FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Návrh autorizačního konceptu v SAP ERP systému pro závod vybrané společnosti
Student:	Lenka Obermajerová
Vedoucí:	Ing. Jiří Cejnar
Studijní program:	Informatika
Studijní obor:	Informační systémy a management
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2019/20

Pokyny pro vypracování

Cílem bakalářské práce je vytvořit návrh autorizačního konceptu v SAP ERP systému se zaměřením na logistiku pro závod společnosti, jejíž jméno bude z důvodů utajení nahrazeno "společnost X".

1) Proveďte analýzu procesů závodu společnosti X se zaměřením na logistiku.
2) Navrhněte základní koncept přístupových práv uživatelů v SAP ERP systému.
3) Vytvořte plán realizace návrhu.
4) Vyhodnoťte náklady na realizaci návrhu.
5) Vyhodnoťte rizika návrhu.
6) Vyhodnoťte přínosy navrhovaného konceptu.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 16. října 2018

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Návrh autorizačního konceptu v SAP ERP systému pro závod vybrané společnosti

Lenka Obermajerová

Katedra softwarového inženýrství
Vedoucí práce: Ing. Jiří Cejnar

12. května 2019

Poděkování

Chtěla bych poděkovat vedoucímu své bakalářské práce Ing. Jiřímu Cejnarovi za vedení práce a příležitost být součástí jeho týmu. Dále chci poděkovat Ing. Matěji Coganovi, Ing. Slavomilu Štefánovi, Martinu Švandovi a všem ostatním kolegům ze společnosti X za čas, za pomoc, za odborné rady i za všechny užitečné informace, které mi během tvorby této práce ochotně poskytli. V neposlední řadě chci poděkovat své rodině a svým přátelům, kteří pro mě byli po celou dobu mého studia velkou oporou.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 12. května 2019 ……

Odkaz na tuto práci

Obermajerová, Lenka. *Návrh autorizačního konceptu v SAP ERP systému pro závod vybrané společnosti.* Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2019.

Abstrakt

Tato práce se zabývá vytvořením návrhu autorizačního konceptu v SAP ERP systému se zaměřením na logistiku pro závod společnosti X. Pomocí vytvoření analýzy procesů oblasti logistiky ve výrobním závodě, která byla vypracována za využití metodiky BPMN, byl vytvořen návrh autorizačního konceptu, který je možné přizpůsobit pro nově vznikající výrobní závody společnosti X. Spolu s ním je vytvořen plán realizace návrhu a odhad nákladů realizace a jsou vyhodnocena rizika a přínosy návrhu. Přínosem této práce je kromě možnosti opakovaného použití návrhu také to, že práci lze využít jako základ dokumentace autorizačního konceptu. Analýza procesů může být použita i v dalších projektech společnosti, nejen při tvorbě autorizačního konceptu.

Klíčová slova autorizace přístupu, řízení bezpečnosti informací, systém SAP ERP, návrh konceptu přístupových práv, strojní průmysl

Abstract

This bachelor thesis deals with creation of authorization concept design in SAP ERP system with focus on logistics for a plant of company X. By creating a process analysis of the logistics area at the plant, that was created using the BPMN methodology, an authorization concept design was created. It can be customized for the emerging manufacturing plants. Along with it, a design implementation plan and an estimate of implementation costs were created and the risks and benefits of the design were assessed. In addition to reusing the design, the benefit of this thesis is that it can be used as a basis for the documentation of authorization concept. Process analysis can also be used in other company projects, not just when creating an authorization concept. Diagrams of this analysis can be found in the appendix.

Keywords access authorization, information security management, system SAP ERP, authorization concept design, machine industry

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Pro firmy jsou informace klíčovým faktorem úspěchu. Pracuje s nimi snad každý jeden zaměstnanec. Ať už se jedná o informace související s aktuální poptávkou po produktech na trhu kvůli dalšímu plánování firmy, o informace o zaměstnancích, které zajímají například personální oddělení, nebo o konkrétní specifikace výrobků, které jsou potřebné přímo v produkci.

V případě, že se tyto informace dostanou do nesprávných rukou, může nastat situace, která společnost (v této práci je pojem společnost uváděn jako synonymum ke slovu firma) negativně ovlivní. Proto je nutné řešit mimo jiné i zabezpečení dat ve společnostech. Jedním ze způsobů zvýšení bezpečnosti informací je umožnění přístupu k informacím jen uživatelům, kteří tyto informace potřebují k výkonu své práce. Přidělení přístupových oprávnění k určitým informacím se nazývá autorizační koncept. Právě touto problematikou se zabývá tato bakalářská práce.

Práce vzniká pro společnost strojírenského průmyslu – jméno společnosti je z důvodu utajení nahrazeno spojením „společnost X“. Společnost v následujících letech plánuje rozšířit své pole působnosti do dalších zemí světa a vytvořit několik výrobních závodů v těchto zemích. Každý tento závod potřebuje autorizační koncept k přístupu do SAP ERP systému, se kterým v jednotlivých závodech pracuje oblast logistiky.

Autorizační koncepty pro jednotlivé výrobní závody jsou velmi podobné a liší se jen v určitých částech, jako například v dostupnosti moderních technologií. Nabízí se proto vytvářet jednotlivé autorizační koncepty na základě jednoho univerzálního autorizačního konceptu vytvořeného pro obecný výrobní závod společnosti X.

Jelikož žádný takový univerzální autorizační koncept společnost X nemá, rozhodla jsem se zvolit si návrh takového autorizačního konceptu jako téma své bakalářské práce. Jelikož působím ve společnosti X na oddělení, které se zabývá administrací a vývojem SAP ERP systému pro logistickou oblast společnosti, je téma zaměřeno právě na přístupová oprávnění v oblasti logistiky.

Práce se zaměřuje na analýzu procesů společnosti, návrh požadovaného autorizačního konceptu, analýzu rizik návrhu a odhad časové i finanční náročnosti jeho realizace. Ke splnění těchto úkolů byly využity interní dokumenty společnosti X a metodiky, podle kterých společnost běžně zadané úkoly řeší.

Práce je strukturována do tří kapitol. První a druhá kapitola představují teoretickou část práce. V první kapitole je nastíněna problematika bezpečnosti informací ve společnostech. Přes toto téma se poté kapitola dostává k teorii autorizačních konceptů. Zároveň je v první kapitole základně vysvětlena metodika BPMN, která je v dalších kapitolách použita pro tvorbu diagramů.

Tato metodika je nejvíce využita ve druhé kapitole, která se zaměřuje především na analýzu procesů v oblasti logistiky výrobního závodu společnosti X. Kromě analýzy procesů je zde nastíněna i struktura výrobního závodu.

Z této analýzy poté vychází praktická část práce – kapitola třetí. V té je vytvořen koncept rolí pro oblast logistiky, společně s jmennou konvencí rolí a postupem přiřazení role uživateli. Pro tento návrh jsou následně zdůrazněna rizika, která návrhu hrozí, a je vytvořen plán realizace tohoto návrhu. Z tohoto plánu pak vychází odhad nákladů na realizaci návrhu autorizačního konceptu.

Kapitola 1

Cíle práce

Cílem bakalářské práce je vytvořit návrh autorizačního konceptu v SAP ERP systému se zaměřením na logistiku pro závod společnosti, jejíž jméno bude z důvodů utajení nahrazeno „společnost X“.

Cílem kapitoly *Teoretický základ* je zdůraznit čtenáři důležitost autorizace z pohledu bezpečnosti informací, seznámit ho se základními pojmy a principy z oblasti autorizace a vysvětlit metodiku BPMN, která je v práci použita.

Cílem kapitoly *Analýza závodu společnosti X* je provést analýzu procesů závodu společnosti X se zaměřením na logistiku. Tato analýza má sloužit jako podklad pro vytvoření návrhu autorizačního konceptu v praktické části.

Kapitola *Návrh autorizačního konceptu*, která představuje praktickou část práce, má za cíl navrhnout základní koncept přístupových práv uživatelů v SAP ERP systému pro závod společnost X se zaměřením na logistiku. Pro tento návrh je následně nutné vytvořit jeho plán realizace a odhadnout náklady této realizace. Zároveň je nutné vyhodnotit rizika a přínosy navrhovaného autorizačního konceptu.

Kapitola 2

Teoretický základ

V této části práce jsou čtenáři poskytnuty informace pro snazší pochopení řešení zadaných problémů. Proto je nutné vysvětlit všechny důležité pojmy, stejně jako postupy, použité v praktické části práce.

2.1 Systém SAP ERP

V této krátké kapitole jsou čtenáři poskytnuty základní informace o společnosti SAP a o systému SAP ERP. Nastiňuje, v jaké oblasti informatiky se práce pohybuje.

Zkratka SAP vznikla z německého *Systeme, Anwendungen, Produkte in der Datenverarbeitung*. To se dá do českého jazyka přeložit jako Systémy, Aplikace, Produkty v oblasti výpočetní techniky.

Jak se uvádí na oficiálních webových stránkách společnosti [1], tato firma, založená v roce 1972, je jedním z největších dodavatelů podnikových aplikací na světě. V dnešní době zasahuje do mnoha podnikových odvětví, jako je strojírenství (automobilový a letecký průmysl), finanční služby (banky, pojišťovny), energetika a přírodní zdroje (chemický průmysl, ropa a plyn, stavební a těžební průmysl), služby (cestování, média, sport a zábava) nebo například spotřební průmysl (maloobchod, móda).

Paleta produktů je v současnosti poměrně široká, systémy jsou určeny speciálně pro určité podnikové oblasti, jako jsou například řízení vztahů se zákazníky, personalistika nebo nákup. Nejsilnější však stále zůstává systém SAP ERP, tedy systém *plánování podnikových zdrojů* (*Enterprise Resource Planning*).

Aplikace ERP se skládají z různých aplikačních modulů, které se zaměřují na určitou část podniku (ekonomické řízení, prodej a marketing, řízení nákupu, výroba, správa lidských zdrojů a další). Díky tomu poté výsledná aplikace může pokrýt a v případě potřeby automatizovat podnikové procesy napříč celou firmou. Zprostředkovává hladkou spolupráci mezi jednotlivými moduly

a sdílení společných dat – například skladový management a oddělení nákupu musí úzce spolupracovat pro zajištění dodávky potřebného materiálu.

Fungování ERP systémů je postaveno na transakcích (řadí se mezi takzvané transakční aplikace). To znamená, že každá akce, která má být v aplikaci provedena, je zajišťována pomocí transakce. Jak uvádí Gála, Pour a Šedivá [2], transakcí je myšlena určitá transformace současného stavu, splňující následující vlastnosti:

- *atomicita* – běh transakce nelze rozdělit, vždy buď celá proběhne, nebo neproběhne vůbec;
- *trvanlivost* – po potvrzení transakce ji není možné nijak zrušit;
- *konzistence* – jedna transakce proběhne vždy stejně podle určitých předem definovaných pravidel;
- *izolovanost* – transakce není nijak závislá na ostatních transakcích (nezasahuje do žádné jiné a neexistuje jiná transakce, která by zasahovala do ní).

ERP systémy jsou nejčastěji dodávané jako typové aplikace. Je tedy nutné systém vždy kastumizovat (upravit ho tak, aby odpovídal konkrétním požadavkům firmy). V rámci tohoto procesu je možné dosáhnout mnoha změn – odstranění nebo přidání funkcionalit, nastavení výchozích hodnot, změna vzhledu, bezpečnost dat (řízení přístupu k nim) a podobně. Část takovýchto změn je nutné provést již v průběhu implementace dodavatelem, jiné lze provádět na interní úrovni, tedy může je provést přímo oprávněný uživatel systému.

2.2 Bezpečnost podnikových informací

Pro lepší pochopení celé problematiky je vhodné vysvětlit nejprve význam dvou základních pojmů, *data* a *informace*, které se mezi sebou často zaměňují. Jak píše Sklenák [3], pojem data označuje *„čísla, text, zvuk, obraz, popř. jiné smyslové vjemy reprezentované v podobě vhodné pro zpracování počítačem“* a je základem, ze kterého po zasazení do kontextu vznikají informace.

Data sama o sobě nám ve velké většině případů nic neříkají. Až data, kterým přiřadíme význam, neboli jak říká Sklenák [3] *„data použitelná a srozumitelná“*, nám jsou užitečná. A právě tato data tvoří informace.

Informace mohou být uloženy psanou formou jako zmíněná data (text, tabulky, soubory, obrázky, videa, …) nebo mohou mít mluvenou podobu a být jedním člověkem předávány druhému ústně. Ať v jedné, nebo v druhé formě, je potřebné udržovat podnikové informace v bezpečí, jelikož jim hrozí mnoho rizik.

Tato rizika mají velmi velký rozsah a týkají se mnoha oblastí společností. Trombley [4] uvádí jako příklady následující situace:

- narušení digitální databáze, kdy se nepovolaná osoba buď úmyslně, nebo omylem dostane k tajným informacím a tyto informace mohou být ukradeny, změněny, zničeny, zkopírovány nebo neoprávněně použity;
- narušení on-line komunikace zapříčiněné například podvodem nebo přítomností malwaru (škodlivého softwaru);
- ztráta, zničení nebo krádež papírových dokumentů.

Všechna tato rizika mohou být zapříčiněna například lidskou chybou, selháním techniky, úmyslem nebo i přírodní katastrofou. Následky jsou pak pro společnosti často velmi nebezpečné.

Je možné, že společnosti kvůli těmto problémům přijdou o důležité informace, které jsou potřeba k jejich činnosti, nebo že se k informacím dostanou cizí osoby. Ty pak s touto informací mohou společnostem uškodit např. jejich použitím ve vlastní prospěch (tím dojde ke snížení konkurenční výhody společností) nebo využitím informací proti společnostem (to může mít za následek pošpinění pověsti nebo například právní postih). Z toho důvodu je nutné klást na bezpečnost informací veliký důraz.

2.2.1 Ochrana podnikových informací

Ochrana informací není důležitá jen kvůli udržení firemního tajemství, ale i z právního hlediska. Jako příklad je možné uvést legislativu Evropské unie (EU) Obecné nařízení na ochranu osobních údajů (*General Data Protection Regulation – GDPR*).

GDPR se vztahuje na kohokoliv, kdo pracuje s osobními údaji občanů Evropské unie – i společnosti se sídlem mimo EU. Jak uvádí Úřad pro ochranu osobních údajů [5], jednou z povinností, které tato legislativa společnostem ukládá, je i povinnost osobní údaje v podobě jak listinných, tak elektronických dokumentů při uchovávání dostatečně zabezpečit. Například listinné dokumenty, které v danou chvíli nejsou potřebné, musí být v uzamčeném prostoru a s údaji uloženými v elektronické podobě může pracovat díky nastavení tajného hesla pouze pověřená osoba. Větší systémy pak musí vést záznamy o tom, kdo a jak k údajům přistupoval.

V každé oblasti podnikání je tedy při kontrole bezpečnosti informací třeba brát v potaz i legislativu, která se k dané oblasti vztahuje. To jsou minimální požadavky, které pak společnosti musí v oblasti bezpečnosti informací splňovat.

Mezinárodní organizace pro normalizaci (*International Organization for Standardization* – ISO) a Mezinárodní elektrotechnická komise (*International Electrotechnical Commission* – IEC) vydaly mezinárodní normy ISO/IEC

27001 (Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky) a ISO/IEC 27002 (Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací). Kosutic [6] vysvětluje, že tyto dvě normy jsou spolu úzce spjaty. Obě se zaměřují na způsoby zabezpečení informací, avšak jen podle normy ISO/IEC 27001 je možné udělat certifikace (tedy ověření nezávislou organizací, že daná společnost splňuje požadavky dané normy). To je užitečné, protože díky tomu stoupá důvěryhodnost firmy v očích obchodních partnerů.

Rozdíl mezi těmito normami je také v jejich rozsahu. Ač se obě zaměřují na stejná témata, ISO/IEC 27002 je rozebírá mnohem více do detailů a poskytuje tak podrobnou příručku všech možností, jak se postavit k bezpečnosti informací.

Pro společnosti je v oblasti ochrany informací důležité *řízení rizik informační bezpečnosti* (*Information Security Risk Management* – ISRM). To se zabývá identifikováním rizik, která informacím hrozí, ohodnocením těchto rizik podle závažnosti, určením nejlepších a cenově nejvýhodnějších řešení, která snižují pravděpodobnost vzniku rizikových situací, a monitorování vytvořeného systému rizik a změn v něm [7].

Bezpečnostní rizika se ve velké míře týkají zaměstnanců a jejich práce s informacemi. Nejen, že mohou zaměstnanci ohrozit používaná data nechtěnou chybou, ale újmu mohou společnosti způsobit i úmyslně. Výzkum společnosti Iron Mountain [8] uvádí, že 32 % zkoumaných zaměstnanců již více než jedenkrát vyneslo ze zaměstnání tajné informace. Zároveň bylo během tohoto výzkumu zjištěno mimo jiné to, že téměř každý třetí zaměstnanec (31 %) by tajné informace vynesl, pokud by byl ze společnosti, kde je zaměstnán, propuštěn.

Další riziko související se zaměstnanci je ohrožení dat nevědomky, pokud se stanou obětí takzvaného sociálního inženýrství. Jak uvádí Národní centrum kybernetické bezpečnosti [9], jedná se o situaci, kdy oběť díky psychické manipulaci uvěří mylné informaci (kterou mohl obdržet různými způsoby – telefonát, e-mail, SMS, …). Na základě této informace pak provede požadovanou akci (klikne na odkaz, odešle peníze, prozradí tajnou informaci a podobně). Svou chybu si často uvědomí až poté, co jsou patrné následky.

Pro firmy je velmi nebezpečnou formou sociálního inženýrství situace, kdy se útočník vydává za nějakého zaměstnance společnosti – může jít o nadřízeného, požadujícího po své asistence okamžité odeslání určité částky peněz pod pohrůžkou velké majetkové či nemajetkové újmy, pokud platba neproběhne okamžitě, nebo o jiného zaměstnance, který zapomněl svá přístupová hesla. K větší důvěryhodnosti jsou používané například e-mailové adresy velice podobné opravdovým adresám daných zaměstnanců, ve kterých je změněn pouze jeden znak a je tedy velmi snadné rozdíl přehlédnout.

Forem sociálního inženýrství je mnoho a často je velmi těžké jej včas odhalit. Proto je nutné počítat i s možností takovéhoto útoku a být na něj připraven.

Z těchto všech důvodů je potřebné, aby risk management společností využíval postupy, jak rizika lidského faktoru minimalizovat. Mezi takové postupy patří například:

- *povinná dovolená* (*mandatory vacation*) – každý zaměstnanec musí ročně využít dovolené trvající minimálně interně určenou dobu (běžně týden až dva) a během tohoto času vykonává jeho práci na jeho pozici jiný zaměstnanec, čímž se častěji odhalí chyby prováděné zaměstnancem na dovolené;

- *rotace pracovních pozic* (*job rotation*) – určitý počet zaměstnanců si po dané době (měsíce až roky) vyměňuje pracovní pozice, čímž se zajistí, že v případě odchodu jednoho z nich je zde stále někdo, kdo ví, co daná pozice obnáší;

- *oddělení povinností* (*separation of duties* – SOD) – práva k jednotlivým činnostem jsou rozdělena mezi více osob, aby se například nemohlo stát, že jeden zaměstnanec vytvoří proces, který poté i sám schválí;

- *princip minimálního oprávnění* (*least privilege*) – každému zaměstnanci jsou přidělena pouze ta oprávnění, která nezbytně potřebuje k výkonu své práce [10].

Zavedením takovýchto procedur do interní politiky však není dostatečným bojem proti úniku tajných informací skrze zaměstnance. Trombley [4] uvádí, že podle výzkumu společností PwC a Iron Mountain má přes 90 % společností v Evropě nějakým způsobem takové bezpečnostní procedury zavedené. Avšak pouze 70 % z nich poté sleduje, jak efektivně jsou tyto postupy dodržovány. V okamžiku, kdy nejsou bezpečnostní politiky pečlivě monitorovány, není možné zaručit, že jsou dodržovány a tím pádem nemusí být rizika lidského faktoru pokryta tak, jak bylo zamýšleno.

Podle Stewarta [10] je možné rozdělit kontrolu a snižování informačních rizik do tří hlavních oblastí – technické (logické), řídící (administrativní) a provozní. Tyto oblasti se netýkají jen informačních technologií, ale všech prostředků, které společnosti k uchování informací používají.

Technická oblast obstarává IT hardware a software, který chrání informační zdroje a řídí přístup k nim. Příkladem mohou být vstupní hesla, čipové karty, biometrické kontroly nebo firewall – síťový prvek, který ohraničuje zabezpečenou síť a propouští jedním nebo druhým směrem pouze data, která splňují předem definovaná filtrovací pravidla [11].

Do řídící oblasti patří především politiky a procedury společností, které definují řízení přístupu. Patří sem například klasifikace dat (tajné, interní, veřejné, …), bezpečnostní školení, prověřování historie uchazečů při náborových pohovorech a pod.

Pod provozní oblast spadají mechanismy, které zajišťují bezpečnost běžných denních procesů (plnění pracovních úkonů). Jako příklady lze uvést politika hesel, audit událostí nebo reakce na incidenty.

2.2.2 IT bezpečnost

Jelikož velká část informací je dnes ukládána v elektronické podobě a zpracovávána různými informačními technologiemi, jsou na informační systémy kladeny vysoké nároky ohledně bezpečnosti. Pro práci s informacemi a pro jejich uchování se často uvádí základní tři pravidla známá pod zkratkou CIA:

- *důvěrnost* (*confidentiality*) – stanovuje jako cíl, že pouze uživatelé, kteří danou informaci potřebují k vykonání své práce, k ní mají umožněn přístup;
- *integrita* (*integrity*) – říká, že informace nesmí být upravena – úmyslně či neúmyslně – procesem nebo uživatelem, který k tomu není oprávněn;
- *dostupnost* (*availability*) – stanovuje, že informace musí být k dispozici uživateli, který ji potřebuje ke své práci a má oprávnění ji používat, v momentě, kdy k ní požaduje přístup [12].

