno děděním tříd podle naznačených závislostí.

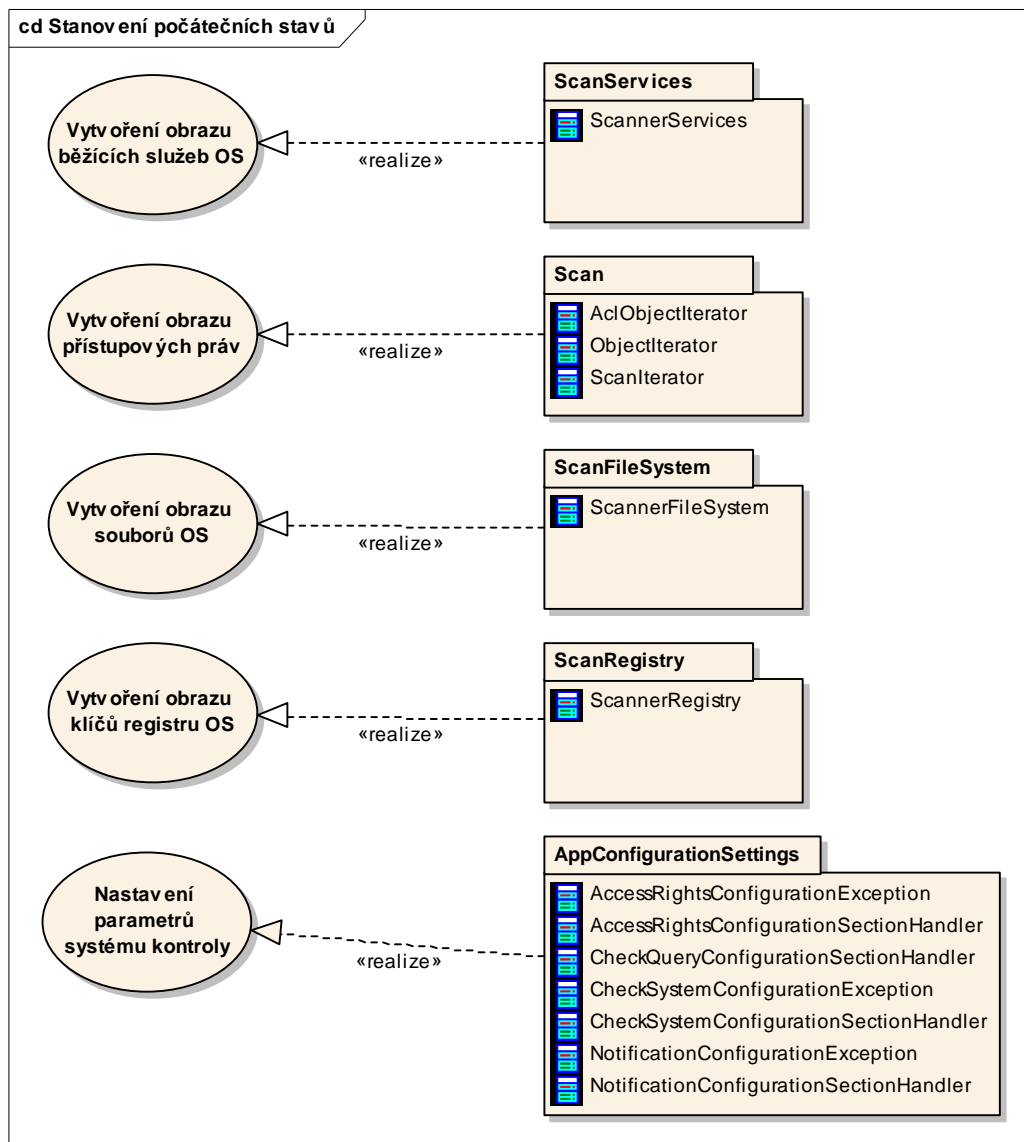


Obr. 7 Závislost podsystémů SysKo

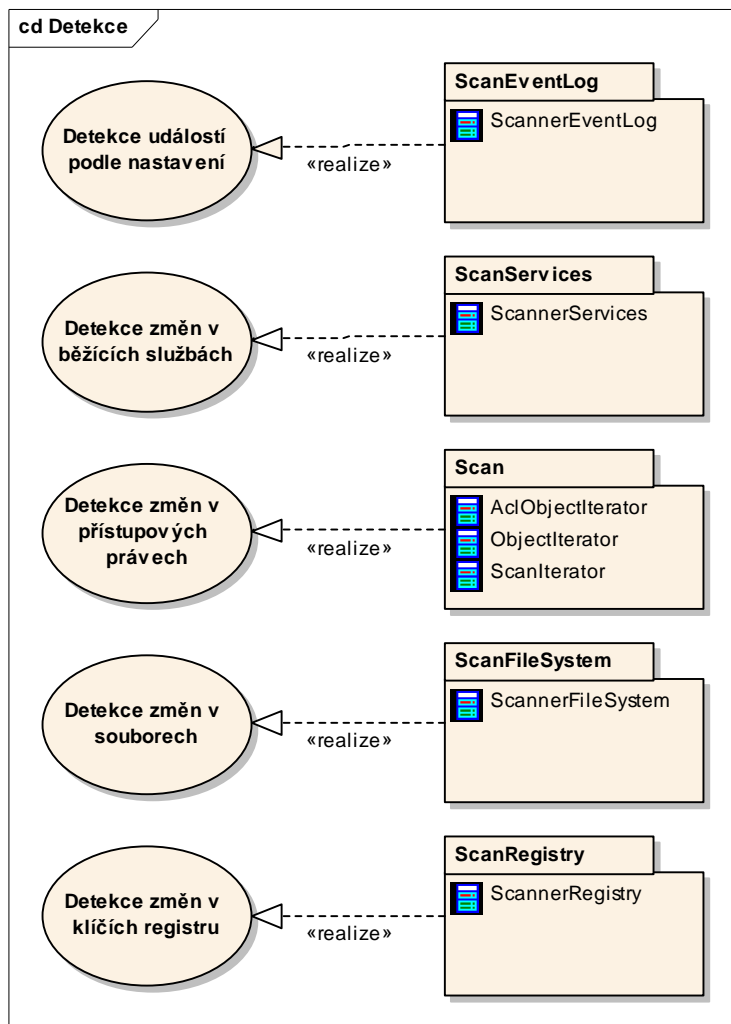
Návaznost návrhových tříd na případy užití z analytické fáze návrhu systému zobrazují následující diagramy.



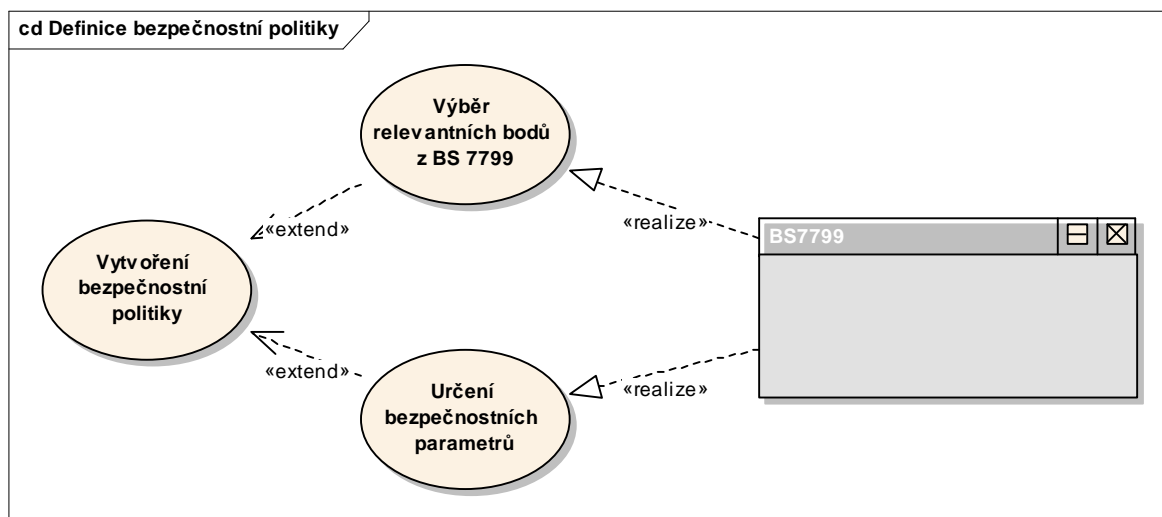
Obr. 8 Realizace Vymezení oblasti kontroly



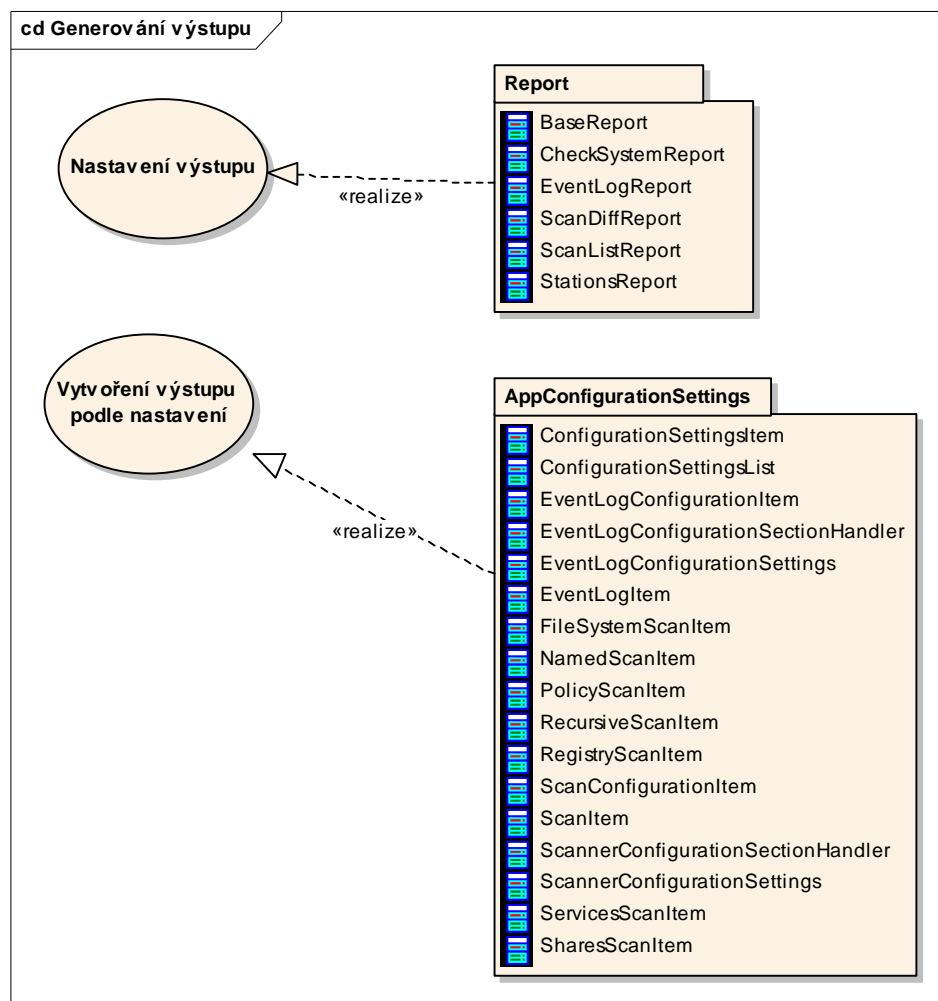
Obr. 9 Realizace Stanovení počátečních stavů



Obr. 10 Realizace Detekce změn



Obr. 11 Realizace Definice bezpečnostní politiky



Obr. 12 Realizace Generování výstupů

1.2.1 Datová vrstva

Tato kapitola obsahuje podsystém návrhových tříd pro datovou vrstvu.

1.2.1.1 Podsystém SysKoDb

Podsystém zabezpečuje spolupráci SysKo a datového zdroje. Skládá se z následujících okruhů návrhových tříd:

- BS7799
- BS7799SQLCmd
- CheckQuery
- CheckSystem
- CheckSystemSQLCmd
- Report
- ReportSQLCmd

- Scan
- ScanSQLCmd

1.2.2 Střední vrstva

Tato kapitola obsahuje podsystémy návrhových tříd pro střední vrstvu.

1.2.2.1 Podsystem SysKoCore

Podsystem obsahuje základní komponenty SysKo, které využívají jak podsystémy střední vrstvy, tak i vrstvy aplikační. Skládá z následujících okruhů návrhových tříd:

- BS7799
- CheckQuery
- CheckSystem
- CheckSystemList
- ScanDiff
- ScanList
- Station
- Report
- EventLog
- Stations

1.2.2.2 Podsystem SysKoAsServer

Podsystem zabezpečuje servis pro serverovou část SysKo. Skládá se z následujících okruhů návrhových tříd:

- AccessRights
- AppConfigurationSettings
- BS7799
- CheckQuery
- CheckSystem
- Notification
- Report
- Scan
- SysKoContext
- SysKoManager

1.2.2.3 Podsystem SysKoServer

Podsystem zabezpečuje ovládání serverové části kódu a obsahuje jeden okruh návrhových tříd:

- SysKoService

1.2.3 Aplikační vrstva

Tato kapitola obsahuje podsystemy návrhových tříd pro aplikační vrstvu.

1.2.3.1 Podsystem SysKoConsole

Podsystem zabezpečuje ovládání klientské části kódu a obsahuje jeden okruh návrhových tříd:

- SysKoConsoleMain

1.2.3.2 Podsystem SysKoAsClient

Podsystem zabezpečuje servis pro klientskou část SysKo. Skládá se z následujících okruhů návrhových tříd:

- AppConfigurationSettings
- CheckQuery
- CheckSystem
- Scan
- ScanEventLog
- ScanFileSystem
- ScanPolicy
- ScanRegistry
- ScanServices
- ScanShares

1.2.3.3 Podsystem SysKoApp

Podsystem obsahuje grafické rozhraní pro definici bezpečnostní politiky ve vztahu k normě BS7799. Skládá se z jednoho okruhu návrhových tříd:

- SysKoApp

1.3 Návrhové třídy

Následuje detailní popis návrhových tříd v jednotlivých vrstvách a podsystemech. Některé třídy jsou odvozené z obecné knihovny tříd firmy WAK System spol. s r.o., jejichž popis není předmětem této zprávy.

1.3.1 Datová vrstva

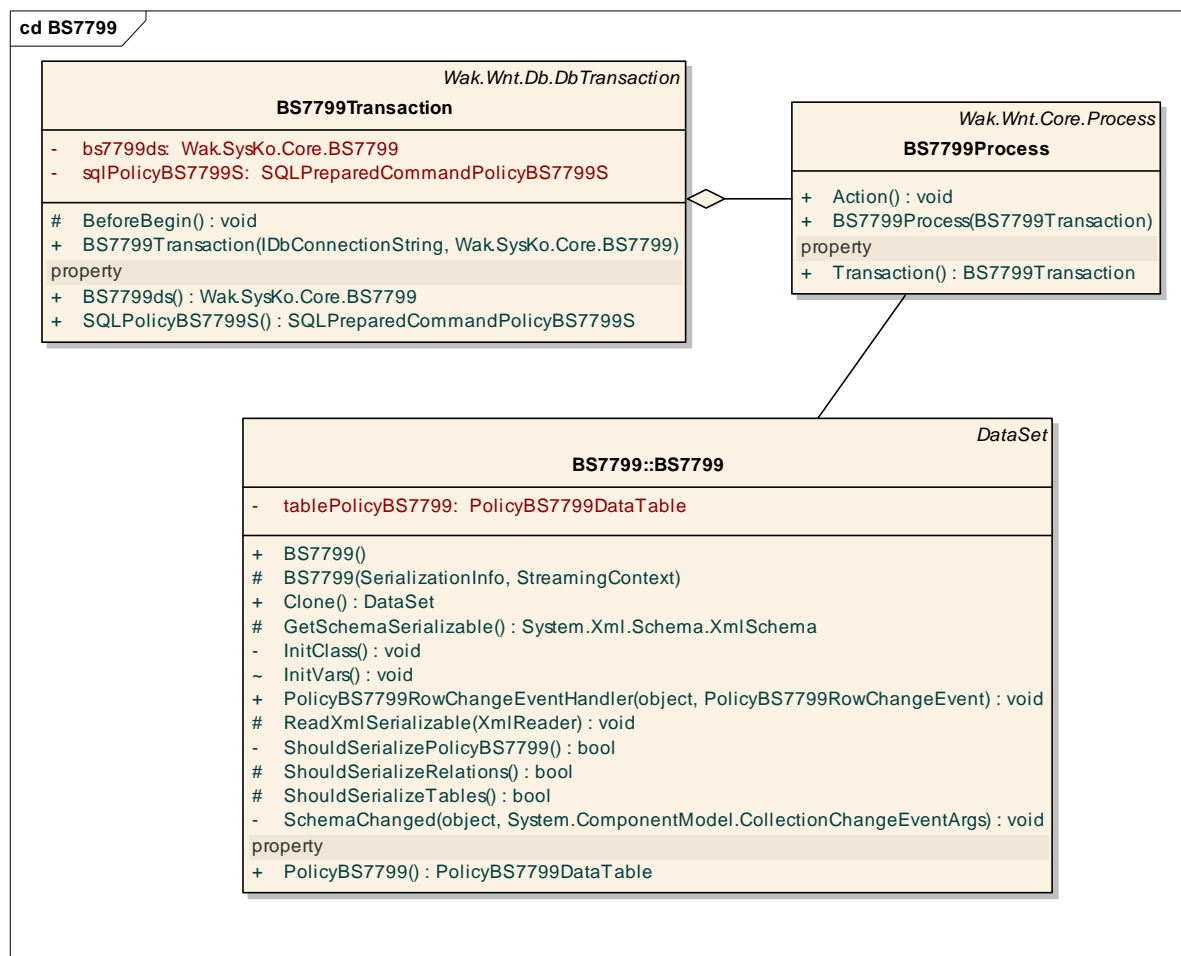
1.3.1.1 Podsystem SysKoDb

Č.	Jednotka	Funkce	Popis
1	BS7799Process	Action	Transakce procesu BS7799.
2	CheckQueryProcess	Action	Transakce procesu CheckQuery.
3	CheckSystemProcess	Action	Transakce procesu CheckSystem.
4	EventLogProcess	Action	Transakce procesu EventLog.
5	ReportProcess	Action	Transakce procesu Report.
6	ReportProcess	CreateDiffResult	Výsledný rozdíl.
7	ReportProcess	GetBinaryValuesAsString	Převod binární hodnoty na řetězec.
8	ReportProcess	GetHashACEs	Vrátí hašovací hodnotu objektu ACL (Access control list).
9	ReportProcess	GetHashValues	Vrátí hašovací hodnotu objektu.
10	ReportProcess	LocateBinaryDiff	Rozdíl mezi dvěma binárními hodnotami.
11	ReportProcess	ProcessBinaryValues	Zpracování binárních hodnot.
12	ReportProcess	ReportACEs	Výstup pro ACL.
13	ReportProcess	ReportCheckItemRequests	Výsledek kontroly.
14	ReportProcess	ReportCheckSystem	Výsledek kontroly systému.
15	ReportProcess	ReportEventLog	Výsledek kontroly událostí (eventlogu).
16	ReportProcess	ReportObjectOSDiff	Celkový výstup rozdílů.
17	ReportProcess	ReportOneScanDiff	Výsledek rozdílu dvou kontrol.
18	ReportProcess	ReportScanDiff	Výsledek scanneru.
19	ReportProcess	ReportScanList	Výsledek dotazu na hledané kontroly.
20	ReportProcess	ReportStations	Výsledek dotazu na stanici.
21	ReportProcess	ReportValue	Výsledek porovnání dvou objektů podle hašovacích hodnot.
22	ReportTransaction	CreateCommands	Hlavní funkce pro výstup výsledků.
23	ScanDiff	ReadXmlSerializable	Načtení datasetu.
24	ScanProcess	Action	Transakce procesu Scan.

Tab. 7 Popis funkcí podsystemu SysKoDb

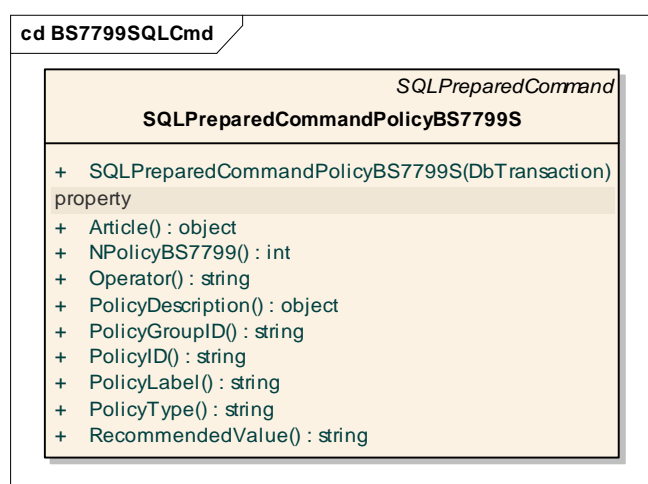
Jednotlivé návrhové třídy zprostředkovávají korektní komunikaci s jednotlivými tabulkami pracovní databáze, resp. s datasety nad těmito tabulkami.

1.3.1.1.1 BS7799



Obr. 13 Diagram tříd BS7799

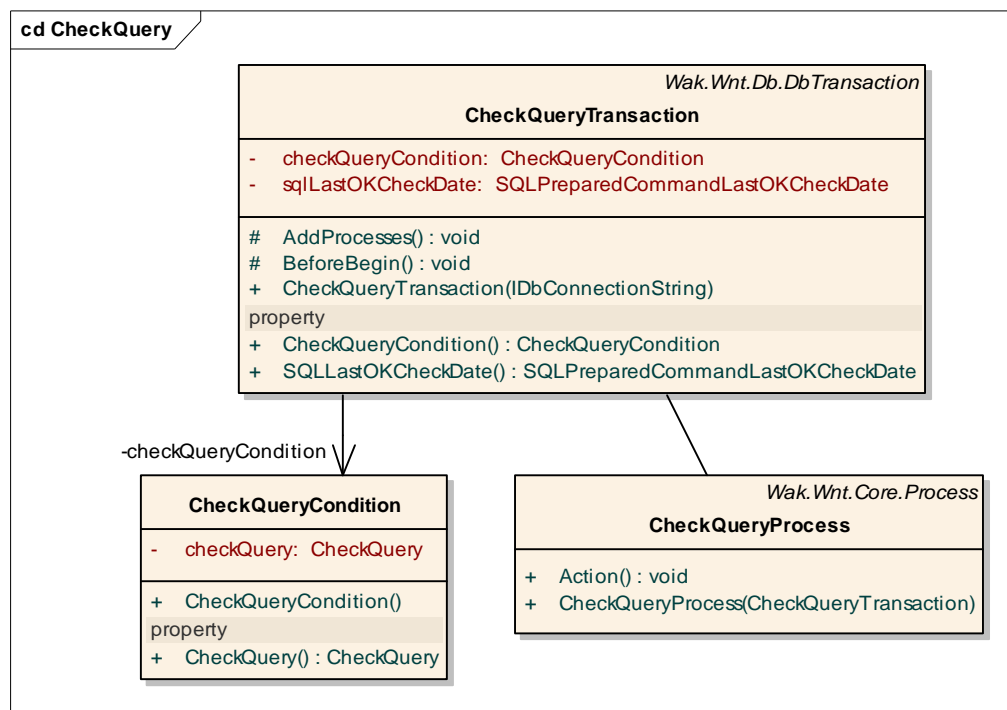
1.3.1.1.2 BS7799SQLCmd



Obr. 14 Diagram tříd BS7799SQLCmd

1.3.1.1.3 CheckQuery

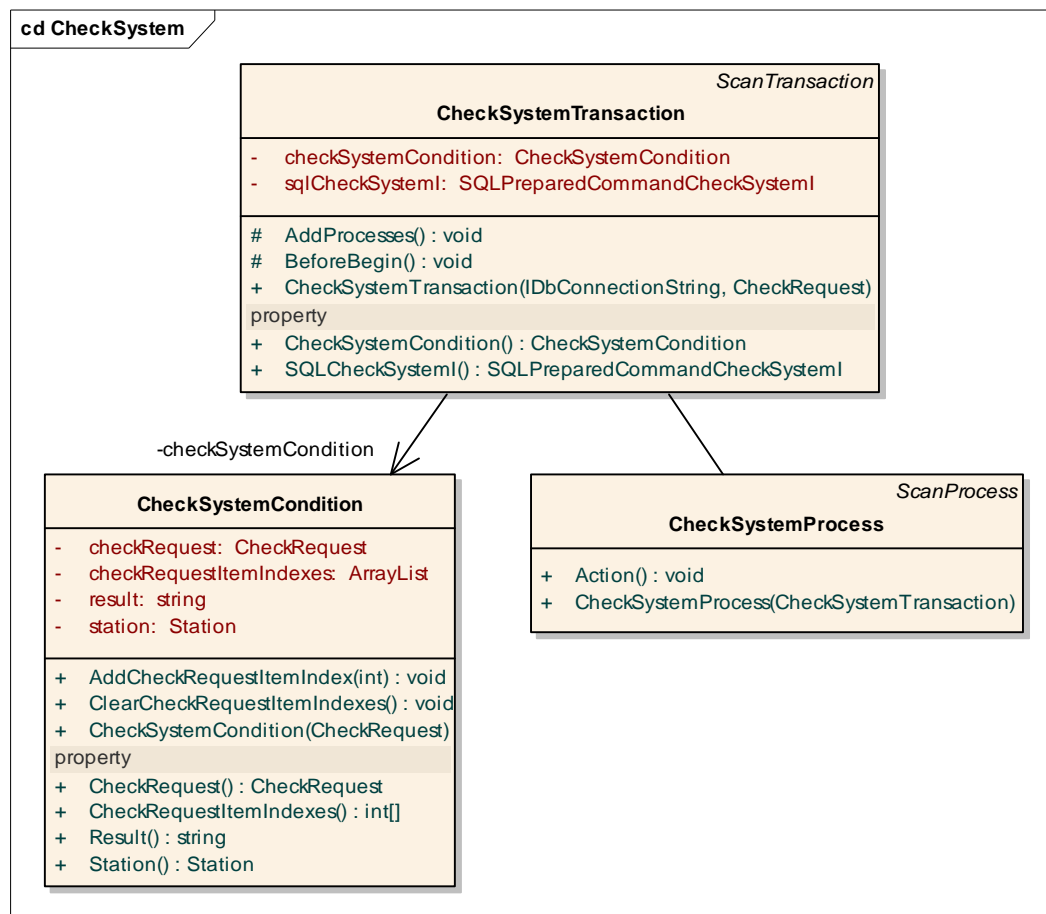
Ukládání výsledku z kontroly OS do databáze.



Obr. 15 Diagram tříd CheckQuery

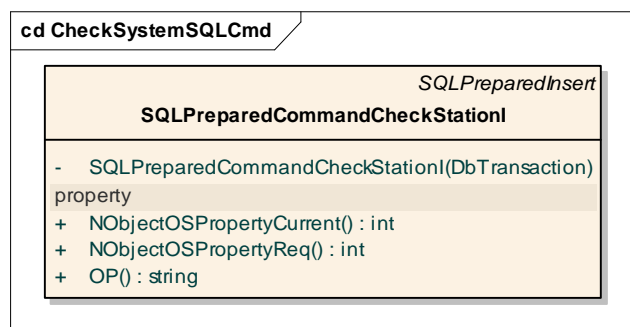
1.3.1.1.4 CheckSystem

Ukládání výsledku z kontroly OS do databáze.



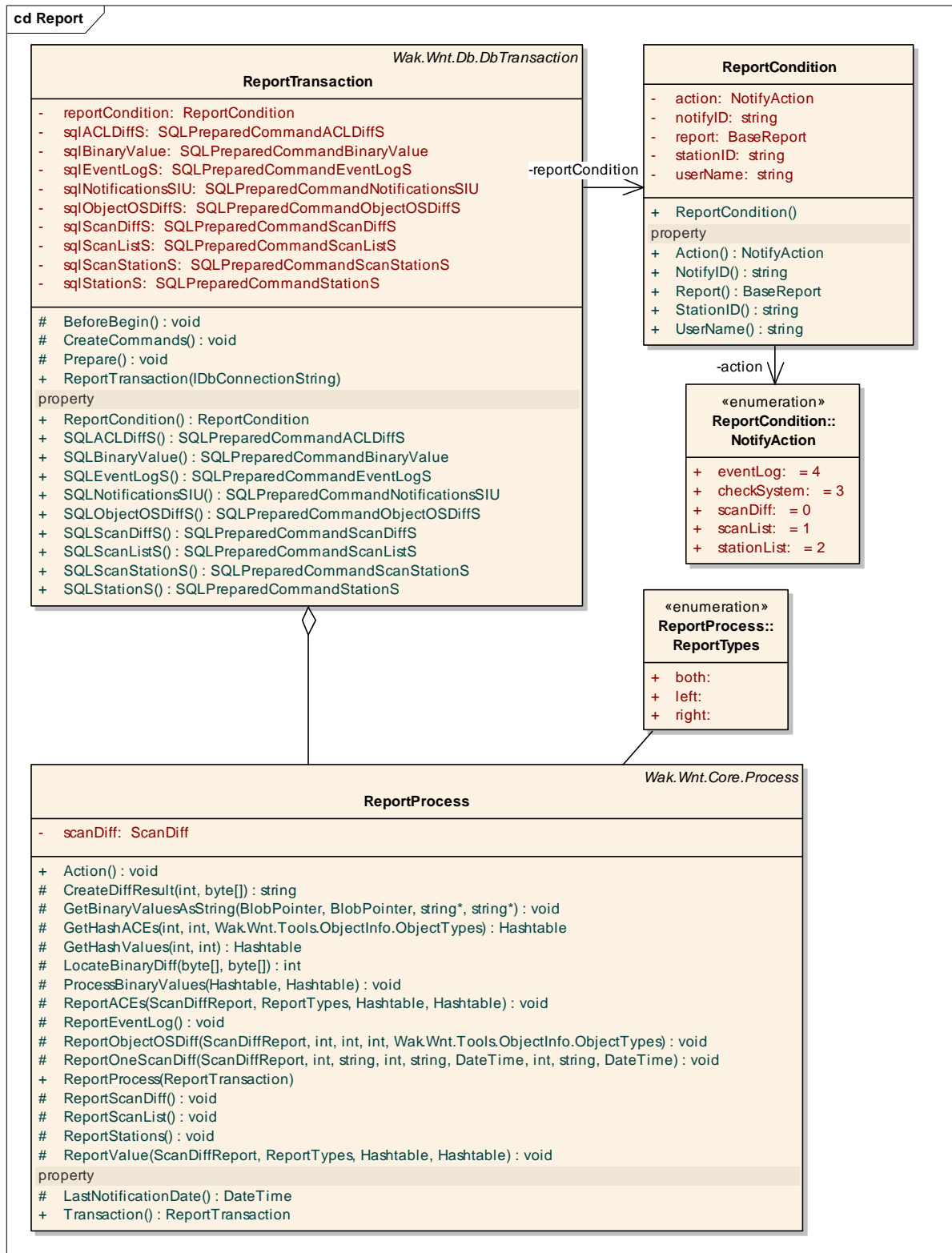
Obr. 16 Diagram tříd CheckSystem

1.3.1.1.5 CheckSystemSQLCmd



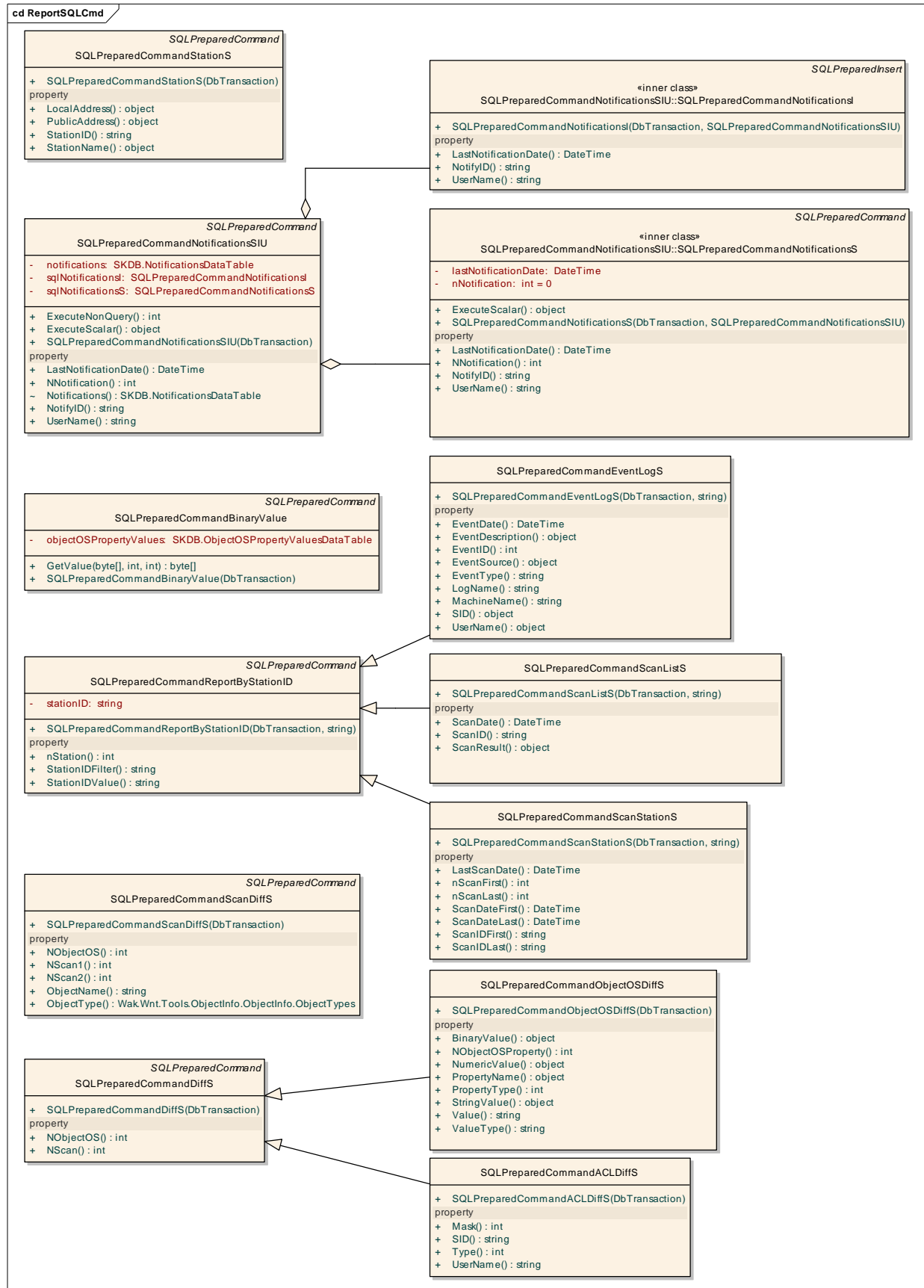
Obr. 17 Diagram tříd SQLSystemSQLCmd

1.3.1.1.6 Report



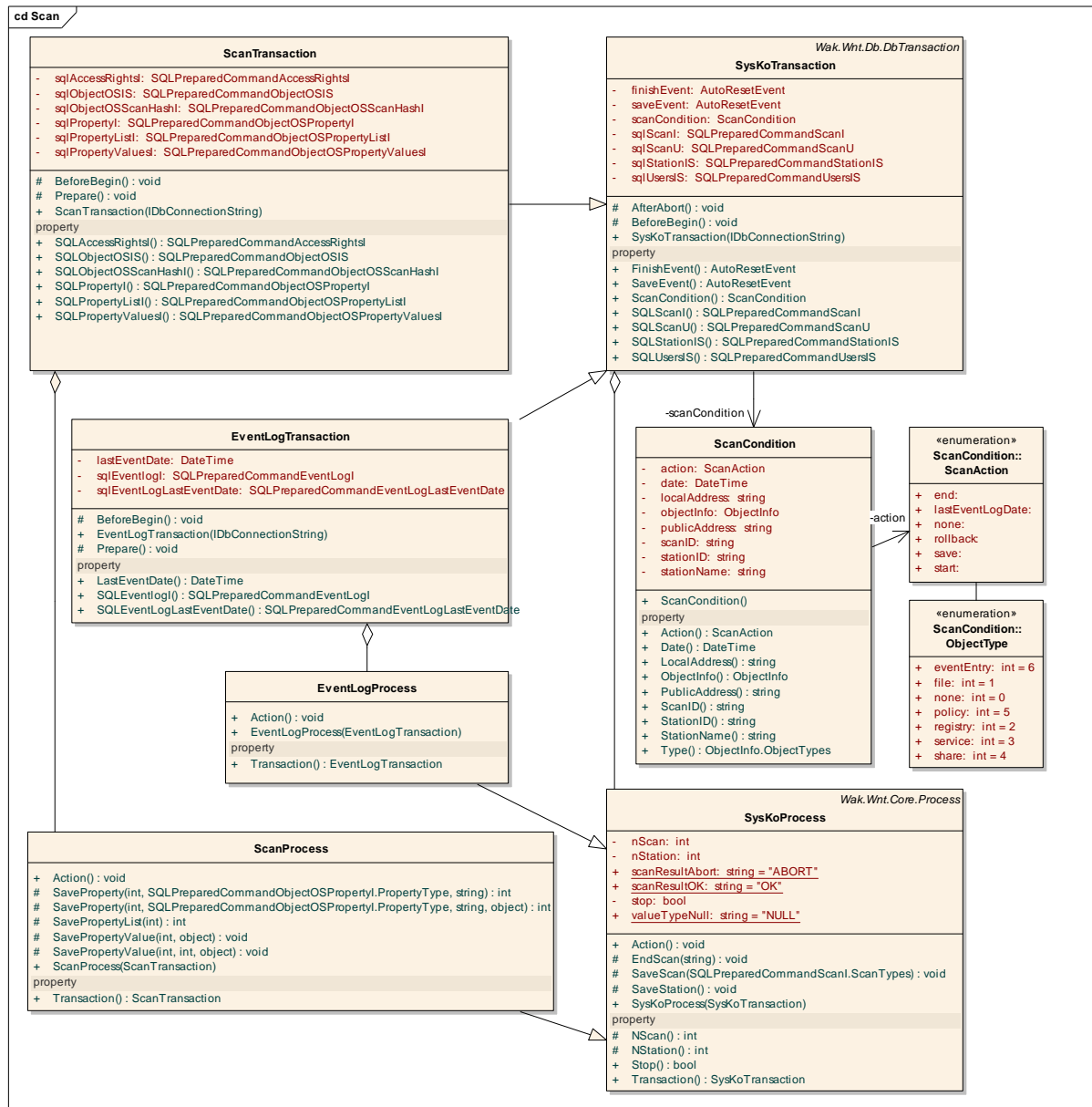
Obr. 18 Diagram tříd Report

1.3.1.1.7 ReportSQLCmd



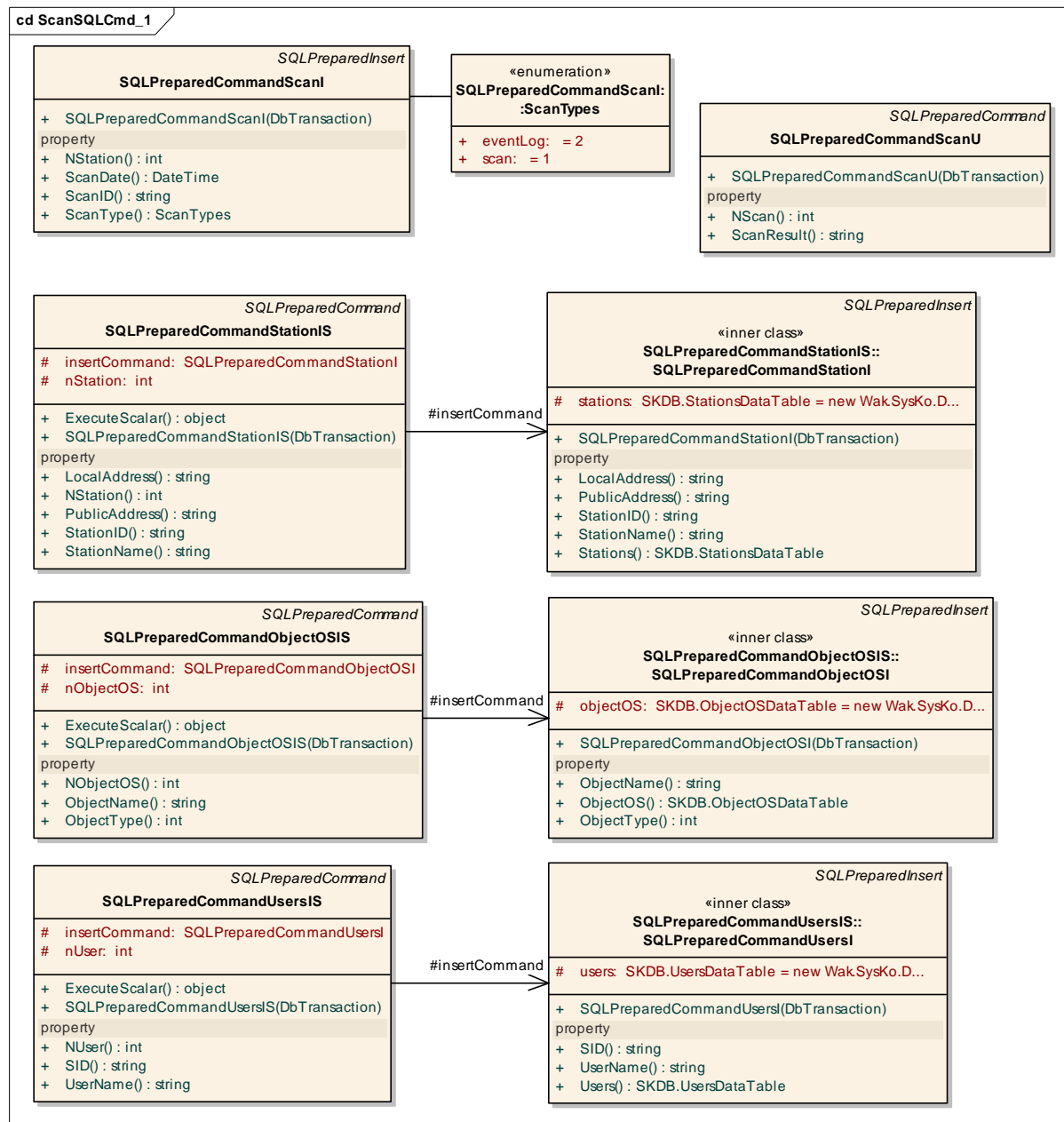
Obr. 19 Diagram tříd ReportSQLCmd

1.3.1.1.8 Scan

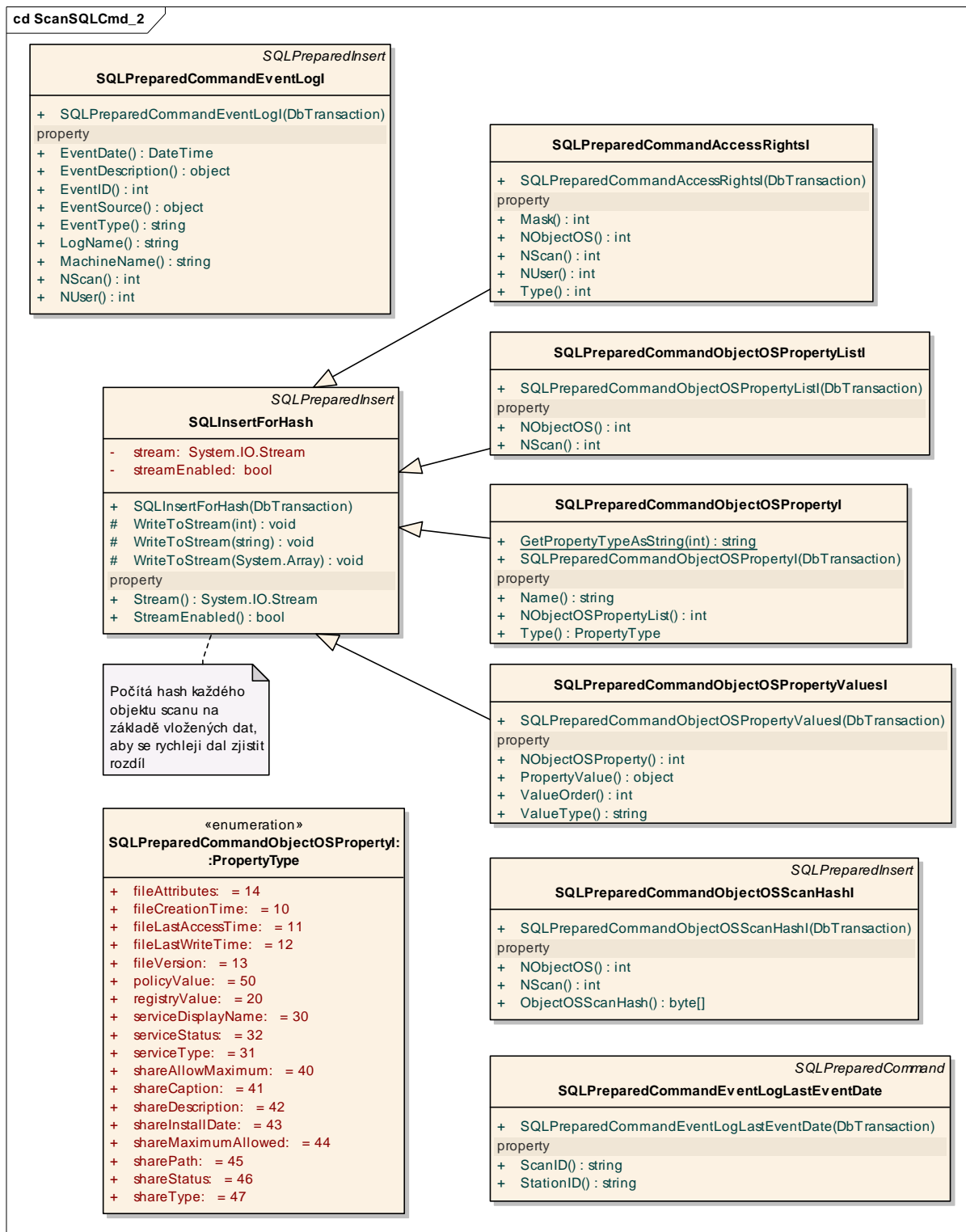


Obr. 20 Diagram tříd Scan

1.3.1.1.9 ScanSQLCmd



Obr. 21 Diagram tříd ScanSQLCmd - část 1

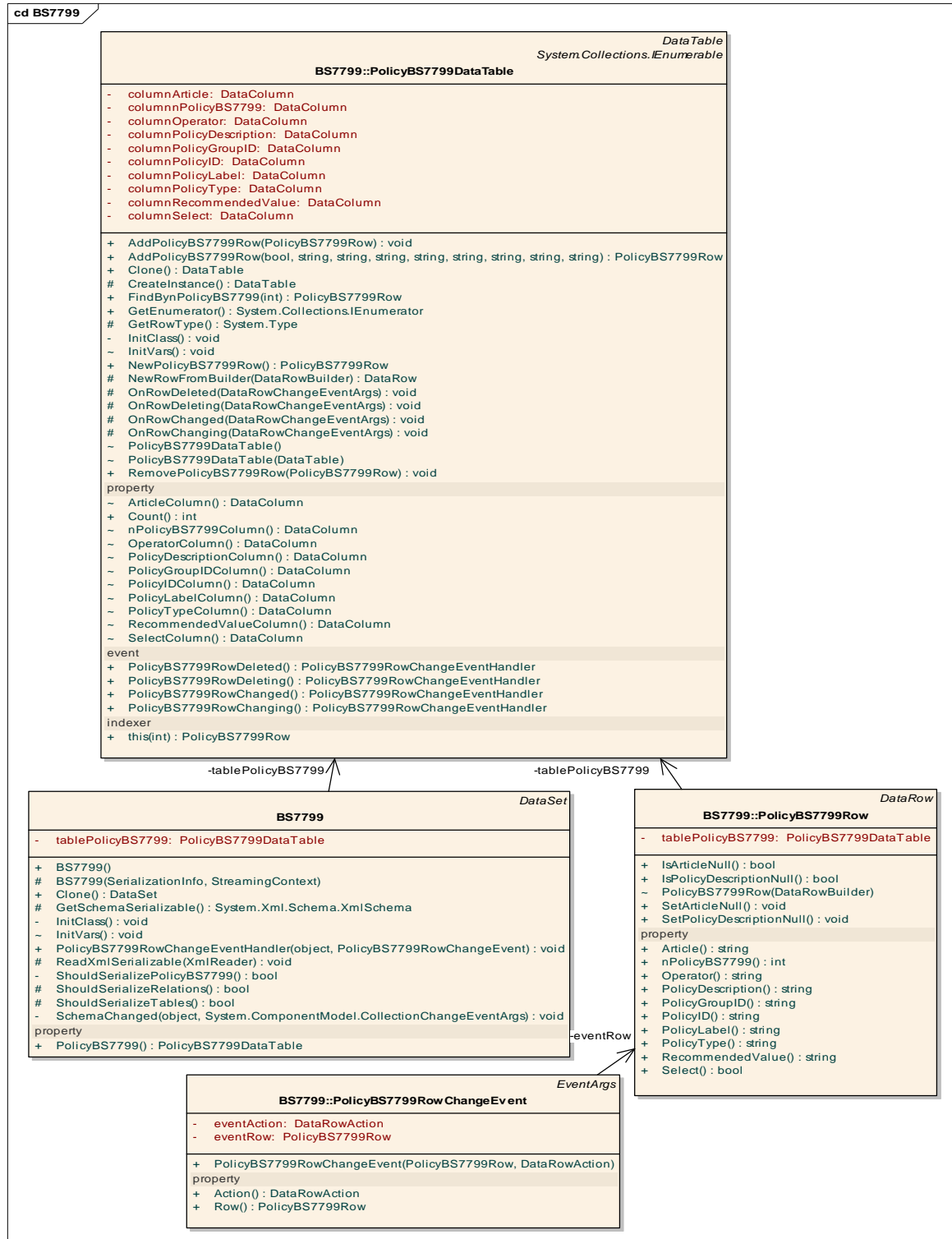


Obr. 22 Diagram tříd ScanSQLCmd - část 2

1.3.2 Střední vrstva

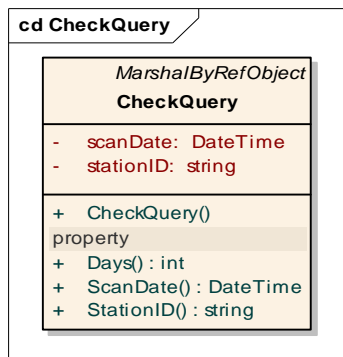
1.3.2.1 Podsystem SysKoCore

1.3.2.1.1 BS7799



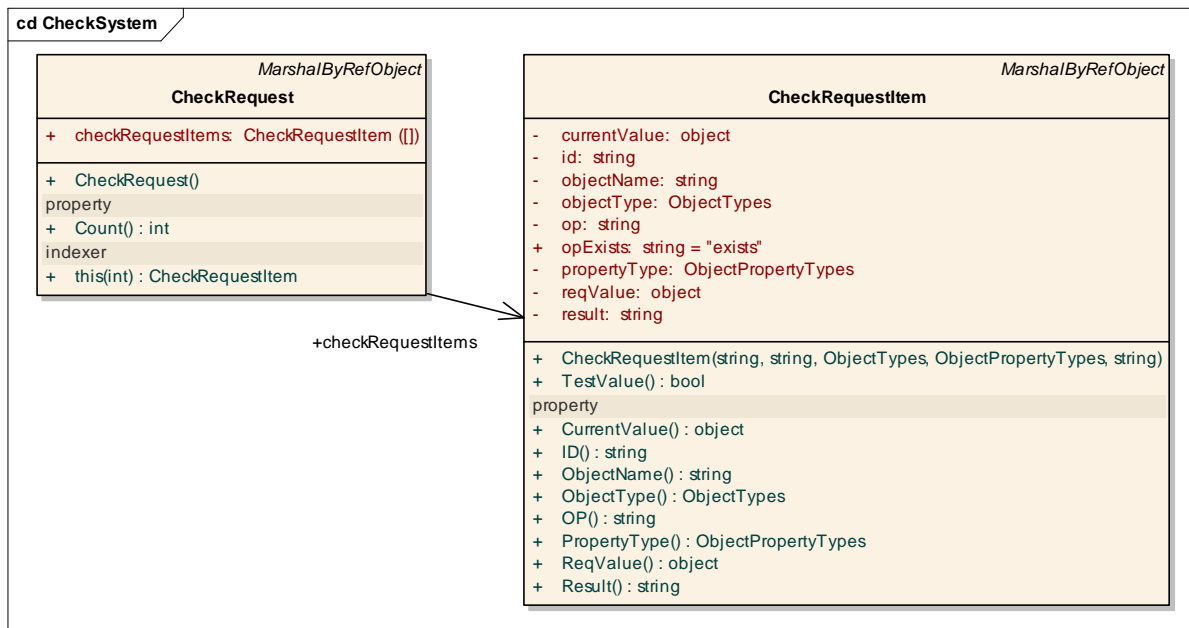
Obr. 23 Diagram tříd BS7799

1.3.2.1.2 CheckQuery



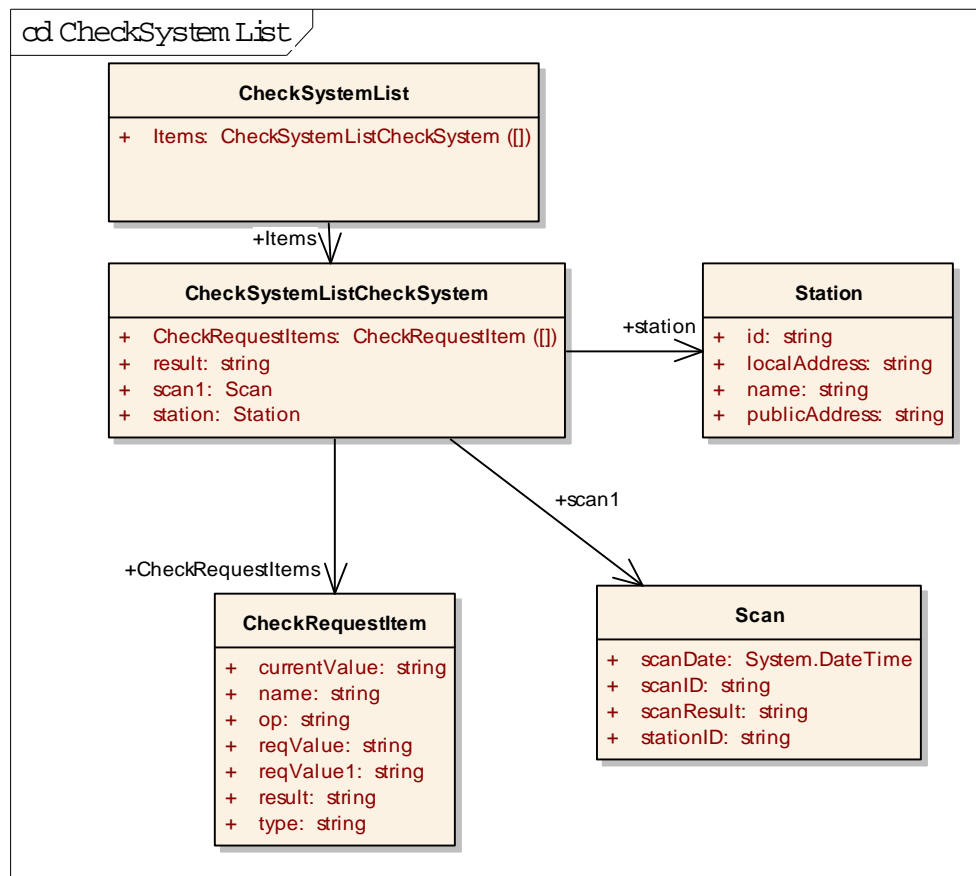
Obr. 24 Diagram tříd CheckQuery

1.3.2.1.3 CheckSystem



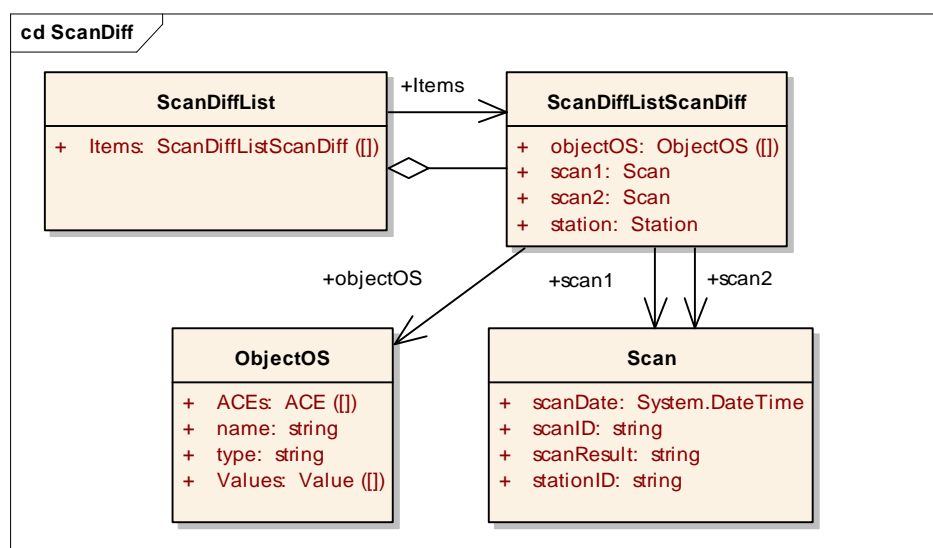
Obr. 25 Diagram tříd CheckSystem

1.3.2.1.4 CheckSystemList



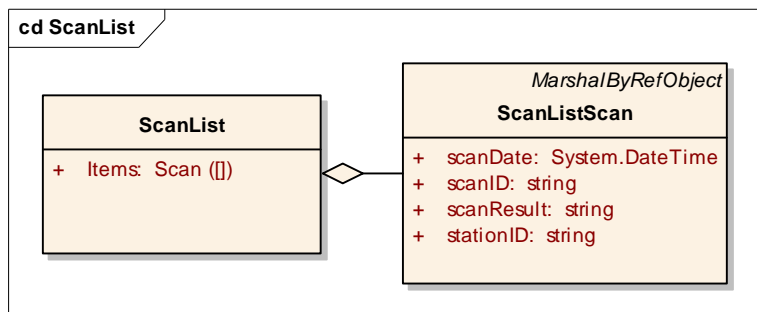
Obr. 26 Diagram tříd CheckSystemList

1.3.2.1.5 ScanDiff



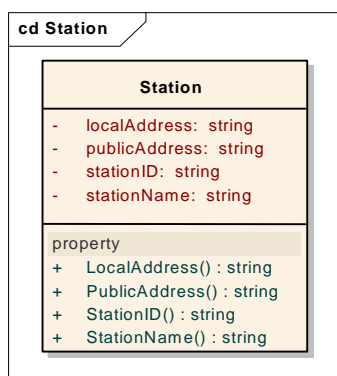
Obr. 27 Diagram tříd ScanDiff

1.3.2.1.6 ScanList



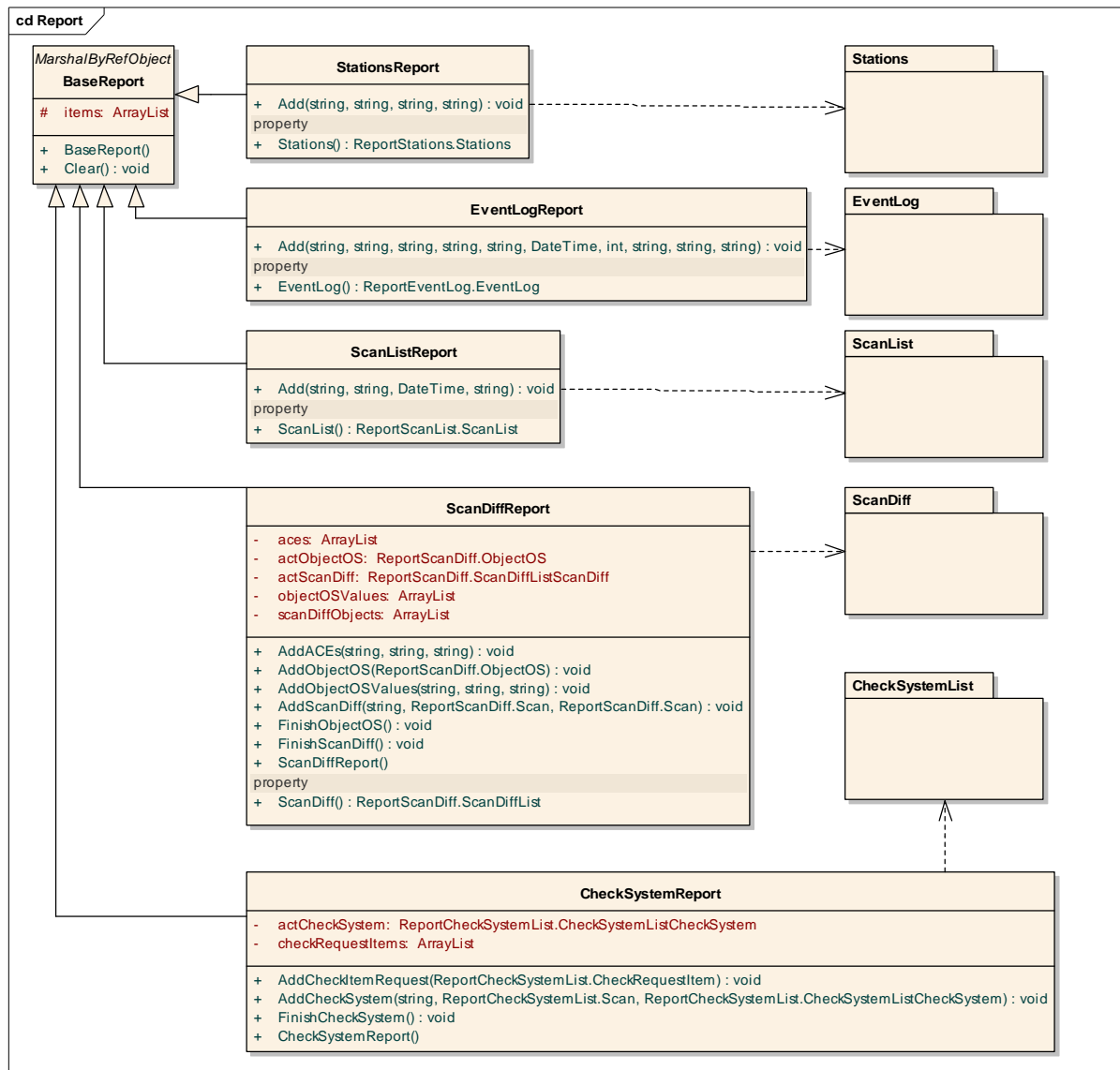
Obr. 28 Diagram tříd ScanList

1.3.2.1.7 Station



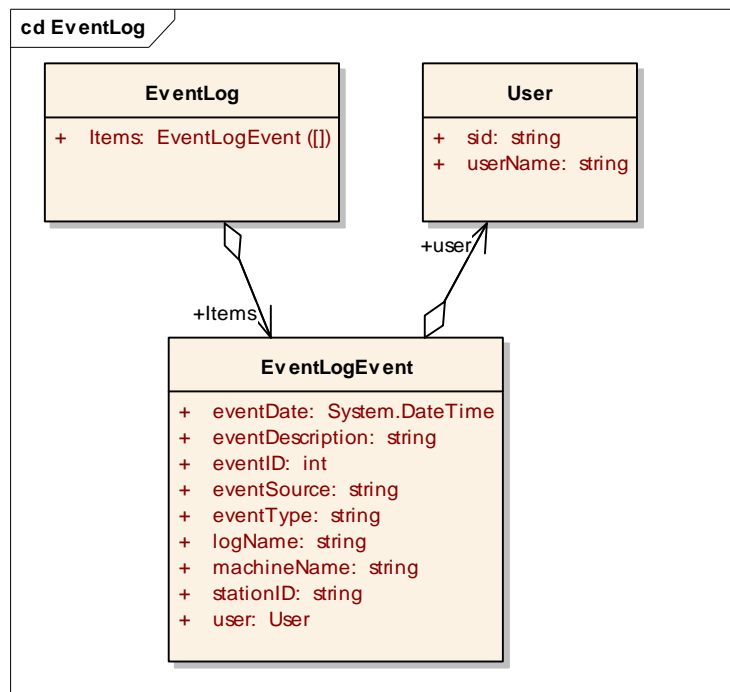
Obr. 29 Diagram tříd Station

1.3.2.1.8 Report



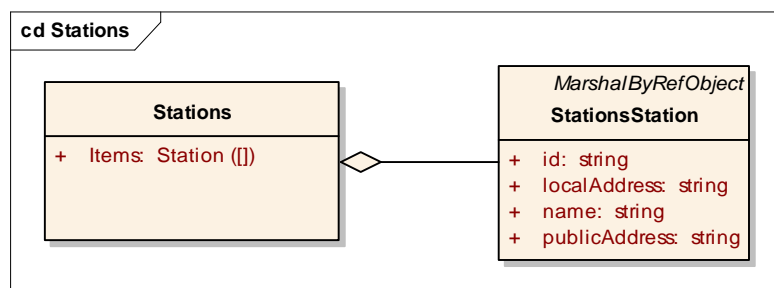
Obr. 30 Diagram tříd Report

1.3.2.1.9 EventLog



Obr. 31 Diagram tříd EventLog

1.3.2.1.10 Stations



Obr. 32 Diagram tříd Stations

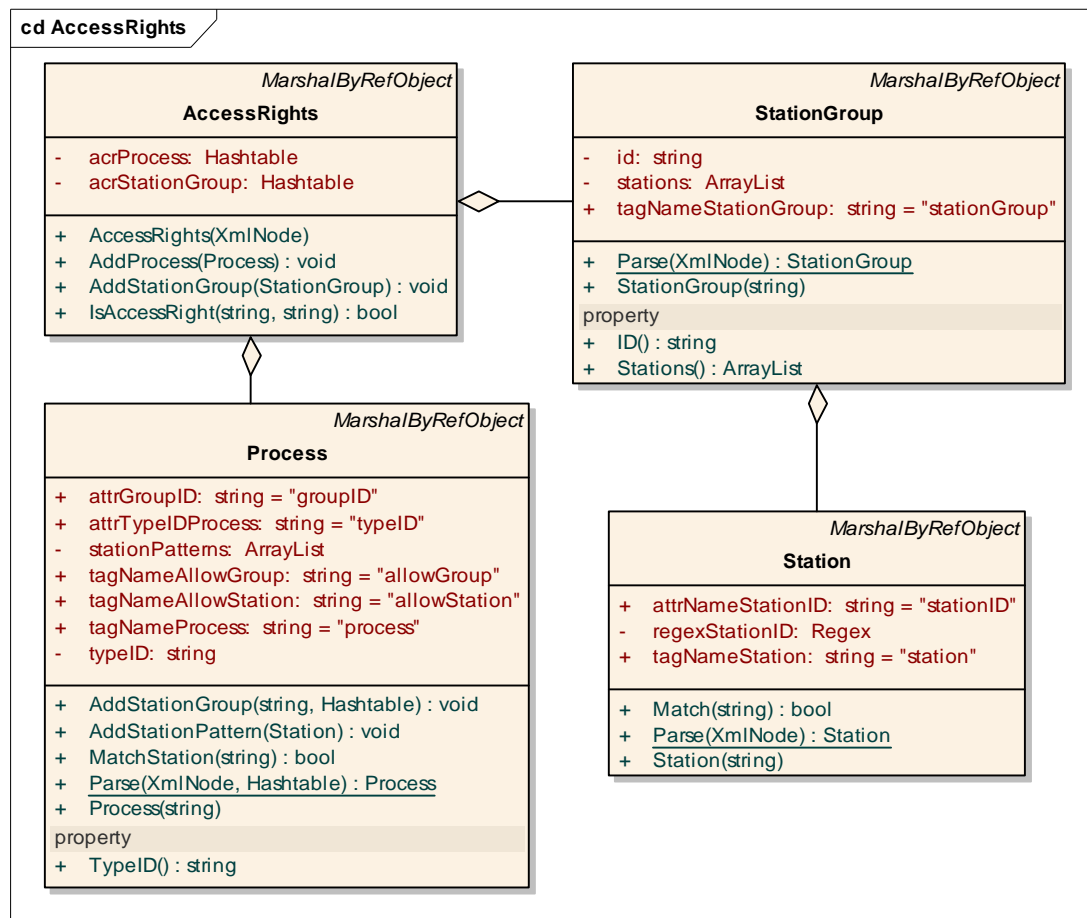
1.3.2.2 Podsystem SysKoAsServer

Č.	Jednotka	Funkce	Popis
1	AccesRights	IsAccessRight	Existence přístupových práv.
2	CheckItem	Parse	Zpracování XML prvku.
3	CheckList	Parse	Zpracování seznamu XML prvků.
4	CheckQuery_tr	Query	Zpracování dotazu na data.
5	CheckQueryConfig	CheckQueryConfig	Konfigurace checkQuery - exclude stanic.
6	CheckQueryConfig	MatchStationID	Vrátí ID stanice.
7	CheckQueryThread	Run	Server pro dotaz na checkQuery přes socket, protocol UDP.
8	CheckStation	Parse	Zpracování XML prvku stanice.