Jak uvádějí Gála, Pour a Šedivá [2], kromě výše uvedeného je při zajišťování bezpečnosti zároveň třeba sledovat i další vlastnosti systému:

- *prokazatelnost* (*authentication*) – zajišťuje, že každá akce, která v systému proběhla, se dá zpětně nalézt a zároveň k ní jde přiřadit uživatel, který ji provedl;
- *nepopíratelnost* (*non-repudiation*) – určuje, že uživatel nemůže popřít, že se účastnil provádění akce;
- *spolehlivost* (*reliability*) – stanovuje, že systém se musí chovat tak, jak je uvedeno v dokumentaci.

Bezpečnost IT systémů se týká všech jeho vrstev. Úplným základem je fyzické zabezpečení hardwaru. Je nutné zajistit, že je hardware uchováván tak, jak je pro jeho správný chod požadováno, že se k němu nedostane nepovolaná osoba, ale i to, že v případě zásahu vnějších vlivů (přírodní katastrofa – např. povodeň – a pod.) nedojde k jeho poškození.

Další oblast, která by mohla ohrozit bezpečnost systému, je síťová komunikace a připojení do sítě obecně. Zde se dá ochrana navýšit například pomocí firewall.

V SAP systémech je pro síťovou komunikaci využívána *zabezpečená síťová komunikace*(*Secure network communication* – SNC) [13].Slouží pro bezpečnější šifrovanou komunikaci a vzdálený přístup mezi různými komponentami SAP systému (ať už klienty nebo servery).

Proti nebezpečnému obsahu a softwaru pomáhá uživateli při jeho práci také antivirový program – kontroluje vstupní i výstupní místa, přes která by se do zařízení mohl dostat vir, a zasáhne v případě, kdy nalezne v datech shodu s obsahem své virové databáze.

V dnešní době takřka nezbytnou částí informační bezpečnosti je kryptografie neboli šifrování. Je několik druhů šifrování. Všechny fungují na principu utajení informace před vnějším pozorovatelem tak, že uživatelé, pro které je informace určena, jsou schopni ji přečíst, avšak nikdo jiný toho není schopen. Používá se při vzdálené komunikaci i při ukládání souborů.

Ve větších společnostech se často zavádí rozdělení systémů na několik podsystémů, čímž se zvyšuje bezpečí pří vývoji a zlepšování daného systému. Běžně využívané dělení je:

- *Vývojový systém* – Veškeré vývojové změny, které mají se systémem proběhnout, vznikají v této části. Jsou zde nahrána pouze neaktuální ukázková data, se kterými lze nové funkcionality běžně zkoušet, avšak nijak neprozrazují skutečné informace nepovolaným osobám. Přístup do tohoto systému mají pouze uživatelé podílející se na vývoji systému. Běžného koncového uživatele se tato část systému netýká.

- *Testovací systém* – Poté, co jsou prováděné změny systému dokončené, jsou nahrány do tohoto systému, ve kterém jsou následně důkladně otestovány, zda opravdu perfektně fungují a je možné je nasadit pro normální použití. Do tohoto systému jsou jednou za určitou (relativně krátkou) dobu nahrávána reálná data společnosti, aby testování bylo efektivní a účinné. Stejně jako vývojový systém, ani testovací systém se koncového uživatele běžně nijak nedotýká.

- *Produkční systém* – Veškeré činnosti, kvůli kterým byl systém v dané společnosti zaveden, probíhají v této části. Vznikají zde reálná používaná data, se kterými na této úrovni pracuje koncový uživatel systému.

Nevýhodou tohoto rozdělení je, že při testování změn v testovacím systému se dostávají reálná data k uživatelům, kteří je potřebují k otestování systému, avšak oni sami je znát nepotřebují. Proto se začíná zavádět ještě čtvrtá část systému, takzvaný maskovací systém. Ten má stejnou funkci jako systém testovací, avšak nahrávaná data jsou před zpřístupněním k použití určitým způsobem zamaskována. Systém je tedy schopný provádět test nad reálnými daty, avšak uživatel se nedozví žádné informace, které nutně nepotřebuje ke své práci.

Další účinnou oblastí informační bezpečnosti, která je zároveň pro tuto práci nejpodstatnější, je *řízení identit a přístupu* (*Identity and Access Management* – IAM). To zajišťuje, aby se ke každé informaci dostal pouze oprávněný uživatel.

Hausman a Cook [14] uvádějí, že se řízení identit a přístupu skládá ze tří kroků:

1. *Identifikace uživatele* – Je to akce uživatele požadujícího přístup, při které prokazuje svou identitu. To může být založeno na čtyřech principech:

   - *Co uživatel ví* – Nejčastější způsob přihlašování je založen na znalosti správné kombinace uživatelského jména a hesla. Při tvorbě hesla je třeba dbát, aby bylo dostatečně silné. Společnosti často předkládají pro zajištění větší bezpečnosti pravidla, jak mají hesla vypadat. Zároveň by mělo být heslo pravidelně obměňováno, čímž lze předejít zneužití prozrazeného hesla.
   - *Co uživatel má* – Zde uživatel využívá pro přihlášení vlastnictví předmětu, který ho identifikuje (např. čipová karta). Tato metoda bývá kombinována s metodou založenou na znalosti, kdy po vložení daného předmětu musí uživatel ještě zadat tajné heslo.
   - *Co uživatel je* – V tomto případě se jedná o takzvanou biometrickou identifikaci. Jejími příklady mohou být otisk prstu či skenování sítnice.
   - *Co uživatel dělá* – Posledním způsobem, který uživatel může využít pro přihlášení, je identifikace založená na chování. Jedná se např. o rukou psaný podpis.

2. *Autentizace uživatele* – V okamžiku, kdy jsou přijaty přihlašovací údaje uživatele (jakéhokoliv z výše uvedených typů), musí systém ověřit, zda jsou zadané údaje správné. Pokud jakýkoliv detail (například špatný formát údajů nebo neexistence údajů v databázi uživatelů) je nesprávný, autentizační proces selže a nedojde k přihlášení uživatele.

   S autentizací souvisí pojem „systém jednotného přihlášení“ (*single sign-on – SSO*). Jedná se o zajištění přístupů do více aplikací pomocí jediného zadání přístupových údajů.

3. *Autorizace přístupu* – Tento krok zjišťuje, zda daný, nyní již přihlášený, uživatel má dostatečná oprávnění pro práci s požadovanými informacemi. Autorizace přístupu je založena na vhodně navrženém autorizačním konceptu celé společnosti a zajišťuje, že každý uživatel pracuje pouze s informacemi, které potřebuje k výkonu své práce. Snižuje se tím tedy riziko vynesení tajných informací mimo firmu.

V některých publikacích bývají první dva kroky spojovány do jednoho a označovány pouze jako autentizace. Poslední krok, autorizace, je více rozebrán v následující kapitole.

2.3 Autorizační koncept

Jak již bylo nastíněno v předchozí kapitole, autorizace, často označována také jako *řízení přístupu* (*access control*), zjišťuje, zda uživatel může pracovat s danou informací. Zároveň určuje, jakým způsobem smí s touto informací nakládat (číst, zapisovat, spouštět program a pod.).

Na rozdíl od identifikace a autentizace, které fungují na principu *all or nothing* (vše nebo nic – buď se činnost zdaří, nebo se nezdaří a žádný stav mezi těmito neexistuje), autorizace obsahuje mnoho variant mezi těmito hraničními stavy (např. uživatel může mít možnost číst dokument, ale už nemusí mít práva k tomu, aby daný dokument jakýmkoliv způsobem upravoval).

Při zavádění autorizace je možné vybrat si z několika typů řízení přístupu (těmi se zabývá kapitola 2.3.1). Existuje několik principů, které ještě více zajišťují zabezpečení systému. Tyto principy je možné určitým způsobem zavést do všech typů řízení přístupu. Stewart [10] zmiňuje jako příklady princip minimálního oprávnění a oddělení povinností, kterým se více věnovala kapitola 2.2.1.

Dále pak ještě uvádí *omezení denního času* (*time-of-day restrictions*). Toto omezení definuje pouze určité denní doby, často dokonce i určité dny v týdnu, kdy daný uživatel může přistoupit k požadovaným datům. Tento princip se využívá například k zajištění, aby se uživatel nemohl k citlivým datům dostat v nejrušnější pracovní době, kdy hrozí, že obsah zahlédne (nebo ho úmyslně sleduje) nepovolaná osoba.

2.3.1 Typy řízení přístupu

Existuje několik způsobů, jak k problematice autorizace přistupovat. Liší se tím, jakým způsobem rozhodují o autorizaci uživatele k určité činnosti. Mezi hlavní patří *Discretionary Access Control*, *Mandatory Access Control* a *Role-Based Access Control*.

2.3.1.1 Discretionary Access Control (DAC)

Discretionary Access Control, což se dá do českého jazyka přeložit jako *diskreční řízení přístupu* (ve slovníku cizích slov [15] je uvedeno, že slovo diskrece znamená *„zachování důvěrných informací v tajnosti, diskrétnost“*).Tento přístup je založen na definování sady pravidel.

Jak uvádějí De Capitani di Vimercati, Foresti a Samarati [16], tato pravidla si lze představit jako trojice *subjekt* (uživatel), *akce* a *objekt*. V okamžiku, kdy uživatel chce provést akci s určitým objektem, systém nejprve musí zkontrolovat, zda takováto trojice uživatele, akce a objektu existuje.

Prostor, kde tyto trojice uchovávat, lze reprezentovat různými způsoby. De Capitani di Vimercati, Foresti a Samarati [16] uvádějí čtyři základní možnosti:

- *Matice přístupu* (*access matrix*) – Systém zajišťující kontrolu přístupu má vytvořenou matici, ve které každý řádek představuje jeden subjekt a každý sloupec reprezentuje jeden objekt. Políčko v řádku s a sloupečku o poté obsahuje seznam akcí, které může subjekt s provádět s objektem o. Přestože je velmi jednoduché matici implementovat přes dvourozměrné pole, její velkou nevýhodou je to, že mnoho subjektů nemá definované akce pro všechny objekty. Tudíž pak v poli vzniká mnoho zbytečných (prázdných) políček. Příklad takové matice je vidět v tabulce 2.1.

Tabulka 2.1: Matice přístupu [16]

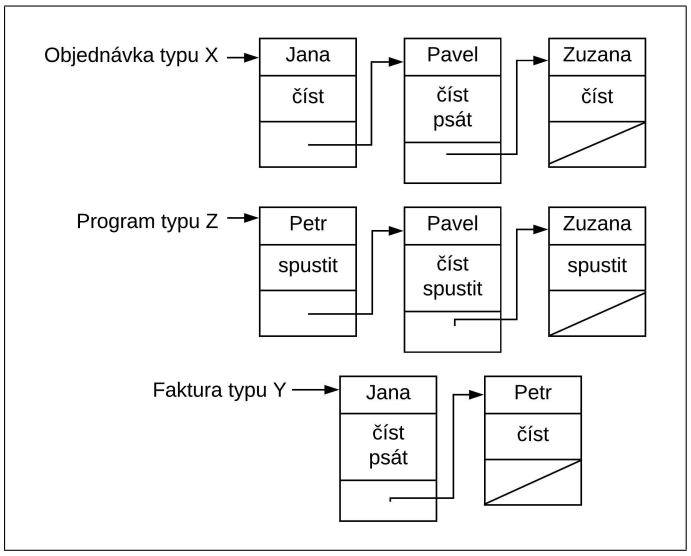
	Objednávka typu X	Faktura typu Y	Program typu Z
Jana	číst	číst, psát	
Petr		číst	spustit
Pavel	číst, psát		číst, spustit
Zuzana	číst		spustit

- *Autorizační tabulka* (*authorization table*) – Políčka matice přístupu, která nejsou prázdná, jsou v tomto modelu uložena v tabulce s atributy subjekt, akce, objekt. Je běžné, že tato tabulka je seskupena a seřazena podle potřeb systému, například podle subjektu, nebo objektu. V tabulce 2.2 je možné vidět data odpovídající matici přístupu z tabulky 2.1 uložená v autorizační tabulce.

Tabulka 2.2: Autorizační tabulka [16]

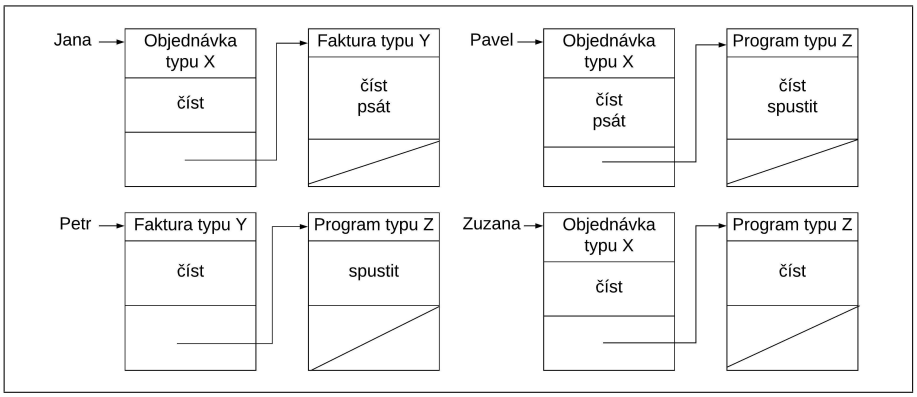
Subjekt	Akce	Druh objektu
Jana	číst	Objednávky typu X
Jana	číst, psát	Faktury typu Y
Petr	číst	Faktury typu Y
Petr	spustit	Programy typu Z
Pavel	číst, psát	Objednávky typu X
Pavel	číst, spustit	Programy typu Z
Zuzana	číst	Objednávky typu X
Zuzana	spustit	Programy typu Z

- *Kontrolní list přístupu* (*access control list – ACL*) – Pro každý objekt je vytvořen seznam subjektů, které s sebou nesou i množiny akcí, které mohou provádět s objektem. Obrázek 2.1 znázorňuje ACL s daty odpovídajícími matici přístupu z tabulky 2.1.



Obrázek 2.1: ACL [16]

- *Kvalifikace* (*capability*) – Dá se říct, že tento model je opakem ACL. Pro každý subjekt totiž vytvoří seznam objektů a u každého objektu má uloženou množinu akcí, které může subjekt s daným objektem provádět. Na obrázku 2.2 je ukázán model kvalifikace odpovídající matici přístupu z tabulky 2.1.



Obrázek 2.2: Kvalifikace [16]

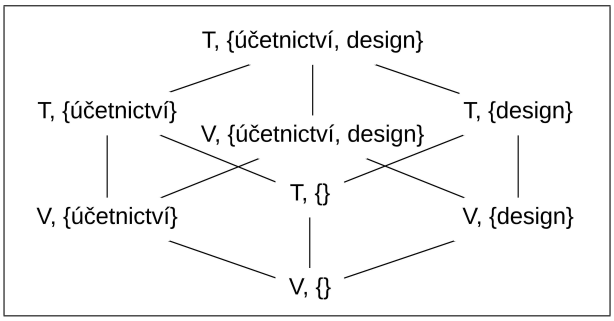
Mezi nespornou výhodu DAC patří možnost definovat abstrakci pro subjekty a objekty. Tím je umožněno vytvářet hierarchickou strukturu, nazývanou jako uživatelské skupiny pro subjekty a třídy objektů pro objekty. Naopak nevýhodou tohoto přístupu je bezbrannost vůči spuštění škodlivých programů.

2.3.1.2 Mandatory Access Control (MAC)

Mandatory Access Control, do češtiny možné přeložit jako *povinné řízení přístupu*, je přístup založený na klasifikaci subjektů a objektů. Nejčastější formou klasifikace je použití páru bezpečnostní stupeň (*security level*) a kategorie. Množina hodnot bezpečnostních stupňů je uspořádanou množinou, kdežto množina kategorií je neuspořádaná. Když využíváme tohoto páru, získáváme pak částečně uspořádanou množinu.

V takto částečně uspořádané množině je využívána relace dominance ($\geq$): Pro dvě přístupové třídy platí, že bezpečnostní stupeň první třídy je větší než bezpečnostní stupeň druhé třídy a zároveň množina kategorií první třídy obsahuje množinu kategorií druhé třídy.

Modelem tohoto přístupu je *mřížka*, kterou tvoří tyto přístupové třídy a jejich vztahy dominance. Příklad je vidět na obrázku 2.3, kde jsou dva stupně bezpečnosti (veřejné = V a tajné = T, kde T $\geq$ V) a dvě kategorie (účetnictví a design).



Obrázek 2.3: Mřížka MAC [16]

Jednou z nevýhod přístupu MAC je, že všechny subjekty i objekty musí být klasifikovány, což jde často špatně zajistit. Navíc, jelikož je přístup vyhodnocován pouze na základě této klasifikace, může být v konečném důsledku moc přísný. Zároveň má však tento přístup, jak uvádí Stewart [10], často nízkou granularitu. Tento problém může zlepšit zavedení principu *need-to-know* (potřeba vědět), který říká, že přístup je umožněn pouze uživatelům, kteří byli přiřazeni na práci, která požaduje využití daných informací. Uživatel tedy musí nejen splňovat dostatečný bezpečnostní stupeň a kategorii, ale i potřebovat požadované informace ke své práci.

2.3.1.3 Role-based Access Control (RBAC)

Pro vytvoření velkých a komplexních modelů vznikl *Role-Based Access Control* (do češtiny přeložené jako *řízení přístupu založené na rolích*). Ten se skládá, jak uvádí Osborn [17], ze tří hlavních komponent a několika různých mapování. Komponentami jsou:

- *uživatelé* – na rozdíl od subjektů používaných v předchozích přístupech nejsou chápáni jako procesy vykonávající zadané příkazy, ale představují samotné lidské bytosti využívající systém;
- *povolení* – spojují jednotlivé objekty s příslušnou operací (módem přístupu), který je validní pro daný objekt – například pro tiskárnu může být jako validní brána operace *užívat*, kdežto pro textový soubor operace *číst* a *psát*;
- *role* – často jsou navržené tak, aby odpovídaly příslušným pracovním pozicím – pro jejich odlišení je vhodné, aby měly každá unikátní název.

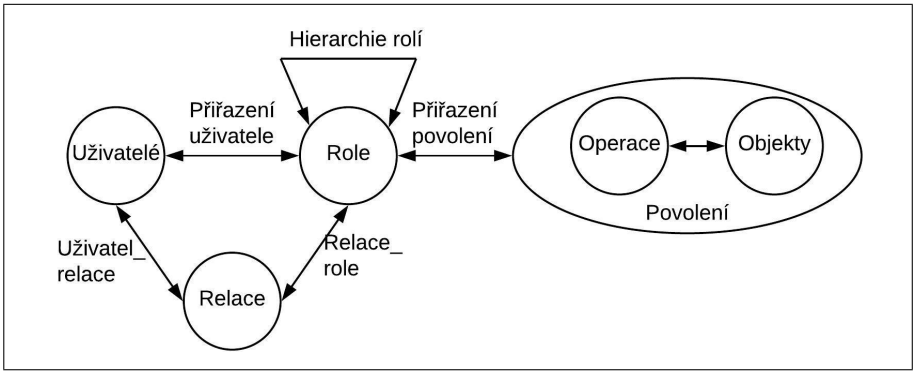
Mezi základní typy mapování patří:

- *mapování přiřazení uživatelů* (*user assignment mapping*) – přiřazuje uživatelům jednotlivé role (platí kardinality, že více uživatelů může mít zapsáno stejnou roli a naopak jeden uživatel může mít zapsáno více rolí);
- *mapování přiřazení povolení* (*permission assigment mapping*) – přiřazuje rolím jejich povolení (stejně jako mapování přiřazení uživatelů má kardinalitu více – více);
- *mapování hierarchie rolí* (*role hierarchy mapping*) – určuje hierarchii mezi rolemi s kardinalitou více – více (zároveň však má omezení, které stanovuje, že v hierarchii nesmí vzniknout cykly – jinak by mohla nastat situace, že více různých rolí má totožnou množinu povolených operací);
- *mapování relací* (*session mapping*) – vyjadřuje dobu, kdy jsou role aktivovány uživateli (kardinalita mezi relacemi a rolemi je více – více, avšak pouze jeden uživatel může být namapován na danou relaci).

Na obrázku 2.4 jsou dány do souvislostí výše popsané pojmy. Vyjadřuje základní myšlenku, jak RBAC funguje.

RBAC řeší, stejně jako všechny ostatní typy řízení přístupu, problematiku oddělení povinností. Dělá to pomocí omezení, která určují, které role by pro dodržení SOD neměly být připsány stejnému uživateli. Lze zvolit buď statické, nebo dynamické oddělení povinností.

U statického oddělení povinností se omezení vztahují na mapování přiřazení uživatelů. Stanovuje, že jeden uživatel může být namapován maximálně na jednu roli z množiny rolí, která je určená daným omezením. Dynamické oddělení povinností nezasahuje do přiřazování uživatelů, ale stanovuje, že konfliktní role nemohou být spuštěny ve stejné relaci.



Obrázek 2.4: Komponenty a mapování RBAC [17]

2.3.2 Autorizační koncept v SAP ERP systému

O autorizačním konceptu v SAP ERP systému je napsáno mnoho několika set stránkových knih. Například publikace *Authorization in SAP Software: Design and Configuration* [18], ze kterého tato práce mimo jiné čerpá, se zabývá pouze autorizací v SAP systémech a má 684 stran.