Č.	Jednotka	Funkce	Popis
9	CheckSystem	CheckSystem	Konfigurační nastavení CheckSystem.
10	CheckSystem	Remove	Odstranění checklistu s ID.
11	CheckSystem	Save	Záznam checklistu s ID.
12	CheckSystem_tr	Check	Ověří naposledy zasláná data.
13	CheckSystem_tr	CheckSystem_tr	Transakce nad checklisty.
14	CheckSystem_tr	TestValue	Testy hodnot pro objekty.
15	Notification	AddNotify	Přidání notifikace.
16	Notification	Notification	Notifikační servis SysKo serveru.
17	NotificationGroup	Parse	Zpracování XML skupiny notifikací.
18	NotificationTarget	Parse	Zpracování XML adresáta.
19	NotificationThread	GetRealFilename	Vrací reálné jméno souboru.
20	NotificationThread	ParseFormatItem	Vrací příslušnou část notifikace.
21	NotificationThread	Run	Spuštění služby notifikace.
22	NotificationThread	SaveOutput	Odeslání výsledku notifikace.
23	NotificationThread	TransformOutput	Úprava formátu výsledku notifikace.
24	Notify	Parse	Zpracování XML prvku notifikace.
25	Process	Parse	Zpracování XML prvku procesu.
26	StationGroup	Parse	Zpracování XML prvku stanice.
27	SysKo_tr	PumpTransaction	Transakce služby scanu.
28	SysKoManager	CleanContexts	Smazání kontextu serveru.
29	SysKoManager	NewSysKoContext	Nový kontext serveru.

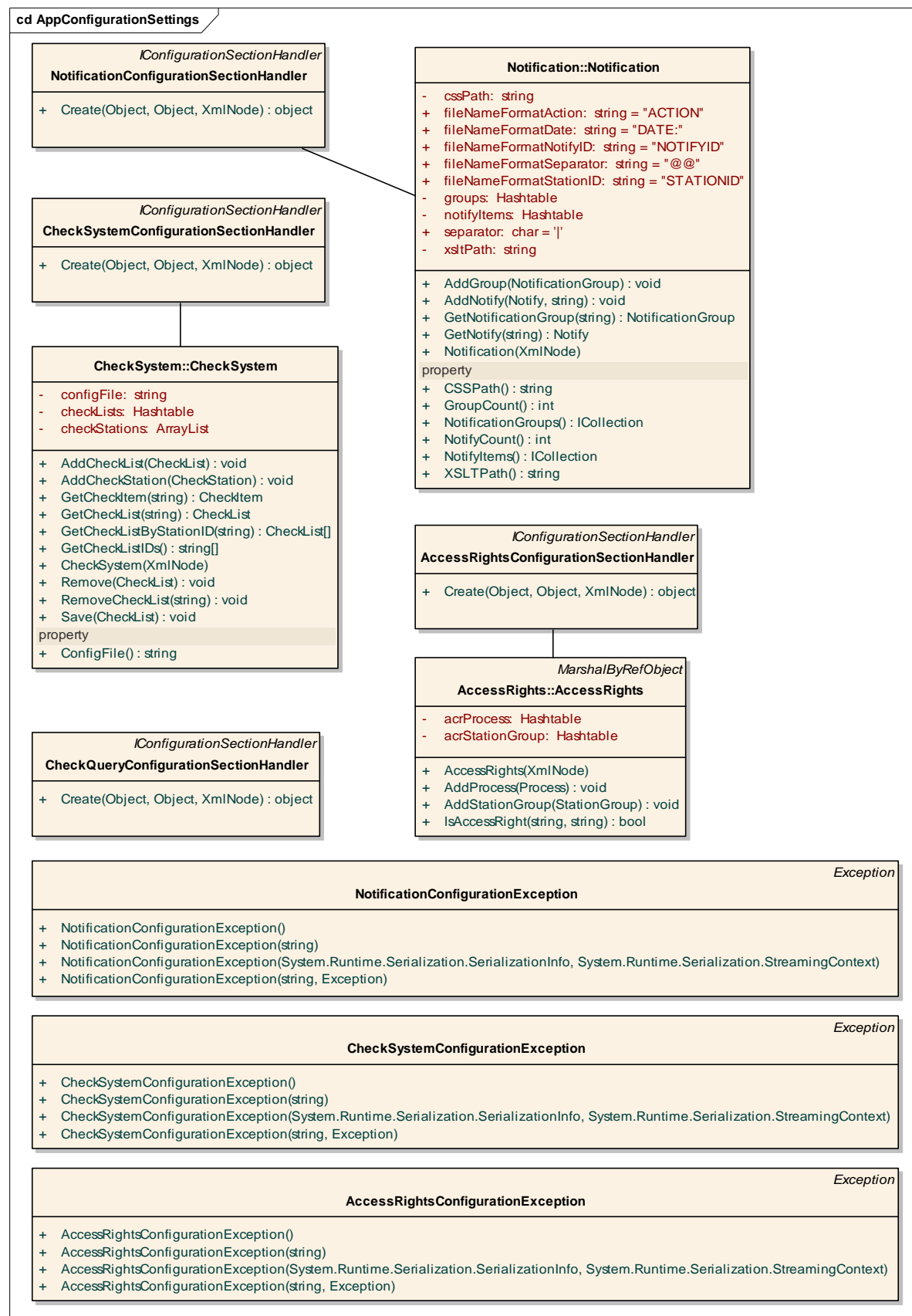
Tab. 8 Popis funkcí podsystému SysKoAsServer

1.3.2.2.1 AccessRights



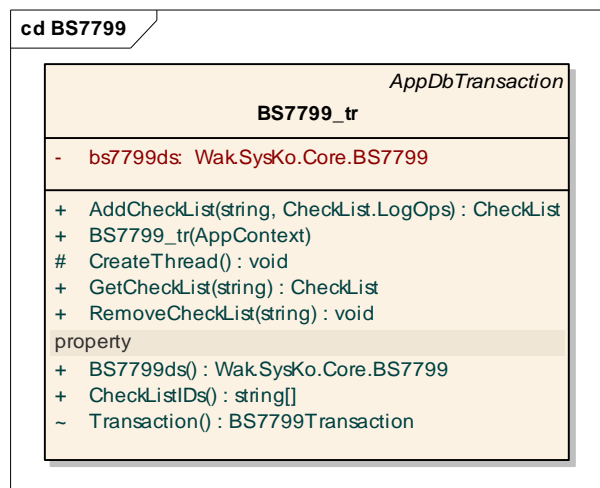
Obr. 33 Diagram tříd AccessRights

1.3.2.2.2 AppConfigurationSettings



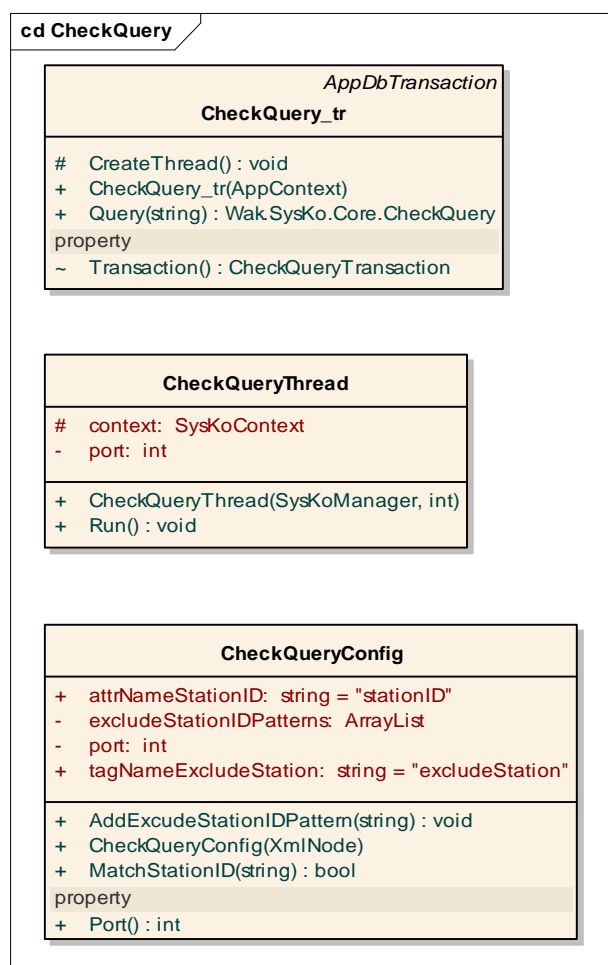
Obr. 34 Diagram tříd AppConfigurationSettings

1.3.2.2.3 BS7799



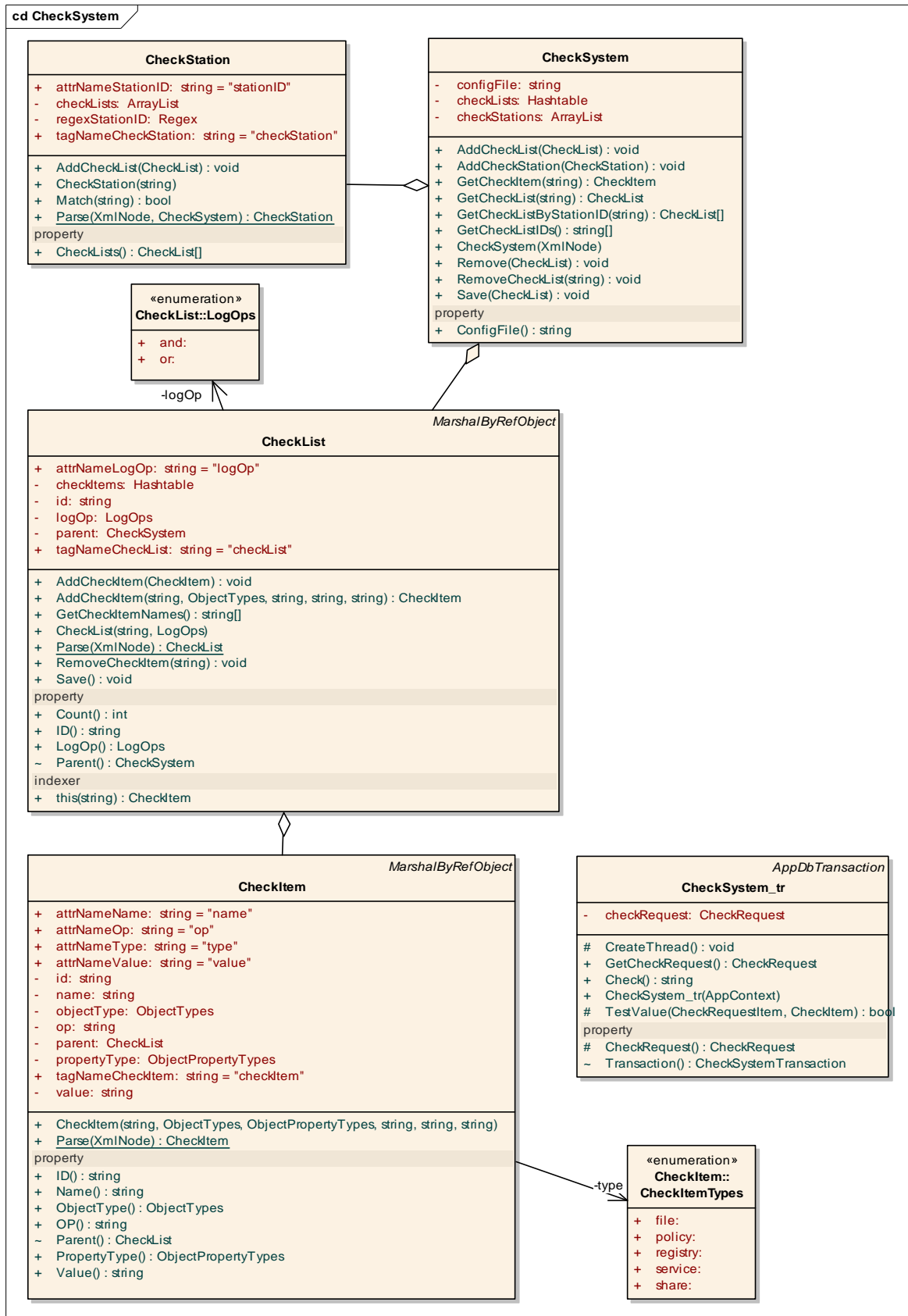
Obr. 35 Diagram tříd BS7799

1.3.2.2.4 CheckQuery



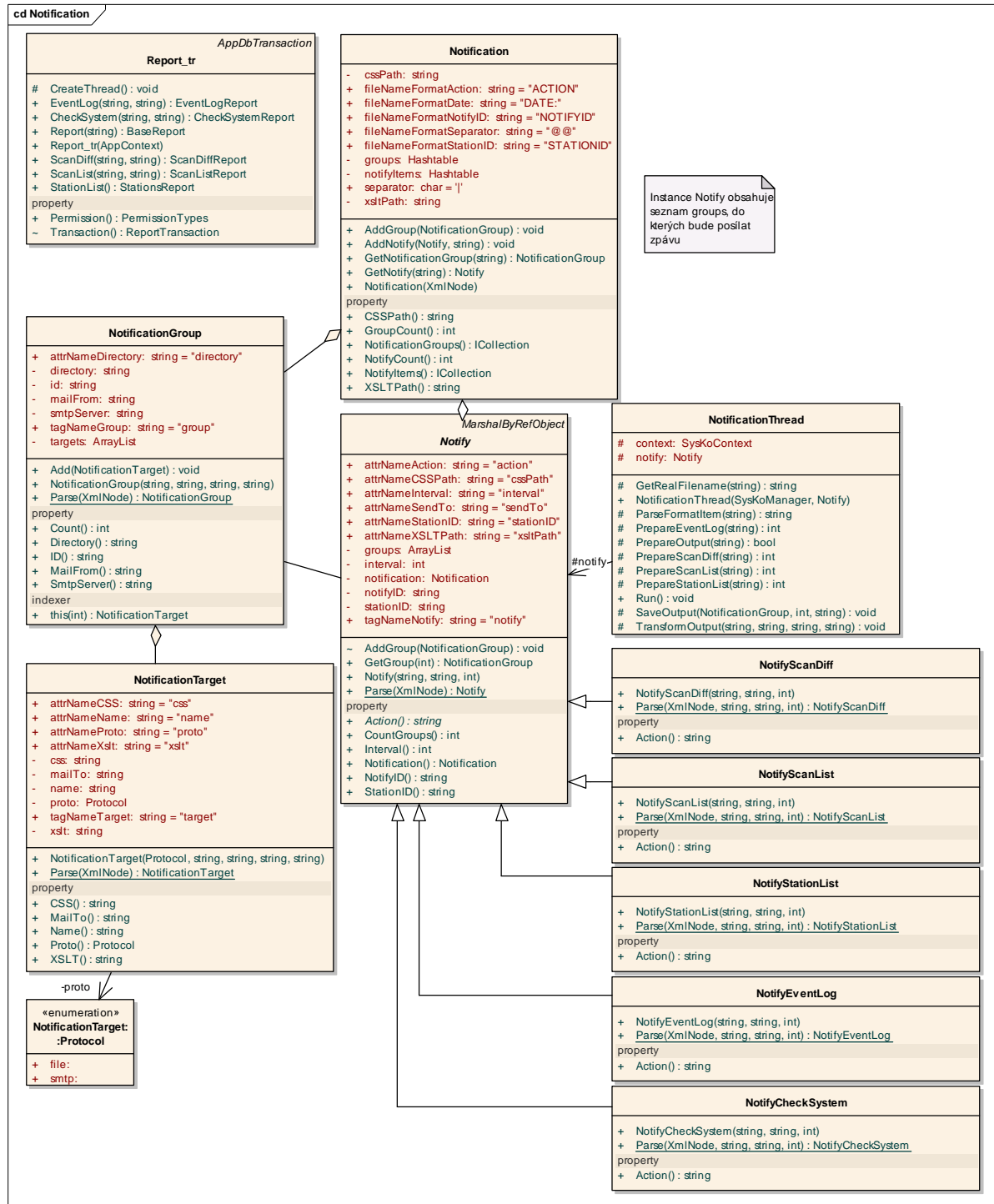
Obr. 36 Diagram tříd CheckQuery

1.3.2.2.5 CheckSystem



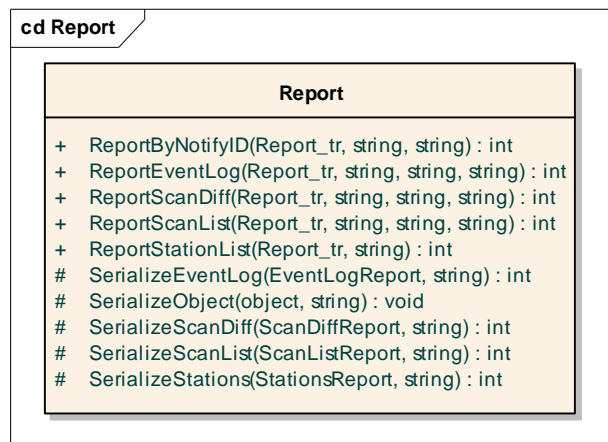
Obr. 37 Diagram tříd CheckSystem

1.3.2.2.6 Notification



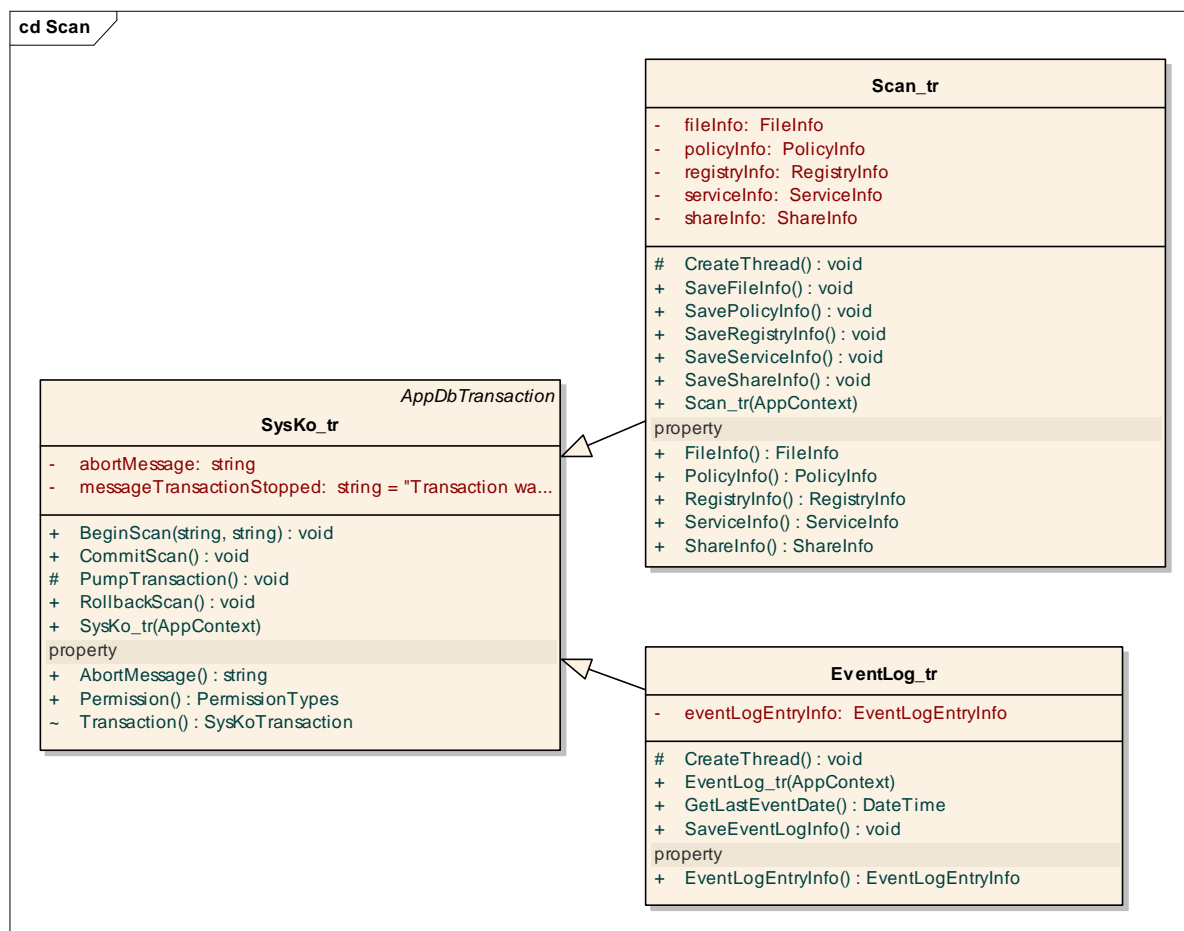
Obr. 38 Diagram tříd Notification

1.3.2.2.7 Report



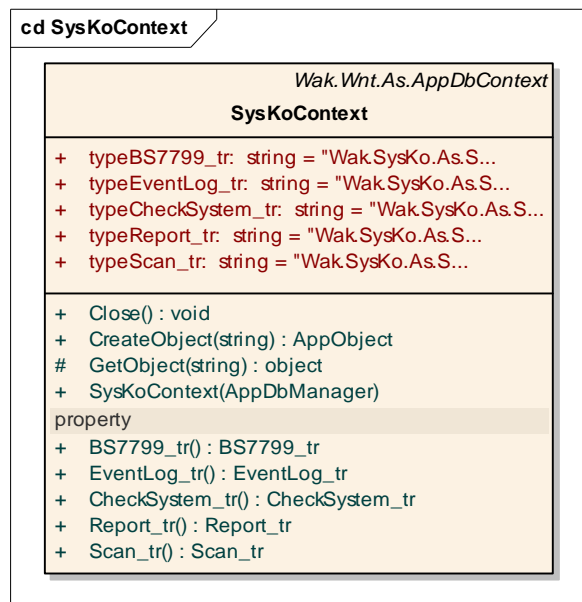
Obr. 39 Diagram tříd Report

1.3.2.2.8 Scan



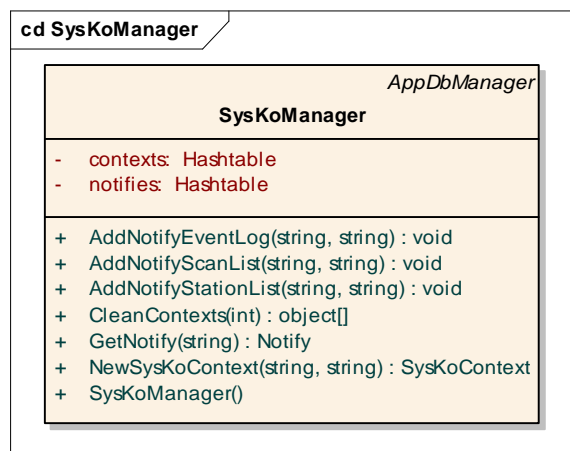
Obr. 40 Diagram tříd Scan

1.3.2.2.9 SysKoContext



Obr. 41 Diagram tříd SysKoContext

1.3.2.2.10 SysKoManager



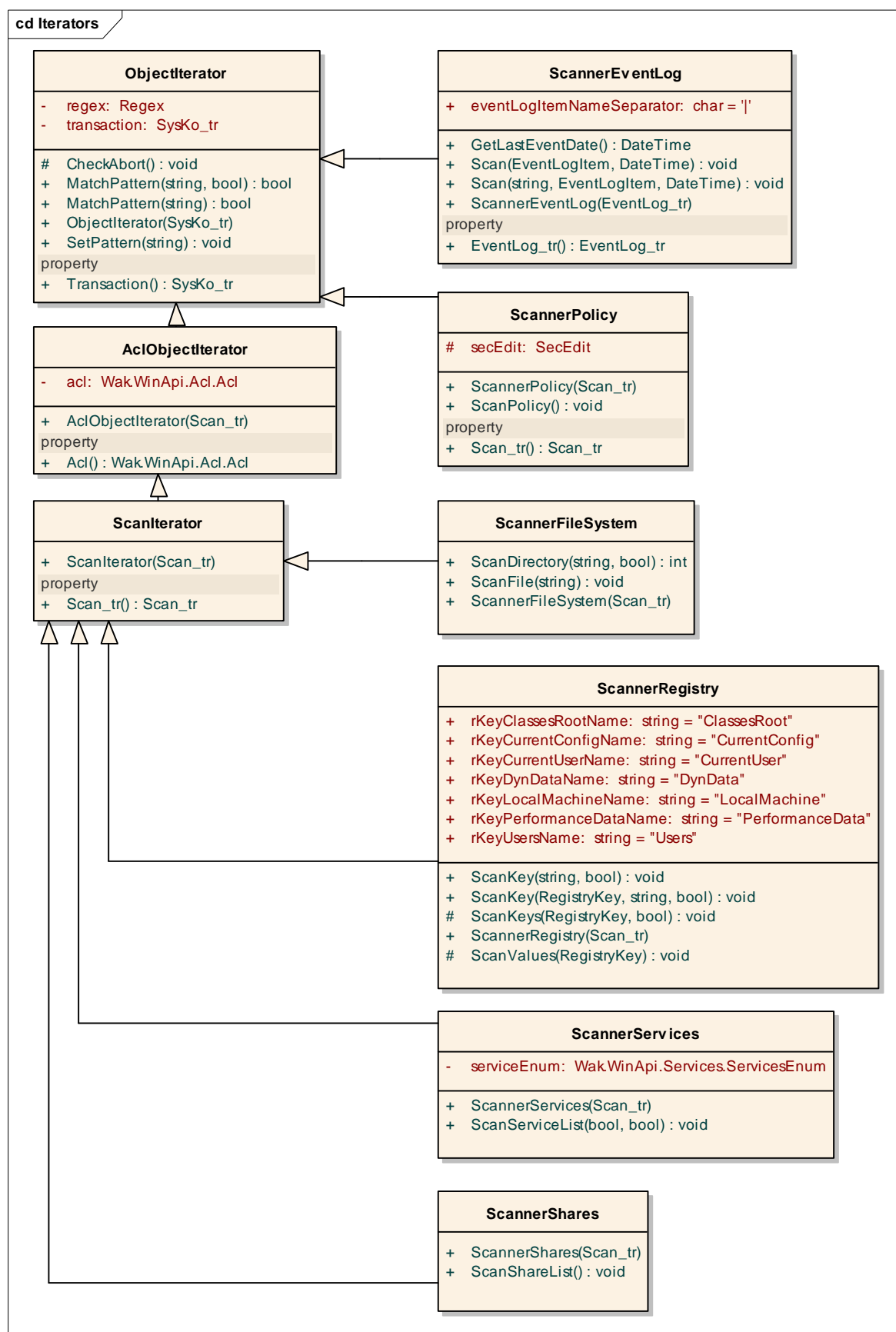
Obr. 42 Diagram tříd SysKoManager

1.3.2.3 Podsystem SysKoAsClient

Č.	Jednotka	Funkce	Popis
1	CheckSystem	Check	Rozcestník podle typu objektu.
2	CheckSystem	CheckFile	Nastavení výsledků pro soubory.
3	CheckSystem	CheckPolicy	Nastavení výsledků pro politiky.
4	CheckSystem	CheckRegistry	Nastavení výsledků pro registry.
5	CheckSystem	CheckService	Nastavení výsledků pro služby.
6	CheckSystem	CheckShare	Nastavení výsledků pro share.
7	ScannerEventLog	Scan	Kontrola událostí (eventlogu).
8	ScannerFileSystem	ScanDirectory	Kontrola adresáře.
9	ScannerFileSystem	ScanFile	Kontrola souboru.

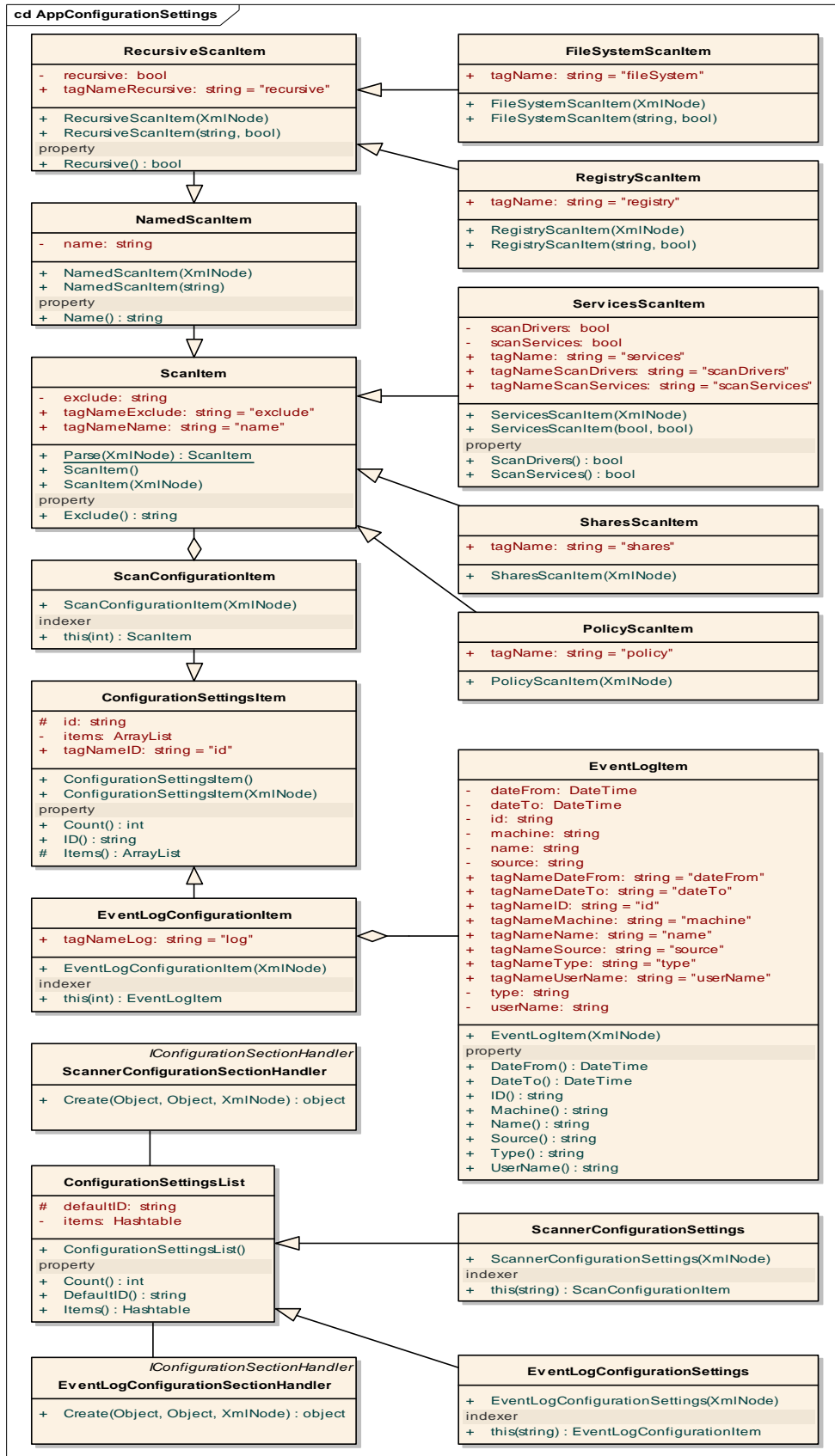
Č.	Jednotka	Funkce	Popis
10	ScannerPolicy	ScanPolicy	Kontrola bezpečnostní politiky.
11	ScannerRegistry	ScanKey	Kontrola klíče registru.
12	ScannerRegistry	ScanValues	Kontroly hodnoty registru.
13	ScannerServices	ScanServiceList	Kontrola služeb.
14	ScannerShares	ScanShareList	Kontrola share.

Tab. 9 Popis funkcí podsystému SysKoAsClient



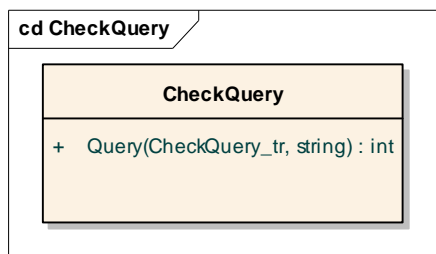
Obr. 43 Schéma iterací jednotlivých součástí OS

1.3.2.3.1 AppConfigurationSettings



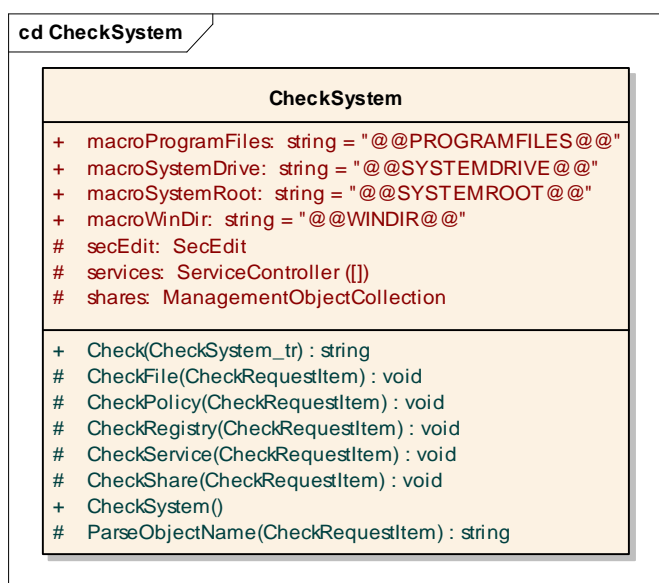
Obr. 44 Diagram tříd AppConfigurationSettings

1.3.2.3.2 CheckQuery



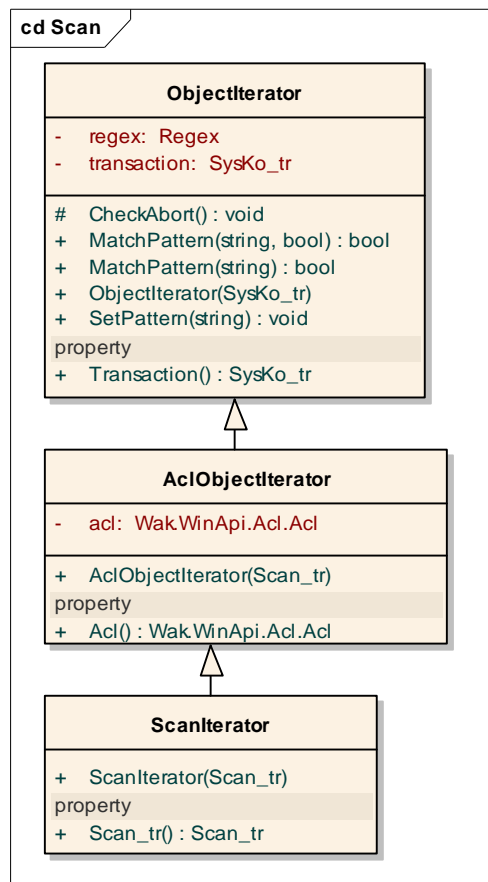
Obr. 45 Diagram tříd CheckQuery

1.3.2.3.3 CheckSystem



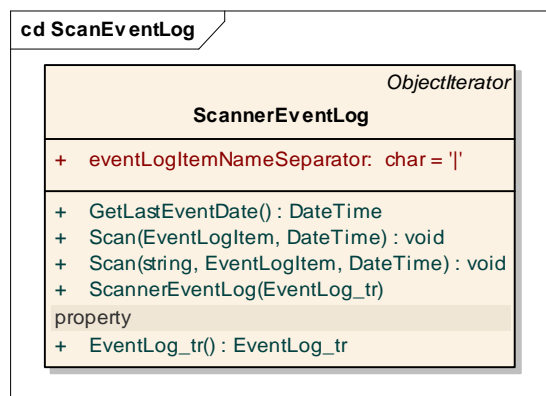
Obr. 46 Diagram tříd CheckSystem

1.3.2.3.4 Scan



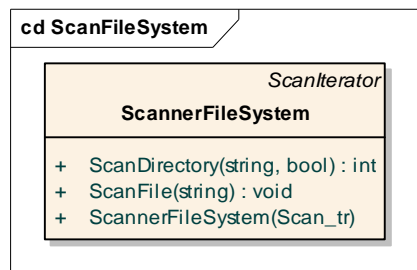
Obr. 47 Diagram tříd Scan

1.3.2.3.5 ScanEventLog



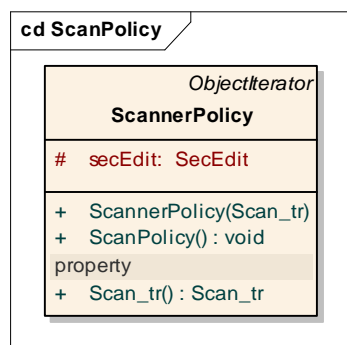
Obr. 48 Diagram tříd ScannerEventLog

1.3.2.3.6 ScanFileSystem



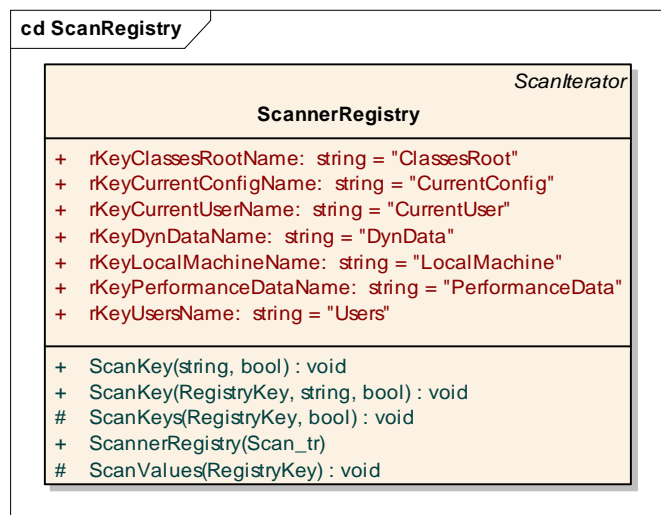
Obr. 49 Diagram tříd ScannerFileSystem

1.3.2.3.7 ScanPolicy



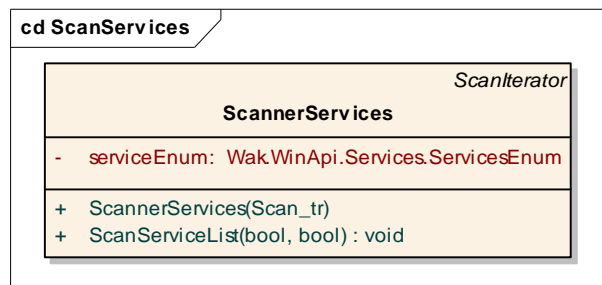
Obr. 50 Diagram tříd ScannerPolicy

1.3.2.3.8 ScanRegistry



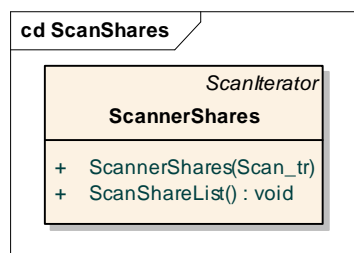
Obr. 51 Diagram tříd ScannerRegistry

1.3.2.3.9 ScanServices



Obr. 52 Diagram tříd ScannerServices

1.3.2.3.10 ScanShares



Obr. 53 Diagram tříd ScannerShares

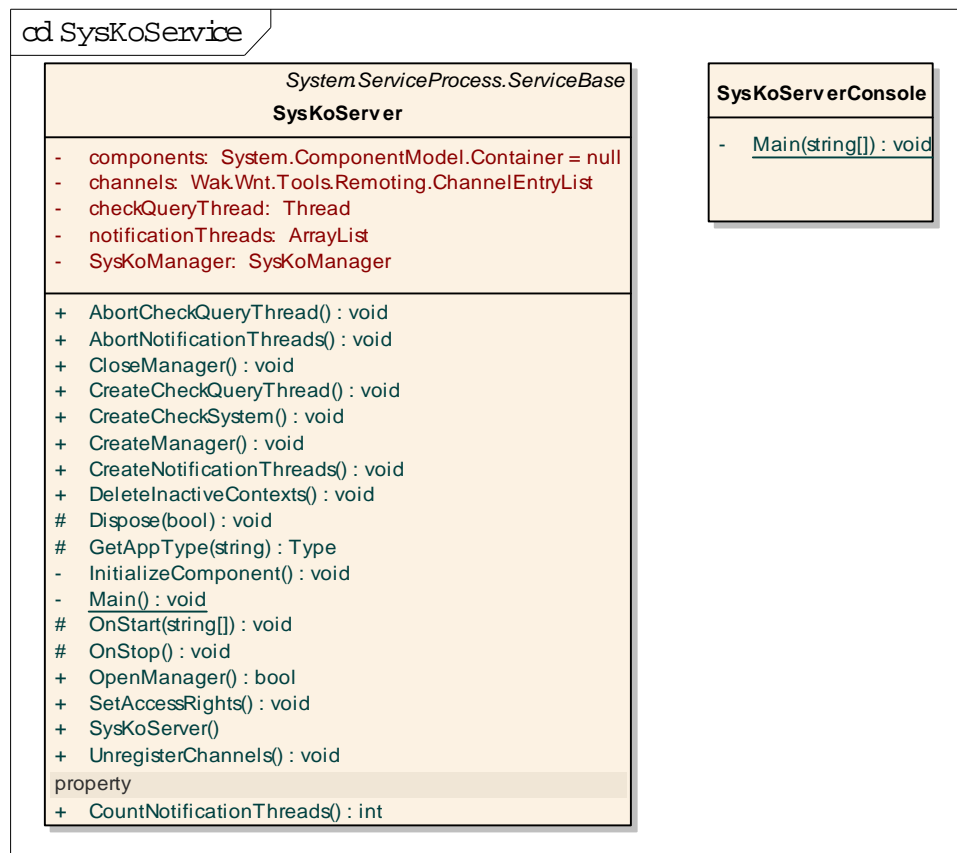
1.3.3 Aplikační vrstva

1.3.3.1 Podsystem SysKoServer

Č.	Jednotka	Funkce	Popis
1	SysKoServer	CreateNotificationThreads	Vytvoření vlákn pro notifikaci.
2	SysKoServer	DeleteInactiveContexts	Smazání kontextu.
3	SysKoServerConsole	Main	Volání hlavní funkce serveru.

Tab. 10 Popis funkcí podsystemu SysKoServer

1.3.3.1.1 SysKoService



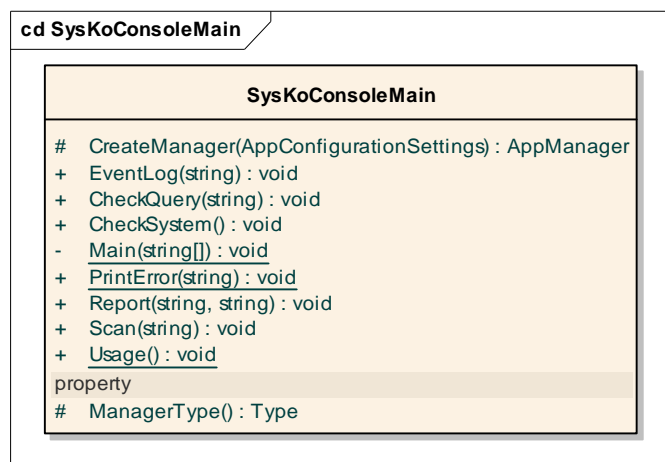
Obr. 54 Diagram tříd SysKoService

1.3.3.2 Podsystem SysKoConsole

Č.	Jednotka	Funkce	Popis
1	SysKoConsoleMain	CheckQuery	Spuštění dotazu.
2	SysKoConsoleMain	CheckSystem	Kontrola systému.
3	SysKoConsoleMain	EventLog	Kontrola událostí (eventlogu).
4	SysKoConsoleMain	Main	Hlavní funkce konzole.
5	SysKoConsoleMain	Scan	Hlavní klient scanneru.

Tab. 11 Popis funkcí podsystemu SysKoConsole

1.3.3.2.1 SysKoConsoleMain



Obr. 55 Diagram tříd SysKoConsoleMain

1.3.3.3 Podsystem SysKoApp

1.3.3.3.1 BSSetup

Obsahuje obrazovku s ovládacími prvky pro práci s body normy BS 7799. Podrobný popis je v uživatelské příručce.

Č.	Jednotka	Funkce	Popis
1	BSSetup	SavePolicy	Uložení změn ve stávající politice. Uložení nové politiky.
2	BSSetup	DeletePolicy	Vymazání stávající politiky.
3	BSSetup	bsItems_Click	Obsluha označení položky seznamu.
4	BSSetup	bsItems_CurrentCellChanged	Obsluha při změně označení položky.
5	BSSetup	FillListIDs	Naplnění seznamu položek.
6	BSSetup	Form1_Load	Vytvoření seznamu položek.
7	BSSetup	InitializeComponent	Naplnění formuláře.
8	BSSetup	Main	Hlavní funkce formuláře.

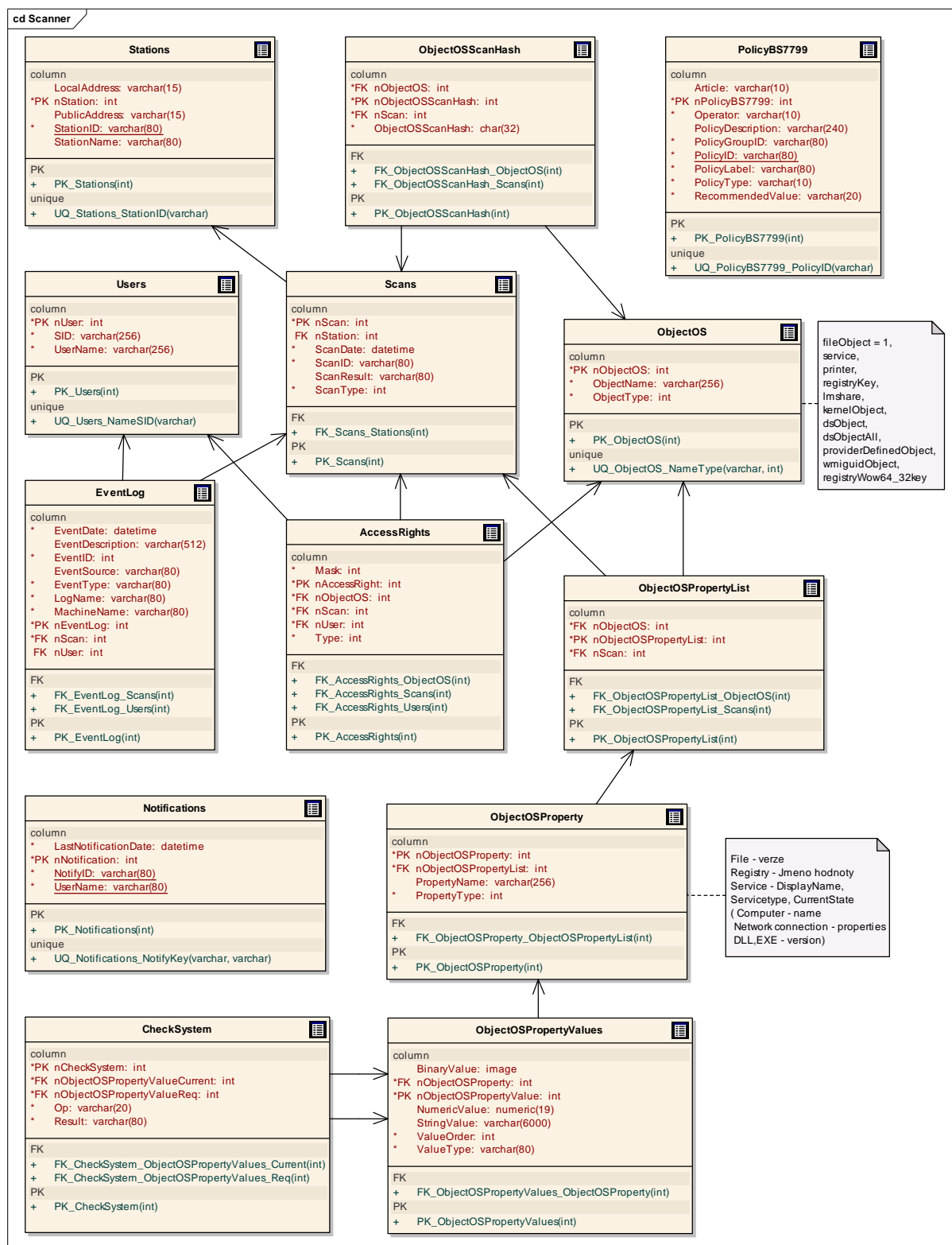
Tab. 12 Popis funkcí podsystemu BSSetup

1.4 Návrh databáze

Analýzou a návrhem tříd byly zároveň vzneseny požadavky na datovou část SysKo.

Každá z tabulek obsahuje sloupec, který obsahuje jedinečné celé číslo v rámci tabulky a díky němuž se realizují případné vazby na další tabulky. Číslování v tomto případě zajišťuje vnitřní mechanismus databáze. Ve schématech je tento sloupec označen hvězdičkou (*).

Vazba začínající PK znamená primární klíč příslušné tabulky. Vazba začínající FK znamená návaznost na další tabulku, jejíž název je obsažen na druhém místě názvu klíče. Na pozici sloupec je označeno vazební pole. Vazba začínající UQ definuje unikátní klíč pro danou tabulku.



Obr. 56 Datové struktury a jejich vazby

AccessRights

Tabulka obsahuje přístupová práva ke všem objektům SysKo.

Sloupec	Popis
---------	-------

Sloupec	Popis
Mask int	Volitelná maska
nAccessRight int	*
nObjectOS int	Jednotlivý objekt
nScan int	Provedená kontrola
nUser int	Uživatel
Typ int	Typ práva

Tab. 13 Struktura AccessRights

Klíč	Sloupec
FK_AccessRights_ObjectOS()	int nObjectOS
FK_AccessRights_Scans()	int nScan
FK_AccessRights_Users()	int nUser
PK_AccessRights()	int nAccessRight

Tab. 14 Klíče AccessRights

CheckSystem

Tabulka obsahuje data pro výsledky kontroly SysKo.

Sloupec	Popis
nCheckSystem int	*
nObjectOSPropertyValueCurrent int	Aktuální hodnota
nObjectOSPropertyValueReq int	Očekávaná hodnota
Op varchar	Operátor
Result varchar	Výsledek kontroly

Tab. 15 Struktura CheckSystem

Klíč	Sloupec
FK_CheckSystem_ObjectOSPropertyValues_Current()	int nObjectOSPropertyValueCurrent
FK_CheckSystem_ObjectOSPropertyValues_Req()	int nObjectOSPropertyValueReq
PK_CheckSystem()	int nCheckSystem

Tab. 16 Klíče CheckSystem

EventLog

Tabulka obsahuje data událostí z event logu.

Sloupec	Popis
EventDate datetime	Datum události
EventDescription varchar	Popis události
EventID int	Identifikace události
EventSource varchar	Místo vzniku události
EventType varchar	Typ události
LogName varchar	Název události

Sloupec	Popis
MachineName varchar	Interní název
nEventLog int	*
nScan int	Provedená kontrola
nUser int	Uživatel

Tab. 17 Struktura EventLog

Klíč	Sloupec
FK_EventLog_Scans()	int nScan
FK_EventLog_Users()	int nUser
PK_EventLog()	int nEventLog

Tab. 18 Klíče EventLog

Notifications

Tabulka obsahuje hlavičky ověřených kontrol OS.

Sloupec	Popis
LastNotificationDate datetime	Poslední poslaná ověřená kontrola za danou akci
nNotification int	*
NotifyID varchar	Identifikace ověřené kontroly
UserName varchar	Uživatel (z kontextu)

Tab. 19 Struktura Notifications

Klíč	Sloupec
PK_Notifications()	int nNotification
UQ_Notifications_NotifyKey()	varchar UserName varchar NotifyID

Tab. 20 Klíče Notifications

ObjectOS

Tabulka obsahuje jednotlivé zkoumané objekty OS.

Sloupec	Popis
nObjectOS int	*
ObjectName varchar	Název objektu
ObjectType int	Typ objektu (fileObject = 1, service, printer, registryKey, lmshare, kernelObject, dsObject, dsObjectAll, providerDefinedObject, wmicguidObject, registryWow64_32key)

Tab. 21 Struktura ObjectOS

Klíč	Sloupec
PK_ObjectOS()	int nObjectOS

UQ_ObjectOS_NameType()	int ObjectType varchar ObjectName
------------------------	--

Tab. 22 Klíče ObjectOS

ObjectOSProperty

Tabulka obsahuje hlavičky zkoumaných objektů v jednotlivých kontrolách.

Sloupec	Popis
nObjectOSProperty int	*
nObjectOSPropertyList int	Seznam hlaviček zkoumaných objektů
PropertyName varchar	Soubor – verze Registr - jméno hodnoty Služba - jméno, typ, současný stav
PropertyType int	Typ objektu

Tab. 23 Struktura ObjectOSProperty

Klíč	Sloupec
FK_ObjectOSProperty_ObjectOSPropertyList()	int nObjectOSPropertyList
PK_ObjectOSProperty()	int nObjectOSProperty

Tab. 24 Klíče ObjectOSProperty

ObjectOSPropertyList

Tabulka obsahuje seznamy zkoumaných objektů.

Sloupec	Popis
nObjectOS int	Objekt OS
nObjectOSPropertyList int	*
nScan int	Kontrola OS

Tab. 25 Struktura ObjectOSPropertyList

Klíč	Sloupec
FK_ObjectOSPropertyList_ObjectOS()	int nObjectOS
FK_ObjectOSPropertyList_Scans()	int nScan
PK_ObjectOSPropertyList()	int nObjectOSPropertyList

Tab. 26 Klíče ObjectOSPropertyList

ObjectOSPropertyValues

Tabulka obsahuje hodnoty k hlavičkám zkoumaných objektů v jednotlivých kontrolách.

Sloupec	Popis
BinaryValue image	Binární hodnota
nObjectOSProperty int	Hlavička objektu
nObjectOSPropertyValue int	*

Sloupec	Popis
NumericValue numeric	Numerická hodnota
StringValue varchar	Řetězcová hodnota
ValueOrder int	Pořadí hodnoty
ValueType varchar	Typ hodnoty

Tab. 27 Struktura ObjectOSPropertyValues

Klíč	Sloupec
FK_ObjectOSPropertyValues_ObjectOSProperty()	int nObjectOSProperty
PK_ObjectOSPropertyValues()	int nObjectOSPropertyValue

Tab. 28 Klíče ObjectOSPropertyValues

ObjectOSScanHash

Tabulka obsahuje hašovací kódy zkoumaných objektů (jedinečná identifikace).

Sloupec	Popis
nObjectOS int	Objekt OS
nObjectOSScanHash int	*
nScan int	Kontrola OS
ObjectOSScanHash char	Hašovací kód

Tab. 29 Struktura ObjectOSScanHash

Klíč	Sloupec
FK_ObjectOSScanHash_ObjectOS()	int nObjectOS
FK_ObjectOSScanHash_Scans()	int nScan
PK_ObjectOSScanHash()	int nObjectOSScanHash

Tab. 30 Klíče ObjectOSScanHash

PolicyBS7799

Tabulka obsahuje body bezpečnostní politiky z BS 7799.

Sloupec	Popis
Article varchar	Kapitola BS 7799
nPolicyBS7799 int	*
Operator varchar	Operátor pro hodnoty
PolicyDescription varchar	Popis politiky
PolicyGroupID varchar	Skupina politiky
PolicyID varchar	Identifikace politiky
PolicyLabel varchar	Název politiky
PolicyType varchar	Typ politiky
RecommendedValue varchar	Doporučená hodnota

Tab. 31 Struktura PolicyBS7799

Klíč	Sloupec
------	---------

Klíč	Sloupec
PK_PolicyBS7799()	int nPolicyBS7799
UQ_PolicyBS7799_PolicyID()	varchar PolicyID

Tab. 32 Klíče PolicyBS7799

Scans

Tabulka obsahuje jednotlivé kontroly OS.

Sloupec	Popis
nScan int	*
nStation int	Stanice
ScanDate datetime	Datum kontroly ve formátu UTC
ScanID varchar	Identifikace kontroly
ScanResult varchar	Výsledek kontroly
ScanType int	Typ kontroly

Tab. 33 Struktura Scans

Klíč	Sloupec
FK_Scans_Stations()	int nStation
PK_Scans()	int nScan

Tab. 34 Klíče Scans

Stations

Tabulka obsahuje číselník stanic klientů.

Sloupec	Popis
LocalAddress varchar	Interní adresa klienta - pokud ji pošle
nStation int	*
PublicAddress varchar	Veřejná adresa klienta
StationID varchar	Identifikace stanice klienta
StationName varchar	Název stanice klienta

Tab. 35 Struktura Stations

Klíč	Sloupec
PK_Stations()	int nStation
UQ_Stations_StationID()	varchar StationID

Tab. 36 Klíče Stations

Users

Tabulka obsahuje číselník uživatelů.

Sloupec	Popis
nUser int	*

Sloupec	Popis
SID varchar	Identifikace uživatele
UserName varchar	Jméno uživatele

Tab. 37 Struktura Users

Klíč	Sloupec
PK_Users()	int nUser
UQ_Users_NameSID()	varchar UserName

Tab. 38 Klíče Users

1.5 Plán testů softwarových jednotek

1.5.1.1 Softwarové jednotky

Seznam funkcí v jednotlivých softwarových jednotkách, u kterých proběhlo testování.

1.5.1.1.1 Podsystem SysKoApp

Číslo testu	Jednotka	Funkce
1.1	BSSetup	SavePolicy
1.2	BSSetup	DeletePolicy
1.3	BSSetup	bsItems_Click
1.4	BSSetup	bsItems_CurrentCellChanged
1.5	BSSetup	FillListIDs
1.6	BSSetup	Form1_Load
1.7	BSSetup	InitializeComponent
1.8	BSSetup	Main

Tab. 39 Testy funkcí SysKoApp

1.5.1.1.2 Podsystem SysKoCore

Obsahuje třídy a funkce, které slouží jako podpora pro metody tříd dalších subsystémů. Proto je zároveň s testováním příslušných metod testována i metoda ze podsystému SysKoCore.

1.5.1.1.3 Podsystem SysKoAsClient

Číslo testu	Jednotka	Funkce
2.1	CheckSystem	Check
2.2	CheckSystem	CheckFile
2.3	CheckSystem	CheckPolicy
2.4	CheckSystem	CheckRegistry
2.5	CheckSystem	CheckService
2.6	CheckSystem	CheckShare
2.7	ScannerEventLog	Scan
2.8	ScannerFileSystem	ScanDirectory
2.9	ScannerFileSystem	ScanFile

Číslo testu	Jednotka	Funkce
2.10	ScannerPolicy	ScanPolicy
2.11	ScannerRegistry	ScanKey
2.12	ScannerRegistry	ScanValues
2.13	ScannerServices	ScanServiceList
2.14	ScannerShares	ScanShareList

Tab. 40 Testy funkcí SysKoAsClient

1.5.1.1.4 Podsystem SysKoAsServer

Číslo testu	Jednotka	Funkce
3.1	AccesRights	IsAccessRight
3.2	CheckItem	Parse
3.3	CheckList	Parse
3.4	CheckQuery_tr	Query
3.5	CheckQueryConfig	CheckQueryConfig
3.6	CheckQueryConfig	MatchStationID
3.7	CheckQueryThread	Run
3.8	CheckStation	Parse
3.9	CheckSystem	CheckSystem
3.10	CheckSystem	Remove
3.11	CheckSystem	Save
3.12	CheckSystem_tr	Check
3.13	CheckSystem_tr	CheckSystem_tr
3.14	CheckSystem_tr	TestValue
3.15	Notification	AddNotify
3.16	Notification	Notification
3.17	NotificationGroup	Parse
3.18	NotificationTarget	Parse
3.19	NotificationThread	GetRealFilename
3.20	NotificationThread	ParseFormatItem
3.21	NotificationThread	Run
3.22	NotificationThread	SaveOutput
3.23	NotificationThread	TransformOutput
3.24	Notify	Parse
3.25	Process	Parse
3.26	StationGroup	Parse
3.27	SysKo_tr	PumpTransaction
3.28	SysKoManager	CleanContexts
3.29	SysKoManager	NewSysKoContext

Tab. 41 Testy funkcí SysKoAsServer

1.5.1.1.5 Podsystem SysKoConsole

Číslo testu	Jednotka	Funkce
4.1	SysKoConsoleMain	CheckQuery
4.2	SysKoConsoleMain	CheckSystem

4.3	SysKoConsoleMain	EventLog
4.4	SysKoConsoleMain	Main
4.5	SysKoConsoleMain	Scan

Tab. 42 Testy funkcí SysKoConsole

1.5.1.1.6 Podsystem SysKoDb

Číslo testu	Jednotka	Funkce
5.1	BS7799Process	Action
5.2	CheckQueryProcess	Action
5.3	CheckSystemProcess	Action
5.4	EventLogProcess	Action
5.5	ReportProcess	Action
5.6	ReportProcess	CreateDiffResult
5.7	ReportProcess	GetBinaryValuesAsString
5.8	ReportProcess	GetHashACEs
5.9	ReportProcess	GetHashValues
5.10	ReportProcess	LocateBinaryDiff
5.11	ReportProcess	ProcessBinaryValues
5.12	ReportProcess	ReportACEs
5.13	ReportProcess	ReportCheckItemRequests
5.14	ReportProcess	ReportCheckSystem
5.15	ReportProcess	ReportEventLog
5.16	ReportProcess	ReportObjectOSDiff
5.17	ReportProcess	ReportOneScanDiff
5.18	ReportProcess	ReportScanDiff
5.19	ReportProcess	ReportScanList
5.20	ReportProcess	ReportStations
5.21	ReportProcess	ReportValue
5.22	ReportTransaction	CreateCommands
5.23	ScanDiff	ReadXmlSerializable
5.24	ScanProcess	Action

Tab. 43 Testy funkcí SysKoDb

1.5.1.1.7 Podsystem SysKoServer

Číslo testu	Jednotka	Funkce
6.1	SysKoServer	CreateNotificationThreads
6.2	SysKoServer	DeleteInactiveContexts
6.3	SysKoServerConsole	Main

Tab. 44 Testy funkcí SysKoServer

1.5.1.2 Testy funkcí

Testy funkcí softwarových jednotek jsou realizovány vždy po vytvoření daného kódu. Tak je potom možné v případě chyb příslušný kód modifikovat. Kontroluje se správnost funkce při změnách jednotlivých parametrů, při kombinaci změn a při absenci nepovinných parametrů.