Tento údaj je zde uveden jako názorná ukázka, že autorizační koncept v souvislosti se SAP systémem je velmi široké téma a pokud by měla tato práce obsáhnout všechny detaily, její délka by rapidně vzrostla. Proto je v této kapitole daná problematika řešena velmi zkráceně, spíše jako hrubý přehled. Čtenáři, kteří by měli o téma hlubší zájem, nechť jsou odkázáni na již zmíněnou knihu Authorization in SAP Software – Design and Configuration [18].

Lehnert, Boniz a Justice [18] pohlížejí na autorizační koncept ze dvou pohledů:

- *technický autorizační koncept* – definuje všechny možnosti, jak mohou být v programu implementovány a prováděny kontroly autorizace a jak pomocí procedur přiřadit autorizace uživateli;

- *business (podnikový) autorizační koncept* – je založen na funkčních a organizačních požadavcích (vychází ze struktury organizace) a určuje, jak by měl být technický autorizační koncept pro danou společnost implementován.

SAP ERP systém využívá pozitivní autorizační koncept. To znamená, že každý uživatel nemá zprvu žádná povolení a je nutné přesně definovat, jaké akce vůči kterým objektům může vykonávat.

Jelikož autorizační koncept v SAP ERP využívá řízení přístupu RBAC, je založen na rolích, které jsou přiřazovány jednotlivým uživatelům. Pro každého z uživatelů je vytvořený *hlavní uživatelský záznam* (*user master record*), do kterého je kromě hlavních informací o uživateli (uživatelské jméno, osobní

data, uživatelské nastavení, přiřazené autorizace, …) zaznamenávána veškerá aktivita uživatele – všechny přístupy do systému a práce s dokumenty.

Z toho důvodu je nutné dodržovat zásadu *one person – one user* (jedna osoba – jeden uživatel), často označovanou jako *princip identity*. Tato zásada má dvě části:

- jeden uživatel musí být přidělen pouze jedné osobě (kvůli trasovatelnosti – i s odstupem času musí být možné zjistit, kdo danou akci provedl);
- jedna osoba má přiřazeného pouze jednoho uživatele (jinak hrozí porušení zásady oddělení povinností – viz kapitola 2.2.1).

Existuje situace, kdy se tato zásada porušuje. Zaměstnanci je přiřazen další uživatel, který byl již dříve používán někým dalším. Těmto uživatelům se může říkat různě, používají se například názvy *emid* (*emergeny ID* = nouzové identifikační číslo) nebo *firefighter* (hasič) uživatel. Jsou přiřazováni v produkčních systémech uživatelům, kteří potřebují provést pro ně neobvyklou akci ve výjimečných situacích [19]. Jejich užívání uživatelem je časově omezeno (například na dobu patnácti minut) a pečlivě monitorováno – veškerá aktivita je zaznamenána, stejně jako data o samotném přiřazení tohoto uživatele zaměstnanci [20].

Díky tomu stále platí, že každá akce je možná přiřadit určité osobě. I když ji provedl tento emid uživatel, existuje záznam o tom, který zaměstnanec měl v době vykonání akce tohoto uživatele přiřazeného.

Pro pochopení, jak autorizační koncept v SAP systémech funguje, je klíčových několik pojmů a vztahy mezi nimi. Přímo v oficiální on-line knihovně SAP se této problematice věnuje několik stran ([21], [22], [23]) ze kterých je vše dobře pochopitelné, a proto z nich následující část práce vychází.

Jednotlivé prvky systému, které mají být chráněny, se seskupují do *autorizačních objektů* (*authorization objects*). V jednom autorizačním objektu může být jeden až deset polí (prvků). Tato pole nemají hodnoty.

Na autorizační objekty jsou navázány *autorizace* (*authorizations*), ve kterých jsou jednotlivým polím přiřazeny hodnoty – každé pole může nabývat jednu nebo více hodnot. Právě autorizace umožňují uživateli provádět určité funkce v systému.

V případě potřeby je možné seskupit autorizační objekty do *autorizačních tříd objektů* (*authorization object class*). Toto seskupení se dělá pro jednotlivé oblasti společnosti (například účetní jednotka). V jedné třídě může být až sto padesát objektů.

Základním prvkem pro definování uživatelských oprávnění jsou *role*. Ty jsou založeny na organizační struktuře společnosti – mohou představovat pracovní pozici, popřípadě její určitou část. Obsahují jednotlivé transakce, zprávy, aplikace a pod., ke kterým má uživatel přístup.

Mezi rolemi je možné odvozování. Tzv. *odvozená role* (*derived role*) se používá v případě, že autorizace pro určité pozice napříč organizací jsou stejné a je

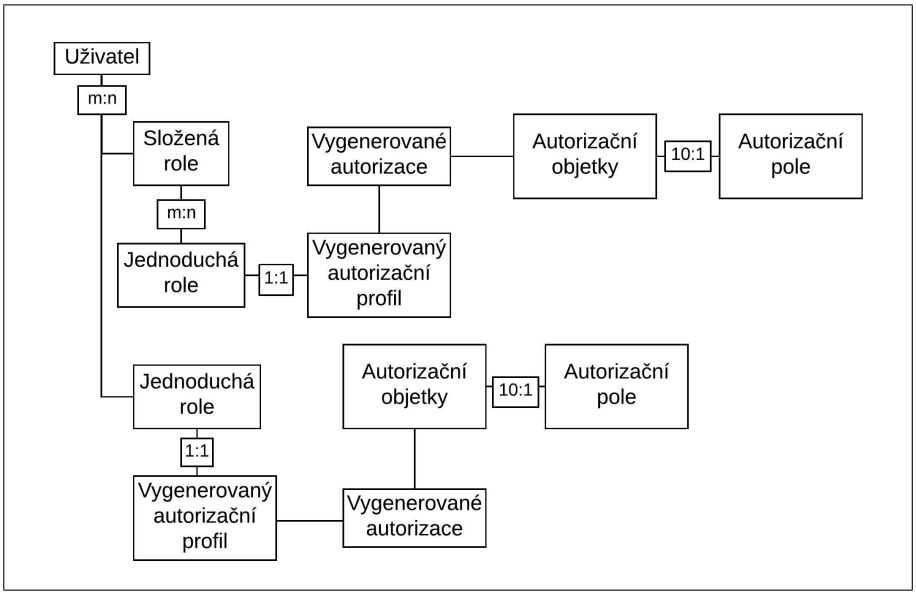
tedy nutné pouze změnit organizační nastavení role s použitím stejných autorizací. V tu chvíli se vytvoří obecná role, od které se poté odvozují jednotlivé odvozené role pro organizační jednotky.

Druhým speciálním typem rolí je *role složená* (*composite role*). Skládá se z libovolného počtu jednoduchých rolí. Vzniká například z důvodu, aby představovala jednu pracovní pozici, která pokrývá více rolí.

Z role je pomocí *generátoru profilů* (*profile generator*) automaticky vytvořen *autorizační profil* (*authorization profile*). Jedná se o list autorizací, které jsou požadovány jednotlivými funkcemi (transakce, report, aplikace, …) v roli. Generátor profilů automaticky všechny autorizace seskupí a některým předvyplní výchozí hodnoty. U zbylých je ještě nutné hodnoty zadat.

Profil je poté přiřazen generátorem profilů k uživateli, přesněji řečeno do hlavního uživatelského záznamu. Odtud se při přihlášení uživatele do systému nahraje do *uživatelského menu* (*user menu*) každá autorizace, která je obsažena v některém z profilů přiřazených danému uživateli.

Toto uživatelské menu slouží poté pro kontrolu oprávnění uživatele. V okamžiku, kdy chce uživatel provést nějakou akci, program kontroluje, že všechny hodnoty autorizace v příslušném poli autorizačního objektu jsou načteny v uživatelském menu. Přiřazování oprávnění uživateli v SAP systému je znázorněno na obrázku 2.5



Obrázek 2.5: Přiřazení oprávnění uživateli v SAP systému [24]

To, zda, kde a jak jsou autorizace kontrolovány, určuje programátor. Pro provedení jedné operace může být potřebné více než jedna autorizace.

On-line knihovna SAP [25] rozděluje postup připsání oprávnění uživateli na pět kroků:

1. připsat transakce, které uživatel potřebuje k výkonu své práce, a jejich typy přístupových práv (číst, spouštět, upravovat, …) jednotlivým pozicím;

2. vytvořit role odpovídající pracovním pozicím a následně připojit požadované transakce;

3. vygenerovat a upravit autorizační profily z připravených rolí;

4. přiřadit role uživatelům;

5. aktualizovat hlavní uživatelský záznam pomocí vygenerovaných profilů.

2.4 Metodika BPMN

V dalších částech práce jsou pro znázornění různých procesů použité diagramy vytvořené podle standardu BPMN (*Business Process Model and Notation* – Modelování a notace podnikových procesů). Tento standard, vydaný skupinou OMG (*Object Management Group* – Skupina správy objektů), umožňuje grafické znázornění podnikových procesů. Notace se zaměřuje na srozumitelnost znázornění i pro netechnické uživatele [26].

V této kapitole jsou uvedeny a vysvětleny prvky standardu BPMN, které jsou použité při tvorbě diagramů v dalších částech práce. Jedná se o stručný přehled, který má čtenáři usnadnit pochopení zmíněných diagramů. Tento přehled vychází z knihy *BPMN Method and Style* [27].

V diagramech této práce jsou použité následující prvky:

- aktivita (*activity*);
- brána (*gateway*);
- událost (*end event*);
- sekvenční tok (*sequence flow*), tok zprávy (*message flow*), asociace (*association*);
- bazén = kontext(*pool*), plavecká dráha = oddíl kontextu (*swim lane*);
- artefakty – datový objekt (*data object*), datové sklady (*data store*), anotace (*annotation*).

V následujících kapitolách jsou jednotlivé prvky blíže vysvětleny.

2.4.1 Aktivity

Aktivity představují stavební prvky diagramů – reprezentují jednotlivé činnosti, které se v průběhu procesu provádějí. Dělí se na tři skupiny:

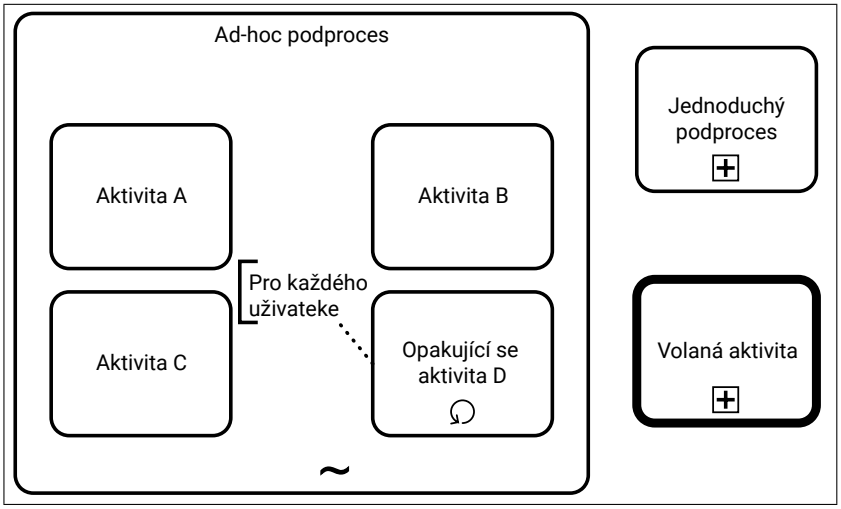
- *Úloha* – Úloha, v anglickém jazyce *task*, představuje dále nedělitelný proces uvnitř modelovaného procesu (aby byla úloha splněna, musí doběhnout všechny činnosti, ze kterých se skládá). V práci se pracuje se třemi typy úloh, které se rozlišují obrázkem v levém horním rohu úlohy:
  - *manuální úloha* – je prováděna bez jakéhokoliv použití počítačového systému;
  - *uživatelská úloha* – je vykonána uživatelem, ale používá počítačový systém;
  - *servisní úloha* – je automatizovaná úloha prováděná pouze počítačovým systémem bez zásahu uživatele.

  Na obrázku 2.6 jsou jednotlivé typy úloh zobrazeny.

Obrázek 2.6: Druhy úloh BPMN

- *Podproces* – Podproces (*Sub-process*) reprezentuje soubor činností (proces) uvnitř modelovaného procesu. Jednotlivé činnosti jsou pro každý podproces blíže specifikované – na rozdíl od úloh je podproces dále dělitelný.V práci jsou používané dva typy podprocesů:
  - *ad-hoc podproces* – skládá se z několika aktivit, které však nemusí proběhnout (ani začít) všechny;
  - *jednoduchý podproces* – používá se pro dekompozici konkrétního procesu.
- *Volání aktivity* – Volání aktivity (*Call Activity*) je speciální typ podprocesu, který však nepředstavuje dekompozici jednoho konkrétního procesu. Tento podproces je možné použít opakovaně na různých místech modelu – i v různých procesech.

V případě, kdy je nutné, aby aktivita probíhala opakovaně, je možné použít *opakující se aktivitu*. Ta značí, že aktivita probíhá, dokud není splněna podmínka, která je k aktivitě připojena asociací. Typy podprocesů, opakující se aktivita a volání aktivity jsou znázorněny na obrázku 2.7.



Obrázek 2.7: Typy podprocesů, opakující se aktivita a volání aktivity v BPMN

2.4.2 Brány

Brány se využívají v okamžiku, kdy je z nějakého důvodu nutné proces rozvětvit. Dělí se na:

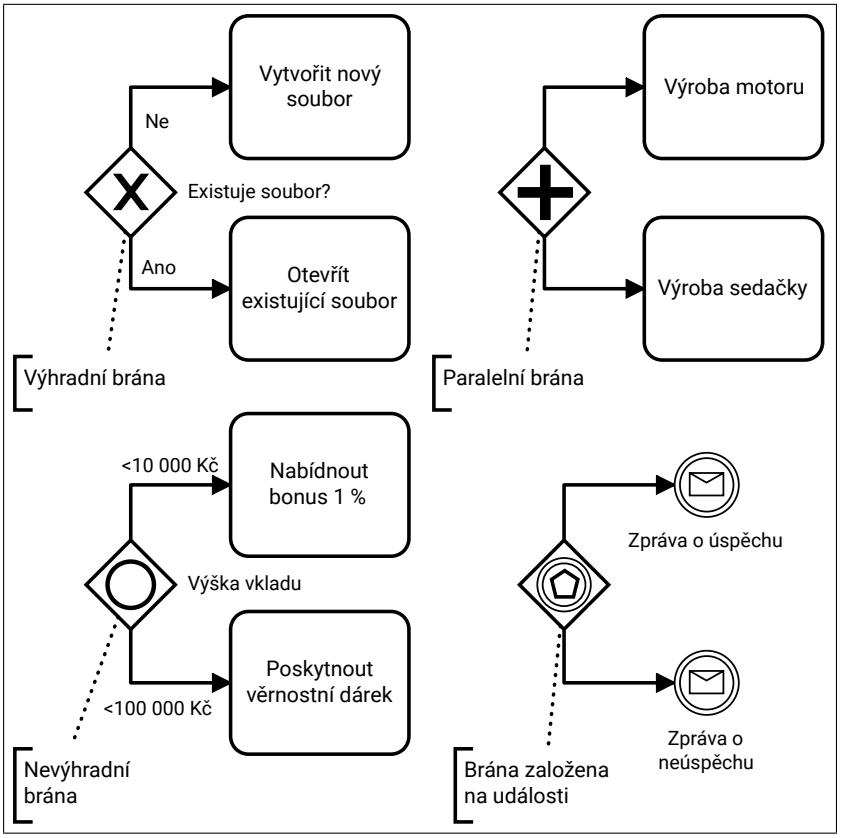
- *výhradní (XOR) brána* – právě jedna z možností je zvolena;
- *paralelní (AND) brána* – probíhají všechny výstupní sekvence paralelně;
- *nevýhradní (OR) brána* – podmínky jsou nezávislé (může se zvolit jedna až všechny možnosti);
- *brána založena na události* – rozhodnutí záleží na určité události (například přijetí jedné zprávy spouští jednu větev procesu, přijetí jiné zprávy spouští druhou větev procesu).

Pokud se má rozvětvený proces v určitém místě opět spojit, je nutné, aby ke spojení byla použita brána, která zařídila rozvětvení procesu. Všechny typy bran jsou zobrazeny na obrázku 2.8.

2.4.3 Události

Události se dělí na čtyři typy:

- *Počáteční událost* (*start event*) – Tato událost zahajuje modelovaný proces.
- *Přechodová událost* (*intermediate event*) – Přechodová událost nastává během procesu – proces ani nezahajuje, ani neukončuje. Jsou dva typy



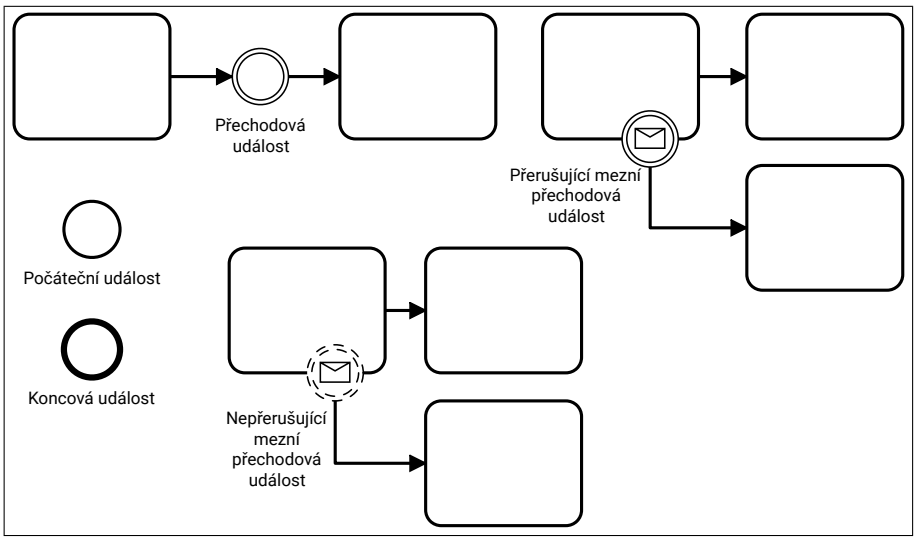
Obrázek 2.8: Druhy bran BPMN

přechodových událostí – *generující* (*throwing)* a *čekající* (*catching*) přechodová událost. Generující přechodová událost vytváří (a případně odesílá) určitý signál nebo zprávu. Čekající přechodová událost čeká, dokud neobdrží určitý signál nebo zprávu.

- *Mezní přechodová událost* (*boundary intermediate event*) – Tato událost nepředstavuje čekání. V průběhu určité aktivity událost naslouchá a v okamžiku obdržení signálu je spuštěn jiný tok (tok výjimky), než jakým by proces pokračoval, pokud by událost signál neobdržela. Mezní přechodová událost může být buď *přerušující*, nebo *nepřerušující*. V případě přerušující události je probíhající aktivita zastavena a proces pokračuje pouze po toku výjimky. Pokud se jedná o nepřerušující událost, pak se spustí tok výjimky, avšak probíhající aktivita se dokončí a proces pokračuje i po normálním toku.

- *Koncová událost* (*end event*) – Touto událostí modelovaný proces končí.

Přehled typů událostí je zobrazen na obrázku 2.9.

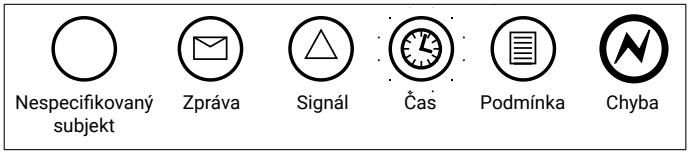


Obrázek 2.9: Typy počátečních událostí BPMN

Různé typy událostí mohou být různého druhu – jsou ovlivňovány jiným subjektem. Těmito subjekty mohou být:

- *nespecifikovaný subjekt* – subjekt, na který událost reaguje, není blíže specifikován (událost může být počáteční nebo koncová);
- *zpráva* – událost reaguje na zprávu, buď zprávu přijímá, nebo ji odesílá (může se jednat o událost počáteční, mezní přechodovou – v těchto dvou případech je zpráva přijímána– nebo o mezní událost, kdy může být zpráva jak přijímána, tak odesílána, nebo koncovou událost – tehdy je zpráva odesílána);
- *signál* – událost reaguje na signál, buď ho přijímá, nebo odesílá (signál se od zprávy liší tím, že může být vyslán z více míst procesu a zároveň může být na více místech procesu přijímán, avšak typy událostí, kdy může být signál přijímán a kdy vysílán, jsou stejné jako u zprávy);
- *čas* – událost vždy reaguje na čas (uběhne určitá doba, nastane určité datum, …);
- *podmínka* – událost čeká na splnění určité podmínky (například proces pokračuje/začne, když je sklad prázdný).
- *chyba* – událost reaguje na chybu v procesu (pokud podproces skončí špatným výsledkem – např. kontrola kreditu a kredit chybí – může na tuto chybu reagovat mezní přechodová událost a v případě špatného výsledku spustit tok výjimky).

Přehled subjektů ovlivňující události je zobrazen na obrázku 2.10.

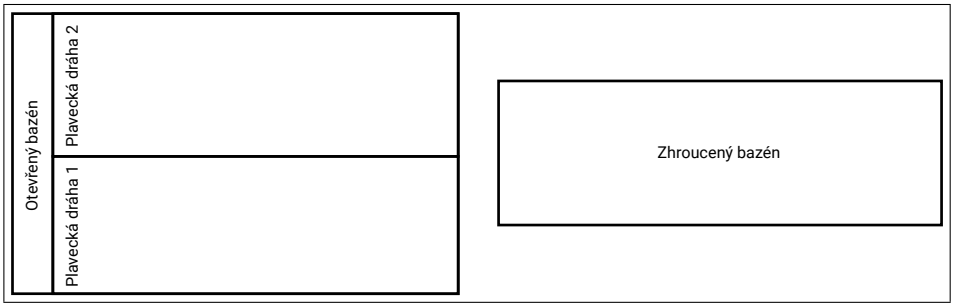


Obrázek 2.10: Subjekty ovlivňující události v BPMN

2.4.4 Bazén a plavecké dráhy

Bazén a *plavecké dráhy* (neboli *pool* a *swimlines*, jak jsou často i v češtině označovány) slouží k organizaci činností. Určují, kdo je zodpovědný za danou aktivitu v procesu. Bazén odděluje různé části organizace a systémy účastnící se procesu. Může být znázorněný jako otevřený, kdy jsou zobrazeny aktivity probíhající uvnitř bazénu, nebo jako takzvaně zhroucený. Zhroucený bazén nezobrazuje detail procesu, slouží pouze pro znázornění komunikace účastníka, kterého představuje, s jinými účastníky procesu.

Plavecké dráhy slouží k rozdělení jednotlivých bazénů. Jednotlivé aktivity jsou do plaveckých drah rozděleny na základě funkcí nebo rolí (například každá plavecká dráha představuje jednu pracovní pozici ve firmě). Bazén a plavecké dráhy jsou zobrazeny na obrázku 2.11.



Obrázek 2.11: Bazény a plavecké dráhy v BPMN

2.4.5 Artefakty

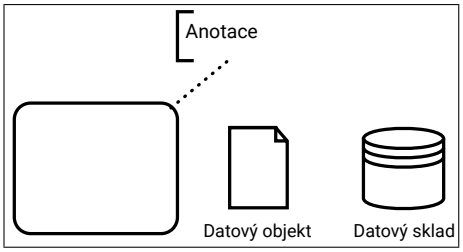
Artefakty umožňují přidávat do modelu doplňující informace. Ty slouží pro jeho lepší čitelnost.

Datový objekt představuje dočasná data v procesu. Mohou k němu přistupovat účastníci daného procesu (jednotlivé plavecké dráhy v bazénu), ale ne mimo proces. V okamžiku, kdy proces skončí, datový objekt zaniká.

Datový sklad reprezentuje trvale ukládaná data (například v databázi). Nepředstavuje však celou databázi, jen její část. Přistupovat k datovým skladům se dá jak uvnitř aktuálního procesu, tak i entitami mimo aktuální proces. Na rozdíl od datového objektu datový sklad existuje i po skončení procesu.

Anotace nijak nezasahují do procesu. Slouží pouze k zpřehlednění a snazšímu pochopení modelu.

Všechny artefakty jsou znázorněny na obrázku 2.12.

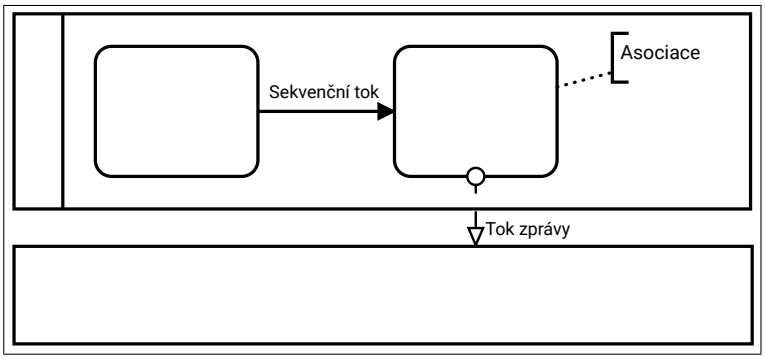


Obrázek 2.12: Artefakty v BPMN

2.4.6 Toky a asociace

Toky a asociace jsou používány pro spojování aktivit, bran, událostí a ostatních částí procesu. Existují tři typy toků, které jsou zobrazeny na obrázku 2.13:

- *Sekvenční tok* – Znázorňuje posloupnost činností v procesu. Vždy začíná i končí v aktivitě, bráně nebo události a nikdy nesmí přesáhnout hranice bazénu ani podprocesu.
- *Tok zprávy* – Představuje pohyb zpráv přes hranice bazénu. Zobrazuje komunikaci mezi jednotlivými bazény.
- *Asociace* – Používá se pro připojení artefaktů k jiným objektům procesu. V případě, že je asociace zobrazena se šipkou, znamená to, že připojovaný objekt je buď vstup (šipka směřuje od připojovaného objektu), nebo výsledek (šipka směřuje do připojovaného objektu).



Obrázek 2.13: Toky v BPMN

Kapitola 3

Analýza závodu společnosti X

Toto je druhá kapitola teoretické části. Zatímco první kapitola se zaměřila na průzkum literatury a vysvětlení důležitých pojmů, tato zkoumá přímo prostředí (tedy oddělení logistiky výrobního závodu), pro které má být autorizační koncept navržen. Celá analýza je vypracována na základě rozhovorů se zaměstnanci společnosti, kteří se zaměřují na jednotlivé analyzované oblasti[20], [28], [29].

Hlavní činností závodu je finální montáž strojů (produktů společnosti) ze součástek, které jim dodává mateřský závod. SAP ERP je v závodě využíván především pro podporu procesů logistiky (získávání materiálu potřebného pro výrobu, uskladnění a organizaci materiálu ve skladech a dodání potřebného materiálu na správnou montážní linku). Ostatní oblasti využívají jiné systémy především z ekonomických a legislativních důvodů.

V následujících kapitolách je provedena analýza procesů oblasti logistiky. Aby bylo lépe pochopitelné, kdo je za jednotlivé kroky v procesech zodpovědný, je v první kapitole popsána struktura společnosti (především oblast logistiky). V příloze B jsou struktura i jednotlivé procesy znázorněny graficky pomocí diagramů.

3.1 Struktura závodu

Jako každý závod a každá společnost, i tento výrobní závod má v čele své vedení, manažery závodu. Ti dohlížejí na celý chod a na správné fungování závodu. Jsou přímými nadřízenými vedoucích jednotlivých oblastí, na které se závod dělí.

Těchto oblastí je dohromady osm:

- řízení kvality;
- finance;
- nákup;

- prodej;
- řízení lidských zdrojů;
- výroba;
- informační technologie;
- logistika.

V příloze B je na obrázku B.1 znázorněná struktura společnosti s bližším detailem zaměřeným na oblast logistiky, kterou se celá tato práce zabývá. Bíle jsou znázorněné oblasti a oddělení, šedě pracovní pozice. V následujících kapitolách jsou jednotlivé oblasti struktury společnosti blíže specifikovány.

3.1.1 Řízení kvality

Toto oddělení koordinuje a usměrňuje činnosti a procesy při vývoji a výrobě stroje s ohledem na kvalitu produktu. Kontroluje kvalitu součástek dovezených do závodu (od mateřského závodu nebo od lokálního dodavatele), provádí laboratorní zkoušky a zjišťuje kvalitu vyrobených strojů.

Zároveň určuje, které součástky a stroje je nutné podrobit kontrole. Navíc provádí školení v oblasti kvality pro zaměstnance závodu.

3.1.2 Finance

Oblast Finance zajišťuje finanční management závodu. Pro zajištění dlouhodobé hospodářské stability závodu spolupracuje účetní oddělení (vedení účetních knih), controlling (řízení podniku), a treasury (správa finančních prostředků). Zároveň do této oblasti spadá oddělení právních záležitostí.

3.1.3 Nákup

Tato oblast zajišťuje nákup výrobního a režijního materiálu a služeb pro závod. Zaměstnanci se starají o tvorbu optimální struktury lokáních dodavatelů, smluvní zajišťování dodávek a snižování materiálových nákladů.

S dodavateli vyjednávají smluvní podmínky a následně kontrolují, že jsou tyto podmínky dodržovány. Komunikují s dodavateli a zodpovídají za celý proces pořízení materiálu od lokálního dodavatele.

3.1.4 Informační technologie

Tato oblast provozuje informační systémy ve spolupráci se všemi pracovišti, která jsou za IT nějakým způsobem zodpovědná. Stará se o aktualizace a základní vývoj systému a správu hardwaru. Zároveň má na starost tvorbu nových uživatelů a přiřazování oprávnění klíčových uživatelů běžným uživatelům.

3.1.5 Prodej

Tato oblast má na starost prodej strojů v regionu, kde se závod nachází. Skrze jednotlivá oddělení se stará o rozvoj a plánování dealerské sítě a analýzu tržní situace v regionu, o tvorbu a strategii cen produktů, plánování odbytu a správu zakázek.

Navíc je oblast zodpovědná za prodej originálních náhradních dílů a příslušenství, stejně jako zajištění poprodejního servisu produktů, v regionu. K této činnosti se mimo jiné řadí i vyřizování záruk.

3.1.6 Řízení lidských zdrojů

Oblast má na starosti činnosti a procesy související se zaměstnanci závodu, včetně ochrany a bezpečnosti závodu. Mezi hlavní činnosti oblasti patří plánování lidských zdrojů a nábor zaměstnanců, péče o zaměstnance (vedení personální administrativy), vzdělávání a rozvoj zaměstnanců, rozvoj hodnotících systémů (systém mezd), sociální služby a programy pro podpory zdraví a veškerá jiná komunikace se zaměstnanci.

Kromě komunikace se zaměstnanci spadají do této oblasti i vnější vztahy závodu. Například zajišťuje koordinaci oficiálních návštěv zástupců veřejných institucí v závodě nebo koordinaci příprav návrhů legislativních a nelegislativních změn v zemi daného závodu.

3.1.7 Výroba

Oblast zajišťuje správu, monitorování, řízení a optimalizaci procesů výroby strojů v závodě. V případě, že se v závodě vyrábí meziprodukty, zodpovídá i za proces jejich výroby.

Do oblasti výroby spadají kromě řízení výroby i samotné výrobní a montážní linky. Pokrývá tedy nejen procesy výroby strojů, ale i údržbu a technický servis montážních linek.

3.1.8 Logistika

Oblast se stará o plánování a řízení všech logistických aktivit závodu. Za správnost fungování oblasti zodpovídá manažer logistiky. Oblast se dělí na dvě hlavní oddělení:

- *Dispozice* – Toto oddělení zajišťuje dodávky nakupovaných dílů a materiálů od dodavatelů (jak od mateřského závodu, tak od lokálních dodavatelů). Cílem oddělení je zajistit jistotu materiálového toku tak, aby nakupovaný materiál a součástky byly při optimálních nákladech, ve správné kvalitě, ve správném množství a ve správném čase na správném místě.

Na oddělení je určen jeden pracovník jako klíčový. Ten se kromě ostatních povinností oddělení dispozic stará o přiřazování rolí uživatelům, schvalování žádostí a o správnost dat zanesených v systému.

- *Operativní logistika* – Jde o oddělení, které provádí příjem materiálu a koordinuje tok a evidenci palet v závodě. Zároveň má na starost procesy související se skladem závodu a interní přepravu materiálu.

  Celé oddělení má na starosti manažer operativní logistiky. Ten zodpovídá za útvary, na které se oddělení dále dělí:

  - *Řízení obalového toku* – Útvar koordinuje oběh a evidenci palet v závodě, stará se o odvoz prázdných obalů, popřípadě o expedici dílů v obalech zabalených, k dodavatelům, zajišťuje skladování obalů, opravu poškozených obalů a šrotaci obalů.

    Za útvar zodpovídá manažer řízení obalového toku. Ten zodpovídá za jednotlivé pracovníky útvaru a za hladký chod útvaru.

  - *Centrální příjem* – Tento útvar koordinuje přijíždějící přepravní prostředky materiálu (nákladní automobily, vlaky a podobně) na vykládku dílů, popřípadě na nakládku prázdných obalů. Řídí nákladní vozidla v areálu závodu a optimalizuje jejich pohyb po areálu. Zároveň provádí příjem dováženého materiálu.

    Za jednotlivé pracovníky příjmu zodpovídá manažer příjmu. Ten se stará o správnou funkci útvaru.

  - *Technická skupina* – Tento útvar koordinuje projekty manipulační a dopravní techniky uvnitř závodu. Kromě toho, že zajišťuje, optimalizuje a dohlíží na efektivní využití dopravní a manipulační techniky v závodě, koordinuje pořizování a vyřazování dopravní a manipulační techniky a zajišťuje evidenci a správu této techniky.

    Za celý útvar zodpovídá manažer technické skupiny. Tomu se zodpovídají vedoucí jednotlivých směn, kteří dohlíží na práci obsluhy manipulační techniky.

3.2 Globální proces závodu

Výrobní závod plánuje výrobu na základě poptávky místního trhu. Plány (počty jednotlivých strojů) následně odešle mateřskému závodu, který je vyhodnotí a vytvoří z nich seznam dílů potřebných k zajištění výroby dle daného plánu. Podle tohoto seznamu poté mateřský závod dodává materiál do výrobního závodu.

Plánování potřeb materiálu (*Material Requirements Planning - MRP*) probíhá z větší míry v mateřském závodě. Ten vysílá materiál a částečně smontované součásti strojů potřebné pro výrobu do výrobního závodu podle aktu-

álního plánu výroby, aniž by si je tento výrobní závod objednal. Tomuto typu dodávání materiálu se říká *push proces*.

Důvodem pro dodávání většiny součástek výrobnímu závodu mateřským závodem je mimo jiné i to, že pro některé části procesu výroby produktu jsou potřebné specifické podmínky. Zajištění těchto podmínek (např. stavba haly a její vybavení nutnými stroji) je však často velmi nákladné. V takovém případě se na místě malé produkce nevyplatí tyto podmínky zajišťovat a vyjde výhodněji hotové součástky do výrobního závodu dopravit ze vzdálenějšího mateřského závodu.

Existuje však i lokálně specifický materiál (a součástky), který se vyrábí v okolí výrobního závodu. Ten je, stejně jako takzvaný A-materiál (materiál, který není použitý přímo v produkci – kancelářské potřeby, počítače, tiskárny a další režijní materiál) a služby (úklid, bezpečnostní služby, mobilní operátoři, …), objednáván od lokálních dodavatelů.

Dodávaný materiál (ať už od jiného závodu nebo od lokálního dodavatele) je výrobním závodem převzat a následně umístěn ve skladu. Odtud je poté podle potřeby dodáván na montážní linku. Spotřebovávaný materiál je odepsán ze skladu na určité nákladové středisko.

Celý proces lze rozdělit do dvou modulů – *Materiálová logistika a dispozice* (plánování výroby, pořízení a příjem materiálu) a *Řízení skladů* (interní manipulace s materiálem – umístění ve skladu, přebalení materiálu, …) – a takto rozdělený je znázorněn na obrázku B.2. V následujících kapitolách je každá část globálního procesu popsaná do detailu.

3.3 Materiálová logistika a dispozice

Materiálová logistika a dispozice (z hlediska systému součást SAP ERP modulu *Řízení materiálu – Material Management*) se stará o zásobování závodu. Mezi klíčové procesy patří:

- plánování potřeb materiálu;
- příjem zboží z mateřského závodu;
- pořizování zboží od lokálního dodavatele;
- pořizování A-materiálu a služeb od lokálního dodavatele.

Každý z těchto klíčových procesů je v následujících kapitolách detailněji rozepsán.

3.3.1 Plánování potřeb materiálu

Z velké části probíhá plánování potřeb materiálu pro produkci a následné zajištění jeho dodání v mateřském závodě. Ve výrobních závodech se plánování potřeb materiálu zaměřuje pouze na materiál od místních dodavatelů.

Mateřský závod dodává výrobnímu závodu datové soubory s plánem spotřeby dílů na lince. To jsou soubory vygenerované speciálním systémem, který počítá potřebné součástky pro naplánovanou výrobu jednotlivých produktů (potřebné součástky pro stejné modely se v čase mění – například změna dodavatele, úprava způsobu výroby a tedy změna potřebných součástek, a podobně). Obsahují identifikaci součástek a pro každý týden množství, kolik součástek bude daný týden potřeba.

Plánování spotřeby materiálu probíhá v týdenních intervalech, protože vzdálenost mezi mateřským a výrobním závodem je veliká a nelze naplánovat dodávky s přesností na dny. Navíc není efektivní posílat materiál zvlášť pro každý den (dopravní náklady jsou příliš vysoké).

Požadavky v datových souborech jsou generovány pro jednotlivé součástky jako předpověď na šest až dvanáct měsíců dopředu. Následně se s blížícím se datem výroby dále upřesňují až do jejich zafixování v takzvané *frozen zone* – období, během kterého se již požadavky na dodavatele nesmí měnit. Toto období se v závislosti na mnoha faktorech (druh součástek, vzdálenost dodavatele od závodu, …) liší pro každou součástku. Dodavatel za tuto dobu musí být schopný nakoupit potřebný materiál pro výrobu dané součástky, vyrobit požadovanou součástku a následně zboží dodat.

Pro materiál, který je zajišťován lokálním dodavatelem, jsou datové soubory ve výrobním závodě zpracovány a jsou z nich zjištěny jednotlivé požadavky na výrobu. Tyto potřeby jsou rozplánovány po týdnech. Systém ve výrobním závodě proto jednou týdně automaticky spouští plánování potřeb materiálu. V případě potřeby je možné spustit toto plánování i kdykoliv jindy ručně. To má na starosti oddělení dispozic.

Při výpočtech množství lokálně dodávaného materiálu, který je nutné zajistit, je brán v úvahu aktuální stav na skladech a porovná se s plány výroby na týden, pro který plánování zrovna probíhá. Výsledkem tohoto procesu je seznam materiálu, který pro budoucí výrobu chybí. U každé položky je zobrazeno množství, které je nutné objednat.

V následujícím kroku se přistoupí k objednávce materiálu od lokálních dodavatelů. Objednání zboží od lokálního dodavatele je součástí procesu pořizování zboží od lokálního dodavatele a je proto popsán v kapitole 3.3.2. Proces plánování potřeb materiálu je znázorněn na obrázku B.3

3.3.2 Pořizování zboží od lokálního dodavatele

Pomocí MRP procesu popsaného výše (viz kapitola 3.3.1) jsou vypočítané požadavky na dodávku materiálu od lokálního dodavatele. Objednání tohoto materiálu může probíhat dvěma způsoby.

Pokud lokální dodavatelé obstarávají dodávky výjimečně, vytváří oddělení nákupu klasické *nákupní objednávky* (*Purchase Order*) zboží, které odesílá dodavateli. Následně čeká oddělení nákupu na potvrzení přijetí objednávky od

dodavatele. Pokud toto potvrzení nepřijde, je nutné zjistit důvod (objednávka nedorazila, požadovaný materiál nemá dodavatel k dispozici, …).

V okamžiku odeslání zboží z objednávky do výrobního závodu pošle dodavatel zároveň i *avízo* (*Advanced Shipping Notification* – ASN), které je v systému zpracováno a na jeho základě vznikne dokument *příchozí dodávka* (*inbound delivery*). To oznamuje zákazníkovi (v tomto případě výrobnímu závodu), že pro něj bylo odeslané zboží, které je v dokumentu vyjmenováno. Zároveň uvádí, kdy zboží dorazí a jakým způsobem je zabaleno. Díky tomu se může závod připravit na jeho přijetí do skladů (například připravit skladové příkazy pro jednotlivé manipulační jednotky) a započítat jej do plánování výroby.

Zároveň s avízem je dodavatelem odeslána i *faktura*. Oba dokumenty jsou poslány elektronicky.

Pro často objednávané zboží jsou oddělením nákupu dojednávány dlouhodobé smlouvy, na které se následně odkazují *plány dodávek* (*scheduling agreements*). V nich jsou specifikovány detaily vztahu mezi dodavatelem a zákazníkem (výrobním závodem). Plány dodávek jsou omezeny buď časem (jsou platné pouze do určitého data), nebo množstvím (platí na dodání určitého počtu daných součástek). Definují například cenu za jednu součástku.

Na základě těchto dohodnutých plánů dodávek jsou poté tvořeny *odvolávky* (*call of / scheduling line*). Je to upozornění dodavateli, že závod potřebuje dodat určité množství součástek přesně v daný den a danou hodinu.

Odvolávky mohou být vytvářeny automaticky systémem jako výsledek MRP procesu (v takovém případě je před odesláním dodavateli systémem požadovaná kontrola pracovníkem dispozic), nebo manuálně. Po obdržení odvolávky dodavatel odešle zákazníkovi potvrzení jejího přijetí a připraví požadované zboží. Pokud zákazník (závod) neobdrží potvrzení přijetí odvolávky, je nutné, aby zjistil příčinu, proč potvrzení nedostal. Další postup je stejný jako u objednávání bez plánů dodávek (tedy obdržení faktury a avíza a přijmutí zboží).

Ať už se jedná o pořízení zboží s použitím nebo bez použití plánů dodávek, je několik způsobů, jak může závod objednávku/odvolávku dodavateli odeslat. V případě opakovaného objednávání nebo při objednávání většího množství součástek je vhodnější místo e-mailové komunikace použít *elektronickou výměnu dat* (*Electronic Data Interchange* – EDI) rozhraní, které umožňuje posílat elektronické dokumenty a následně je automaticky zpracovávat.

Hlavně při objednávání malého množství součástek, popřípadě pokud dodavatel nemá možnost využít předchozí způsob, je možné použít e-mailovou zprávu napsanou zaměstnancem. Objednávka může být napsaná přímo ve zprávě nebo přiložena jako příloha.

Celý proces pořízení zboží od lokálního dodavatele je znázorněn na obrázcích B.4, B.5 a B.6.