Funkce odvozené ze základních jsou testovány souběžně s tvorbou kódu. Zde se totiž jedná pouze o správné volání funkce základní se správně utvořenými parametry.

Časový harmonogram testů se přizpůsobuje tvorbě kódu, protože je jeho nedílnou součástí.

1.6 Vyhodnocení návrhového modelu

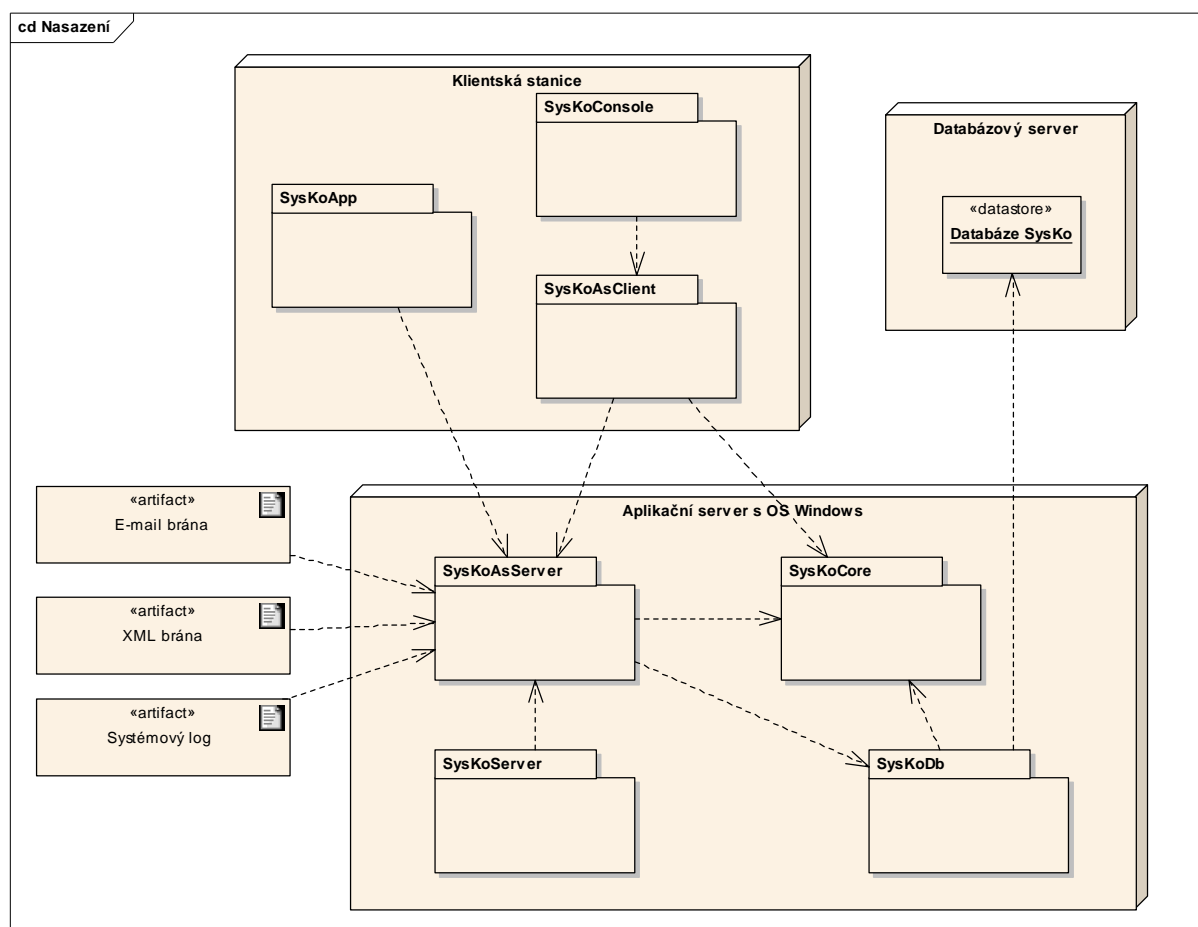
Návrhový model je poslední etapou přípravných prací před vlastní realizací systému. Výsledky analytického modelu byly rozpracovány do konkrétních návrhů jednotlivých tříd, databázových struktur a jejich propojení do celého systému.

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

2. - Implementace IS

2.1 Implementační model

Obrázek znázorňuje nasazení subsystémů na hardware.



Obr. 57 Nasazení podsystémů

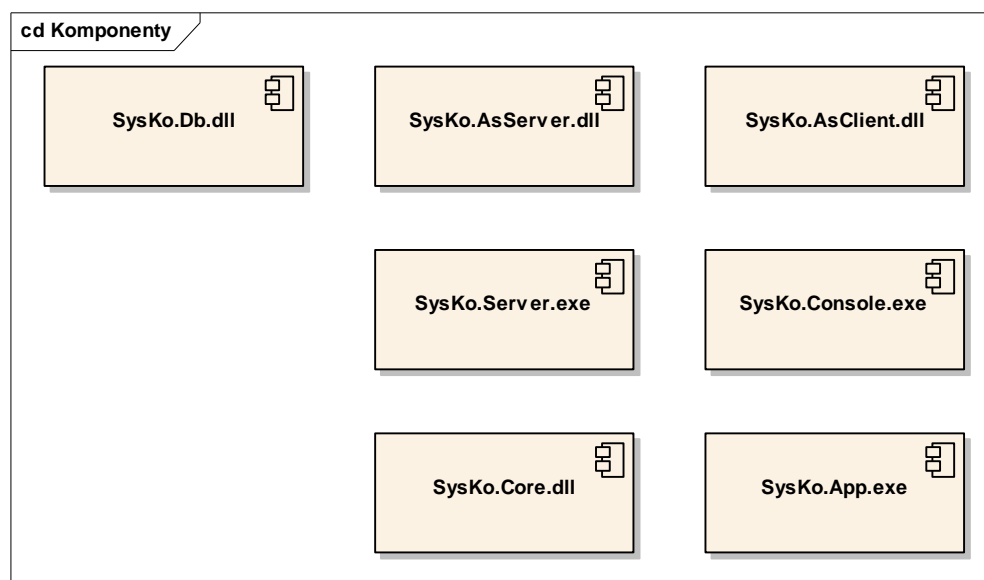
Na databázovém serveru, který může být nainstalován buď na stejném stroji společně s aplikačním serverem nebo na úplně odděleném stroji (např. kvůli zabezpečení nebo minimalizaci ztrát při havárii), je instalována pracovní databáze s databázovým strojem, v našem případě předpokládáme Microsoft SQL Server. Ten pomocí služeb ADO.NET komunikuje s datovou vrstvou, reprezentovanou v našem případě podsystémem SysKoDb.

Tento podsystém, stejně jako další, používá funkce podpůrné knihovny pro celý systém. V našem případě je to podsystém SysKoCore, který je umístěn, stejně jako SysKoDb, na aplikačním serveru.

Hlavní částí střední vrstvy je podsystém SysKoAsServer, který využívá podporu knihovny SysKoCore a datové části SysKoDb. Zprostředkovává podporu aplikačnímu serveru SysKoServer a klientské části.

Klientská část obsahuje část konzolovou, reprezentovanou podsystémem SysKoConsole, podporovanou podsystémem SysKoAsClient. Ten komunikuje s vlastním serverem pomocí technologie .NET remoting. V tomto konkrétním případě jde o komunikaci na binární úrovni, ale v případě problémů (např. při průchodu firewallem) ji lze změnit na komunikaci pomocí HTTP.

Poslední částí je podsystém SysKoApp umístěný v klientské části. Je to grafické rozhraní, kterým se ovládá volba bodů bezpečnostní politiky podle normy BS 7799.



Obr. 58 Diagram tříd SysKo

Výše uvedeným podsystémům odpovídají příslušné komponenty buď ve formě dynamických knihoven DLL nebo ve formě spustitelných souborů EXE.

2.2 Tvorba databáze

Součástí implementace jsou skripty, které obsahují celý servis ohledně tvorby a provozování databázových tabulek. Jsou i uloženy v instalačním souboru.

Název	Typ	Popis
Sqlscripts.sql	Tabulky	Struktury tabulek včetně klíčů a vazeb.
Scandiff.sql	Procedura	Zjištění rozdílů mezi dvěma kontrolami.
ScanStations.sql	Procedura	Zjištění provedených kontrol pro danou stanici.
VwObjectOSScanHash.sql	View	Hašovací kód a kontrola daného objektu.
VwScanDiff.sql	View	Podpora procedury Scandiff.sql.
VwScanObjectsOS.sql	View	Seznam kontrol (scanů) k jednotlivým objektům.

Tab. 45 Popis databázových skriptů

2.3 Kód servisní vrstvy

Kód servisní vrstvy (datová a střední část) byl vytvořen. Výsledkem jsou přeložené komponenty podle kapitoly B.1. Všechny komponenty jsou podepsané s certifikátem pro ověření jejich pravosti.

Komponenta
SysKo.Db.dll
SysKo.Core.dll
SysKo.AsServer.dll
SysKo.Server.exe

Tab. 46 Komponenty servisní vrstvy

2.4 Testy servisní vrstvy

Samostatné testování servisní vrstvy jako celku bez podpory aplikační vrstvy je velmi omezené. Při předpokladu ukončeného testování jednotlivých metod použitých tříd máme k dispozici kompaktní soubor funkcí splňujících požadavky zadání pro tuto část systému. Proto zde nebudou uvedeny žádné testy ani testovací data.

Hlavní testovací práce jsou dále obsaženy v kapitole o kvalifikačních testech softwaru.

2.5 Kód aplikační vrstvy

Kód aplikační vrstvy byl vytvořen. Výsledkem jsou přeložené komponenty podle kapitoly B.1. Všechny komponenty jsou podepsané s certifikátem pro ověření jejich pravosti.

Komponenta
SysKo.AsClient.dll
SysKo.Console.exe
SysKo.App.exe

Tab. 47 Komponenty aplikační vrstvy

2.6 Integrace servisní a aplikační vrstvy

Integrace obou vrstev probíhala zároveň s tvorbou aplikační vrstvy software. Spojení obou částí je realizováno přes .NET remoting, viz. kapitola B.1 Implementační model.

2.7 Testy aplikační vrstvy

Samostatné testování aplikační vrstvy jako celku bez podpory servisní vrstvy nemá smysl s výjimkou testu grafického rozhraní.

Výchozím stavem je uložená testovací bezpečnostní politika v databázi. Její data jsou součástí instalačního souboru. Testy probíhají chronologicky podle pořadí v tabulce.

Č.	Test	Popis testu	Očekávaný výsledek
1	Načtení bezpečnostní politiky	Výběr názvu politiky z kombo boxu.	Do seznamu se načtou body bezpečnostní politiky.
2	Uložení bezpečnostní politiky	Změna hodnoty v poli akt.hodnota, zapsání nového jména politiky do kombo boxu a uložení.	V kombo boxu bude jméno nové bezpečnostní politiky, při načtení původní politiky se vrátí změna ve zvoleném poli akt.hodnota.
3	Vrácení změn	Změna několika hodnot v poli akt.hodnota, změna označení u několika řádků, stisknutí tlačítka pro návrat změn.	Změněným hodnotám bude vrácena hodnota původní.
4	Označit vše, Zrušit vše	Stisknutí tlačítka Označit vše, pak tlačítka Zrušit vše.	Po první akci se označí všechny řádky, po druhé se všechny odoznačí.
5	Smazání bezpečnostní politiky	Výběr názvu politiky z kombo boxu, stisk tlačítka Smazat.	Vybraná politika se vymaže ze seznamu a její název z kombo boxu.

Tab. 48 Testy grafického rozhraní

Grafické rozhraní bylo testováno podle výše uvedené sekvence a uvedené výsledky byly ve shodě s výsledky očekávanými.

Hlavní testovací práce jsou dále obsaženy v kapitole o kvalifikačních testech softwaru.

2.8 Kvalifikační testy

2.8.1 Kvalifikační požadavky

První částí kvalifikačních testů je stanovení seznamu požadavků, které musí hotový software splňovat. Můžeme vyjít ze seznamu funkčních požadavků z analytické části.

Č.	Požadavek	Kvalifikační požadavek
1.	PF.01	SysKo obsahuje bezpečnostní politiku.
2.	PF.02	Bezpečnostní politika podle PF.01 obsahuje bezpečnostní parametry.
3.	PF.03	Bezpečnostní politika podle PF.01 obsahuje relevantní body z BS 7799.
4.	PF.04	SysKo detekuje změny ve sledovaných službách.
5.	PF.05	SysKo detekuje změny ve sledovaných souborech.
6.	PF.06	SysKo detekuje změny ve sledovaných klíčích registru.
7.	PF.07	SysKo detekuje změny ve sledovaných přístupových právech.
8.	PF.08	SysKo detekuje události vybraných typů.
9.	PF.09	SysKo poskytuje informace o kontrolách a změnách.
10.	PF.10	SysKo zasílá informace o kontrolách a změnách elektronickou poštou.
11.	PA.01	SysKo obsahuje seznam sledovaných služeb.
12.	PA.02	SysKo obsahuje seznam sledovaných souborů.

Č.	Požadavek	Kvalifikační požadavek
13.	PA.03	SysKo obsahuje seznam sledovaných klíčů registru.
14.	PA.04	SysKo obsahuje seznam sledovaných přístupových práv.
15.	PA.05	SysKo obsahuje seznam podmínek pro sledování událostí.
16.	PA.06	SysKo obsahuje seznam kontrol a změn bezpečnostního nastavení.
17.	PA.07	SysKo obsahuje obrazy sledovaných služeb.
18.	PA.08	SysKo obsahuje obrazy sledovaných souborů.
19.	PA.09	SysKo obsahuje obrazy sledovaných klíčů registru.
20.	PA.10	SysKo obsahuje obrazy sledovaných přístupových práv.
21.	PA.11	SysKo poskytuje informace o kontrolách a změnách podle nastavení.
22.	PA.12	SysKo obsahuje nastavení pro výstup informací.
23.	PZ.01	SysKo detekuje přítomnost požadovaných bezpečnostních prvků na vzdálené stanici.
24.	PZ.02	SysKo obsahuje informace o kontrolách vzdálené stanice.

Tab. 49 Seznam kvalifikačních požadavků

Požadavky PZ.01 a PZ.02 jsou nové požadavky na funkčnost softwaru podle změn v zadání projektu. Nahradily požadavky PA.13 a PA.14, které byly na základě těchto změn vypuštěny. Dokumentované změny jsou součástí roční zprávy projektu odevzdané v předešlém období.

2.8.2 Seznam kvalifikačních testů

Ke každému kvalifikačnímu požadavku jsou následně přiřazeny testy pro kontrolu splnění daného požadavku společně s termínem provedení. Termín je stanoven vzhledem k dokončení konkrétní akce při instalaci nebo vzhledem k provedení jiného testu. Všechny akce, které předpokládají práci s některou součástí SysKo, jsou popsány v uživatelské, resp. systémové příručce.

Č.poř.	Č.testu	Popis testů	Termín provedení
1.	T01	Databázová kontrola bezpečnostní politiky.	po naplnění databáze
2.	T02	Vizuální kontrola přítomnosti a správnosti.	po provedení T01
3.	T03	Kontrola článků bezpečnostní politiky podle oficiální verze normy BS 7799.	po provedení T02
4.	T04	Detekce nové služby.	po provedení T29
	T05	Detekce změny nastavení služby.	po provedení T04
	T06	Detekce odstranění služby.	po provedení T04
5.	T07	Detekce nového souboru.	po provedení T29
	T08	Detekce změny atributů souboru.	po provedení T07
	T09	Detekce odstranění souboru.	po provedení T07
6.	T10	Detekce nového klíče registru.	po provedení T29
	T11	Detekce změny klíče registru.	po provedení T10
	T12	Detekce odstranění klíče registru.	po provedení T10
7.	T13	Detekce změny přístupových práv na službě.	po provedení T04
	T14	Detekce změny přístupových práv na souboru.	po provedení T07
	T15	Detekce změny přístupových práv na klíči registru.	po provedení T10
8.	T16	Detekce události vybraného typu.	po provedení T04
9.	T17	Kontrola existence a obsahu výstupních sestav	po provedení testů

Č.poř.	Č.testu	Popis testů	Termín provedení
10.	T18	Kontrola odeslání e-mailu s obsahem	po provedení testů
11.	T19	Vizuální kontrola konfiguračního souboru, který musí obsahovat definice sledovaných služeb.	po konfiguraci služeb
12.	T20	Vizuální kontrola konfiguračního souboru, který musí obsahovat definice sledovaných souborů.	po konfiguraci souborů
13.	T21	Vizuální kontrola konfiguračního souboru, který musí obsahovat definice sledovaných klíčů registru.	po konfiguraci klíčů registru
14.	T22	Vizuální kontrola konfiguračního souboru, který musí obsahovat definice přístupových práv.	po konfiguraci přístupových práv
15.	T23	Vizuální kontrola konfiguračního souboru, který musí obsahovat podmínky pro sledování událostí.	po konfiguraci sledování událostí
16.	T24	Kontrola existence konfiguračních souborů, které obsahují popis kontrol a nastavení.	po instalaci SysKo
17.	T25	Kontrola tabulky s obrazy sledovaných služeb.	před a po T04
18.	T26	Kontrola tabulky s obrazy sledovaných souborů.	před a po T07
19.	T27	Kontrola tabulky s obrazy sledovaných klíčů registru.	před a po T10
20.	T28	Kontrola tabulek s obrazy na existenci přístupových práv.	po provedení T25, T26 a T27 (jednotlivě)
21.	T29	Kontrola běhu serveru kontroly a detekce změn.	po instalaci SysKo
22.	T30	Kontrola existence konfiguračních souborů, které obsahují nastavení výstupu.	po instalaci SysKo
23.	T31	Detekce přítomnosti předepsaných bezpečnostních prvků na vzdálené stanici.	po instalaci SysKo a klientské části na stanici
24.	T32	Kontrola výstupních sestav s provedenými kontrolami na vzdálené stanici.	po provedení T31

Tab. 50 Popis testů

K některým testům je dále rozepsáno detailnější provedení.

2.8.2.1.1.1 T04. Detekce nové služby

1. Vytvoření obrazu služeb systému.
2. Vložení předem definované služby (SysKoTestSvc.exe je v instalačním souboru). Instalace se provede pomocí instalátoru InstallUtil.exe, který je součástí instalace frameworku .NET (volání **InstallUtil.exe SysKoTestSvc.exe** z konzole).
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenána přítomnost nové služby SysKoTestSvc.

2.8.2.1.1.2 T05. Detekce změny nastavení služby

1. Po provedení testu T.04 je služba SysKoTestSvc nainstalována a máme zaznamenán aktuální obraz služeb.

2. Typ spuštění je změněn z ručně na automaticky a zastavená služba je spuštěna.
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenány změny výše uvedených parametrů u služby SysKoTestSvc.

2.8.2.1.1.3 T06. Detekce odstranění služby

1. Po provedení testu T.04 je služba SysKoTestSvc nainstalována a máme zaznamenán aktuální obraz služeb.
2. Odebrání služby SysKoTestSvc se provede pomocí instalátoru InstallUtil.exe (viz. výše) voláním **InstallUtil.exe /u SysKoTestSvc.exe** z konzole.
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenáno odebrání služby SysKoTestSvc ze systému.

2.8.2.1.1.4 T07. Detekce nového souboru

1. Vytvoření obrazu souborů systému. Obraz musí zahrnovat kontrolu systémové disku na soubory s příponou .txt.
2. Vložení předem definovaného souboru (SysKoTestFile.txt je součástí instalačního souboru) na systémový disk.
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenána přítomnost nového souboru SysKoTestFile.txt.

2.8.2.1.1.5 T08. Detekce změny atributů souboru

1. Po provedení testu T.07 je soubor SysKoTest File.txt uložen na systémovém disku a máme zaznamenán aktuální obraz souborů.
2. Je změněna délka souboru přidáním znaků do souboru a změněn atribut (např. ReadOnly na Ano).
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenány změny výše uvedených atributů souboru SysKoTestFile.txt.

2.8.2.1.1.6 T09. Detekce odstranění souboru

1. Po provedení testu T.07 je soubor SysKoTest File.txt uložen na systémovém disku a máme zaznamenán aktuální obraz souborů.
2. Soubor SysKoTest File.txt je vymazán ze systémového disku .
4. Spuštění detekce a kontrola výsledku. Musí být zaznamenáno odebrání souboru SysKoTest File.txt ze systému.

2.8.2.1.1.7 T10. Detekce nového klíče registru

1. Vytvoření obrazu klíčů registru systému. Obraz musí zahrnovat kontrolu složky HKEY_LOCAL_MACHINE.
2. Do sekce HKEY_LOCAL_MACHINE\SOFTWARE je vložen nový klíč TEST. Do něj vložena nova textová hodnota pojmenovaná jako **Text**, nová binární hodnota pojmenovaná **Binar** a nova hodnota DWORD jménem **Dword**.
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenána přítomnost nového klíče HKEY_LOCAL_MACHINE\SOFTWARE\TEST obsahujícího výše uvedené hodnoty.

2.8.2.1.1.8 T11. Detekce změny klíče registru

1. Po provedení testu T.10 jsou v klíči HKEY_LOCAL_MACHINE\SOFTWARE\TEST uloženy hodnoty Text, Binar a Dword a máme zaznamenán aktuální obraz klíčů registru.
2. Jsou změněny údaje hodnot Text, Binar a Dword.
4. Spuštění detekce a kontrola výsledku. Musí být zaznamenány změny výše uvedených hodnot klíče HKEY_LOCAL_MACHINE\SOFTWARE\TEST.

2.8.2.1.1.9 T12. Detekce odstranění klíče registru

1. Po provedení testu T.10 jsou v klíči HKEY_LOCAL_MACHINE\SOFTWARE\TEST uloženy hodnoty Text, Binar a Dword a máme zaznamenán aktuální obraz klíčů registru.
2. Celý klíč HKEY_LOCAL_MACHINE\SOFTWARE\TEST je vymazán z registrů.
5. Spuštění detekce a kontrola výsledku. Musí být zaznamenáno odebrání celého klíče HKEY_LOCAL_MACHINE\SOFTWARE\TEST včetně hodnot.

2.8.2.1.1.10 T13. Detekce změny přístupových práv na službě

1. Po provedení testu T.04 je služba SysKoTestSvc nainstalována a máme zaznamenán aktuální obraz služeb.
2. Je změněno přístupové právo služby.
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenána změna v přístupových právech služby SysKoTestSvc.

2.8.2.1.1.11 T14. Detekce změny přístupových práv na souboru

1. Po provedení testu T.07 je soubor SysKoTest File.txt uložen na systémovém disku a máme zaznamenán aktuální obraz souborů.
2. Je změněno přístupové právo souboru.
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenána změna v přístupových právech souboru SysKoTest File.txt.

2.8.2.1.1.12 T15. Detekce změny přístupových práv na klíči registru

1. Po provedení testu T.10 jsou v klíči HKEY_LOCAL_MACHINE\SOFTWARE\TEST uloženy hodnoty Text, Binar a Dword a máme zaznamenán aktuální obraz klíčů registru.
2. Jsou změněna přístupová práva hodnoty Text, Binar a Dword klíče HKEY_LOCAL_MACHINE\SOFTWARE\TEST.
3. Spuštění detekce a kontrola výsledku. Musí být zaznamenána změna v přístupových právech klíče HKEY_LOCAL_MACHINE\SOFTWARE\TEST.

2.8.2.1.1.13 T16. Detekce události vybraného typu

1. Po provedení testu T.04 je nainstalována služba SysKoTestSvc, která obsahuje vyvolání události v protokolu aplikací (kontrola pomocí Prohlížeče událostí).
2. Detekce událostí je zkonfigurována na detekci události typu informace v aplikačním protokolu (logu).
3. Spustíme službu SysKoTestSvc, která musí vyvolat událost ve zdroji SysKoTest (v popisu je SysKo test service start).

2.8.2.1.1.14 T18. Kontrola odeslání e-mailu s obsahem

1. Použijeme akci z testu T16, musí být nastaveno odeslání zpráv e-mailem na definovanou adresu.
2. Na této adrese pak zkontrolujeme příchod zprávy s obsahem z testu T.16.

2.8.2.1.1.15 T29. Kontrola běhu serveru kontroly a detekce změn

1. Instalace serveru jako služby **SysKo.Server.exe** se provede pomocí instalátoru InstallUtil.exe, který je součástí instalace frameworku .NET (volání **InstallUtil.exe SysKo.Server.exe** z konzole).
2. Spuštění a kontrola se děje pomocí prohlížeče služeb.
3. Správnost detekce je kontrolována v jiných testech.

2.8.2.1.1.16 T31. Detekce přítomnosti předepsaných bezpečnostních prvků na vzdálené stanici

1. Předpokladem je běžící server SysKo a úspěšná instalace klientské části na vzdálené stanici. Server je zkonfigurován na detekci klientské části a je nastavena UDP konfigurace.
2. Stanice bez instalovaného antivirového programu volá službu kontroly systému (CheckSystem) na serveru. Výsledkem je zaznamenána nepřítomnost antiviru, zaznamenaná ve výstupní sestavě.

3. Dotaz klientského programu s akcí checkQuery nepřítomnost ověří (počet dní od posledního úspěšného testu je velký). Dále nepřítomnost ověří dotaz pomocí skriptu client_connect.py (na klientské stanici musí být instalován interpret jazyka Python).
4. Na stanici se instaluje antivirový program.
5. Body 2. a 3. se opakují s tím, že je zaznamenána přítomnost antivirového programu (počet dní od posledního úspěšného testu je 0).

2.9 Vyhodnocení implementace

Byl vytvořen a otestován kód aplikace SysKo a byla vytvořena servisní databáze. Podle postupu kvalifikačního testování byla aplikace testována na přítomnost a správnost všech požadovaných funkcí. Chyby a nesrovnalosti v kódu byly odstraněny a software byl upraven podle výsledků testování. Aplikace je funkční a připravena k nasazení na konkrétní informační systém.

2.10 Protokol o kvalifikačním testování software

Protokol o kvalifikačním testování software obsahuje chronologii softwarových testů a může být použit jako samostatný dokument. Pro každý bod je třeba zaznamenat výsledek.

Pořadí	Č. testu	Název testu	Výsledek
1.	T01	Součást instalace.	ú
2.	T24	Kontrola podle systémové příručky.	ú
3.	T30	Kontrola podle systémové příručky.	ú
4.	T29	Kontrola v prohlížeči služeb.	ú
5.	T02	Vizuální kontrola, porovnání s instalačními daty.	ú
6.	T03	Kontrola podle článků normy BS7799.	ú
7.	T19	Kontrola konfigurace služeb.	ú
8.	T25	Kontrola před scanem služeb.	ú
9.	T04	Instalace služby.	ú
10.	T25	Kontrola po scanu služeb.	ú
11.	T28	Kontrola přístupových práv na službu.	ú
12.	T17	Kontrola výstupu.	ú
13.	T18	Kontrola e-mailu.	ú
14.	T05	Práce se službou.	ú
15.	T17	Kontrola výstupu.	ú
16.	T16	Kontrola událostí vyvolaných testem T05.	ú
17.	T17	Kontrola výstupu.	ú
18.	T13	Přístupová práva služby.	ú
19.	T06	Smazání služby.	ú
17.	T17	Kontrola výstupu.	ú
18.	T20	Kontrola konfigurace souborů.	ú
19.	T07	Natažení souboru.	ú
20.	T26	Kontrola po scanu souborů.	ú
21.	T28	Kontrola přístupových práv na soubor.	ú

Pořadí	Č. testu	Název testu	Výsledek
22.	T17	Kontrola výstupu.	ú
23.	T08	Práce se souborem.	ú
24.	T17	Kontrola výstupu.	ú
25.	T14	Přístupová práva na soubor.	ú
26.	T09	Smazání souboru.	ú
27.	T17	Kontrola výstupu.	ú
28.	T21	Kontrola konfigurace klíčů registru.	ú
29.	T10	Vytvoření klíče registru.	ú
30.	T27	Kontrola po scanu klíčů registru.	ú
31.	T28	Kontrola přístupových práv na klíč registru.	ú
32.	T17	Kontrola výstupu.	ú
33.	T11	Práce se klíčem registru.	ú
34.	T17	Kontrola výstupu.	ú
35.	T15	Přístupová práva na klíč registru.	ú
36.	T12	Smazání klíče registru.	ú
37.	T17	Kontrola výstupu.	ú
38.	T31	Kontrola stanice podle konfigurace.	ú
39.	T32	Kontrola výstupu.	ú
40.	T18	Kontrola e-mailu může proběhnout v závislosti na konfiguraci.	ú

Tab. 51 Protokol o kvalifikačním testování software

3. – Kvalifikační testování systému

3.1 Plán kvalifikačního testování systému

3.1.1 Kvalifikační požadavky

První částí kvalifikačních testů je stanovení seznamu požadavků, které musí provozovaný systém splňovat.

Č.	Požadavek	Kvalifikační požadavek
1.	PKS01	Databázový server splňuje hardwarová kritéria.
2.	PKS02	Aplikační server splňuje hardwarová kritéria.
3.	PKS03	Databázový server splňuje softwarová kritéria.
4.	PKS04	Aplikační server splňuje softwarová kritéria.
5.	PKS05	Vzdálená stanice splňuje hardwarová a softwarová kritéria (jen v případě umožnění testů vzdálené stanice).
6.	PKS06	Aplikace SysKo dokáže detekovat změnu ve sledovaných službách OS a vygenerovat příslušný výstup.
7.	PKS07	Aplikace SysKo dokáže detekovat změnu ve sledovaných souborech OS a vygenerovat příslušný výstup.
8.	PKS08	Aplikace SysKo dokáže detekovat změnu ve sledovaných klíčích registru OS a vygenerovat příslušný výstup.
9.	PKS09	Aplikace SysKo dokáže detekovat událost v protokolu událostí (event log) a vygenerovat příslušný výstup.
10.	PKS10	Aplikace SysKo dokáže detekovat změnu v nastavení bezpečnostní politiky a vygenerovat příslušný výstup.
11.	PKS11	Aplikace SysKo dokáže detekovat nastavení vzdálené stanice a vygenerovat příslušný výstup.

Tab. 52 Seznam kvalifikačních požadavků systému

Prvních pět požadavků obsahuje kritéria, jejichž splněním je podmíněna správná funkce aplikace SysKo. Splněním dalších požadavků je aplikace SysKo kvalifikačně otestována na konkrétním OS.

3.1.2 Seznam kvalifikačních kritérií

Jsou uvedeny minimální a doporučené hodnoty pro splnění hardwarových a softwarových kritérií. Tato kritéria musí být splněna před instalací aplikace SysKo z důvodu zajištění její korektní funkce.

Požadavek	Č.	Kritérium	Minimální hodnota	Doporučená hodnota
PKS01	1.	Počítač a procesor	Pentium 166 Mhz ¹	verze Pentium 4
	2.	Paměť	64 MB	512 MB
	3.	Volné místo na disku	200 MB ²	1 GB

	4.	Jednotka	CD – ROM	DVD RW
	5.	Zobrazení	VGA monitor	VGA monitor s rozlišením 800x600, 256 barev
	6.	Síťové připojení	Ethernet 100 Mbit/s	Ethernet 1 Gbit/s
PKS02	7.	Počítač a procesor	Pentium III 700 Mhz ³	verze Pentium 4
	8.	Paměť	128 MB	512 MB
	9.	Volné místo na disku	370 MB ⁴	1GB
	10.	Jednotka	CD – ROM	DVD ROM
	11.	Zobrazení	VGA monitor s rozlišením 800x600, 256 barev	VGA monitor s rozlišením 800x600, 256 barev
	12.	Síťové připojení	Modem 64 kbit/s	Ethernet 100 Mbit/s
PKS03	13.	Operační systém	Windows NT 4.0 se service packem 6a (SP6a) ⁵	Windows Server 2003 SP 1
	14.	Databáze	MS SQL Data Engine (MSDE)	MS SQL Server 2000 SP4
	15.	Další software	-	MS Internet Explorer 6
PKS04	16.	Operační systém	Windows NT 4.0 se service packem 6a (SP6a) ⁵	Windows Server 2003 s poslední verzí service packu
	17.	Podpora SysKo	.NET Framework 1.1 ⁶	.NET Framework 2.0 ⁶
	18.	Další software	MS Internet Explorer 6, MDAC 2.7 ⁷	MS Internet Explorer 6, MDAC 2.7
PKS05	19.	Operační systém	Windows 2000 Professional SP4	Windows XP SP1 a vyšší
	20.	Podpora SysKo	.NET Framework 1.1, interpret jazyka Python ⁸	.NET Framework 1.1, interpret jazyka Python

Tab. 53 Popis kritérií

¹ případně procesor, který odpovídá požadavkům instalovaného software (SQL Server)

² závisí na množství uchovávaných dat, resp. pravidelnosti údržby místa na disku ze strany správce aplikace

³ případně procesor, který odpovídá požadavkům instalovaného OS

⁴ v závislosti na dalších požadavcích instalovaného OS

⁵ SysKo nezaručuje správnou funkci sledování bezpečnostní politiky z důvodu nekompatibility s vyššími verzemi serverových operačních systémů Windows

⁶ viz Soupis citací [17]

⁷ viz Soupis citací [18]

⁸ viz Soupis citací [19]

3.2 Testovací data

Data potřebná k testování systému podle kvalifikačních požadavků PKS06 až PKS09 jsou uložena v instalačním souboru. Jsou použita stejná data jako pro kvalifikační testování software (viz. kapitola B 8.2 Seznam kvalifikačních testů).

3.3 Kvalifikační testování

Nutným předpokladem kvalifikačního testování systému je správně a kompletně dokončená instalace SysKo na testovaném systému. Pak se postupuje podle připravených testovacích postupů a výsledky jsou dokumentovány.

3.3.1.1.1.1 **PKS06. Aplikace SysKo dokáže detekovat změnu ve sledovaných službách OS a vygenerovat příslušný výstup**

Je vytvořena nová služba a nová konfigurace pro testování služeb OS. Je proveden scan služeb před instalací a spuštěním služby a po ní. Generovaný rozdíl je dokumentován jako součást výsledků testu.

Služba je odebrána z OS a po provedení scanu služeb je generovaný rozdíl dokumentován jako součást výsledků testu.

3.3.1.1.1.2 **PKS07. Aplikace SysKo dokáže detekovat změnu ve sledovaných souborech OS a vygenerovat příslušný výstup**

Je vytvořen a uložen nový soubor a vytvořena nová konfigurace pro testování souborů. Je proveden scan souborů před vytvořením souboru a po něm. Generovaný rozdíl je dokumentován jako součást výsledků testu.

Soubor je odebrán a po provedení scanu souborů je generovaný rozdíl dokumentován jako součást výsledků testu.

3.3.1.1.1.3 **PKS08. Aplikace SysKo dokáže detekovat změnu ve sledovaných klíčích registru OS a vygenerovat příslušný výstup**

Je vytvořen a uložen nový klíč registru s hodnotami a vytvořena nová konfigurace pro testování klíčů registru. Je proveden scan klíčů registru před vytvořením nového klíče a po něm. Generovaný rozdíl je dokumentován jako součást výsledků testu.

Klíčů registru je odebrán a po provedení scanu klíčů registru je generovaný rozdíl dokumentován jako součást výsledků testu.

3.3.1.1.1.4 **PKS09. Aplikace SysKo dokáže detekovat událost v protokolu událostí (event log) a vygenerovat příslušný výstup**

Je vytvořena nová služba a nová konfigurace pro sledování událostí OS. Po spuštění služby je výsledek sledování událostí dokumentován jako výsledek testu.

3.3.1.1.5 PKS10. Aplikace SysKo dokáže detekovat změnu v nastavení bezpečnostní politiky a vygenerovat příslušný výstup

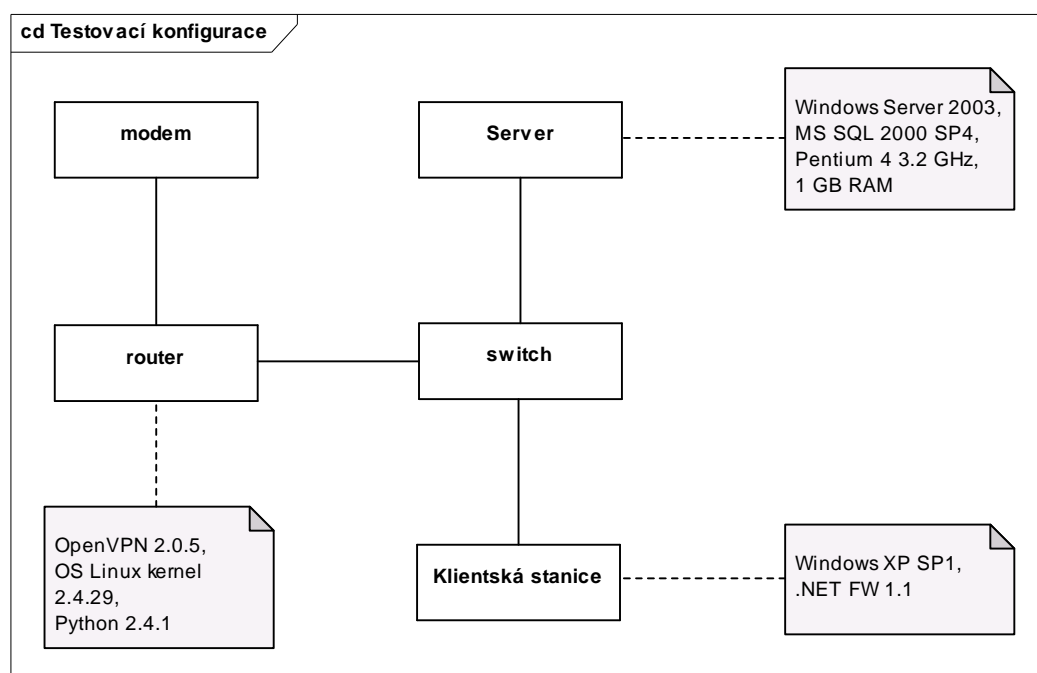
Je změněna hodnota bodu bezpečnostní. Je proveden scan politiky před změnou a po ní. Generovaný rozdíl je dokumentován jako výsledek testu.

3.3.1.1.6 PKS11. Aplikace SysKo dokáže detekovat nastavení vzdálené stanice a vygenerovat příslušný výstup

Je konfigurován server i vzdálená stanice pro kontrolu systému. Je provedena kontrola stanice před a po instalování antivirového programu. Výstup každé z kontrol je dokumentován jako součást výsledků testu.

3.4 Vyhodnocení integrace a testů systému

Testování SysKo bylo provozováno na následující konfiguraci.



Obr. 59 Testovací konfigurace

Byly provedeny kvalifikační testy podle kapitoly C.3. Jejich výsledky zachycuje následující kapitola C.5 Protokol o kvalifikačním testování systému.

3.5 Protokol o kvalifikačním testování systému

Byly provedeny kvalifikační testy systému podle kapitoly C.3.

Č.	Požadavek	Kvalifikační požadavek	Výsledek
K.1	PKS06	Aplikace SysKo dokáže detekovat změnu ve sledovaných službách OS a vygenerovat příslušný výstup.	ú

K.2	PKS07	Aplikace SysKo dokáže detekovat změnu ve sledovaných souborech OS a vygenerovat příslušný výstup.	ü
K.3	PKS08	Aplikace SysKo dokáže detekovat změnu ve sledovaných klíčích registru OS a vygenerovat příslušný výstup.	ü
K.4	PKS09	Aplikace SysKo dokáže detekovat událost v protokolu událostí (event log) a vygenerovat příslušný výstup.	ü
K.5	PKS10	Aplikace SysKo dokáže detekovat změnu v nastavení bezpečnostní politiky a vygenerovat příslušný výstup.	ü
K.6	PKS11	Aplikace SysKo dokáže detekovat nastavení vzdálené stanice a vygenerovat příslušný výstup.	ü

Tab. 54 Protokol o kvalifikačním testování systému

Dále jsou uvedeny poznámky k realizovaným testům.

Test K.1:

Byl vytvořen záznam v konfiguračním souboru (id=scantest, element <services>) a byla vytvořena nová služba SysKoTestSvc pomocí testovací třídy Wak.SysKo.SysKoTestSvc. Po provedení testu byly zjištěny změny v přítomnosti a v průběhu testu byla zjištěna změna stavu služby.

Test K.2:

Byl vytvořen záznam v konfiguračním souboru (id=scantest, element <fileSystem> s cestou na určený adresář). V průběhu testů byl testovací soubor SysKoTestFile.txt uložen a měněn. Po provedení jednotlivých částí testu byly zjištěny změny v přítomnosti souboru a zjištěny změny v jeho attributech.

Test K.3:

Byl vytvořen záznam v konfiguračním souboru (id=scantest, element <registry>) a do registrů vložen nový klíč LocalMachine\Software\SysKo podle pokynů. Po provedení testu byly zjištěny změny v přítomnosti klíče a změny v nastavených hodnotách. Testována byla řetězcová hodnota a také přístupová práva ke klíči registru.

Test K.4:

Byl vytvořen záznam v konfiguračním souboru (id=scantest, element <services>) a byla vytvořena nová služba SysKoTestSvc pomocí testovací třídy Wak.SysKo.SysKoTestSvc. Byl založen další záznam pro sledování událostí (id=evltest, element <log>). Testovací služba byla spuštěna. Po provedení testu byla zjištěna přítomnost událostí v aplikační části, které testovací služba generovala.

Test K.5:

Byl vytvořen záznam v konfiguračním souboru (id=scantest, element <policy>). Byla změněna minimální délka hesla a proveden test. Po jeho provedení byla tato změna zaznamenána.

Test K.6:

Je konfigurován server i vzdálená stanice pro kontrolu systému. Je nastavena UDP konfigurace serveru. Na klientské stanici je nainstalován interpret jazyka Python. Stanice bez instalovaného antivirového programu volala službu kontroly systému na serveru a přítomnost antiviru nebyla zaznamenána. Po instalaci antiviru byla zaznamenána přítomnost antivirového programu (počet dní od posledního úspěšného testu byl 0).

4. – Instalace a akceptace systému

4.1 Instalační program

Instalace systému probíhá pomocí instalačního souboru, který obsahuje všechna data potřebná k umístění a úspěšnému spuštění aplikace v systému v komprimované formě. Obsah instalačního souboru je popsán dále.

Soubory s názvem začínajícím Wak.Wnt jsou podpůrné knihovny firmy WAK System spol. s r.o., jejichž vlastnosti a metody aplikace SysKo využívá. Popis těchto knihoven není předmětem činnosti tohoto projektu.

adresář	soubor	popis
syskoserver	Wak.SysKo.Server.exe	Aplikační server.
	Wak.SysKo.Server.exe.config	Konfigurační soubor.
	Wak.SysKo.As.Server.dll, Wak.SysKo.Core.dll, Wak.SysKo.Db.dll, Wak.Wnt.As.dll, Wak.Wnt.Core.dll, Wak.Wnt.Db.dll, Wak.Wnt.Mail.dll, Wak.Wnt.Tools.dll	Podpůrné knihovny.
	css/checkSystem.css, css/scanDiff.css	Kaskádové styly pro výstupní sestavy.
	xslt/html_checkSystem.xslt, xslt/html_eventLog.xslt, xslt/html_scanDiff.xslt, xslt/html_scanList.xslt, xslt/html_stationList.xslt	Šablony výstupních sestav do XML.
	Wak.SysKo.Console.exe	Aplikační konzola.
syskoconsole	Wak.SysKo.Console.exe.config	Konfigurační soubor.
	LibCpp.dll, LibCppM.dll, Wak.SysKo.As.Client.dll, Wak.SysKo.As.Server.dll, Wak.SysKo.Core.dll, Wak.SysKo.Db.dll, Wak.Wnt.As.dll, Wak.Wnt.Core.dll, Wak.WinApi.dll, Wak.Wnt.As.dll, Wak.Wnt.Core.dll, Wak.Wnt.Db.dll, Wak.Wnt.Mail.dll, Wak.Wnt.Tools.dll	Podpůrné knihovny.

adresář	soubor	popis
syskoapp	Wak.SysKo.App.exe	Spuštění editace bezpečnostních politik.
	Wak.SysKo.App.exe.config	Konfigurační soubor.
	Wak.SysKo.As.Server.dll, Wak.SysKo.Core.dll, Wak.SysKo.Db.dll, Wak.Wnt.As.dll, Wak.Wnt.Core.dll, Wak.Wnt.Db.dll, Wak.Wnt.Mail.dll, Wak.Wnt.Tools.dll	Podpůrné knihovny.
	BS7799/ importPolicyTable.cmd	Import dat z XML na SQL server.
	BS7799/PolicyBS7799.xml	Data BS 7799 ve formě XML.
	BS7799/Wak.Tools.XmlDb.exe, BS7799/Wak.Wnt.Db.dll, BS7799/Wak.Wnt.Generators.D b2XsdLib.dll	Podpůrné knihovny.
	Procedures/ScanDiff.sql, Procedures/ScanStations.sql	Procedury SQL serveru.
SQLscripts	Tables/sqlscripts.sql	Script pro generování tabulek.
	Views/vwObjectOSScanHash.s ql, Views/vwScanDiff.sql, Views/vwScanObjectsOS.sql	Pomocné views pro procedury.
	client_connect.py	Script pro testování vzdálené stanice (pro OpenVPN)
	Wak.SysKo.SysKoTestSvc.exe	Testovací služba.
Testy	SysKoTestFile.txt	Testovací soubor.

Tab. 55 Obsah instalačního souboru

Postup vlastní instalace SysKo je popsán v dalším textu.

4.2 Plán zavádění IS

Plán zavádění SysKo spočívá v následujících krocích.

Pořadí	Popis akce zavádění
1.	Splnění minimálních kritérií PKS01, PKS02, PKS03 a PKS04 kvalifikačního testování systému, na kterém bude SysKo provozováno.
2.	Vytvoření adresáře SysKo na aplikačním serveru a rozbalení obsahu instalačního souboru.
3.	Převedení adresáře SQL z vytvořeného adresáře na datový server a spuštění připravených scriptů.
4.	Splnění minimálních kritérií PKS05 pro referenční stanici.
5.	Příprava vstupních a výstupních konfiguračních souborů aplikace.
6.	Kvalifikační otestování připraveného systému.

7.	Provedení školení pro vybrané uživatele poskytovatele.
8.	Vyplnění Protokolu o převzetí IS.

Tab. 56 Kroky zavádění aplikace SysKo

Poznámky k vybraným bodům instalace:

Ad 2. Je třeba zachovat originální strukturu adresářů z instalačního souboru.

Ad 3. Obsahem jsou struktury tabulek, procedury a další servisní funkce ve formě scriptů popsané výše. Postupným spouštěním je vytvořena struktura servisní databáze. Další součástí jsou i data BS 7799 připravená k naplnění tabulky ve formě XML.

Ad 4. Referenční stanice slouží k ověření funkce SysKo, nemusí být nutně součástí systému pro ostrý provoz.

Ad 5. Viz Uživatelská příručka.

Ad 6. Kvalifikační testování systému. Výsledek zachycen v Protokolu o kvalifikačním testování systému.

Ad 7. Budoucí administrátor systému je seznámen s funkcemi SysKo a s jeho údržbou.

4.3 Instalace, akceptační přezkoumání, kompletace

Instalace na cílovém systému ISOKR byla úspěšně provedena. Uživatel poskytovatele byl seznámen s použitím aplikace SysKo a jeho konfigurací. Konfigurace byla upravena podle přání poskytovatele.

4.4 Protokol o převzetí IS

Pro předání IS byl vytvořen Protokol o převzetí IS, jenž je uveden na následující straně a je možné ho vytisknout jako samostatný dokument.

WAK SYSTEM, spol. s r.o.

Petržilkova 2564/21

158 00 Praha 5

Příjemce

Ministerstvo dopravy ČR

Nábřeží L. Svobody 12

110 15 Praha 1

Poskytovatel

PŘEDÁVACÍ PROTOKOL K PROJEKTU

č. 1F43D/007/030

System automatizované kontroly a detekce změn bezpečnostního nastavení informačních systémů založený na specifikaci bezpečnostní politiky podle standardu BS7799.

Poskytovatel potvrzuje převzetí výsledků projektu a zaškolení

Předáno dne:

Poskytovatel:

Příjemce:

5. – Výstupní dokumentace

5.1 Systémová příručka IS

Dokument “Systémová příručka IS“ je uveden v dalším textu a dá se použít jako samostatný manuál.

5.2 Uživatelská příručka IS

Dokument “Uživatelská příručka IS“ je uveden v dalším textu a dá se použít jako samostatný manuál.

5.3 Školící a učební testy

Jako školící a učební texty se použije Uživatelská příručka, která obsahuje příklady nastavení SysKo a postup při práci s aplikací. Pro nastavení systému podle kapitoly C.1.2 Seznam kvalifikačních kritérií je dále možné použít dokumentaci pro software na adresách <http://www.microsoft.com/downloads/results.aspx?freetext=framework&DisplayLang=en>^[17], <http://msdn.microsoft.com/data/mdac/downloads/default.aspx>^[18], <http://www.python.org/download/>^[19].

Postup je ve shodě se standardem 005/02.01^[4], kde je pro tento účel možné použít dokumenty vzniklé v průběhu vývoje IS nebo jejich části.

E.1 - Systémová příručka IS

Obsah

Úvod	1
1. Popis	1
2. Konfigurační soubory na straně serveru	2
2.1 Konfigurační soubor SysKoServer	2
2.1.1 Element <configuration>.....	2
2.1.2 Element <configSections>	3
2.1.3 Element <sysko>	3
2.1.4 Element <appConnectionString>	3
2.1.5 Element <notification>.....	4
2.1.6 Element <group>.....	4
2.1.7 Element <target>	4
2.1.8 Element <notify>.....	5
2.1.9 Element <checkSystem>	6
2.1.10 Element <checkList>.....	6
2.1.11 Element <checkItem>.....	7
2.1.12 Element <checkStation>	7
2.1.13 Element <checkQuery>	7
2.1.14 Element <excludeStation>	8
2.1.15 Element <accessRights>.....	8
2.1.16 Element <stationGroup>	8
2.1.17 Element <station>	9
2.1.18 Element <process>	9
2.1.19 Element <allowGroup>	9
2.1.20 Element <wak.wnt.remoting>	10

2.1.21	Element <channel>.....	10
2.2	Konfigurační soubory na straně klienta.....	10
2.2.1	Konfigurační soubor SysKoConsole	10
2.2.2	Element <configuration>.....	11
2.2.3	Element <configSections>	11
2.2.4	Element <sysko>	12
2.2.5	Element <appSettings>	12
2.2.6	Element <scanner>	12
2.2.7	Element <scan>	12
2.2.8	Element <fileSystem>	13
2.2.9	Element <registry>	13
2.2.10	Element <services>	14
2.2.11	Element <shares>	14
2.2.12	Element <policy>	14
2.2.13	Element <eventLog>	15
2.2.14	Element <events>	15
2.2.15	Element <log>	15
2.3	Konfigurační soubor SysKoApp	16
3.	Výstupní soubory.....	17
3.1	scanDiff	17
3.1.1	Element <scanDiffList>	18
3.1.2	Element <scanDiff>	18
3.1.3	Element <station>	18
3.1.4	Element <scan1>	18
3.1.5	Element <scan2>	19
3.1.6	Element <name>	19
3.1.7	Element <type>	20

3.1.8	Element <Values>	20
3.1.9	Element <ACEs>.....	20
3.2	EventLog	21
3.2.1	Hierarchie elementů	21
3.2.2	Element <EventLog>	21
3.2.3	Element <event>	21
3.2.4	Element <user>	22
3.2.5	Element <stationID>	22
3.2.6	Element <logName>.....	22
3.2.7	Element <machineName>	23
3.2.8	Element <eventDate>.....	23
3.2.9	Element <eventID>	23
3.2.10	Element <eventType>	23
3.2.11	Element <eventSource>	24
3.2.12	Element <eventDescription>.....	24
3.3	scanList.....	24
3.3.1	Hierarchie elementů	24
3.3.2	Element <scanList>.....	25
3.3.3	Element <scan>	25
3.3.4	Element <stationID>	25
3.3.5	Element <scanID>.....	25
3.3.6	Element <scanDate>.....	26
3.3.7	Element <scanResult>.....	26
3.4	Stations	26
3.4.1	Element <Stations>	26
3.4.2	Element <station>	27
3.4.3	Element <id>	27

3.4.4	Element <name>	27
3.4.5	Element <localAddress>	28
3.4.6	Element <publicAddress>	28
3.5	CheckSystemList	28
3.5.1	Element <CheckSystemList>	29
3.5.2	Element <CheckSystem>	29
3.5.3	Element <scan>	30
3.5.4	Element <checkRequestItem>.....	30
3.5.5	Element <name>	30
3.5.6	Element <type>	30
3.5.7	Element <currentValue>	31
3.5.8	Element <op>	31
3.5.9	Element <reqValue>.....	31
3.5.10	Element <result>	31
4.	Seznam typů a struktur	32
4.1	Základní datové typy	32
4.2	Jednoduché odvozené typy	32
4.2.1	Jednoduché typy použité v konfiguračních souborech.....	32
4.3	Komplexní typy	34
4.3.1	Komplexní typy použité v konfiguračních souborech.....	34
4.3.2	Komplexní typy použity ve výstupních souborech	36
	Soupis citací	39

Úvod

Systémová příručka popisuje syntaxi a význam jednotlivých nastavitelných položek konfiguračních souborů systému a význam položek výstupních sestav.




1. Popis

Systém je koncipován jako aplikace s rozhraním ve formě univerzálních souborů formátu XML. Možnosti dalšího rozšíření a obohacení systému dalšími formami vstupu a výstupu jsou velké a relativně jednoduché.

Systém obsahuje tři konfigurační soubory, dva klientské (SysKoApp\App.config a SysKoConsole\App.config) a jeden serverový (SysKoServer\App.config). Pro kontrolu validity jsou k těmto XML souborům připojena odpovídající XML schémata (AppConfig.xsd).

Dále systém obsahuje 5 schémat ve formátu XSLT, s jejichž pomocí jsou vytvořeny příslušné výstupní sestavy.

V dalších kapitolách je popsán význam jednotlivých položek a jejich syntaxe pomocí XML schémat. Ve XML schématech jsou použity následující typy relací.

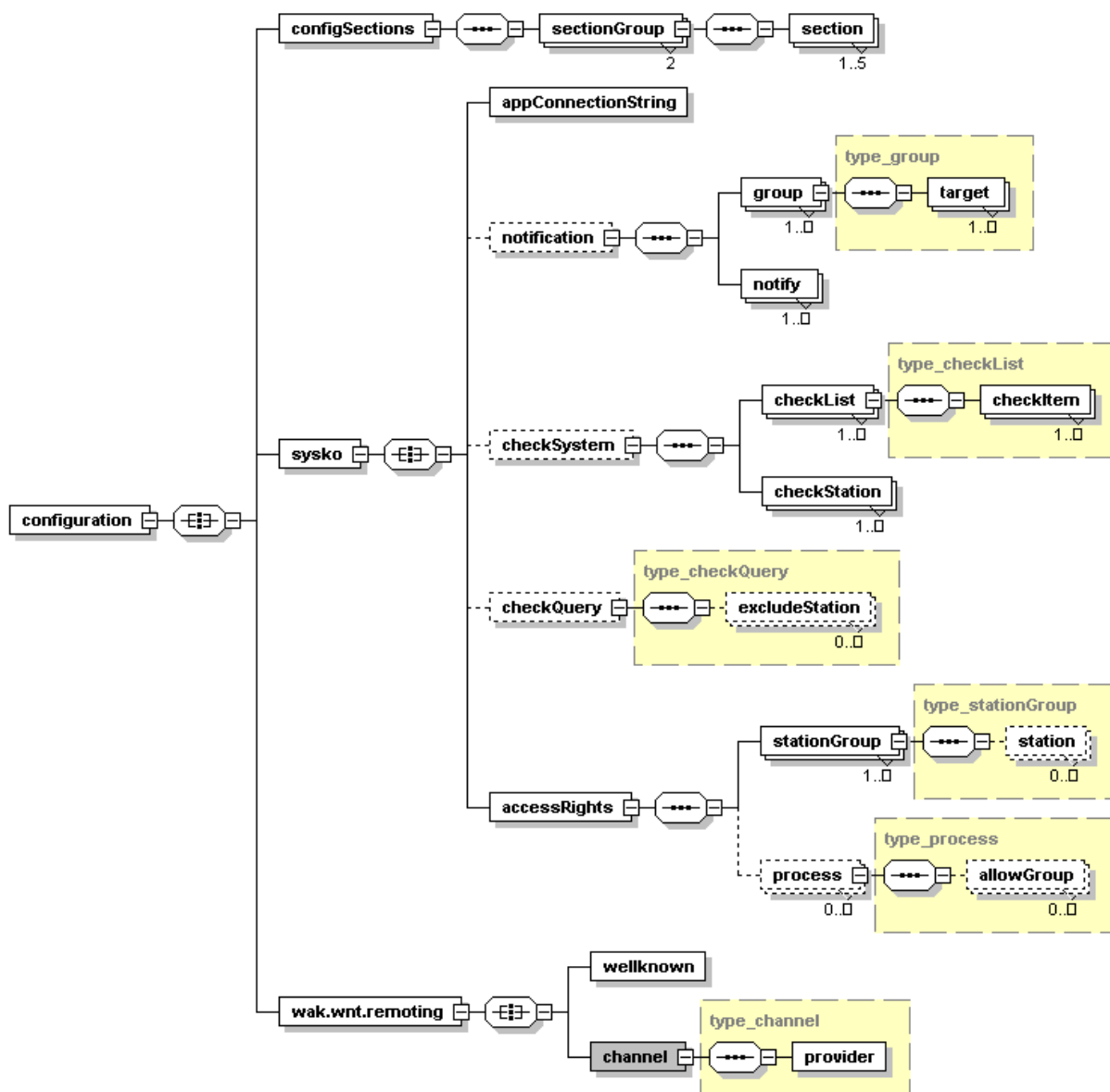
Seznam relací	Popis
	Vnořené elementy mohou být v libovolném pořadí.
	Vnořný element bude jeden z několika možných.
	Vnořené elementy musejí odpovídat specifikovanému pořadí.

Tab. 1 Relace XML schémat

2. Konfigurační soubory na straně serveru

2.1 Konfigurační soubor SysKoServer

Struktura konfiguračního souboru SysKoServer\App.config je určena XML schématem SysKoServerAppConfig.xsd.



Obr. 1 Hierarchie konfiguračního souboru SysKoServer

2.1.1 Element <configuration>

Název elementu: configuration

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Kořenový element celého XML dokumentu.

2.1.2 Element <configSections>

Název elementu: configSections

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Tento element obsahuje konfigurační údaje nutné pro samotný systém. Tato sekce není určena k modifikaci pro nastavení uživatelských parametrů systému.

2.1.3 Element <sysko>

Název elementu: sysko

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Kořenový element pro nastavení uživatelských parametrů systému.

2.1.4 Element <appConnectionString>

Název elementu: appConnectionString

Atributy: string database, string server, string uid, string pwd

Min. výskyt: 1

Max. výskyt: 1

Popis:

Atributy tohoto elementu obsahují konfigurační údaje pro přihlášení k databázi. Atribut database určuje jméno databáze na serveru určeném atributem server. Atributy uid a pwd určují uživatelské jméno a heslo pro přístup k databázi.

2.1.5 Element <notification>

Název elementu: notification

Atributy: string xsltPath, string cssPath

Min. výskyt: 0

Max. výskyt: 1

Popis:

Atributy xsltPath a cssPath určují adresář se soubory s XSL transformací, resp. adresář s CSS styly. XSL transformace ve spojení s CSS stylem určuje výslednou podobu výstupní XHTML stránky (sestavy), která je generována systémem.

2.1.6 Element <group>

Název elementu: group

Atributy: string id, string smtpserver, string mailfrom, string directory

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Atribut id jednoznačně identifikuje skupinu tvořenou elementem <group>. Na takto identifikovanou skupinu se lze poté odkazovat pomocí hodnoty atributu sendTo v elementu <notify> viz. 2.1.9. Atribut smtpserver určuje SMTP server, který se použije pro odeslání notifikace z elektronické adresy mailfrom. Atribut directory určuje adresář na serveru pro ukládání notifikací. Atributy: smtpserver a mailfrom mají smysl pouze tehdy, je-li hodnotou atributu proto vnořeného elementu <target> (viz. 2.1.8) řetězec “smtp”. Je-li hodnotou atributu proto řetězec “file” má význam atribut directory.

2.1.7 Element <target>

Název elementu: target

Atributy: type_protokol proto, string xslt, string css, string name

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Atribut proto určuje způsob notifikace. Je-li hodnotou atributu proto řetězec “file”, výsledkem notifikace je XHTML stránka (sestava) uložená v adresáři specifikovaným atributem directory rodičovského elementu <group>. Je-li hodnotou atributu proto řetězec “smtp”, výsledkem notifikace je XHTML stránka (sestava), zasílaná na elektronickou adresu specifikovanou

atributem directory rodičovského elementu <group>. Atributy xslt a css specifikují soubor s XSL transformací, resp. s CSS stylem. Pro použití XSL transformace, resp. CSS stylu podle druhu notifikace, existuje možnost vložit do hodnot atributů xslt a css makro @@ACTION@@. Makro @@ACTION@@ nabývá hodnot typu type_action, podle hodnoty atributu action referujícího elementu <notify>. Reference je realizována pomocí atributu sendTo. Takto jsou jednotlivé notifikace rozesílány skupinám identifikovaným atributem id. Atribut name určuje jméno souboru výsledné notifikace. V jeho těle lze použít makra @@ACTION@@ a @@DATE:type_dateFormat@@. V řetězci type_dateFormat mají jednotlivé znaky speciální význam určující výsledný formát data, které je výstupem makra @@DATE:type_dateFormat@@, type_dateFormat je typu string.

Formátovací řetězec	Popis
“d”	Den v měsíci. Jednociferné dny nezačínají nulou.
“dd”	Den v měsíci. Jednociferné dny začínají nulou.
“dddd”	Název dne v týdnu.
“M”	Měsíc vyjádřen číslem. Jednociferné nezačínají nulou.
“MM”	Měsíc vyjádřen číslem. Jednociferné začínají nulou.
“MMM”	Název měsíce.
“y”	Rok bez století. Jestliže je rok bez století menší než 10, je rok zobrazen bez nul na začátku.
“yy”	Rok bez století. Jestliže je rok bez století menší než 10, je rok zobrazen s nulami na začátku.
“yyyy”	Čtyřciferný rok, obsahující století.
“h”	Hodina v 12 hodinovém značení. Jednociferné nezačínají nulou.
“hh”	Hodina v 12 hodinovém značení. Jednociferné začínají nulou.
“H”	Hodina v 24 hodinovém značení. Jednociferné nezačínají nulou.
“HH”	Hodina v 24 hodinovém značení. Jednociferné začínají nulou.
“m”	Minuta. Jednociferná nezačíná nulou.
“mm”	Minuta. Jednociferná začíná nulou.
“s”	Sekunda. Jednociferná nezačíná nulou.
“ss”	Sekunda. Jednociferná začíná nulou.
“f”	Desetina sekundy

Tab. 2 Význam speciálních znaků v řetězci type_dateFormat

2.1.8 Element <notify>

Název elementu: notify

Atributy: string id, type_action action, string stationID, string sendTo,
unsignedInt interval

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <notify> určuje typ notifikace, která se bude posílat skupině definované pomocí elementu <group>. Umožňuje nastavit délku periody, v níž bude docházet k notifikacím, a specifikovat stanice, které mají být obsahem notifikace.

Atribut id je jedinečným identifikátorem elementu. Atribut action určuje typ notifikace, ve spojení se stationID specifikuje stanice a typ reportu, které jsou předmětem notifikace. Hodnotou atributu stationID je regulární výraz popisující IP adresu stanice. Atribut sendTo odkazuje na cíl notifikace. Tím je skupina definována elementem <group> s jedinečným identifikátorem atributem id. Periodicitu notifikací stanovuje atribut interval, doba periody je udávána v minutách. Je-li hodnota atributu interval rovna nule, je notifikace vypnuta.

2.1.9 Element <checkSystem>

Název elementu: checkSystem

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <checkSystem> obsahuje seznam testů, definovaných v elementech <checkList> a vazby jednotlivých testů na seznam stanic, které jsou definovány v elementech <checkStation>.