3.3.3 Příjem zboží od lokálního dodavatele

Příjem zboží od lokálního dodavatele je proces (znázorněný na obrázku B.7), kdy závod obdrží objednané zboží a převezme ho od dodavatele. Pracovník příjmu potvrdí přijetí, čímž se navýší množství daných součástek v systému o dodaný počet, a vystaví příjmový doklad, pokud je požadován. Následně zkontroluje, že balení dodaných materiálů je zavedeno v systému a že odpovídá požadovanému standardu, podle kterého má být daný materiál zabalený. Pokud je materiál špatně zabalen, je manipulační jednotka odeslána na přebalení (proces popsaný v kapitole 3.4.2).

Při příjmu jsou jednotlivé manipulační jednotky označeny *skladovými příkazy*. Následný proces umístění materiálu na pozici je popsán v kapitole 3.4.1.

Aby bylo možné dodávku zaplatit finančním oddělením, je nutné zkontrolovat a potvrdit fakturu. Pracovník příjmu při přebírání zboží kontroluje, že dodávka obsahuje všechny fakturované položky. V případě, že se při kontrole vyskytne nějaká nesrovnalost, podniknou se kroky předem domluvené ve smlouvě uzavřené s daným dodavatelem. Pokud je vše v pořádku, potvrdí příslušný pracovník fakturu a systém ji předá na účetní oddělení k zaplacení.

3.3.4 Příjem zboží z mateřských závodů

Jelikož jsou součástky z mateřského závodu dodávány do výrobního závodu pomocí push procesu, závod nemusí součástky objednávat – mateřský závod je expeduje sám podle plánu výroby strojů. Zaslání potřebných dokumentů a průběh dodání materiálu do výrobního závodu probíhá podobně jako u dodávky od lokálního dodavatele.

Rozdílem je však použití speciálního nástroje, který výrazně zjednodušuje a urychluje přijetí materiálu částečnou automatizací zpracování potřebných dokumentů. Pro pokračování ve zpracování dalšího kroku stačí vždy potvrzení povolaného pracovníka. Není tedy nutné ručně zpracovávat velké množství dat, která při dodávaní mnoha součástek vznikají, což proces urychlí. Tento nástroj není standardní součástí SAP ERP systému, ale jde o vývoj na míru zákazníkovi.

Nástroj obdrží avízo s položkami, které dodavatel odeslal, a s informacemi o nich. Zpracuje ho podle plánu dodávek a vytvoří příchozí dodávku. Na jejím základě poté vznikne popis jednotlivých manipulačních jednotek. Následně, pokud je požadován, je vygenerován *dokument o převzetí*, který musí pracovník příjmu při převzetí zboží potvrdit, stejně jako vygenerované skladové příkazy, které jsou reprezentovány štítky umístěnými na jednotlivých manipulačních jednotkách. Proces je znázorněný na obrázku B.8.

3.3.5 Pořizování A-materiálu a služeb od lokálního dodavatele

Pořizování A-materiálu a služeb od lokálního dodavatele (znázorněné na obrázku B.9) je podobný proces jako pořizování zboží od lokálního dodavatele (kapitola 3.3.2). Avšak A-materiál i služby jsou objednávány nezávisle na produkci, a proto zde existují určité rozdíly.

Proces začíná vytvořením požadavku na obstarání nějakého materiálu, zboží nebo služby. Požadavek do systému ručně vkládají zaměstnanci, kteří danou věc potřebují. Požadavek následně musí projít schvalovacím řízením – musí být schválen a v případě, že je schválen, je vytvořena nákupní objednávka.

Pořizování A-materiálu a služeb je řízeno manuálně oddělením nákupu za pomoci klasických SAP ERP funkcionalit. Požadovaný materiál je buď ručně vložen do dokumentu nákupní objednávky, nebo je převzat ze schválené žádosti z minulého kroku.

Nákupní objednávka je poslána e-mailem dodavateli. Ten potvrdí přijetí objednávky. Pokud tak neučiní, zjišťuje nákupní oddělení důvod.

Po zpracování objednávky a odeslání požadovaného zboží pošle dodavatel avízo a fakturu. Z avíza je u zákazníka, tedy ve výrobním závodě, pracovníkem příjmu vytvořen v souladu s objednávkou dokument přijetí zboží (je-li požadován), který je po převzetí zboží potvrzen. Zároveň je při přijetí zboží nutné, aby pracovník příjmu zkontroloval fakturu a v případě, že je vše v pořádku, ji potvrdil, a tím předal na účetní oddělení.

V případě, že se jedná o objednání služeb, je proces o něco jednodušší. Není vytvářen dokument o převzetí, ale *potvrzení o provedení práce*. Rozdíl je v tom, že při přijetí zboží je toto zboží zavedeno do systému, kdežto příjem služeb se do systému nezavádí.

3.4 Řízení skladů

Řízení skladů (*Warehouse Management - WM*) se skládá z těhto procesů:

- umístění materiálu;
- přebalení materiálu;
- rozdělení materiálu;
- fyzická inventura materiálu;
- vyřazení materiálu;
- zásobování montážní linky;
- kontrola kvality.

Těmito klíčovými procesy se blíže zabývají následující kapitoly. V každé z nich je detailněji specifikován jejich průběh.

3.4.1 Umístění materiálu

Tento proces (obrázek B.10) je používán pro umístění materiálu do skladu tak, aby byl později snadno dohledatelný. Pracovník příjmu vytvoří skladový příkaz s informacemi o pozici, kam má být jednotka uložena (číslo skladu, oddělení, regál, pozice v regálu,…), a s čárovým kódem, díky kterému je možné manipulační jednotku identifikovat. Tento skladový příkaz, reprezentován štítkem, je připevněn na manipulační jednotku.

Pracovník obsluhy manipulační techniky vyzvedne manipulační jednotku, která je označena skladovým příkazem. Poté, co ji dopraví na správné místo, potvrdí umístění materiálu. To může probíhat dvěma způsoby, v závislosti na vybavení skladu:

- Pokud je celý sklad pokryt wi-fi sítí a každý pracovník obsluhy manipulační techniky má k dispozici přenosný skener, naskenuje pracovník obsluhy manipulační techniky, který manipulační jednotku dopravil na místo, čárový kód na skladovém příkazu, a tím ho potvrdí.
- V případě, že podmínky v prvním bodě nejsou splněny, odtrhne pracovník obsluhy manipulační techniky část příkazu s čárovým kódem a odnese ho svému vedoucímu směny. Ten naskenuje čárový kód, a tím potvrdí umístění materiálu.

3.4.2 Přebalení materiálu

Tento proces je používán pro přebalení nevhodně zabaleného materiálu. Příkladem může být například materiál zabalený v kartonových krabicích, který musí být přebalen do standardně označených běžně používaných boxů. Celý proces je znázorněn na obrázku B.11.

Pracovník příjmu zboží vytvoří skladový příkaz. Pracovník obsluhy manipulační techniky vyzvedne manipulační jednotku z jejího místa ve skladu, převeze ji do přebalovací zóny a potvrdí skladový příkaz. Manipulační jednotka je příslušným zaměstnancem přebalena do správného materiálu.

Po přebalení materiálu pracovník, který na činnost dohlížel, na manipulační jednotku připevní nový skladový příkaz pro přepravu zpět do skladu. Manipulační jednotku tedy přebere opět pracovník obsluhy manipulační techniky, převeze ji na předem určenou pozici a potvrdí skladový příkaz.

3.4.3 Rozdělení materiálu

Rozdělení materiálu je speciální případ procesu přebalení materiálu. Je využíván v situacích, kdy materiál z jedné manipulační jednotky je potřeba přemístit do několika menších manipulačních jednotek.

Taková situace může nastat například, pokud od dodavatele přijde v balení velké množství materiálu a pro další práci s ním je vhodnější, aby byl materiál zabalen po menších počtech. Dalším příkladem může být potřeba oddělit různé druhy materiálu ve chvílích, kdy od dodavatele přijdou míchané manipulační jednotky (v jednom balení je několik druhů materiálu). V takovou chvíli je nutné manipulační jednotku rozdělit a každý druh zabalit do (minimálně jedné) manipulační jednotky zvlášť.

Proces (znázorněný na obrázku B.11) začíná stejně jako proces přebalení materiálu. Příslušným pracovníkem příjmu je vytvořen skladový příkaz, na což reaguje pracovník obsluhy manipulační techniky. Ten manipulační jednotku převeze do přebalovací zóny a potvrdí skladový příkaz. V přebalovací zóně je manipulační jednotka rozbalena a podle požadavků jsou zabaleny dohromady jednotlivé části manipulační jednotky, čímž vzniknou nové menší manipulační jednotky.

Po dokončení balení pracovník, který je za balení zodpovědný, na každou manipulační jednotku nalepí nový skladový příkaz. Pracovníci obsluhy manipulační techniky přeberou jednotlivé manipulační jednotky, převezou je na určené pozice ve skladu a potvrdí příslušný skladový příkaz dané manipulační jednotky.

3.4.4 Kontrola kvality

Je běžné, že během životního cyklu manipulační jednotky vznikne potřeba otestovat kvalitu daného materiálu. Může se jednat o pravidelné náhodné kontroly nebo může být manipulační jednotka vybrána záměrně, jelikož existuje podezření, že by mohla obsahovat poškozený nebo nekvalitní materiál. Testuje se buď celá manipulační jednotka, nebo jen reprezentativní vzorek z ní.

Zaměstnancem oddělení řízení kvality je vytvořen skladový příkaz, který nařizuje přesunout manipulační jednotku, jejíž část je testována, na příslušné místo kontroly. V tu chvíli je jednotka zablokována v systému, aby s ní nemohlo být dále manipulováno (především aby nemohla být přiřazena do produkce). Pracovník obsluhy manipulační techniky manipulační jednotku přesune dle pokynů a potvrdí skladový příkaz.

Následně je provedena samotná kontrola kvality materiálu. Na jejím základě je celá manipulační jednotka (i v případě, kdy byla testována pouze její část) ohodnocena jako:

- *Bez závad* – Zaměstnancem oddělení řízení kvality je vytvořen skladový příkaz. Pracovník obsluhy manipulační techniky přepraví manipulační jednotku na určené místo ve skladu a potvrdí skladový příkaz. Tím je jednotka odblokována a může s ní být dále manipulováno.

- *Vadná* – Podle závažnosti vady a po domluvě s dodavatelem je rozhodnuto, zda bude součástka sešrotována, vrácena dodavateli, nebo opravena. V prvním případě je spuštěn klasický proces šrotace materiálu,

v druhém případě je materiál odeslán dodavateli. Pokud má být závada opravena, je dále nutné rozhodnout, zda se jedná o závadu, kterou je možné opravit přímo v závodě, nebo zda je nutné odeslat materiál na opravu k dodavateli. I v případě opravy přímo v závodě je nutné k tomuto kroku přistoupit až po domluvě s dodavatelem.

Celý proces je znázorněn na obrázku B.13.

3.4.5 Šrotace materiálu

Tento proces (obrázek B.14) je využíván v případě, že je nutné vyřadit materiál z evidence. Důvodem může být například jeho poničení pracovníkem nebo poškození při přepravě.

V okamžiku zjištění závady je vedoucím směny technické skupiny materiál převeden na příslušné nákladové středisko. Tím je vyřazen ze skladové evidence a může být sešrotován.

3.4.6 Zásobování montážní linky

Proces (znázorněný na obrázku B.15) zajišťuje zásobování montážní linky materiálem ze skladu. Je založen na tom, že každá krabice s materiálem je identifikovatelná pomocí odjímatelné karty.

V prostorách linky se pohybuje zaměstnanec výroby, který kontroluje stav součástek na jednotlivých stanovištích (podle velikosti linky může být zaměstnanců více a jsou jim přiřazeny jednotlivé části montážní linky). V okamžiku, kdy začne docházet určitá součástka (nebo nějaký materiál), tento zaměstnanec naskenuje kartu na krabici s docházejícími součástkami a odešle tím informace o jejich nedostatku do systému.

V některých závodech je možné, že určité součástky jsou monitorovány automaticky. V místě, odkud jsou na stanovišti součástky odebírány, je umístěno laserové čidlo. V okamžiku, kdy množství součástek klesne pod hranici tímto čidlem vytvořenou, posílá čidlo automaticky identifikaci docházejících součástek systému.

Ten identifikuje, odkud má být odebrána další krabice obsahující potřebnou součástku. Je automaticky vytvořen skladový příkaz. Následně je obsluhou manipulační techniky krabice přivezena na požadované místo na lince a je potvrzen skladový příkaz. Vedoucí směny technické skupiny následně odepíše součástky ze skladové evidence na nákladové středisko.

3.4.7 Fyzická inventura materiálu

Ze zákona je uložena povinnost provádět minimálně jednou za rok fyzickou kontrolu (inventuru) majetku. Velká část této kontroly probíhá ve skladech materiálu. Jejím cílem je odhalit rozdíly mezi fyzickým a systémovým skladem (to, co ve skladu skutečně fyzicky je, proti tomu, co je vedeno v systému, že je

ve skladu). Zároveň se provádí i průběžná inventura, kdy se majetek kontroluje postupně v průběhu celého roku.

Proces roční a průběžné inventury je podobný, avšak liší se v přístupu k materiálu. Roční inventura začíná zastavením celé výroby. Následně jsou pro jednotlivé pracovníky obsluhy manipulační techniky, kteří mají provést fyzickou inventuru, vytvořeny manažerem technické skupiny *inventární dokumenty*, které pokryjí veškerý uskladněný materiál. Inventární dokument je složen z jednotlivých položek (součástky, manipulační jednotky, …), které mají být přepočítány. Detail inventárního dokumentu a kolik položek bude obsahovat záleží na vnitřních předpisech závodu.

Při průběžné inventuře dochází nejprve k vybrání relevantních dat, která mají tvořit jeden inventární dokument, manažerem technické skupiny. Tato data představují většinou jednu polici nebo jeden regál ve skladu (během roku by měl projít průběžnou inventurou celý sklad). V okamžiku, kdy je inventární dokument vytvořen, jsou všechny položky na něm obsaženy zablokovány a není umožněna žádná manipulace s nimi (nejde je někam přemístit, použít ve výrobě, …).

V obou typech inventury je poté inventární dokument vytištěn a následuje fyzické počítání daných položek. Jednotlivé počty jsou nejprve zapsány do vytištěné podoby inventárního dokumentu a až po dokončení celé práce jsou manažerem technické skupiny zapsány do systému.

Rozdíly mezi skutečností a hodnotami v systému jsou manažerem technické skupiny vyhodnoceny a pro každou manipulační jednotku jsou nastaveny správné hodnoty množství jednotlivých materiálů. V tuto chvíli je v případě průběžné inventury materiál opět uvolněn pro manipulaci a v případě roční inventury se spouští výroba.

Posledním krokem procesu je zpracování vzniklých rozdílů zaměstnancem oddělení controllingu. Toho je docíleno pomocí vytvoření příslušného finančního dokumentu, čímž jsou rozdíly zavedeny i do účetnictví. Celý proces fyzické inventury materiálu je zobrazen na obrázku B.16.

3.4.8 Řízení toku palet

Speciální oblast řízení skladů se zaměřuje na řízení toku palet, na kterých je materiál do závodu dodáván. Některé palety jsou vratné, a proto evidované v systému (na rozdíl od nevratných palet, o kterých se záznamy nedělají).

Vratné palety jsou po vyložení materiálu uloženy ve speciálních skladech na palety. Záleží na domluvě mezi závodem a dodavatelem, jakým způsobem jsou palety vraceny.

Pokud posílá závod dodavateli nějaké zboží, mohou být palety použity pro jeho přepravu. Tedy naplněny jiným materiálem/zbožím a poslány zpět. Další možností je palety skladovat a poté poslat dodavateli zpět velké množství prázdných palet.

V případě, že je vratná paleta poničená, je uložena ve speciálním skladě. Ten je po určitém čase vyprázdněn a všechny poničené palety jsou buď opraveny a uskladněny mezi vratné palety, nebo zlikvidovány.

Řízení těchto procesů je z velké části automatizováno. Množství palet počítá systém na základě dovezeného zboží od dodavatelů (u zboží je vyznačeno, že je převáženo na vratné paletě). Po naplnění kapacity poté systém vystavuje automaticky skladový příkaz k přesunu palet (buď k převozu zpět dodavateli, nebo k likvidaci poničených palet). Celý proces je zobrazen na obrázku B.17.

Jelikož se výrobní závody často nacházejí v oblastech značně vzdálených od mateřských závodů, jsou náklady na dopravu poměrně vysoké. Proto se k použití vratných palet přistupuje jen zřídka (likvidace nevratných palet vyjde výhodněji než jejich doprava zpět do mateřského závodu).

Kapitola 4

Návrh autorizačního konceptu

Tato kapitola představuje praktickou část práce. Vychází z analýzy závodu společnosti v minulé kapitole. Popisuje navržený autorizační koncept pro závod společnosti X se zaměřením na logistiku. Zároveň poskytuje časový a finanční plán pro realizaci tohoto návrhu.

4.1 Uživatelé

K systému ve výrobním závodě přistupují tři skupiny uživatelů. Jsou jimi:

- administrátor;
- klíčový uživatel;
- běžný uživatel.

Uživatelé typu *administrátor* nejsou přímo součástí výrobního závodu. Systém výrobního závodu je spravován centrálně společně se všemi ostatními SAP ERP systémy společnosti v hlavním závodě společnosti. V této skupině uživatelů se nacházejí uživatelé, kteří mají na starost vývoj systému ve vývojovém prostředí na základě požadavků klíčových uživatelů.

Dále jsou v této skupině i uživatelé starající se o vývoj přístupových oprávnění (například vytváření nových rolí) a administrátoři systému, kteří se starají o správné fungování celého systému. Žádný z těchto uživatelů nespadá do výrobního závodu.

Klíčoví uživatelé jsou zkušení zaměstnanci závodu, kteří se dobře orientují v běhu oddělení, které jim bylo svěřeno. Jsou zodpovědní za správnost dat v systému. Starají se o to, aby všechna data zanesená do systému odpovídala skutečnosti.

Navíc mají na starost vytváření nových uživatelů, přidělování rolí a autorizací uživatelům, schvalování žádostí o přidělení oprávnění od jiných klíčových

uživatelů, kontrolu žádostí o přístup k transakcím, funkcím nebo datům v jejich oddělení.

Zároveň shromažďují žádosti o vývoj nových funkcionalit nebo rolí v systému. Pokud jsou tyto žádosti schváleny, předají je klíčoví uživatelé administrátorům v hlavním závodě.

Běžní uživatelé mají přiřazené role, které jim umožňují pouze vykonávat jejich náplň práce. Nemají žádné oprávnění pro správu systému (nemohou například přidělovat role jiným uživatelům, mohou pouze o přidělení role zažádat).

4.2 Postup přiřazení přístupových oprávnění

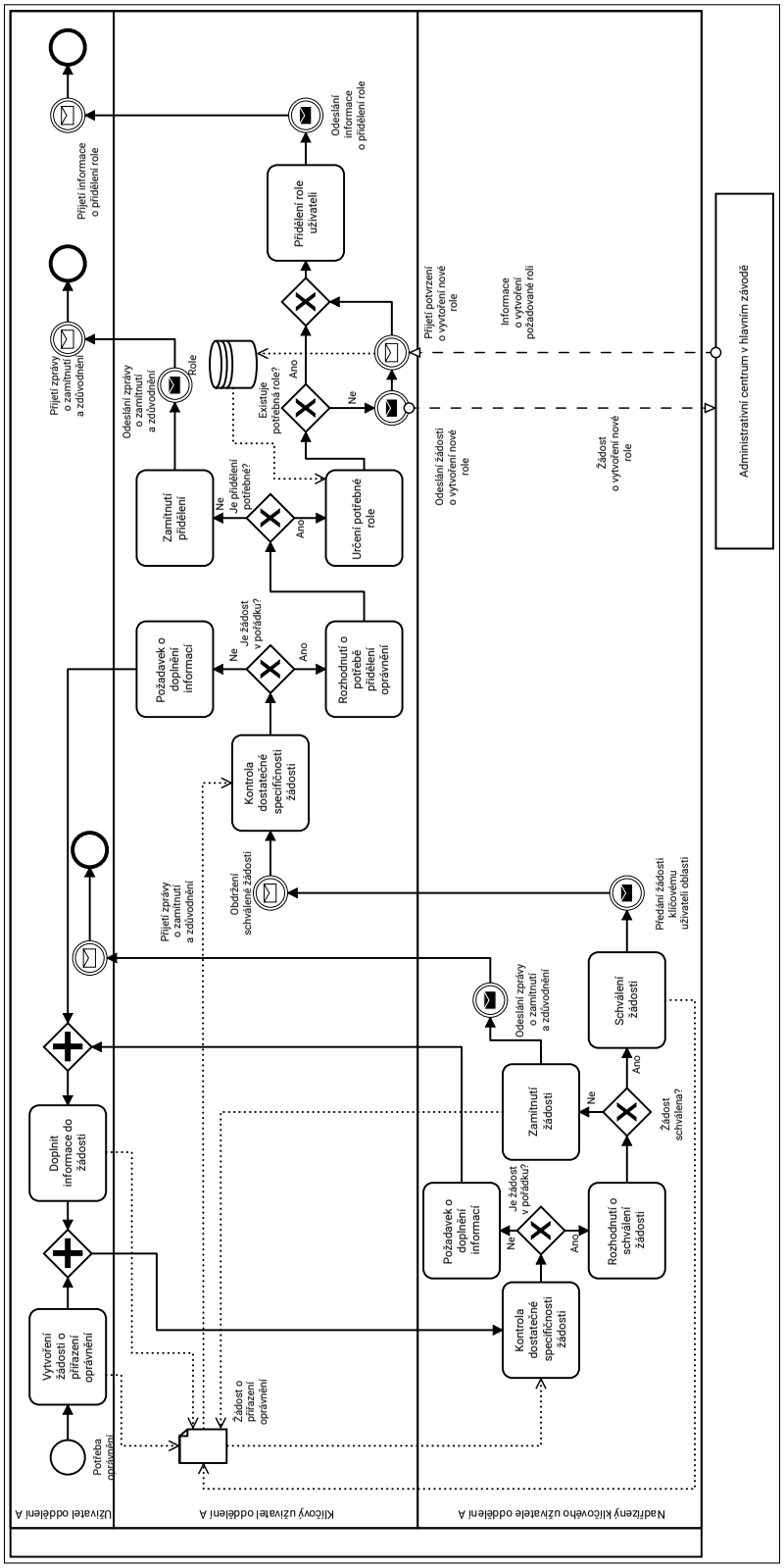
Při přiřazování nových oprávnění je nutné dodržovat následující postup, který zabraňuje přiřazení oprávnění nepovolané osobě. Tento proces je znázorněn v diagramu na obrázku 4.1.

Uživatel v systému vytvoří žádost o přiřazení přístupových oprávnění. Tato žádost je předána vedoucímu oddělení a ten nejprve rozhodne, zda je žádost dostatečně detailní a zda je pochopitelné, jaká oprávnění jsou požadována. Pokud ne, je žádost vrácena na doplnění uživateli.

Pokud je vše v pořádku, rozhoduje vedoucí, zda uživatel potřebuje požadované přístupy a zda je možné mu přístupy přiřadit. Pokud ne, je žádost vedoucím zamítnuta a uživateli odeslána informace o zamítnutí a zdůvodnění vedoucího. V opačném případě je žádost schválena a předána klíčovému uživateli oddělení ke zpracování.

Klíčový uživatel nejprve opět kontroluje, zda je žádost z jeho pohledu dostatečně specifická a pokud ne, vrací ji uživateli na doplnění. Pokud je vše v pořádku, rozhoduje i on, zda jsou požadavky na přiřazení přístupových oprávnění opodstatněné. Pokud ne, je přiřazení zamítnuto, uživatel je informován a dostane zdůvodnění od klíčového uživatele.

Pokud je přiřazení povoleno, rozhoduje klíčový uživatel, zda existuje role, která požadavky na oprávnění splňuje. V případě, že ne, odesílá klíčový uživatel žádost o vytvoření nové role na administrativní centrum v hlavním závodě. Po jejím vytvoření, stejně jako v případě, že potřebná role existuje, je přiřazena uživateli. Ten je o přiřazení následně informován.



Obrázek 4.1: Postup přiřazení přístupových oprávnění

4.3 Jmenná konvence

Pro udržení přehlednosti je nutné dodržovat jednotnou jmennou konvenci, neboli pravidla pro pojmenovávání rolí, napříč celým autorizačním konceptem. V názvu role je podle této jmenné konvence uveden mimo jiné klient, který představuje část celé společnosti (tato část reprezentuje například jednu zemi, závod, nebo jednu právní entitu společnosti).

Dále se v názvu nachází oblast závodu, do které role spadá (oblasti vycházejí z analýzy struktury závodu (v kapitole 3.1)), a samotné pojmenování role. Jelikož je návrh orientován na strukturu společnosti, vycházejí tato pojmenování z jednotlivých pracovních pozic.

Obecný název role je: *Z:XYZ_AB_NAZEV_ROLE_XXXXXXXXX*. Vysvětlení jednotlivých částí je v tabulce 4.1.

Tabulka 4.1: Vysvětlení vzoru názvu rolí

Pozice	Hodnota	Komentář
1	Zákaznická role	Z (vždy)
2	Oddělovač	: (vždy)
3 – 5	Klient	SAS = Klient Slovensko SAD = Klient Německo …
6	Oddělovač	_ (vždy)
7 – 8	Oblast závodu	GO = Government (Vedení) QC = Quality control (Kontrola kvality) FI = Finance (Finance) PU = Purchase (Nákup) SA = Sale (Prodej) HR = Human Resources (Lidské zdroje) PR = Production (Výroba) LO = Logistics (Logistika)
9	Oddělovač	_ (vždy)
10 – 29	Název role	Libovolný text o délce maximálně dvacet znaků

4.4 Role se zaměřením na logistiku

V této kapitole se nachází seznam rolí pro oblast logistiky, které jsou potřebné v každém výrobním závodě. Seznam oprávnění pro manažera závodu představuje pouze seznam oprávnění týkajících se oblasti logistiky.

Tento seznam představuje základ rolí výrobního závodu. Některé výrobní závody mohou potřebovat i další role. Stejně tak může i v průběhu fungování závodu nastat situace, kdy bude nutné přiřadit uživateli odlišná oprávnění, a proto vytvořit novou roli. Při tom je vždy nutné dbát na zásadu SOD a na to, aby role měla vždy pouze ta oprávnění, která uživatel opravdu potřebuje.

- Manažer závodu
  (Z:XYZ_GO_PLANT_MANAGER) má oprávnění:
  - vytvořit a zobrazit žádost v systému (vytvoření nového uživatele, přiřazení role uživateli);
  - schválit/zamítnout žádost v systému – pokud žádost nevytvořil on;
  - vytvořit, zobrazit, upravit a mazat skladové příkazy;
  - zobrazit změnové dokumenty skladových příkazů;
  - zobrazit faktury;
  - vytvořit, zobrazit, upravit a mazat příjmové doklady;
  - zobrazit změnové dokumenty příjmových dokladů;
  - zobrazit příchozí dodávky;
  - vytvořit, zobrazit, upravit a mazat odvolávky;
  - zobrazit změnové dokumenty odvolávek;
  - schválit automaticky vytvořené odvolávky;
  - zobrazit přijaté avízo;
  - zobrazit informace o dodavatelích.
- Manažer logistiky
  (Z:XYZ_LO_LOGISTICS_MANAGER) má oprávnění:
  - vytvořit a zobrazit žádost v systému (vytvoření nového uživatele, přiřazení role uživateli);
  - schválit/zamítnout žádost v systému – pokud žádost nevytvořil on;
  - vytvořit, zobrazit, upravit a mazat skladové příkazy;
  - zobrazit změnové dokumenty skladových příkazů;
  - zobrazit faktury;
  - vytvořit, zobrazit, upravit a mazat příjmové doklady;
  - zobrazit změnové dokumenty příjmových dokladů;

  - zobrazit příchozí dodávky;
  - vytvořit, zobrazit, upravit a mazat odvolávky;
  - zobrazit změnové dokumenty odvolávek;
  - schválit automaticky vytvořené odvolávky;
  - zobrazit přijaté avízo;
  - zobrazit informace o dodavatelích.

- Manažer operativní logistiky (Z:XYZ_LO_OPERATIV_LOGIST_MNGR) má oprávnění:
  - vytvořit a zobrazit žádost v systému (vytvoření nového uživatele, přiřazení role uživateli);
  - schválit/zamítnout žádost v systému – pokud žádost nevytvořil on;
  - vytvořit, zobrazit, upravit a mazat skladové příkazy;
  - zobrazit změnové dokumenty skladových příkazů;
  - zobrazit faktury;
  - vytvořit, zobrazit, upravit a mazat příjmové doklady;
  - zobrazit změnové dokumenty příjmových dokladů;
  - zobrazit příchozí dodávky.

- Manažer řízení obalového toku (Z:XYZ_LO_PACKING_CONTROL_MNGR) je klíčový uživatel a má oprávnění:
  - vytvořit a zobrazit žádost v systému (vytvoření nového uživatele, přiřazení role uživateli);
  - schválit/zamítnout žádost v systému – pokud žádost nevytvořil on;
  - přiřadit oprávnění uživateli na svém oddělení – které sám neschválil, ani nevytvořil žádost o přiřazení;
  - zobrazit, upravit a mazat informace o vratných paletách;
  - zobrazit změnové dokumenty informací o vratných paletách;
  - vytvořit, zobrazit, upravit a mazat skladový příkaz týkající se vratných palet;
  - zobrazit změnové dokumenty skladových příkazů týkajících se vratných palet.

- Pracovník řízení obalového toku (Z:XYZ_LO_PACKING_CONTROL_WORK) má oprávnění:
  - zobrazit informace o vratných paletách;
  - vytvořit, zobrazit a upravit skladový příkaz týkající se vratných palet;
- Manažer příjmu (Z:XYZ_LO_INCOME_MANAGER) je klíčový uživatel a má oprávnění:
  - vytvořit a zobrazit žádost v systému (vytvoření nového uživatele, přiřazení role uživateli);
  - schválit/zamítnout žádost v systému – pokud žádost nevytvořil on;
  - přiřadit oprávnění uživateli na svém oddělení – které sám neschválil, ani nevytvořil žádost o přiřazení;
  - zobrazit a potvrdit/zamítnout fakturu přijímaného zboží;
  - odeslat potvrzenou fakturu na finanční oddělení;
  - vytvořit, zobrazit, upravit a mazat příjmový doklad;
  - potvrdit/zamítnout příjmový doklad, který nevytvořil on;
  - zobrazit změnové dokumenty příjmových dokladů;
  - zobrazit dokument příchozí dodávky;
  - vytvořit, zobrazit, upravit a mazat skladový příkaz;
  - zobrazit změnové dokumenty skladových příkazů;
  - v případě příjmu z mateřského závodu potvrdit/zamítnout nutnost rozdělit manipulační jednotku;
  - v případě příjmu z mateřského závodu potvrdit/zamítnout nutnost přebalit manipulační jednotku;
  - zobrazit a upravit záznamy o balení manipulační jednotky;
  - zobrazit změnové dokumenty záznamů o balení manipulační jednotky;
  - v případě příjmu z mateřského závodu potvrdit správnost záznamů o balení manipulační jednotky.
- Pracovník příjmu (Z:XYZ_LO_INCOME_WORKER) má oprávnění:
  - zobrazit fakturu přijímaného zboží;
  - vytvořit, zobrazit a upravit příjmový doklad;
  - potvrdit/zamítnout příjmový doklad, který nevytvořil on;

  - zobrazit dokument příchozí dodávky;
  - vytvořit, zobrazit a upravit skladový příkaz;
  - v případě příjmu z mateřského závodu potvrdit/zamítnout nutnost rozdělit manipulační jednotku;
  - v případě příjmu z mateřského závodu potvrdit/zamítnout nutnost přebalit manipulační jednotku;
  - zobrazit a upravit záznamy o balení manipulační jednotky;
  - v případě příjmu z mateřského závodu potvrdit/zamítnout správnost záznamů o balení manipulační jednotky.

- Manažer technické skupiny (Z:XYZ_LO_TECHNICAL_GROUP_MNGR) je klíčový uživatel a má oprávnění:
  - vytvořit a zobrazit žádost v systému (vytvoření nového uživatele, přiřazení role uživateli);
  - schválit/zamítnout žádost v systému – pokud žádost nevytvořil on;
  - přiřadit oprávnění uživateli na svém oddělení – které sám neschválil, ani nevytvořil žádost o přiřazení;
  - vytvořit, zobrazit, upravit, mazat a tisknout inventární dokument;
  - zobrazit změnové dokumenty inventárního dokumentu;
  - zobrazit a aktualizovat počty materiálu v systému;
  - zobrazit změnové dokumenty počtu materiálu v systému;
  - vytvořit. zobrazit, upravit a mazat skladový příkaz;
  - zobrazit změnové dokumenty skladových příkazů;
  - naskenovat čárový kód skladového příkazu a potvrdit tím skladový příkaz, který nevytvořil on.

- Vedoucí směny (Z:XYZ_LO_SHIFT_LEADER) má oprávnění:
  - vytvořit, zobrazit a upravit skladový příkaz;
  - naskenovat čárový kód skladového příkazu a potvrdit tím skladový příkaz.

- Pracovník obsluhy manipulační techniky (Z:XYZ_LO_HANDLING_TECH_WORKER) přistupuje do systému pouze tehdy, pokud je závod pokryt wi-fi sítí a pracovník má k dispozici přenosný skener. V takovém případě je pracovník oprávněn:
  - zobrazit skladový příkaz;
  - naskenovat čárový kód skladového příkazu a potvrdit tím skladový příkaz.
- Klíčový uživatel dispozic (Z:XYZ_LO_DISPOSITION_MANAGER_) je klíčový uživatel a má oprávnění:
  - vytvořit a zobrazit žádost v systému (vytvoření nového uživatele, přiřazení role uživateli);
  - schválit/zamítnout žádost v systému – pokud žádost nevytvořil on.
  - přiřadit oprávnění uživateli na svém oddělení – které sám neschválil, ani nevytvořil žádost o přiřazení;
  - manuálně spustit plánování potřeb materiálu;
  - zobrazit, upravit a mazat soubor s požadavky na výrobu;
  - zobrazit změnové dokumenty souborů s požadavky na výrobu;
  - zobrazit, upravit a mazat soubor potřebného materiálu (položek k objednání);
  - zobrazit změnové dokumenty souboru potřebného materiálu;
  - schválit automaticky vytvořenou odvolávku;
  - vytvořit odvolávku ručně;
  - zobrazit, upravit a mazat odvolávku;
  - zobrazit změnové dokumenty odvolávek;
  - odeslat odvolávku, kterou nevytvořil on, dodavateli;
  - zobrazit přijaté avízo;
  - zobrazit informace o dodavateli.
- Pracovník dispozic (Z:XYZ_LO_DISPOSITION_WORKER) má oprávnění:
  - zobrazit soubor s požadavky na výrobu;
  - zobrazit soubor potřebného materiálu (položek k objednání);
  - schválit automaticky vytvořenou odvolávku;
  - vytvořit a zobrazit odvolávku ručně;
  - odeslat odvolávku, kterou nevytvořil on, dodavateli;
  - zobrazit přijaté avízo;
  - zobrazit informace o dodavateli.

4.5 Plán realizace návrhu

Realizace návrhu se dělí na několik úseků, které na sebe časově navazují. Některé úseky probíhají ve vývojovém centru, jiné přímo ve výrobním závodě, pro který je návrh vytvářen. Jednotlivými úseky jsou:

- *Implementace autorizačního konceptu* – Implementace jedné role zabere v průměru polovinu pracovního dne, tedy čtyři hodiny. V návrhu pro logistiku je vytvořeno dvanáct rolí. Celková implementace tedy zabere 4 x 12 hodin (48 hodin = 6 pracovních dní).
- *Tvorba dokumentace* – Tvorba dokumentace probíhá v průběhu implementace autorizačního konceptu a po dokončení implementace musí být dokončena i dokumentace. Dokončení dokumentace trvá 2 pracovní dny (16 hodin).
- *Testování na úrovni vývojových pracovníků* – Toto testování provádějí vývojoví pracovníci, popřípadě testeři z oddělení vývoje. Testování probíhá přímo ve výrobním závodě a trvá 5 pracovních dní (40 hodin).
- *Testování uživateli* – Testování přímo v závodě provádějí zaměstnanci závodu (budoucí uživatelé) pod dohledem testerů z oddělení vývoje, kteří prováděli testy na úrovni vývojových pracovníků. Toto testování trvá dva týdny, tedy 10 pracovních dní (80 hodin).
- *Školení* – Po dokončení testování probíhá zaškolení klíčových uživatelů testery společnosti, která koncept implementovala. Toto školení trvá 1 den (8 hodin).
- *Podpora na místě* – Po skončení testování zůstávají testeři ve výrobním závodě a poskytují technickou podporu. Školení a tato podpora probíhají souběžně. Podpora na místě je poskytována 5 pracovních dní (40 hodin).
- *Dovolené, nemoci* – Je nutné počítat s neočekávanými situacemi, jako jsou nemoci nebo dovolené zaměstnanců, které mohou realizaci zdržet. Jako rezerva pro tyto situace je počítán jeden týden (5 pracovních dní – 40 hodin).
- *Celková délka realizace* – Realizace návrhu bude trvat 33 pracovních dní (264 hodin).

Plán realizace návrhu je zobrazen na obrázku 4.2.

Úkol		Dny	
		Pracovní	Celkem
Implementace autorizačního konceptu	Úkol	6	8
	Rezerva	1	1
Tvorba dokumentace	Úkol	2	2
	Rezerva	0	0
Tesování na úrovní vývojářů	Úkol	5	7
	Rezerva	1	1
Testování uživateli	Úkol	10	14
	Rezerva	2	4
Školení uživatelů	Úkol	1	1
	Rezerva	0	0
Podpora na místě	Úkol	5	7
	Rezerva	1	1
Celková délka realizace		33	45

Obrázek 4.2: Plán realizace návrhu

4.6 Náklady na realizaci návrhu

Pro výpočet nákladů na realizaci návrhu autorizačního konceptu je potřebné znát ceny práce zaměstnanců, počty zaměstnanců, kteří se na realizaci budou podílet, i ceny dalších výdajů. Tyto informace jsou shrnuty v následujícím textu. Všechny údaje o cenách vycházejí z běžných cen společnosti X přepočítaných z eur na české koruny při kurzu 1 EUR = 26 Kč.

Ceny práce zaměstnanců jsou přibližně:

- vývojový pracovník / tester: 1 300 Kč/h – 2 600 Kč/h (odvíjí se od zkušenosti pracovníka);
- externí zaměstnanec výrobního závodu: 260 Kč/h;
- interní zaměstnanec výrobního závodu: 130 Kč/h.

Počty potřebných zaměstnanců v jednotlivých fázích realizace návrhu jsou:

- implementace autorizačního konceptu: jeden vývojový pracovník;
- tvorba dokumentace: jeden vývojový pracovník;
- testování na úrovni vývojových pracovníků: tři vývojoví pracovníci (testeři);
- testování uživateli: deset zaměstnanců závodu (interní nebo externí) za dohledu tří vývojových pracovníků;
- školení uživatelů: čtyři interní zaměstnanci (klíčoví uživatelé) výrobního závodu a jeden školitel (vývojový pracovník);
- podpora: tři vývojoví pracovníci.

Ceny dalších výdajů (náklady na dopravu a pobyt vývojových pracovníků / testerů v místě výrobního závodu (od začátku testů vývojovými pracovníky až do skončení místní podpory – 34 dní):

- doprava: 120 000 Kč/osoba;
- ubytování: 2 600 Kč/den/osoba;
- strava: 1 300 Kč/den/osoba.

Výsledné náklady závisí na přístupu výrobního závodu vůči hrazení práce svých zaměstnanců. Je několik možností, jaký přístup zvolit.

Testování uživateli mohou provádět externí zaměstnanci, kterým je práce hrazena, a školení pořádat mimo pracovní dobu interních zaměstnanců. V tom případě je nutné započítat do nákladů i čas interních zaměstnanců na školení. Tato možnost je použita při výpočtu nákladů v tabulce 4.2.

Tabulka 4.2: Náklady na realizaci návrhu při využití externích zaměstnanců a zahrnutí interních zaměstnanců do nákladů

Úsek realizace	počet člh	cena celkem v Kč
Implementace	48	62 400 – 124 800
Tvorba dokumentace	16	20 800 – 41 600
Testování vývojovými pracovníky	120	156 000 – 312 000
Testování uživateli – externí pracovníci	800	208 000
Testování uživateli – vývojoví pracovníci	48	62 400 – 124 800
Školení – školitel	8	10 400 – 20 800
Školení – zaměstnanec	32	4 160
Podpora	120	156 000 – 312 000
Doprava vývojových pracovníků	–	360 000
Ubytování vývojových pracovníků	–	265 200
Strava vývojových pracovníků	–	132 600
Celkem	1 176	1 437 960 – 1 905 960

Další možností je provedení testování uživateli externími zaměstnanci, ale školení interních zaměstnanců následně pořádat v rámci pracovní doby zaměstnanců. Tím se čas interních zaměstnanců na školení nepromítne do nákladů realizace návrhu. Přesné náklady na realizaci návrhu v případě této možnosti jsou vypočítány v tabulce 4.3.

Nebo je možné provádět i testování uživateli interními zaměstnanci v rámci jejich pracovní doby. To znamená nezahrnovat do nákladů ani testování uživateli. S touto možností jsou vypočítány náklady v tabulce 4.4.

Poslední možností je provádění testů uživateli interními zaměstnanci a toto testování stejně jako školení provést mimo pracovní dobu zaměstnanců. Tedy i jejich práce by měla být v nákladech uvedena. Tato poslední možnost je použita při výpočtu nákladů v tabulce 4.5.

Tabulka 4.3: Náklady na realizaci návrhu při využití externích zaměstnanců a nezahrnutí interních zaměstnanců do nákladů

Úsek realizace	počet člh	cena celkem v Kč
Implementace	48	62 400 – 124 800
Tvorba dokumentace	16	20 800 – 41 600
Testování vývojovými pracovníky	120	156 000 – 312 000
Testování uživateli – externí pracovníci	800	208 000
Testování uživateli – vývojoví pracovníci	48	62 400 – 124 800
Školení – školitel	8	10 400 – 20 800
Podpora	120	156 000 – 312 000
Doprava vývojových pracovníků	–	360 000
Ubytování vývojových pracovníků	–	265 200
Strava vývojových pracovníků	–	132 600
Celkem	1 144	1 433 800 – 1 901 800

Tabulka 4.4: Náklady na realizaci návrhu při nevyužití externích zaměstnanců a nezahrnutí interních zaměstnanců do nákladů

Úsek realizace	počet člh	cena celkem v Kč
Implementace	48	62 400 – 124 800
Tvorba dokumentace	16	20 800 – 41 600
Testování vývojovými pracovníky	120	156 000 – 312 000
Testování uživateli – vývojoví pracovníci	48	62 400 – 124 800
Školení – školitel	8	10 400 – 20 800
Podpora	120	156 000 – 312 000
Doprava vývojových pracovníků	–	360 000
Ubytování vývojových pracovníků	–	265 200
Strava vývojových pracovníků	–	132 600
Celkem	344	1 225 800 – 1 693 800

Tabulka 4.5: Náklady na realizaci návrhu při nevyužití externích zaměstnanců a zahrnutí interních zaměstnanců do nákladů

Úsek realizace	počet člh	cena celkem v Kč
Implementace	48	62 400 – 124 800
Tvorba dokumentace	16	20 800 – 41 600
Testování vývojovými pracovníky	120	156 000 – 312 000
Testování uživateli – interní pracovníci	800	104 000
Testování uživateli – vývojoví pracovníci	48	62 400 – 124 800
Školení – školitel	8	10 400 – 20 800
Školení – zaměstnanec	32	4 160
Podpora	120	156 000 – 312 000
Doprava vývojových pracovníků	–	360 000
Ubytování vývojových pracovníků	–	265 200
Strava vývojových pracovníků	–	132 600
Celkem	1 176	1 333 960 – 1 801 960

4.7 Rizika vytvořeného návrhu

Existuje několik rizik, která ohrožují kvalitu autorizačního konceptu. Je nutné o nich vědět a dodržovat postupy, jak se daným rizikům vyhnout. Rizika návrhu jsou uvedena v tabulkách 4.6, 4.7, 4.8, 4.9.