2.1.10 Element <checkList>

Název elementu: checkList

Atributy: string id, type_logOp logOp

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <checkList> obsahuje seznam kontrolovaných položek, definovaných v elementech <checkItem>.

Atribut id je jedinečným identifikátorem elementu <checkList>. Logický operátor logOp stanovuje, stačí-li pro úspěšný test splnit pouze jednu podmínku, nebo je nutno splnit všechny. Je-li hodnotou operátoru “and”, je nutno splnit všechny podmínky definované elementy <checkItem>. Je-li hodnotou operátoru “or”, stačí splnit pouze jednu podmínku. Implicitní hodnota operátoru logOp je “and”.

2.1.11 Element <checkItem>

Název elementu: checkItem

Atributy: string id, type_type type, string name, type_operator op, string value

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <checkItem> popisuje typ a způsob kontroly položky.

Atribut id je jedinečným identifikátorem elementu <checkItem>. Atribut type a name specifikuje typ testované položky, resp. její název. Hodnota atributu op funguje jako operátor mezi operandem value a operandem tvořeným hodnotou položky name.

Hodnotou atributu name mohou být makra @@WINDIR@@, @@SYSTEMDRIVE@@, @@SYSTEMROOT@@ a @@PROGRAMFILES@@. Jejich hodnotami jsou potom odpovídající hodnoty prostředí tak, jak jsou nastaveny v OS.

Hodnotou atributu value může být makro @@TODAY@@, jeho hodnotou je potom aktuální datum. Je-li hodnotou atributu value makro @@TODAY@@, může být zapsáno ve tvaru @@TODAY@@+počet_dnů, resp. @@TODAY@@-počet_dnů, kde počet_dnů je typu unsignedInt a představuje časový posun od aktuálního data v jednotkách dnů.

2.1.12 Element <checkStation>

Název elementu: checkStation

Atributy: string stationID, string checkList

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <checkStation> umožňuje asociovat a slučovat testy definované elementem <checkList> s libovolnými stanicemi.

Atribut id je jedinečným identifikátorem elementu <checkStation>. Hodnotou atributu stationID je regulární výraz popisující IP adresu stanice, pro níž se provedou testy specifikované atributem checkList. V atributu checkList lze vyjmenovat více testů a spojit je ve tvaru test1|test2, kde znak '|' je oddělovač typu type_itemSeparator.

2.1.13 Element <checkQuery>

Název elementu: checkQuery

Atributy: type_portNumber port

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <checkQuery> definuje UDP port služby CheckQuery.

2.1.14 Element <excludeStation>

Název elementu: excludeStation

Atributy: string stationID

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <excludeStation> definuje stanice, které mohou využívat služby CheckQuery.

Hodnotou atributu stationID je regulární výraz popisující IP adresu stanice, která má přístup k službě CheckQuery.

2.1.15 Element <accessRights>

Název elementu: accessRights

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <accessRights> obsahuje definici skupin stanic a jejich práv pro přístup k jednotlivým procesům systému.

2.1.16 Element <stationGroup>

Název elementu: stationGroup

Atributy: string id

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <stationGroup> obsahuje seznam stanic, definovaných pomocí vnořeného elementu <station>.

Atribut id je jedinečným identifikátorem elementu.

2.1.17 Element <station>

Název elementu: station

Atributy: string stationID

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <station> definuje stanice, které jsou součástí skupiny rodičovského elementu <stationGroup>.

Hodnotou atributu stationID je regulární výraz popisující IP adresu stanice.

2.1.18 Element <process>

Název elementu: process

Atributy: string typeID

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <process> identifikuje proces systému, k němuž mají přístup stanice definované vnořeným elementem <allowGroup>.

Atribut typeID identifikuje proces systému.

2.1.19 Element <allowGroup>

Název elementu: allowGroup

Atributy: string groupID

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <allowGroup> definuje skupinu stanic, které mají možnost přístupu k procesu systému identifikovaného atributem typeID vnějšího elementu <process>.

Hodnotou atributu groupID je identifikátor elementu <stationGroup>.

2.1.20 Element <wak.wnt.remoting>

Název elementu: wak.wnt.remoting

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Tento element obsahuje konfigurační údaje nutné pro běh samotného systému. Tato sekce není určena k modifikaci pro nastavení uživatelských parametrů systému, vyjma vnořeného elementu <channel>.

2.1.21 Element <channel>

Název elementu: channel

Atributy: string ref, type_portNumber port

Min. výskyt: 1

Max. výskyt: 1

Popis:

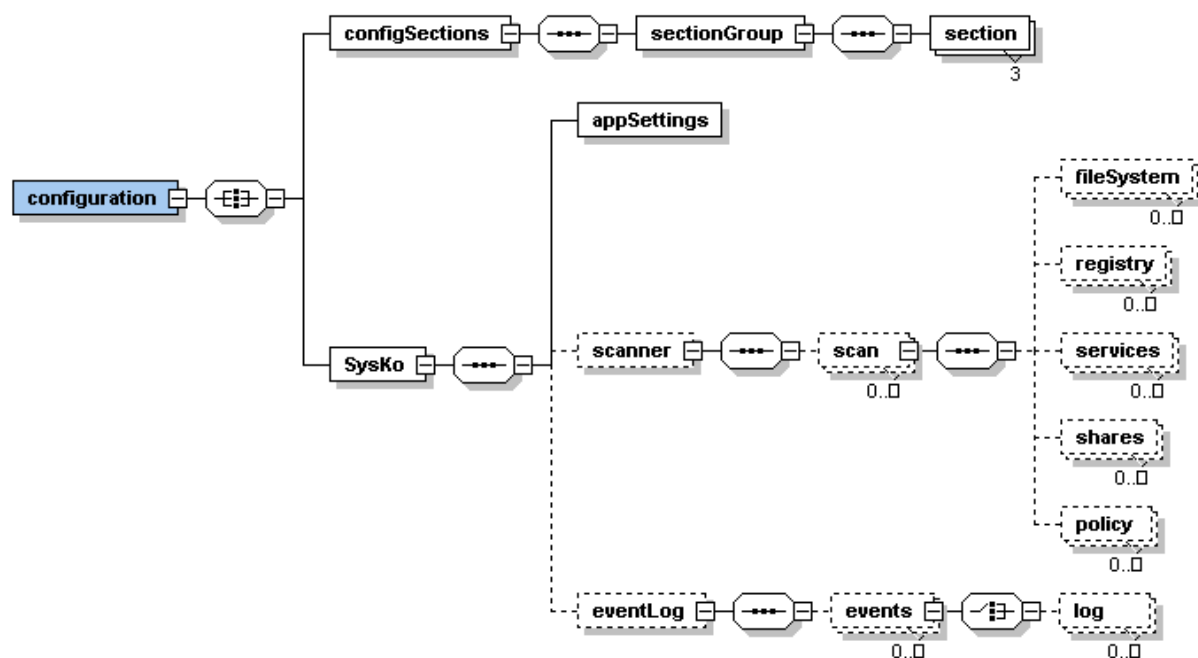
Element <channel> definuje komunikační protokol a číslo portu, na kterém probíhá komunikace mezi klientem a serverem.

Atribut ref definuje komunikační protokol. Atribut port definuje číslo portu.

2.2 Konfigurační soubory na straně klienta

2.2.1 Konfigurační soubor SysKoConsole

Struktura konfiguračního souboru SysKoConsole\App.config je určena XML schématem SysKoConsoleAppConfig.xsd.



Obr. 2 Hierarchie konfiguračního souboru SysKoConsole

2.2.2 Element <configuration>

Název elementu: configuration

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Kořenový element celého XML dokumentu.

2.2.3 Element <configSections>

Název elementu: configSections

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Tento element obsahuje konfigurační údaje nutné pro samotný systém. Tato sekce není určena k modifikaci pro nastavení uživatelských parametrů systému.

2.2.4 Element <sysko>

Název elementu: sysko

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Kořenový element pro nastavení uživatelských parametrů systému.

2.2.5 Element <appSettings>

Název elementu: appSettings

Atributy: type_bool remoteManager, string remoteManagerUrl

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <appSetting> definuje použití a URL vzdálené služby manažeru.

Atribut remoteManager definuje přítomnost vzdálené služby manažeru. Je-li hodnotou řetězec “true”, je použita vzdálená služba manažeru lokalizována URL adresou atributu remoteManagerUrl.

2.2.6 Element <scanner>

Název elementu: scanner

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <scanner> obsahuje seznam jednotlivých testů definovaných pomocí vnořených elementů <scan>.

2.2.7 Element <scan>

Název elementu: scan

Atributy: string id

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <scan> reprezentuje jeden test. Test je definovaný vnořenými elementy, které specifikují položky jež jsou předmětem testu.

Atribut id je jedinečný identifikátor elementu <scan>.

2.2.8 Element <fileSystem>

Název elementu: fileSystem

Atributy: string name, type_boolInt recursive, string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <fileSystem> specifikuje cestu v lokálním souborovém systému a způsob vyhledávání.

Atribut name specifikuje cestu v lokálním souborovém systému. Atribut recursive definuje testování podadresářů. Je-li jeho hodnotou "1", jsou testovány i podadresáře na cestě definované atributem name. Hodnotou atributu exclude je regulární výraz popisující jména souborů, která nemají být zahrnuty do testu.

2.2.9 Element <registry>

Název elementu: registry

Atributy: string name, type_boolInt recursive, string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <registry> specifikuje větev v systémovém registru OS a způsob vyhledávání.

Atribut name specifikuje větev v systémovém registru OS. Atribut recursive definuje testování podřízených větví. Je-li jeho hodnotou "1", jsou testovány i podřízené větve na cestě definované atributem name. Hodnotou atributu exclude je regulární výraz popisující klíče, které nemají být zahrnuty do testu.

2.2.10 Element <services>

Název elementu: services

Atributy: type_boolInt scanDrivers, type_boolInt scanServices, string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <services> specifikuje testování ovladačů a služeb systému.

Atribut scanDrivers definuje testování ovladačů OS. Je-li hodnotou atributu scanDrivers “1”, ovladače OS jsou testovány, při hodnotě “0” ovladače OS nejsou testovány. Atribut scanServices definuje testování služeb OS. Je-li hodnotou atributu scanServices “1”, služby OS jsou testovány, při hodnotě “0” služby OS nejsou testovány. Hodnotou atributu exclude je regulární výraz popisující název služby nebo ovladače, které nemají být zahrnuty do testu.

2.2.11 Element <shares>

Název elementu: shares

Atributy: string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <shares> specifikuje testování sdílených prostředků OS.

Hodnotou atributu exclude je regulární výraz popisující název sdíleného prostředku, který nemá být zahrnut do testu.

2.2.12 Element <policy>

Název elementu: policy

Atributy: string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <policy> specifikuje testování bezpečnostní politiky OS.

Hodnotou atributu exclude je regulární výraz popisující název bezpečnostní politiky, která nemá být zahrnuta do testu.

2.2.13 Element <eventLog>

Název elementu: eventLog

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <eventLog> obsahuje seznam jednotlivých sestav mapujících události definované pomocí vnořených elementů <event>.

2.2.14 Element <events>

Název elementu: events

Atributy: string id

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <events> reprezentuje jednu sestavu. Sestava je definována vnořenými elementy, které specifikují položky jež jsou mapovány.

Atribut id je jedinečný identifikátor elementu <events>.

2.2.15 Element <log>

Název elementu: events

Atributy: string name, string machine, string dateFrom, string dateTo

string type, string source, string ID, string userName

Min. výskyt: 0

Max. výskyt: neomezen

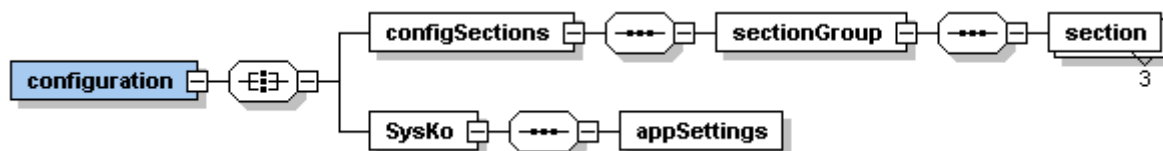
Popis:

Element <log> specifikuje události určené k monitorování.

Volitelné atributy elementu <log> popisují, jaké parametry musí událost splňovat. Atribut name označuje druh protokolu události. Možné hodnoty jsou “system” a “application”, případně jejich kombinace zapsaná pomocí type_itemSeparator. Atribut machine označuje jméno počítače. Atribut dateFrom a dateTo stanovují, v jakém časovém intervalu událost vznikla. Atribut type určuje typ události. Možné hodnoty jsou “Information”, “Error”, “FailureAudit”, “Warning” a “SuccessAudit”. Atribut source označuje zdroj události. Atribut ID je identifikačním číslem události. Atribut userName označuje jméno uživatelského účtu, pod kterým došlo k události.

2.3 Konfigurační soubor SysKoApp

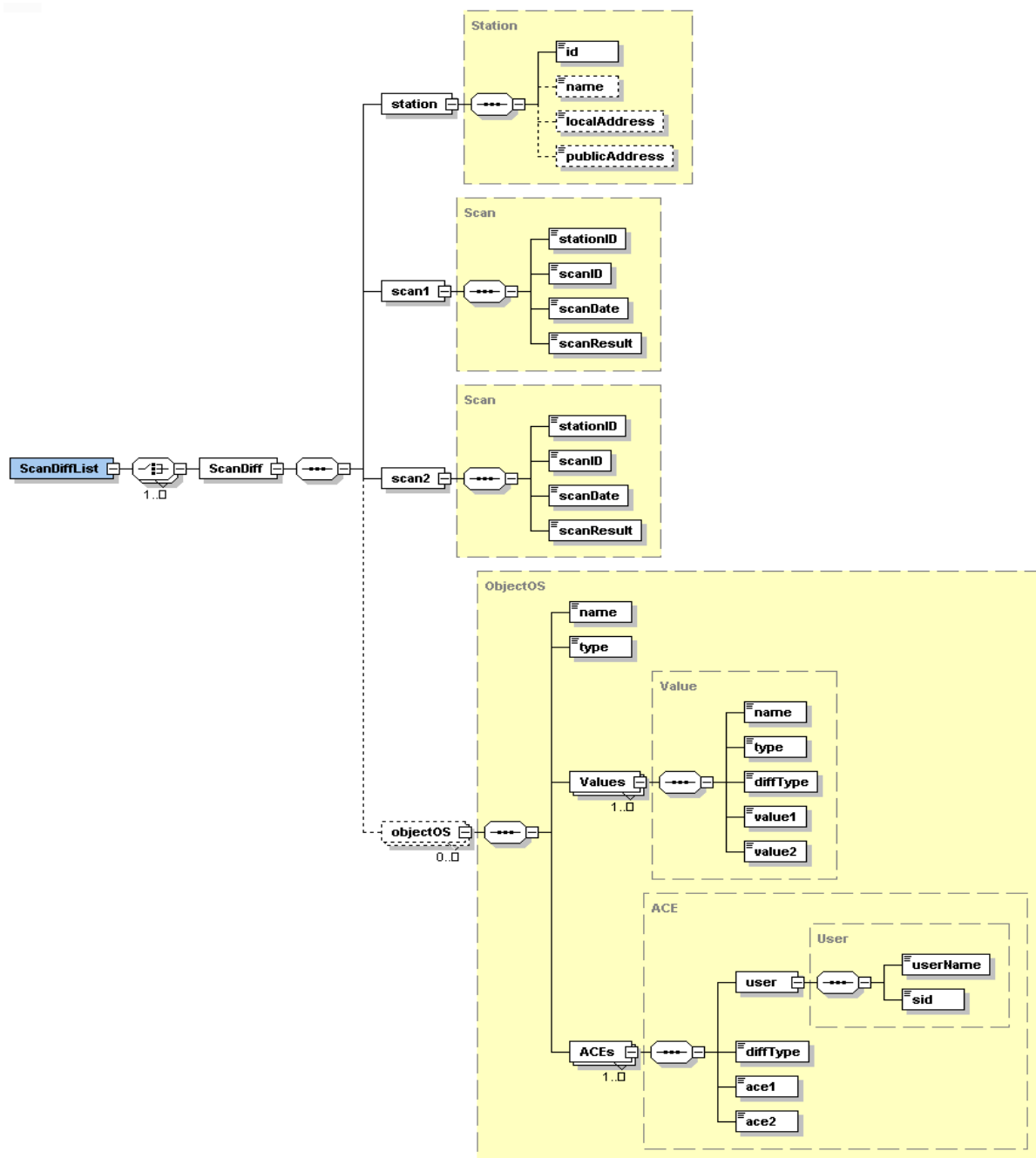
Struktura konfiguračního souboru SysKoApp\App.config je určena XML schématem SysKoConsoleAppConfig.xsd. Hodnoty elementů se v tomto konfiguračním souboru nenastavují.



Obr. 3 Hierarchie konfiguračního souboru SysKoApp

3. Výstupní soubory

3.1 scanDiff



Obr. 4 Schéma výstupního souboru scanDiff

ScanDiff popisuje vzniklé difference mezi scan1 a scan2. Struktura výstupního souboru scanDiff je určena XML schématem scanDiff.xsd.

3.1.1 Element <scanDiffList>

Název elementu: scanDiffList

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanDiffList> je kořenovým elementem výstupu scanDiff.

3.1.2 Element <scanDiff>

Název elementu: scanDiff

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanDiff> popisuje pomocí vnořených elementů difference dvou bezpečnostních kontrol.

3.1.3 Element <station>

Název elementu: station

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <station> je typu Station. Specifikuje stanici u které byla zapnuta notifikace typu scanDiff.

3.1.4 Element <scan1>

Název elementu: scan1

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scan1> je typu Scan, představuje referenční scan, ke kterému se změny vztahují.

3.1.5 Element <scan2>

Název elementu: scan2

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scan2> je typu Scan, představuje porovnávaný scan vůči vzoru.

3.1.5.1 Element <objectOS>

Název elementu: objectOS

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <objectOS> uchovává informace o změně.

3.1.6 Element <name>

Název elementu: name

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <name> označuje položku změny.

3.1.7 Element <type>

Název elementu: type

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <type> označuje typ položky změny a nabývá hodnot typu type_type.

3.1.8 Element <Values>

Název elementu: Values

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <Values> je typu type_Value. Jeho vnořené elementy popisují změnu hodnoty. Element <name> znamená jméno položky, <type> je typ položky, <diffType> představuje typ změny, <value1> představuje původní hodnotu a <value2> hodnotu po změně.

3.1.9 Element <ACEs>

Název elementu: Values

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

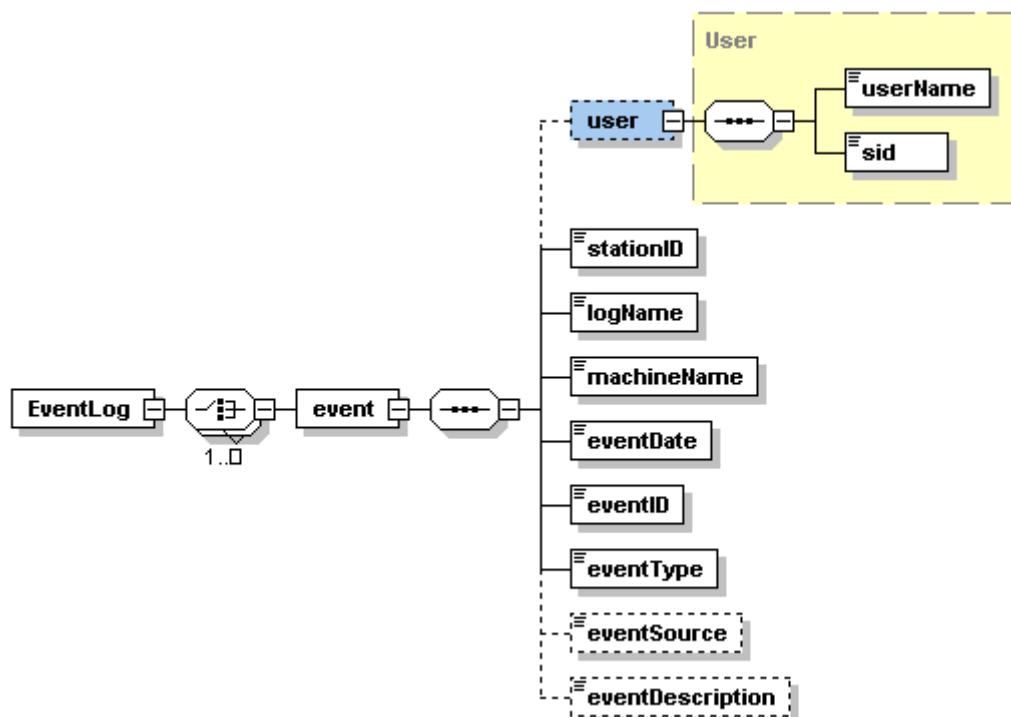
Popis:

Element <ACEs> je typu type_ACE. Jeho vnořené elementy popisují změnu hodnot ACE (access control entry), pro uživatele identifikovaného elementem <user>. Element <ace1> znamená hodnotu ACE před změnou, <ace2> hodnotu ACE po změně. Element <diffType> představuje typ změny.

3.2 EventLog

3.2.1 Hierarchie elementů

Struktura výstupního souboru eventLog je určena XML schématem eventLog.xsd.



Obr. 5 Schéma výstupního souboru eventLog

3.2.2 Element <EventLog>

Název elementu: EventLog

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <EventLog> je kořenový element výstupu EventLog.

3.2.3 Element <event>

Název elementu: event

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <event> pomocí vnořených elementů popisuje jednu událost.

3.2.4 Element <user>

Název elementu: user

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <user> identifikuje uživatele.

3.2.5 Element <stationID>

Název elementu: stationID

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <stationID> obsahuje ID stanice.

3.2.6 Element <logName>

Název elementu: logName

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <logName> obsahuje jméno logu.

3.2.7 Element <machineName>

Název elementu: machineName

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <machineName> obsahuje jméno počítače.

3.2.8 Element <eventDate>

Název elementu: eventDate

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <eventDate> obsahuje datum události.

3.2.9 Element <eventID>

Název elementu: eventID

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <eventID> identifikuje událost.

3.2.10 Element <eventType>

Název elementu: eventType

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <eventType> obsahuje typ události.

3.2.11 Element <eventSource>

Název elementu: eventSource

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <eventSource> identifikuje zdroj události.

3.2.12 Element <eventDescription>

Název elementu: eventDescription

Atributy: žádné

Min. výskyt: 1

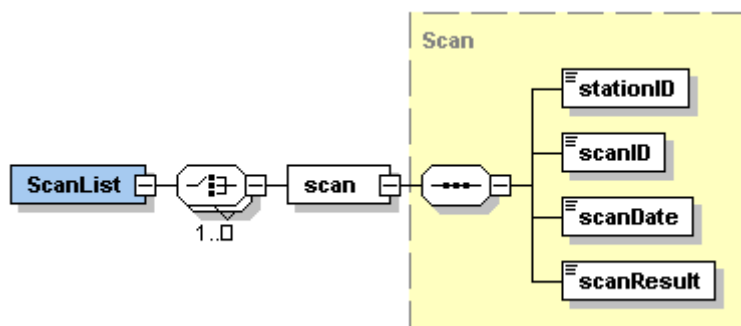
Max. výskyt: 1

Popis:

Element <eventDescription> obsahuje detailnější popis události.

3.3 scanList

3.3.1 Hierarchie elementů



Obr. 6 Schéma výstupního souboru scanList

Struktura výstupního souboru scanList je určena XML schématem scanList.xsd.

3.3.2 Element <scanList>

Název elementu: scanList

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanList> je kořenovým elementem výstupu scanList.

3.3.3 Element <scan>

Název elementu: scan

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scan> popisuje pomocí vnořených elementů jeden scan.

3.3.4 Element <stationID>

Název elementu: stationID

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <stationID> identifikuje stanici, na které proběhl scan.

3.3.5 Element <scanID>

Název elementu: scanID

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanID> je identifikátorem scanu.

3.3.6 Element <scanDate>

Název elementu: scanDate

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanDate> obsahuje datum scanu.

3.3.7 Element <scanResult>

Název elementu: scanResult

Atributy: žádné

Min. výskyt: 1

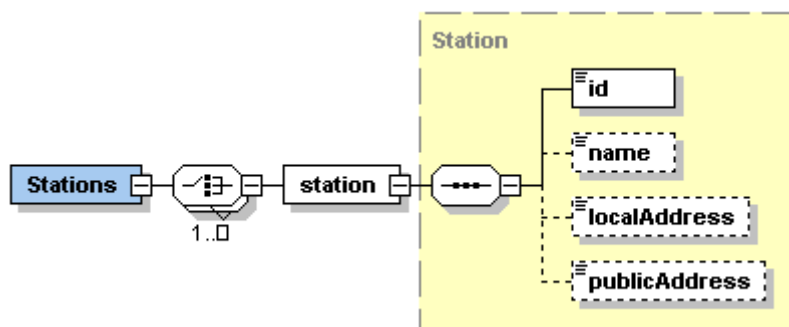
Max. výskyt: 1

Popis:

Element <scanResult> obsahuje výsledek scanu.

3.4 Stations

Struktura výstupního souboru stations je určena XML schématem stations.xsd.



Obr. 7 Schéma výstupního souboru Stations

3.4.1 Element <Stations>

Název elementu: Stations

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <Stations> je kořenovým elementem výstupu Stations.

3.4.2 Element <station>

Název elementu: station

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <station> popisuje pomocí vnořených elementů jednu stanici.

3.4.3 Element <id>

Název elementu: id

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <id> identifikuje stanici.

3.4.4 Element <name>

Název elementu: name

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <name> obsahuje jméno stanice.

3.4.5 Element <localAddress>

Název elementu: localAddress

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <localAddress> obsahuje lokální adresu stanice.

3.4.6 Element <publicAddress>

Název elementu: publicAddress

Atributy: žádné

Min. výskyt: 0

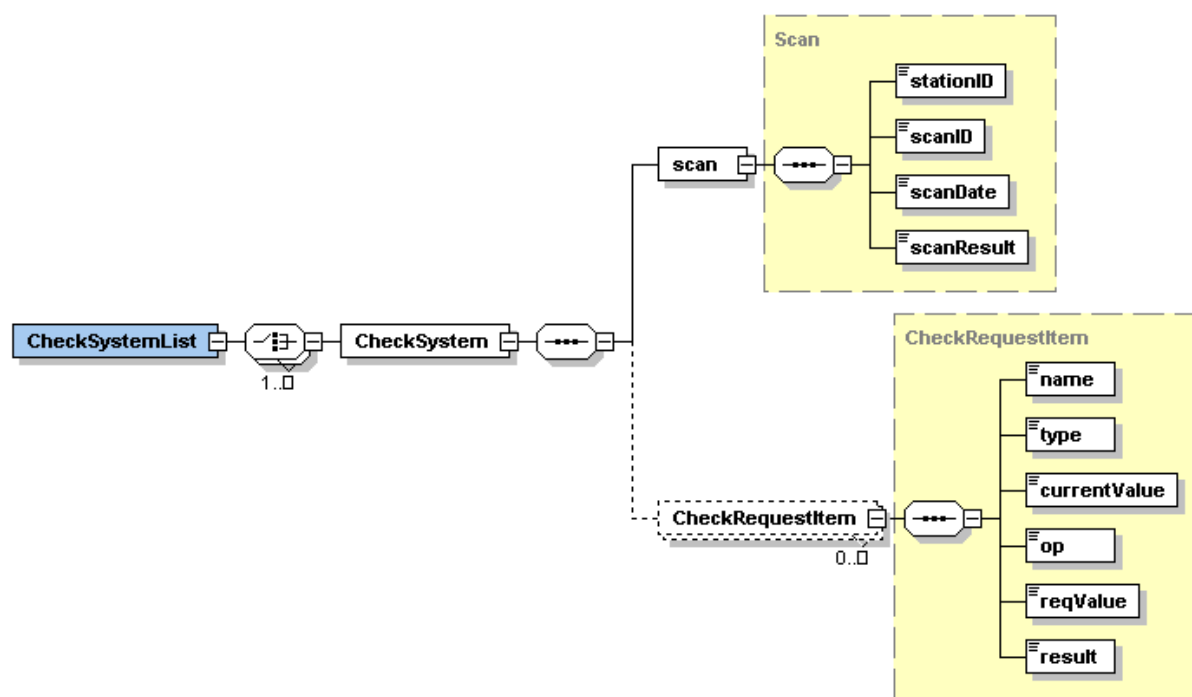
Max. výskyt: 1

Popis:

Element <publicAddress> obsahuje veřejnou adresu stanice.

3.5 CheckSystemList

Struktura výstupního souboru checkSystemList je určena XML schématem checkSystemList.xsd.



Obr. 8 Schéma výstupního souboru checkSystemList

3.5.1 Element <CheckSystemList>

Název elementu: CheckSystemList

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <CheckSystemList> je kořenovým elementem výstupu CheckSystemList.

3.5.2 Element <CheckSystem>

Název elementu: checkSystem

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <checkSystem> popisuje pomocí vnořených elementů výsledek kontroly CheckSystem.

3.5.3 Element <scan>

Název elementu: scan

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scan> popisuje pomocí vnořených elementů jeden scan.

3.5.4 Element <checkRequestItem>

Název elementu: checkRequestItem

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <checkRequestItem> popisuje výsledek kontroly definované elementem <checkItem>.

3.5.5 Element <name>

Název elementu: name

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <name> obsahuje jméno testované položky.

3.5.6 Element <type>

Název elementu: type

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <type> obsahuje typ testované položky.

3.5.7 Element <currentValue>

Název elementu: currentValue

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <currentValue> obsahuje současnou hodnotu testované položky.

3.5.8 Element <op>

Název elementu: op

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <op> obsahuje operátor aplikovaný na currentValue a reqValue.

3.5.9 Element <reqValue>

Název elementu: reqValue

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <reqValue> obsahuje požadovanou hodnotu testované položky.

3.5.10 Element <result>

Název elementu: result

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element `<result>` obsahuje výsledek porovnávání obsahů elementů `<reqValue>` a `<currentValue>` pomocí operátoru definovaného v elementu `<op>`.

4. Seznam typů a struktur

4.1 Základní datové typy

Typ	Popis	Příklad
String	řetězec znaků	Abc
UnsignedInt	nezáporné celé číslo, číslo je v rozsahu od 0 do 4294967295, což odpovídá 32bitovému celému číslu	7, 657
DateTime	datum a čas	2005-07-05T10:58:53+02:00, 2005-07-05T08:58:53Z

Tab. 3 Základní použité datové typy

4.2 Jednoduché odvozené typy

Jednoduché odvozené typy jsou definovány restrikcí základních datových typů definovaných v kapitole 4.1.

4.2.1 Jednoduché typy použité v konfiguračních souborech

4.2.1.1 type_protokol

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot "smtp" a "file".

4.2.1.2 type_portType

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot "tcp" a "udp".

4.2.1.3 type_action

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “stationList”, “eventLog”, “scanList”, “scanDiff” a “checkSystem”.

4.2.1.4 type_type

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “policy”, “file”, “registry”, “service” a “share”.

4.2.1.5 type_operator

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “=”, “>”, “>=”, “<”, “<=”, “date_>”, “date_>=”, “date_<”, “date_<=”, “date_>”, “ver_>”, “ver_>=”, “ver_<”, “ver_<=” a “exists”.

4.2.1.6 type_portNumber

Numerický typ, vzniklý restrikcí typu unsignedInt.

Může nabývat numerické hodnoty v intervalu 1024 až 65535 včetně.

4.2.1.7 type_logOp

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “or” a “and”.

4.2.1.8 type_itemSeparator

Výčtový typ, vzniklý restrikcí typu string.

Je definován hodnotou “|”.

4.2.1.9 type_bool

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “true” a “false”.

4.2.1.10 type_boolInt

Numerický typ, vzniklý restrikcí typu unsignedInt.

Může nabývat numerických hodnot 0 a 1.

4.3 Komplexní typy

Komplexní typy definují strukturu typů za pomoci výčtu atributů, podřízených elementů a jejich relací.

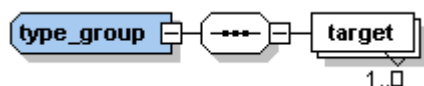
4.3.1 Komplexní typy použité v konfiguračních souborech

4.3.1.1 type_section

Definuje množinu atributů.

4.3.1.2 type_group

Definuje množinu atributů a relaci.



Obr. 9 Typ relace mezi type_group a target

4.3.1.3 type_target

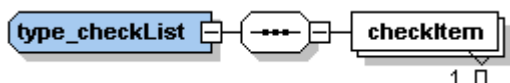
Definuje množinu atributů.

4.3.1.4 type_notify

Definuje množinu atributů.

4.3.1.5 type_checkList

Definuje množinu atributů a relaci.



Obr. 10 Typ relace mezi type_checklist a checkItem

4.3.1.6 type_checkItem

Definuje množinu atributů.