Tabulka 4.6: Riziko 01 – Nekvalitní dokumentace

Název	Nekvalitní dokumentace
Vlastník	Administrátor autorizací
Zranitelnost	Nepravidelné a nekvalitní doplňování dokumentace
Pravděpodobnost výskytu	50 %
Dopad	Dokumentace neodpovídá realitě, v případě potřeby tedy není možné snadno se v konceptu pomocí dokumentace zorientovat.
Plán pro mitigaci rizika	Pevně stanovené pravidelné termíny pro kontrolu aktuálnosti dokumentace a pravidelné doplňování.
Krizový plán	Přepsání dokumentace, případně přepsání neaktuálních částí dokumentace.

Tabulka 4.7: Riziko 02 – Nevhodný přístup k datům

Název	Nevhodný přístup k datům
Vlastník	Klíčový uživatel pro dané oddělení závodu
Zranitelnost	Nepozornost při přiřazování oprávnění
Pravděpodobnost výskytu	10 %
Dopad	Uživateli jsou přiřazena oprávnění k akcím, která nepotřebuje a neměl by mít. Může se tedy dostat k citlivým informacím a zvyšuje se riziko jejich úniku nebo poškození.
Plán pro mitigaci rizika	Křížové pravidlo při přiřazení oprávnění – jedna osoba musí schválit žádost o přiřazení oprávnění, druhá osoba přiřazení oprávnění provádí.
Krizový plán	Odstranit všechna práva uživateli a následně přiřadit pouze potřebná práva.

Tabulka 4.8: Riziko 03 – Porušení zásady oddělení povinností

Název	Porušení zásady oddělení povinností
Vlastník	Klíčový uživatel pro dané oddělení závodu
Zranitelnost	Nepozornost při přiřazování oprávnění
Pravděpodobnost výskytu	10 %
Dopad	Uživatel má více práv, než má mít. Může provést proces, který má být rozdělený mezi více uživatelů, celý sám. Tím je ztracena kontrola nad akcemi. Příkladem je, když uživatel může vytvořit objednávku a zároveň ji potvrdit a odeslat.
Plán pro mitigaci rizika	Křížové pravidlo při přiřazení oprávnění – jedna osoba musí schválit žádost o přiřazení oprávnění, druhá osoba přiřazení oprávnění provádí.
Krizový plán	Odstranit všechna práva uživateli, jehož oprávnění zásadu SOD porušují, a přiřadit jednotlivá práva více různým uživatelům.

Tabulka 4.9: Riziko 04 –Nedostatečná oprávnění uživatele

Název	Nedostatečná oprávnění uživatele
Vlastník	Klíčový uživatel pro dané oddělení závodu
Zranitelnost	Nepozornost při přiřazování oprávnění, nesprávná definice požadavku v žádosti od uživatele
Pravděpodobnost výskytu	35 %
Dopad	Uživatel nemá dostatečná oprávnění pro přístup k datům – nemůže vykonávat svou práci
Plán pro mitigaci rizika	Při nejasnostech v žádosti o přiřazení možnost požadovat dovysvětlení. Přesná definice všech pracovních pozic.
Krizový plán	Vytvoření nové žádosti o přiřazení oprávnění, popřípadě požadovat vytvoření nové role.

4.8 Přínosy navrhovaného konceptu

Navrhovaný autorizační koncept má několik přínosů. Jelikož koncept vychází ze struktury závodu, je koncept srozumitelný a snadno udržitelný. Ve společnosti je každá pozice definovaná – je specifikováno, jaká je náplň práce pracovníka na dané pozici. Z této specifikace lze poté snadno vycházet při definici nutných oprávnění.

S tím zároveň souvisí i větší bezpečnost informací, jelikož díky specifikaci pozic je jasné, k čemu která role oprávnění potřebuje. Díky tomu nejsou zaměstnanci přiřazena oprávnění, která ve skutečnosti k výkonu své práce nepotřebuje.

Tento návrh zároveň dodržuje pravidlo oddělení povinností. Jeden pracovník nemůže zahájit určitý proces, například vytvořit odvolávku, a zároveň proces dokončit (odvolávku potvrdit a odeslat). Vždy je proces rozdělen minimálně mezi dva pracovníky. To je další přínos pro zvýšení bezpečnosti informací společnosti X.

Dalším přínosem je oddělení administrativních rolí od navrhovaného autorizačního konceptu. V případě změny technické podpory je snazší přebrání této funkce novou společností pro technickou podporu od té původní.

Dobře definovaný autorizační koncept je zároveň výhodný při komunikaci s auditory. Díky kvalitnímu autorizačnímu konceptu je snazší získat různé IT certifikáty. Tyto certifikáty poté zvyšují prestiž společnosti. Zákazníci rozhodující se mezi několika společnostmi k obdrženým certifikátům mohou přihlédnout a společnost X si na jejich základě vybrat.

Z ekonomického hlediska je výhodné, že tento autorizační koncept lze použít opakovaně s případnými úpravami. Dojde tedy ke snížení nákladů nejen za opakovaný návrh podobného konceptu, ale i za opakovanou implementaci konceptu.

Závěr

Cílem práce bylo vytvořit analýzu procesů závodu společnosti X se zaměřením na logistiku a návrh autorizačního konceptu v SAP ERP systému pro závod společnosti X se zaměřením na logistiku. Zároveň bylo cílem vytvořit plán realizace a vyhodnotit náklady na provedení návrhu a vyhodnotit rizika a přínosy návrhu.

V průběhu vytváření analýzy procesů se uskutečnilo několik konzultací se zaměstnanci společnosti X, kteří mají na starosti vývoj v SAP ERP systému za oblast logistiky pro celou společnost. Pomocí těchto konzultací bylo možné vytvořit analýzu logistických procesů výrobního závodu. Zároveň s touto analýzou vznikl obecný přehled struktury oblasti logistiky výrobního závodu.

Na základě těchto analýz následně bylo možné vytvořit návrh autorizačního konceptu pro oblast logistiky. Součástí tohoto konceptu je závazná jmenná konvence, kterou by se měli řídit všichni zaměstnanci při jakékoliv budoucí tvorbě rolí. Dále je součástí také postup, jak správně přiřadit roli uživateli, aby nedošlo k porušení žádného z bezpečnostních pravidel. Hlavní částí návrhu je však přehled rolí, které jsou pro oblast logistiky výrobního závodu nezbytné.

Jednotlivé role korespondují s pracovními pozicemi v závodě. Každá role má přiřazená veškerá oprávnění, která v rámci logistických procesů potřebuje. Toho bylo docíleno díky využití informací získaných z procesní analýzy.

Pro tento návrh autorizačního konceptu byl poté vytvořen plán realizace a odhad nákladů realizace. Odhad nákladů byl vytvořen ve čtyřech variantách, jelikož existuje více možností, jak může výrobní závod přistupovat k proplácení práce svých zaměstnanců.

Zároveň byla vyhodnocena rizika, která návrhu hrozí, a způsoby, jak tato rizika eliminovat, popřípadě co dělat, když se riziko stane skutečností. Na druhou stranu byly vyhodnoceny i přínosy navrhovaného autorizačního konceptu. Mezi tyto přínosy patří mimo zvýšení bezpečnosti informací i snížení nákladů za opakované vytváření autorizačních konceptů pro jednotlivé výrobní závody.

Práce se zaměřuje na obecný návrh autorizačního konceptu pro oblast

logistiky. V budoucnu by proto bylo vhodné zaměřit se na vytvoření návrhu autorizačního konceptu pro další oblasti výrobního závodu, stejně jako na detailní návrh technické stránky konceptu.

Mezi hlavní přínosy celé práce patří kromě vytvoření návrhu autorizačního konceptu i fakt, že práci bude možné použít jako základ dokumentace autorizačního konceptu. Zároveň bude možné použít procesní analýzu i v dalších projektech společnosti, nejen při tvorbě autorizačního konceptu. Práce bude v následujících měsících použita pro tvorbu autorizačního konceptu nově vznikajícího výrobního závodu v jihovýchodní Asii.

Bibliografie

1. *Global Company Information* [online]. SAP. [cit. 2019-03-10]. Dostupné z: https://www.sap.com/corporate/en/company.html.
2. GÁLA, Libor; POUR, Jan; ŠEDIVÁ, Zuzana. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing, 2015. ISBN 978-80-247-5457-4.
3. SKLENÁK, Vilém. *Data, informace, znalosti a Internet*. Praha: C.H. Beck, 2001. ISBN 80-717-9409-0.
4. TROMBLEY, Sue. Managing your information risk. *Computer Fraud & Security* [online]. Roč. 2015, č. 7, s. 5–9 [cit. 2018-11-27]. ISSN 1361-3723. Dostupné z DOI: 10.1016/S1361-3723(15)30065-8.
5. *GDPR stručně* [online]. Úřad pro ochranu osobních údajů [cit. 2018-11-27]. Dostupné z: https://www.uoou.cz/gdpr%5C%2Dstrucne/ds-4843/p1=4843.
6. KOSUTIC, Dejan. ISO 27001 vs. ISO 27002. *Advisera* [online] [cit. 2018-09-27]. Dostupné z: https://advisera.com/27001academy/knowledgebase/iso-27001-vs-iso-27002/.
7. WEBB, Jeb; AHMAD, Atif; MAYNARD, Sean B.; SHANKS, Graeme. A situation awareness model for information security risk management. *Computers & Security* [online]. 2014, č. 44, s. 1–15 [cit. 2018-11-15]. ISSN 0167-4048. Dostupné z DOI: 10.1016/j.cose.2014.04.005.
8. When Employees Leave So Does Your Data, Research Reveals. *Iron Mountain* [online] [cit. 2018-11-27]. Dostupné z: https://investors.ironmountain.com/default.aspx?SectionId=5cc5ecae-6c48-4521-a1ad-480e593e4835%5C%5C&LanguageId=1%5C%5C&PressReleaseId=35917aff-775b-481e-9dd2-50df556c6aab.

9. *Sociální inženýrství* [online]. Národní centrum kybernetické bezpečnosti [cit. 2019-02-17]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/.

10. STEWART, James Michael. *CompTIA security+ review guide*. 3rd ed. Indianapolis, IN: SYBEX, A Wiley Brand, 2014. ISBN 978-1118901373.

11. AL-SHAER, Ehab S.; HAMED, Hazem H. Firewall Policy Advisor for Anomaly Discovery and Rule Editing. In: GOLDSZMIDT, Germán; SCHÖNWÄLDER, Jürgen (ed.). *Integrated Network Management VIII* [online]. IFIP — The International Federation for Information Processing, vol. 118. Boston, MA: Springer US, 2003, s. 17–30 [cit. 2018-10-09]. ISBN 978-1-4757-5521-3. ISSN 1868-4238. Dostupné z DOI: 10.1007/978-0-387-35674-7_2.

12. BUTLER, Chris. *IT security interviews exposed: secrets to landing your next information security job*. Indianapolis, IN: Wiley Publishing, Inc, 2007. ISBN 978-0-471-77987-2.

13. *Secure Network Communications (SNC)* [online]. SAP Documentation [cit. 2019-03-10]. Dostupné z: https://help.sap.com/doc/saphelp_nw70ehp1/7.01.16/en-US/e6/56f466e99a11d1a5b00000e835363f/frameset.htm.

14. HAUSMAN, Kalani Kirk; COOK, Susan L. *IT architecture for dummies*. Hoboken, NJ: Wiley Pub., 2011. ISBN 978-0-470-55423-4.

15. *Pojem diskrece* [online]. ABZ slovník cizích slov [cit. 2018-12-11]. Dostupné z: https://slovnik-cizich-slov.abz.cz/web.php/slovo/diskrece.

16. DE CAPITANI DI VIMERCATI, Sabrina; FORESTI, Sara; SAMARATI, Pierangela. Authorization and Access Control. In: *Security, Privacy, and Trust in Modern Data Management* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, s. 39–53 [cit. 2018-11-27]. ISBN 978-3-540-69860-9. Dostupné z DOI: 10.1007/978-3-540-69861-6_4.

17. OSBORN, Sylvia L. Role-Based Access Control. In: *Security, Privacy, and Trust in Modern Data Management* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, s. 55–70 [cit. 2018-11-27]. ISBN 978-3-540-69860-9. Dostupné z DOI: 10.1007/978-3-540-69861-6_5.

18. LEHNERT, Volker; BONITZ, Katharina; JUSTICE, Larry. *Authorizations in SAP software: design and configuration*. Boston, MA: Galileo Press, 2011. ISBN 978-1-59229-342-1.

19. *Firefighter IDs* [online]. SAP Documentation [cit. 2019-03-10]. Dostupné z: https://help.sap.com/doc/saphelp_grcac10/10.0/en-US/e9/140404e23d4075866bc9c93ba98be1/frameset.htm.

20. Rozhovor s Ing. Matějem COGANEM, IT Business analytikem na oddělení údržby a managementu SAP logistiky společnosti X. Mladá Boleslav 20. 3. 2019.

21. *The Authorization Concept* [online]. SAP Library [cit. 2019-03-10]. Dostupné z: https://help.sap.com/doc/saphelp_470/4.7/en-US/4f/993844446d11d189700000e8322d00/frameset.htm.

22. *Authorizations, Profiles and the Profile Generator* [online]. SAP Library [cit. 2019-03-10]. Dostupné z: https://help.sap.com/doc/saphelp_470/4.7/en-US/52/671273439b11d1896f0000e8322d00/content.htm?loaded_from_frameset=true.

23. *The Profile Generator* [online]. SAP Library [cit. 2019-03-10]. Dostupné z: https://help.sap.com/doc/saphelp_470/4.7/en-US/b2/050a94dd0111d2961f0000e82de14a/content.htm?loaded_from_frameset=true.

24. *AS ABAP Authorization Concept* [online]. SAP Documentation [cit. 2019-03-10]. Dostupné z: https://help.sap.com/doc/saphelp_srm70/7.0/en-US/52/671285439b11d1896f0000e8322d00/frameset.htm.

25. *Role Administration* [online]. SAP Library [cit. 2019-03-10]. Dostupné z: https://help.sap.com/doc/saphelp_nw70/7.0.31/en-US/52/6714a9439b11d1896f0000e8322d00/content.htm?no_cache=true.

26. *About the Business Process Model and Notation Specification Version 2.0.2* [online]. Object Management Group [cit. 2019-05-10]. Dostupné z: https://www.omg.org/spec/BPMN/.

27. SILVER, Bruce. *BPMN method and style: with BPMN implementer's guide*. 2nd ed. Aptos: Cody-Cassidy Press, 2011. ISBN 978-0-9823681-1-4.

28. Rozhovor s Ing. Slavomilem ŠTEFÁNEM, IT systémovým analytikem na oddělení údržby a managementu SAP logistiky společnosti X. Mladá Boleslav 5. 4. 2019.

29. Rozhovor s Martinem ŠVANDOU, odborným koordinátorem IS na oddělení údržby a managementu SAP logistiky společnosti X. Mladá Boleslav 25. 3. 2019.

Příloha **A**

Seznam použitých zkratek

ACL Access Control List (Kontrolní list přístupu)

BPMN Business Process Modeling and Notation (Modelování a notace podnikových procesů)

CIA Confidentiality, Integrity, Availability (Důvěrnost, integrita, dostupnost)

ČLH Člověkohodina

DAC Discretionary Access Control (Diskreční řízení přístupu)

EDI Electronic Data Interchange (Elektronická výměna dat)

ERP Enterprise Resource Planning (Plánování podnikových zdrojů)

EU European Union (Evropská unie)

GDPR General Data Protection Regulation (Obecné nařízení na ochranu osobních údajů)

IAM Identity and Access Management (Řízení identit a přístupu)

IEC International Electrotechnical Commission (Mezinárodní elektrotechnická komise)

ISRM Information Security Risk Management (Řízení rizik informační bezpečnosti)

ISO International Organization for Standardization (Mezinárodní organizace pro normalizaci)

IT Information Technology (Informační technologie)

MAC Mandatory Access Control (Povinné řízení přístupu)

MRP Material Requirements Planning (Plánování potřeby materiálu)

OMG Object Management Group (Skupina správy objektů)

RBAC Role-based Access Control (Řízení přístupu založené na rolích)

SAP Systeme, Anwendungen, Produkte in der Datenverarbeitung (Systémy, Aplikace, Produkty v oblasti výpočetní techniky)

SOD Separation of Duties (Oddělení povinností)

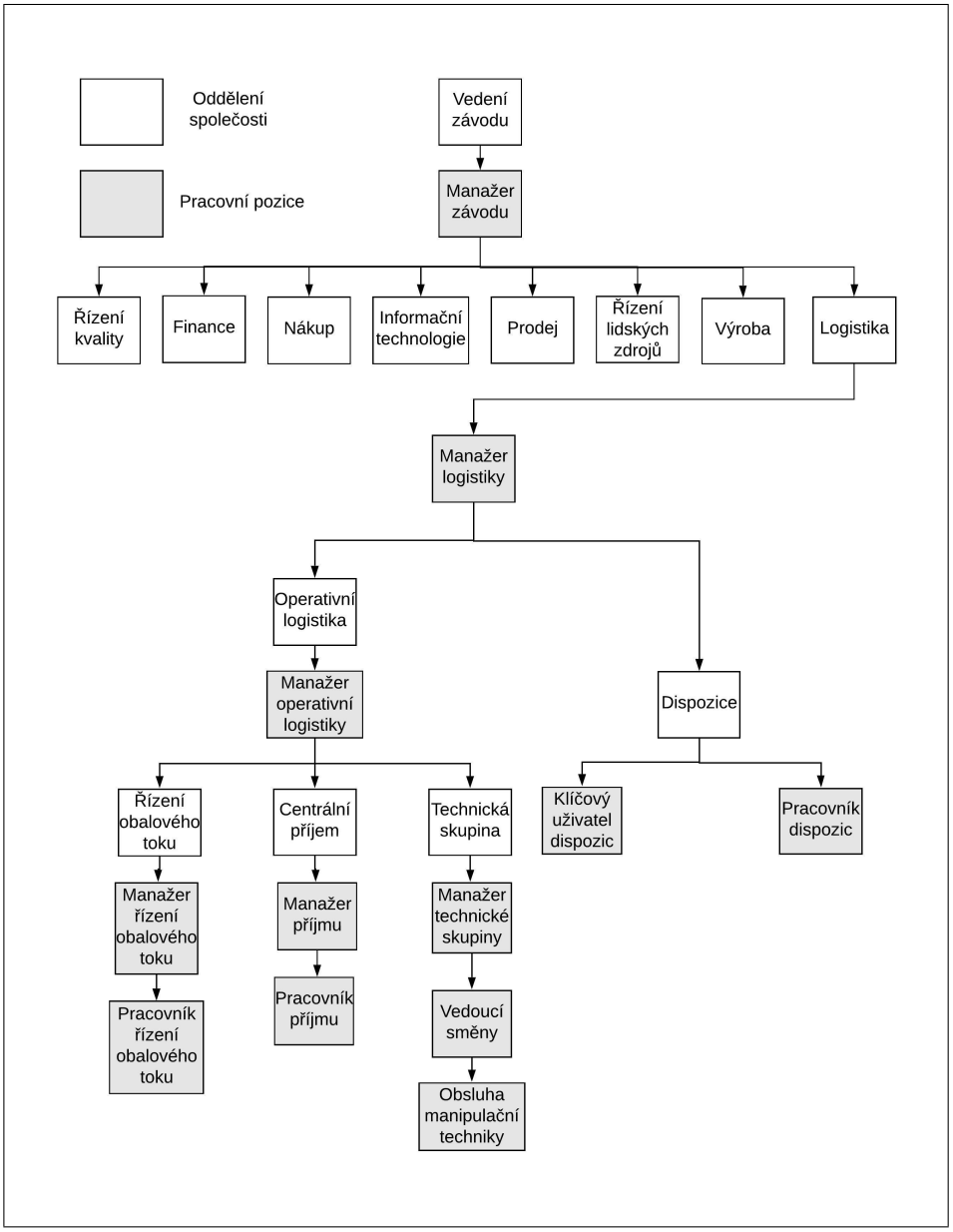
SNC Secure Network Communication (Zabezpečená síťová komunikace)

SSO Single Sign-On (Systém jednotného přihlášení)