4.3.1.7 type_stationID

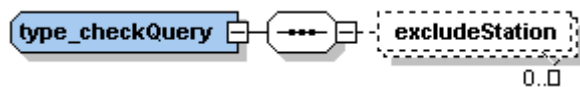
Definuje množinu atributů.

4.3.1.8 type_checkStation

Definuje množinu atributů.

4.3.1.9 type_checkQuery

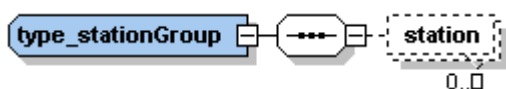
Definuje množinu atributů a relací.



Obr. 11 Typ relace mezi type_checkQuery a excludeStation

4.3.1.10 type_stationGroup

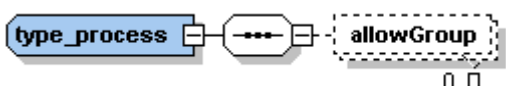
Definuje množinu atributů a relací.



Obr. 12 Typ relace mezi type_stationGroup a station

4.3.1.11 type_process

Definuje množinu atributů a relací.



Obr. 13 Typ relace mezi type_process a allowGroup

4.3.1.12 type_allowGroup

Definuje množinu atributů.

4.3.1.13 type_wellknown

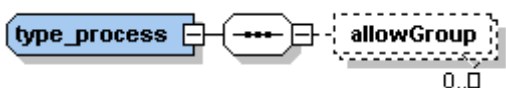
Definuje množinu atributů.

4.3.1.14 type_provider

Definuje množinu atributů.

4.3.1.15 type_process

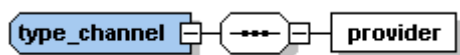
Definuje množinu atributů a relací.



Obr. 14 Typ relace mezi type_process a allowGroup

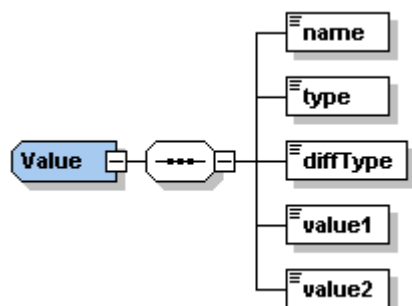
4.3.1.16 type_channel

Definuje množinu atributů a relací.



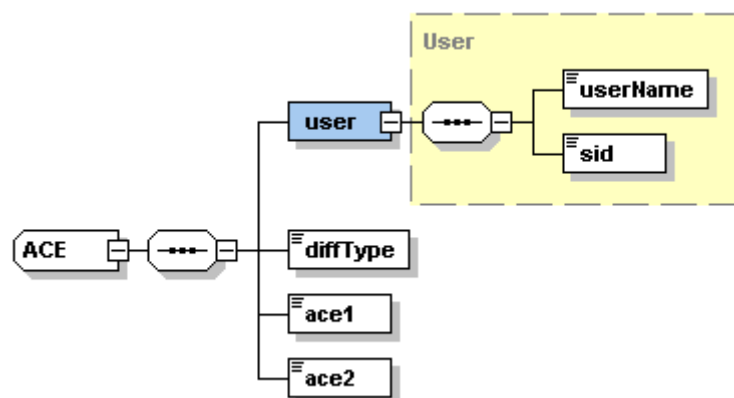
Obr. 15 Typ relace mezi type_channel a provider

4.3.1.17 type_Value



Obr. 16 Typ relace mezi type_Value a jeho vnořenými elementy

4.3.1.18 type_ACE

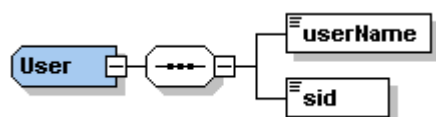


Obr. 17 Typ relace mezi type_ACE a jeho vnořenými elementy

4.3.2 Komplexní typy použity ve výstupních souborech

4.3.2.1 Typ User

Typ User se skládá z elementu userName a sid. Kde userName označuje jméno uživatele a sid je identifikátorem uživatele.

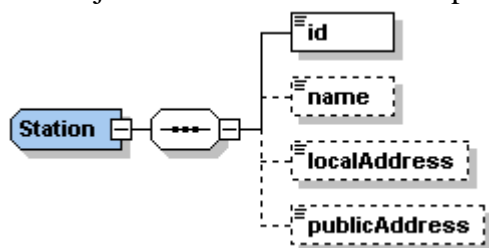


Obr. 18 Typ relace mezi typem User a jeho vnořenými elementy

4.3.2.2 Typ Station

Typ Station skládá z elementu id, name, localaddress a publicaddress.

Element <id> je identifikátorem notifikace, <name> označuje jméno stanice, <localAddress> obsahuje lokální adresu stanice a <publicAddress> veřejnou adresu stanice.

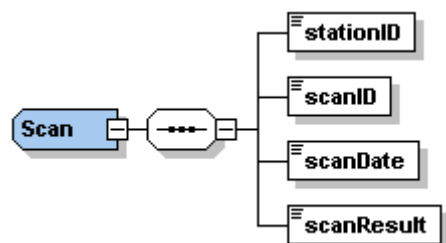


Obr. 19 Typ relace mezi typem Station a jeho vnořenými elementy

4.3.2.3 Typ Scan

Typ Scan se skládá z elementu stationID, scanID, scanDate a scanResult.

Element <stationID> je identifikátorem notifikace, <scanID> je identifikátorem scanu. <scanDate> obsahuje datum scanu a <publicResult> výsledek scanu.



Obr. 20 Typ relace mezi typem Scan a jeho vnořenými elementy

Soupis citací

[1] Microsoft Corporation: Regular Expressions as a Language [online] Dostupné na World Wide Web:

<http://msdn.microsoft.com/library/default.asp?url=/library/enus/cpguide/html/cpconregularexpressionsaslanguage.asp>

[2] W3C World Wide Web Consortium: Extensible Markup Language (XML) [online] Dostupné na World Wide Web: <http://www.w3.org/XML/>

[3] W3C World Wide Web Consortium: XML Schema [online] Dostupné na World Wide Web: <http://www.w3.org/XML/Schema>

[4] W3C World Wide Web Consortium: Cascading Style Sheets [online] Dostupné na World Wide Web: <http://www.w3.org/Style/CSS>

[5] W3C World Wide Web Consortium: Extensible HyperText Markup Language [online] Dostupné na World Wide Web: <http://www.w3.org/TR/xhtml1>

[6] Wikipedia: User Datagram Protocol [online] Dostupné na World Wide Web: http://en.wikipedia.org/wiki/User_Datagram_Protocol

Slovníky

Zkratky

Zkratka	Význam
OS	Operační systém

Tab. 4 Slovník zkratk

Termíny

Termín	Význam
Regulární výraz	Regulární výraz (regular expression) je speciální řetězec znaků, který představuje určitý vzor (masku) pro textové řetězce.
Reference	Vztah (odkaz) mezi dvěma elementy dokumentu.
Atribut	Atribut je označení datového prostoru, uchovávající datovou hodnotu. Je specifikován jménem, případně typem a rozsahem uchovávaných hodnot.
XML	Extensible Markup Language. Značkovací jazyk popisující strukturu dokumentu.
XML schéma	XML schéma popisuje strukturu XML dokumentu.
CSS	Cascading Style Sheet. Technologie pro přidávání stylu k webovým dokumentům.
XHTML	Extensible HyperText Markup Language. Značkovací jazyk.
SMTP	Simple Mail Transfer Protocol - jednoduchý protokol pro odesílání a přenos pošty mezi poštovními servery.
IP adresa	IP adresa je jedinečná adresa počítače. IP adresa se udává ve tvaru xxx.xxx.xxx.xxx, kde xxx je číslo v rozsahu 0 až 255. Může vypadat například takto: 127.0.0.1
makro	Je identifikováno uvozujícím a ukončujícím řetězcem "@@". Po vyhodnocení systémem je jeho hodnota nahrazena významem makra. Např. hodnotou makra @@WINDIR@@ může být řetězec "C:\WINNT".
UDP	User Datagram Protocol
ACE	Access Control Entry. Obsahuje množinu přístupových práv a bezpečnostní identifikátor, který identifikuje uživatele pro kterého jsou práva povolena, zakázána a auditována.

Tab. 5 Slovník termínů

E.2 - Uživatelská příručka IS

Obsah

Úvod.....	1
1. Popis.....	1
2. Konfigurační soubor SysKoServer	2
2.1 Příklad nastavení	2
3. Nastavení kontroly BS7779	6
4. Sledování událostí.....	8
4.1 Příklad nastavení konfiguračního souboru	8
4.2 Příklad výstupního souboru	9
5. Sledování souborů	11
5.1 Příklad nastavení konfiguračního souboru	11
5.2 Příklad výstupního souboru	12
6. Sledování služeb OS	15
6.1 Příklad nastavení konfiguračního souboru	15
6.2 Příklady výstupních souborů	16
7. Sledování registrů.....	19
7.1 Příklad nastavení konfiguračního souboru	19
7.2 Příklad výstupního souboru scanDiff	20
8. Sledování bezpečnostní politiky	21
8.1 Příklad nastavení konfiguračního souboru	21
8.2 Příklad výstupního souboru scanDiff	22

Úvod

Uživatelská příručka ukazuje na příkladech možnosti nastavení jednotlivých položek konfiguračních souborů systému. Součástí je i popis výstupů.

1. Popis

Systém je koncipován jako aplikace s rozhraním ve formě univerzálních souborů formátu XML. Možnosti dalšího rozšíření a obohacení systému dalšími formami vstupu a výstupu jsou velké a relativně jednoduché.

Následující příklady popisují výstupní soubory a možná nastavení serverového konfiguračního souboru `SysKoServer\App.config` a klientského konfiguračního souboru `SysKoConsole\App.config`. Tučným písmem je popsán příslušný komentář.

2. Konfigurační soubor SysKoServer

V následující kapitole je uvedeno možné nastavení serverového konfiguračního souboru.

2.1 Příklad nastavení

```
<configuration>
```

Sekce <configSections> není určena k nastavení uživatelských parametrů systému.

```
<configSections>
```

```
<sectionGroup name="sysko">
```

```
<section name="appConnectionString"  
type="Wak.Wnt.Db.DbConnectionStringConfigurationSectionHandler, Wak.Wnt.Db" />
```

```
<section name="notification"  
type="Wak.SysKo.As.Server.NotificationConfigurationSectionHandler,  
Wak.Sysko.As.Server" />
```

```
<section name="checkSystem"  
type="Wak.SysKo.As.Server.CheckSystemConfigurationSectionHandler,  
Wak.Sysko.As.Server" />
```

```
<section name="accessRights"  
type="Wak.SysKo.As.Server.AccessRightsConfigurationSectionHandler,  
Wak.Sysko.As.Server" />
```

```
<section name="checkQuery"  
type="Wak.SysKo.As.Server.CheckQueryConfigurationSectionHandler,  
Wak.Sysko.As.Server" />
```

```
</sectionGroup>
```

```
<sectionGroup name="wak.wnt.remoting">
```

```
<section name="appConnectionString"  
type="Wak.Wnt.Db.DbConnectionStringConfigurationSectionHandler, Wak.Wnt.Db" />
```

```
<section name="wellknown"  
type="Wak.Wnt.Tools.Remoting.RemotingConfigurationSectionHandler, Wak.Wnt.Tools" />
```

```
<section name="channel"  
type="Wak.Wnt.Tools.Remoting.RemotingConfigurationSectionHandler, Wak.Wnt.Tools" />
```

```
</sectionGroup>
```

```
</configSections>
```

Zde začíná sekce <sysko> ta je určena k nastavení uživatelských parametrů systému.

```
<sysko>
```

```
<appConnectionString database="sysko" server="server1" uid="sa" pwd="sa" />
```

Specifikuje databázi pojmenovanou “sysko”, s oprávněním pro přístup uživatelského jména a hesla “sa”, umístěnou na serveru pojmenovaném “server1”.

```
<notification >
```

```
<group id="fileReport" smtpserver="smtpserver" mailfrom="sysko@test.cz"
directory="c:\program files\SysKo\output">
```

Atributem id je definována jedna skupina s identifikátorem “fileReport”. Atribut smtpserver definuje SMTP server pojmenován “smtpserver”. Výstupy budou ukládány do adresáře “c:\program files\SysKo\output”, definovaného atributem directory.

```
<target proto="file" xslt="" css="@ @ACTION@ @.css" name="@ @DATE:yyyy-MM-
ddTHH-mm-ss@ @_ @ACTION@ @.xml" />
```

Atributem proto je nastaven způsob notifikace pomocí výstupních souborů. Atribut xslt je nastaven na prázdnou hodnotu. Takto není na výstupní soubor použita XSL transformace a soubor zůstane ve formátu XML. Pokud bychom chtěli použít XSL transformaci, definovali bychom hodnotu atributu xslt např. takto: "html_ @ @ACTION@ @.xslt". Atribut css není při prázdném atributu xslt podstatný. V atributu name je použito makro @ @ACTION@ @ a @ @DATE@ @, makro @ @ACTION@ @ bude nahrazeno hodnotou atributu odkazujícího elementu <notify>. Hodnotou makra @ @DATE:yyyy-MM-ddTHH-mm-ss@ @ bude datum notifikace.

```
</group>
```

```
<notify id="stationList" action="stationList" sendTo="fileReport" interval="20" />
```

Atributem id je tato notifikace identifikována jako "stationList". Typ notifikace je nastaven atributem action na "stationList". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Periodicita notifikace je 20 minut.

```
<notify id="eventLog" action="eventLog" sendTo="fileReport" stationID="192.168.% "
interval="20" />
```

Atributem id je tato notifikace identifikována jako "eventLog ". Typ notifikace je nastaven atributem action na "eventLog". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Předmětem notifikace jsou stanice jejichž IP adresa začíná na "192.168". Periodicita notifikace je 20 minut.

```
<notify id="scanList" action="scanList" sendTo="fileReport" stationID="192.168.%"  
interval="20" />
```

Atributem id je tato notifikace identifikována jako "scanList". Typ notifikace je nastaven atributem action na "scanList". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Předmětem notifikace jsou stanice jejichž IP adresa začíná na "192.168". Periodicita notifikace je 20 minut.

```
<notify id="scanDiff" action="scanDiff" sendTo="fileReport" stationID="192.168.%"  
interval="20" />
```

Atributem id je tato notifikace identifikována jako "scanDiff". Typ notifikace je nastaven atributem action na "scanDiff". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Předmětem notifikace jsou stanice jejichž IP adresa začíná na "192.168". Periodicita notifikace je 20 minut.

```
<notify id="checkSystem" action="checkSystem" sendTo="fileReport" interval="20"/>
```

Atributem id je tato notifikace identifikována jako "checkSystem". Typ notifikace je nastaven atributem action na "checkSystem". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Periodicita notifikace je 20 minut.

```
</notification>
```

```
<accessRights>
```

```
<stationGroup id="localhost">
```

```
  <station stationID="^" />
```

```
</stationGroup>
```

Je definována skupina stanic, která je atributem id identifikována jako localhost.

```
<process typeID="Wak.SysKo.As.Server.Scan_tr">
```

```
  <allowGroup groupID="localhost" />
```

```
</process>
```

K procesu "Wak.SysKo.As.Server.Scan_tr" má povolena přístup skupina stanic identifikována jako "localhost". V následujících elementech <process> se skupině "localhost" povoluje přístup k dalším procesům.

```
<process typeID="Wak.SysKo.As.Server.EventLog_tr">
```

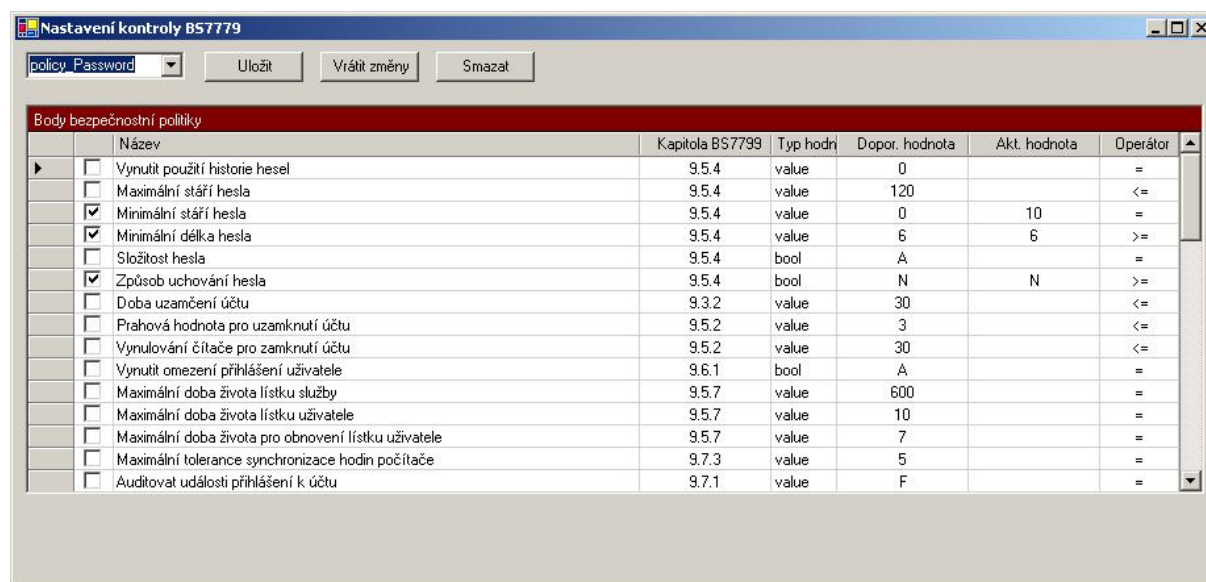
```
  <allowGroup groupID="localhost" />
```

```
</process>
```

```
<process typeID="Wak.SysKo.As.Server.Report_tr">
  <allowGroup groupID="localhost" />
</process>
<process typeID="Wak.SysKo.As.Server.BS7799_tr">
  <allowGroup groupID="localhost" />
</process>
<process typeID="Wak.SysKo.As.Server.CheckSystem_tr">
  <allowGroup groupID="localhost" />
</process>
<process typeID="Wak.SysKo.As.Server.CheckQuery_tr">
  <allowGroup groupID="localhost" />
</process>
</accessRights>
</sysko>
<wak.wnt.remoting>
  <wellknown mode="Singleton" name="SysKoManager"
  type="Wak.SysKo.As.Server.SysKoManager" />
  <channel ref="tcp" port="10082">
Komunikace se SysKoManagerem bude probíhat přes protokol tcp na portu 10082.
  <provider type="Wak.Wnt.Tools.Remoting.IPCheckerSinkProvider, Wak.Wnt.Tools" />
  </channel>
</wak.wnt.remoting>
</configuration>
```

3. Nastavení kontroly BS7779

Pro nastavení vzoru bezpečnostní politiky slouží grafické rozhraní. Aktuální vzor je pak v případě testů porovnáván se skutečnou politikou sledovaného OS.



Obr. 1 Nastavení bezpečnostní politiky

Nastavení bezpečnostní politiky respektuje doporučení normy BS 7799. Popis jednotlivých sloupců:

- zaškrtnutý řádek ukazuje, že pro daný bezpečnostní parametr je nastavena vzorová hodnota
- název obsahuje přesný název bezpečnostního parametru podle používaného OS
- kapitola BS 7799 odkazuje na příslušnou část normy BS 7799
- typ hodnoty se vztahuje k hodnotě bezpečnostního parametru
- dopor. hodnota obsahuje optimální hodnotu podle BS 7799
- akt. hodnotu je možné přepsat, a tak nastavit vlastní vzor bezpečnostní politiky
- operátor se vztahuje k porovnání aktuální hodnoty bezpečnostního parametru a skutečné hodnoty parametru aktuální bezpečnostní politiky OS

Ovládací prvky:

Seznam definovaných bezpečnostních politik – uvedeny názvy, ze kterých je možné si vybrat. Při zadání nové vlastní politiky stačí do boxu zapsat vlastní název.

Tlačítko Uložit – uloží aktuálně zpracovávanou bezpečnostní politiku.

Tlačítko Vrátil změny – načte z databáze původní politiku před změnami v případě chybné definice.

Tlačítko Smazat – smaže aktuálně zpracovávanou bezpečnostní politiku.

4. Sledování událostí

4.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

Sekce <configSections> není určena k nastavení uživatelských parametrů systému.

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

**Element <appSetting> definuje použití remoteManageru na URL
tcp://localhost:10082/SysKoManager.**

```
<eventLog>
```

```
<events id="evttest">
```

Identifikuje test, který sleduje události jako "evttest".

```
<log name="system\application" source="SysKoTest" />
```

Hodnota "system\application" atributu name elementu <log> specifikuje událost ze zdroje identifikovaného jménem "SysKoTest" ze systémového, nebo aplikačního logu.

```
</events>
```

```
</eventLog>
```

```
</SysKo>
```

```
</configuration>
```

4.2 Příklad výstupního souboru

```
<EventLog xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<event>
```

Element <event> popisuje jednu událost.

```
<stationID>192.168.168.15</stationID>
```

192.168.168.15 je IP adresa stanice na níž došlo k události.

```
<logName>application</logName>
```

Druh události.

```
<machineName> STANICE </machineName>
```

Jméno stanice.

```
<eventDate>2006-01-30T17:39:56.0000000+01:00</eventDate>
```

Datum události.

```
<eventID>0</eventID>
```

ID události.

```
<eventType>Information</eventType>
```

Typ události.

```
<eventSource>SysKoTest</eventSource>
```

Zdroj události.

<eventDescription>SysKo test service Start.</eventDescription>

Popis události.

</event>

</EventLog>

5. Sledování souborů

5.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

Sekce <configSections> není určena k nastavení uživatelských parametrů systému.

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

**Element <appSetting> definuje použití remoteManageru na URL
tcp://localhost:10082/SysKoManager.**

```
<scanner>  
<scan id="scantest">  
  <fileSystem name="c:\Program files\SysKo\test" recursive="0" />  
</scan>
```

**Identifikuje scan jako "scantest". Sledovaným adresářem je "c:\Program
files\SysKo\test". Prohledávání podadresářů je atributem recursive vypnuto.**

```
</scanner>
```

```
</SysKo>
```

```
</configuration>
```

5.2 Příklad výstupního souboru

```
<ScanDiffList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<ScanDiff>
```

```
<station>
```

```
<id>192.168.168.15</id>
```

IP adresa sledované stanice.

```
</station>
```

```
<scan1>
```

Scan před změnou.

```
<scanID>scantest</scanID>
```

ID scanu.

```
<scanDate>2006-01-30T18:23:11.5600000+01:00</scanDate>
```

Datum scanu.

```
</scan1>
```

```
<scan2>
```

Scan po změně.

```
<scanID>scantest</scanID>
```

ID scanu.

```
<scanDate>2006-01-30T18:23:27.3770000+01:00</scanDate>
```

Datum scanu.

```
</scan2>
```

```
<objectOS>
```

```
<name>c:\Program files\SysKo\test\SysKoTestFile.txt</name>
```

Celá cesta k souboru.

```
<type>file</type>
```

Typ.

<Values>

<name>fileLastWriteTime</name>

Čas poslední modifikace souboru.

<diffType><></diffType>

Operátor nerovnosti <>. Značí že soubor byl modifikován.

<value1>2006-01-30T18:17:14.4266190</value1>

<value2>2006-01-30T18:23:22.6968304</value2>

</Values>

<Values>

<name>fileAttributes</name>

Atributy souboru.

<diffType>=</diffType>

Operátor rovnosti =. Značí že atributy souboru nebyly modifikovány.

<value1>32</value1>

<value2>32</value2>

</Values>

<Values>

<name>fileCreationTime</name>

Datum vytvoření souboru. Značí že soubor byl modifikován.

<diffType>=</diffType>

Operátor rovnosti =. Značí že datum vytvoření souboru nebylo modifikováno.

<value1>2006-01-30T18:15:52.6338534</value1>

Datum vytvoření souboru.

<value2>2006-01-30T18:15:52.6338534</value2>

Datum vytvoření souboru.

</Values>

<ACEs>

Access Control Entry

<user>

<userName>DOMENA\STANICE</userName>

Jméno stanice

<sid>S-1-5-21-591665024-1611875846-1847928074-1010</sid>

Bezpečnostní identifikační číslo.

</user>

<diffType>=</diffType>

Operátor rovnosti =. značí že ACE u DOMENA\STANICE nebylo modifikováno.

<ace1>Allow:rd|wd|ad|re|we|ex|dc|ra|ea</ace1>

<ace2>Allow:rd|wd|ad|re|we|ex|dc|ra|ea</ace2>

</ACEs>

</objectOS>

</ScanDiff>

</ScanDiffList>

6. Sledování služeb OS

6.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

Sekce <configSections> není určena k nastavení uživatelských parametrů systému.

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"
```

```
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"
```

```
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"
/>
```

```
</sectionGroup>
```

```
</configSections>
```

Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.

```
<SysKo>
```

```
<appSettings remoteManager="true"
```

```
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

Element <appSetting> definuje použití remoteManageru na URL tcp://localhost:10082/SysKoManager.

```
<scanner>
```

```
<scan id="scantest">
```

```
<services scanDrivers="0" scanServices="1" />
```

```
</scan>
```

Identifikuje scan jako "scantest". Hodnota "1" atributu scanServices zapíná sledování služeb.

```
</scanner>
```

```
</SysKo>
```

```
</configuration>
```

6.2 Příklady výstupních souborů

6.2.1 ScanDiff

```
<ScanDiffList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<ScanDiff>
```

```
<station>
```

```
<id>192.168.168.15</id>
```

```
</station>
```

Scan1.

```
<scan1>
```

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T17:24:20.5270000+01:00</scanDate>
```

```
</scan1>
```

Scan2.

```
<scan2>
```

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T17:40:59.9630000+01:00</scanDate>
```

```
</scan2>
```

```
<objectOS>
```

```
<name>SysKoTestSvc</name>
```

Jméno služby.

```
<type>service</type>
```

Sledovaný typ - služba.

```
<Values>
```

```
<name>serviceDisplayName</name>
```

```
<diffType>=</diffType>
```

```

    <value1>SysKoTestSvc</value1>
    <value2>SysKoTestSvc</value2>
  </Values>
  <Values>
    <name>serviceType</name>
    <diffType>=</diffType>
    <value1>16</value1>
    <value2>16</value2>
  </Values>
  <Values>
    <name>serviceStatus</name>
    <diffType>&lt;&gt;</diffType>

```

Operátor nerovnosti <>. Značí změnu stavu služby.

```

    <value1>1</value1>
    <value2>4</value2>
  </Values>
</objectOS>
</ScanDiff>
</ScanDiffList>

```

6.2.2 ScanList

Obsahem notifikace ScanList je seznam scanu.

```

<ScanList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <scan>

```

```

    <stationID>192.168.168.15</stationID>

```

IP adresa stanice.

```

    <scanID>scantest</scanID>

```

ID scanu.

```
<scanDate>2006-01-30T17:24:20.5270000+01:00</scanDate>
```

Datum scanu.

```
<scanResult>OK</scanResult>
```

Výsledek scanu.

```
</scan>
```

```
</ScanList>
```

6.2.3 StationList

Seznam stanicí které se kdy připojily.

```
<Stations xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<station>
```

```
<id>192.168.168.15</id>
```

IP adresa stanice.

```
<publicAddress>192.168.168.15</publicAddress>
```

Veřejná IP adresa stanice.

```
</station>
```

```
</Stations>
```

7. Sledování registrů

7.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

Sekce <configSections> není určena k nastavení uživatelských parametrů systému.

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

**Element <appSetting> definuje použití remoteManageru na URL
tcp://localhost:10082/SysKoManager.**

```
<scanner>  
<scan id="scantest">  
  <registry name="LocalMachine\Software\SysKo" recursive="1" />  
</scan>
```

**Identifikuje scan jako "scantest". Atribut name definuje
"LocalMachine\Software\SysKo" jako sledovanou větev v registrech. Hodnota "1"
atributu recursive zapíná sledování podřízených větví registru.**

```
</scanner>
```

```
</SysKo>
```

```
</configuration>
```

7.2 Příklad výstupního souboru scanDiff

```
<ScanDiffList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
  <ScanDiff>
```

```
    <station>
```

```
      <id>192.168.168.15</id>
```

IP adresa sledované stanice.

```
    </station>
```

```
    <scan1>
```

Scan1.

```
      <scanID>scantest</scanID>
```

```
      <scanDate>2006-01-30T18:27:53.3600000+01:00</scanDate>
```

```
    </scan1>
```

```
    <scan2>
```

Scan2.

```
      <scanID>scantest</scanID>
```

```
      <scanDate>2006-01-30T18:28:09.7970000+01:00</scanDate>
```

```
    </scan2>
```

```
    <objectOS>
```

```
      <name>HKEY_LOCAL_MACHINE\Software\SysKo</name>
```

Sledovaná větev v registru.

```
      <type>registry</type>
```

```
      <Values>
```

```
        <name>HKEY_LOCAL_MACHINE\Software\SysKo\StringValue</name>
```

Změna hodnoty položky StringValue.

```
        <diffType>&lt;&gt;</diffType>
```

```
        <value1>2</value1>
```

```
        <value2>3</value2>
```

```
      </Values>
```

```
    </objectOS>
```

```
  </ScanDiff>
```

```
</ScanDiffList>
```

8. Sledování bezpečnostní politiky

8.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

Sekce <configSections> není určena k nastavení uživatelských parametrů systému.

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

Element <appSetting> definuje použití remoteManageru na URL tcp://localhost:10082/SysKoManager.

```
<scanner>  
<scan id="scantest">  
  <policy exclude="^signature$" />  
</scan>
```

Identifikuje scan jako "scantest". Element <policy> definuje sledování bezpečnostní politiky. Ze sledování je vyloučena bezpečnostní politika jejíž název odpovídá regulárnímu výrazu ^signature\$.

```
</scanner>
```

```
</SysKo>
```

```
</configuration>
```

8.2 Příklad výstupního souboru scanDiff

```
<ScanDiffList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<ScanDiff>
```

```
<station>
```

```
<id>192.168.168.15</id>
```

IP adresa sledované stanice.

```
</station>
```

```
<scan1>
```

scan1.

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T18:42:55.1130000+01:00</scanDate>
```

```
</scan1>
```

```
<scan2>
```

scan2.

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T18:44:30.6970000+01:00</scanDate>
```

```
</scan2>
```

```
<objectOS>
```

```
<name>Policy</name>
```

```
<type>policy</type>
```

Typ bezpečnostní politika.

```
<Values>
```

```
<name>MinimumPasswordAge</name>
```

Minimální stáří hesla

<diffType>=</diffType>

<value1>0</value1>

<value2>0</value2>

</Values>

<Values>

<name>MinimumPasswordLength</name>

Minimální délka hesla

<diffType><></diffType>

Operátor nerovnosti <>, značí změnu.

<value1>6</value1>

Stará minimální délka hesla

<value2>5</value2>

Nová minimální délka hesla

</Values>

</objectOS>

</ScanDiff>

</ScanDiffList>

Slovníky

Zkratky

Zkratka	Význam
OS	Operační systém

Tab. 1 Slovník zkratk

Termíny

Termín	Význam
Regulární výraz	Regulární výraz (regular expression) je speciální řetězec znaků, který představuje určitý vzor (masku) pro textové řetězce.
Reference	Vztah (odkaz) mezi dvěma elementy dokumentu.
Atribut	Atribut je označení datového prostoru, uchovávající datovou hodnotu. Je specifikován jménem, případně typem a rozsahem uchovávaných hodnot.
XML	Extensible Markup Language. Značkovací jazyk popisující strukturu dokumentu.
CSS	Cascading Style Sheet. Technologie pro přidávání stylu k webovým dokumentům.
SMTP	Simple Mail Transfer Protocol - jednoduchý protokol pro odesílání a přenos pošty mezi poštovními servery.
IP adresa	IP adresa je jedinečná adresa počítače. IP adresa se udává ve tvaru xxx.xxx.xxx.xxx, kde xxx je číslo v rozsahu 0 až 255. Může vypadat například takto: 127.0.0.1
makro	Je identifikováno uvozujícím a ukončujícím řetězcem "@@". Po vyhodnocení systémem je jeho hodnota nahrazena významem makra. Např. hodnotou makra @@WINDIR@@ může být řetězec "C:\WINNT".
ACE	Access Control Entry. Obsahuje množinu přístupových práv uživatele k danému objektu. Součástí je i bezpečnostní identifikátor.
notifikace	Odeslání reportu o sledovaných událostech. Podle nastavení je formou reportu soubor uložený na disk nebo odeslaný el. poštou.
localhost	Místní adresa právě používané stanice. Odpovídá IP adrese 127.0.0.1
Scan	Zjištění aktuálního stavu objektu.
URL	Uniform Resource Locator. URL je standardizovaný řetězec znaků identifikující zdroj a způsob přístupu k němu.

Tab. 2 Slovník termínů