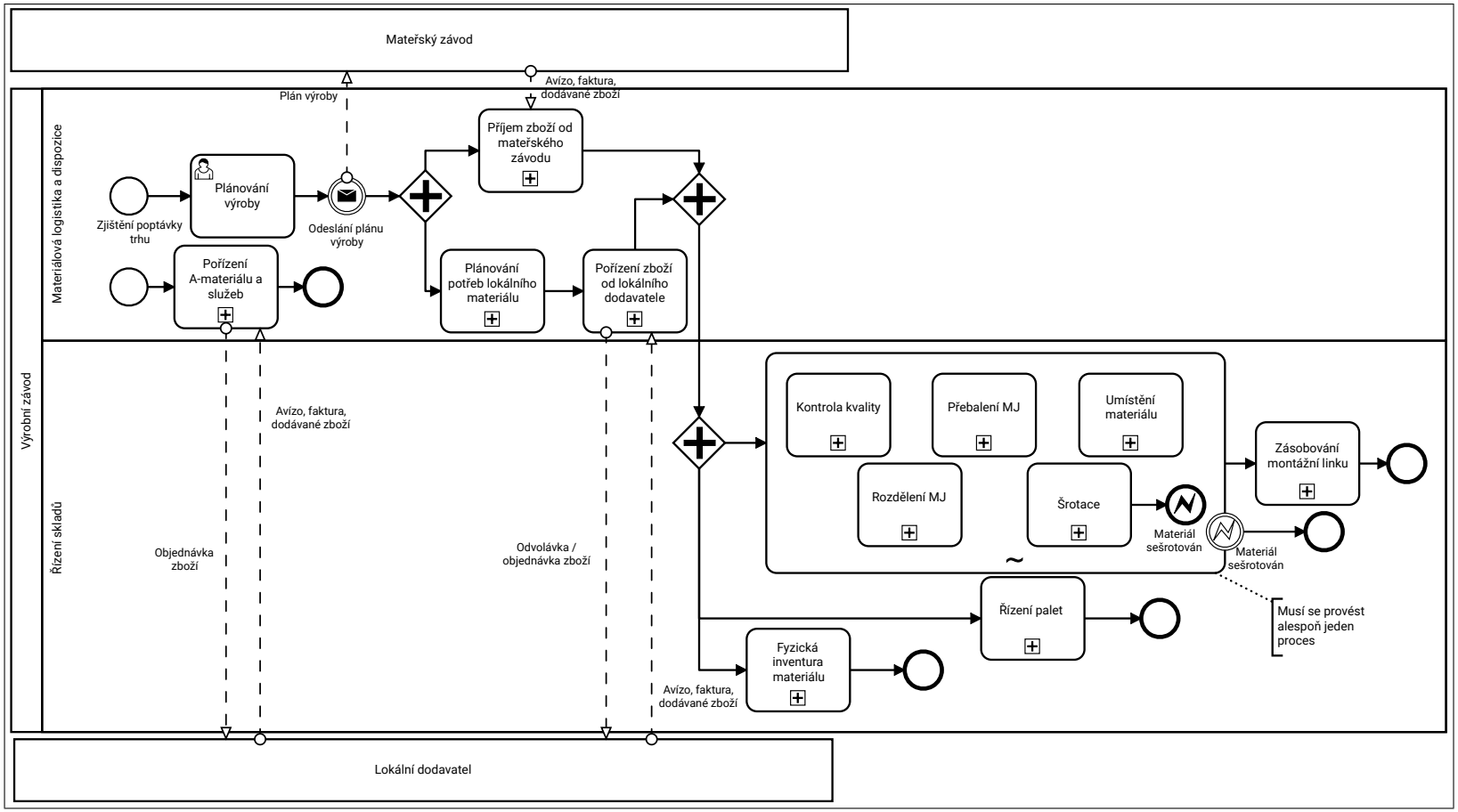
WM Warehouse Management (Řízení skladů)

Příloha B

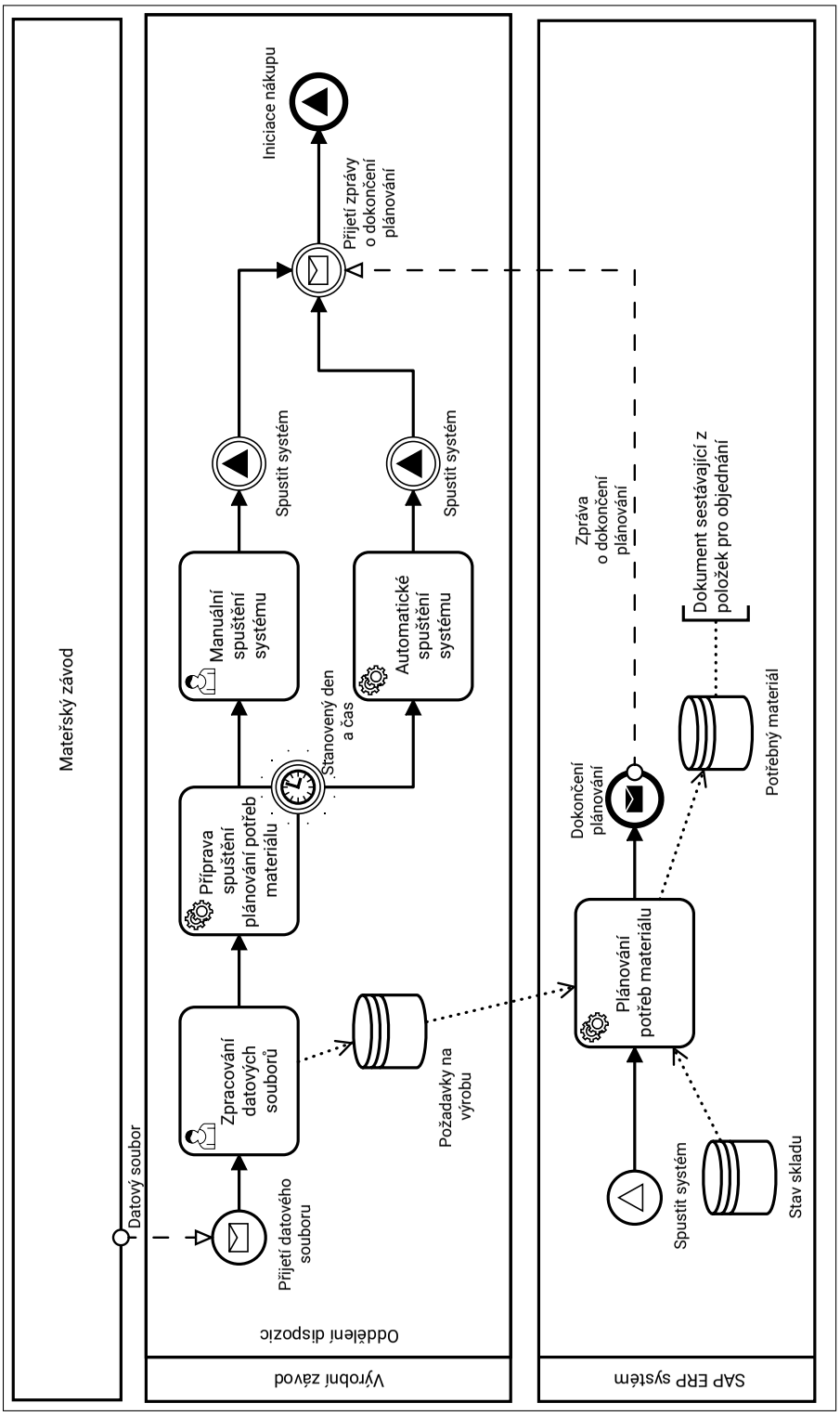
Diagramy struktury a procesů společnosti X



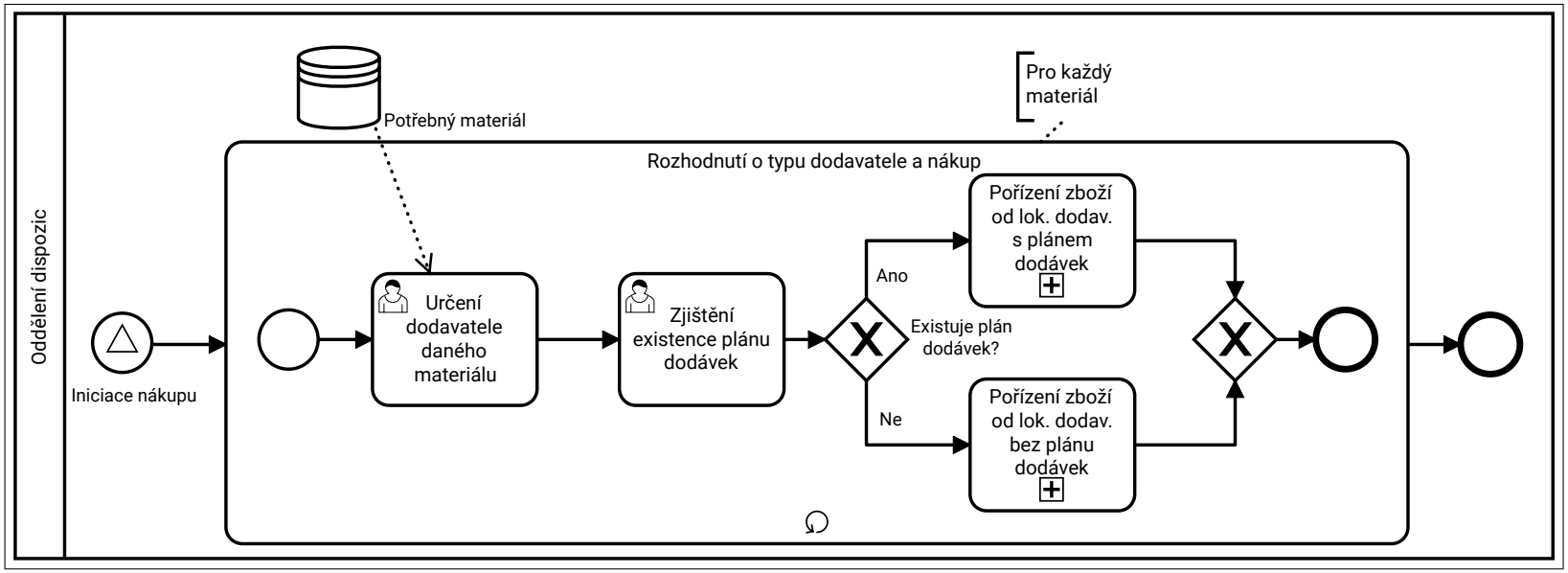
Obrázek B.1: Struktura závodu společnosti X



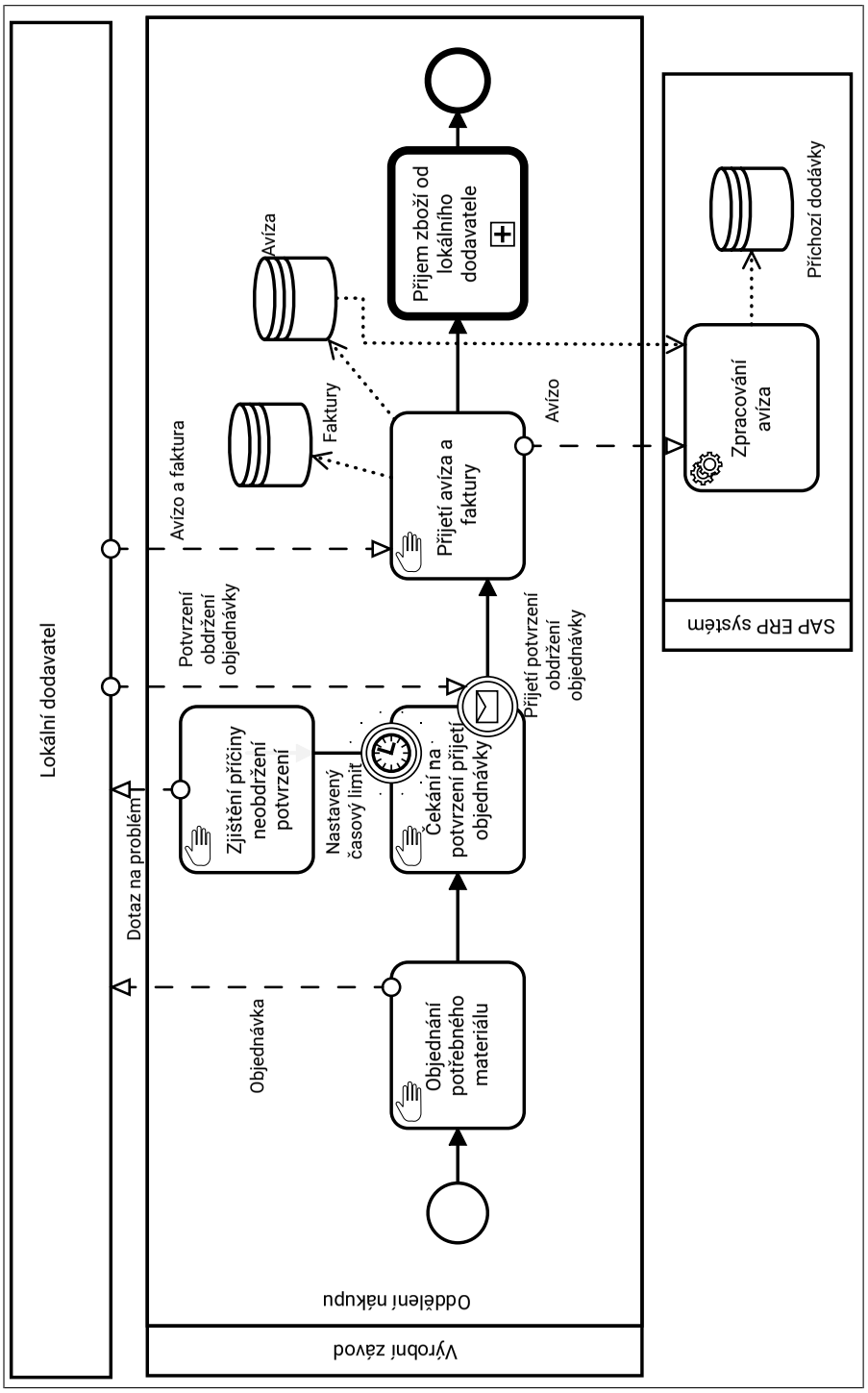
Obrázek B.2: Globální proces logistiky v závodě společnosti X



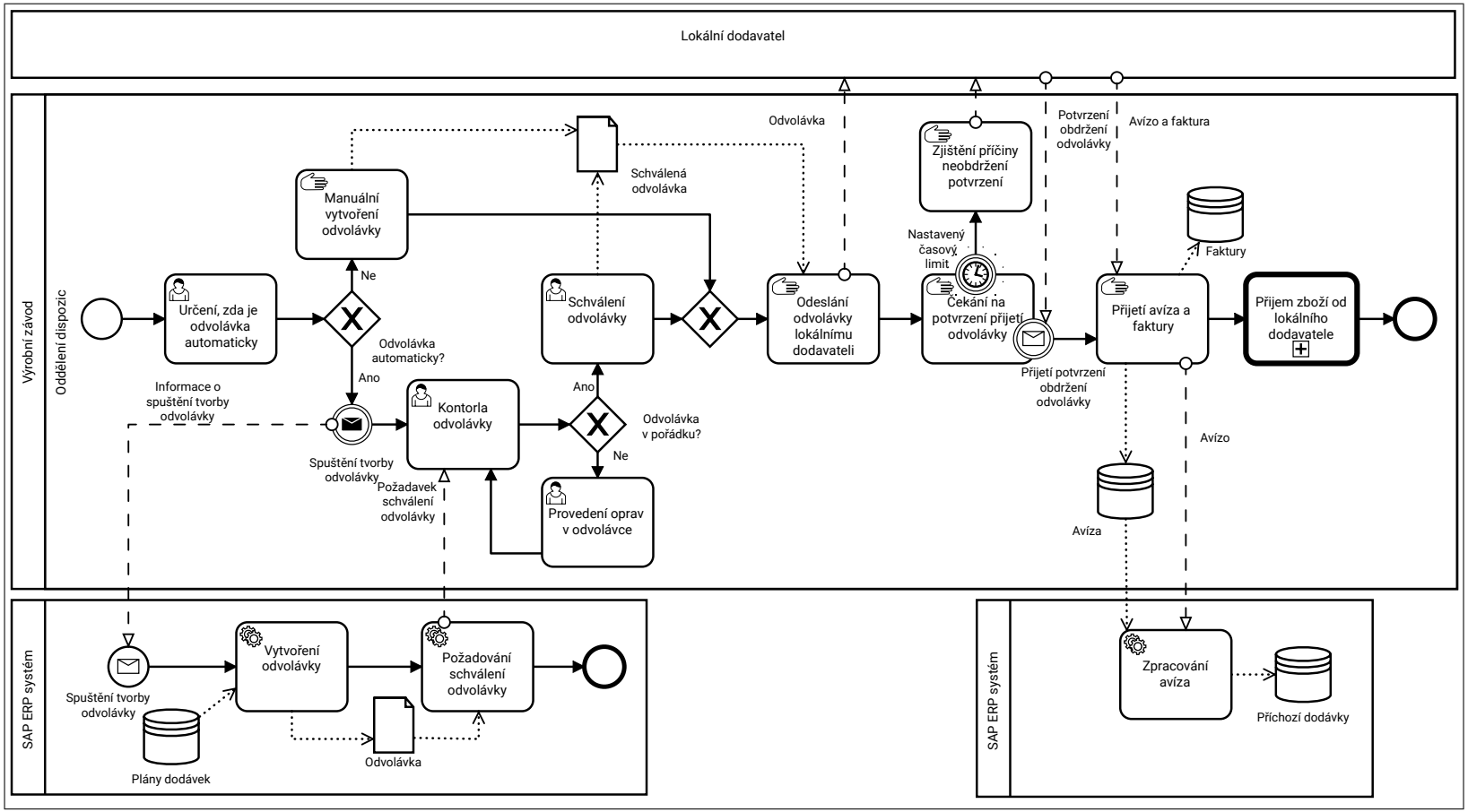
Obrázek B.3: Plánování potřeb lokálního materiálu



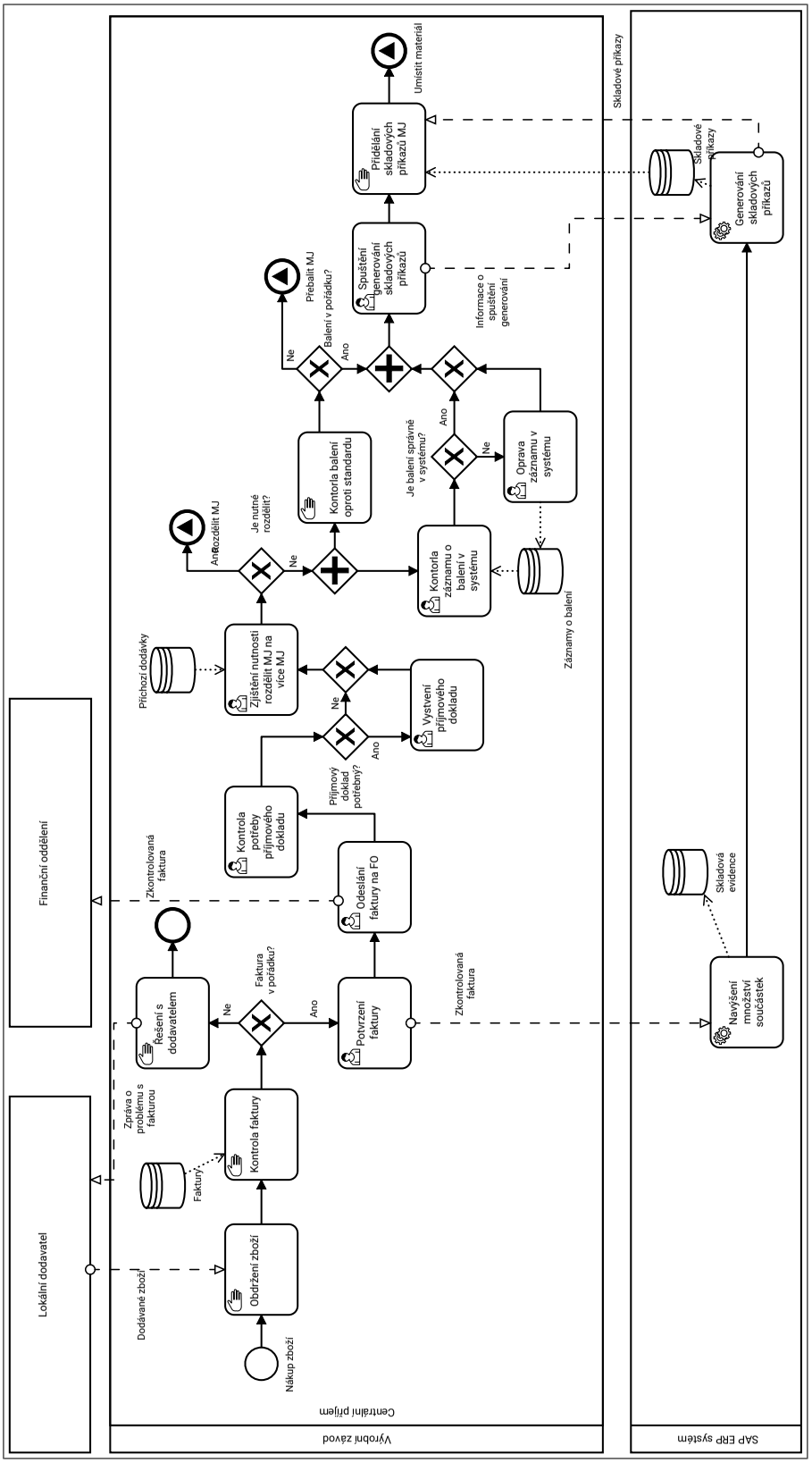
Obrázek B.4: Pořízení zboží od lokálního dodavatele



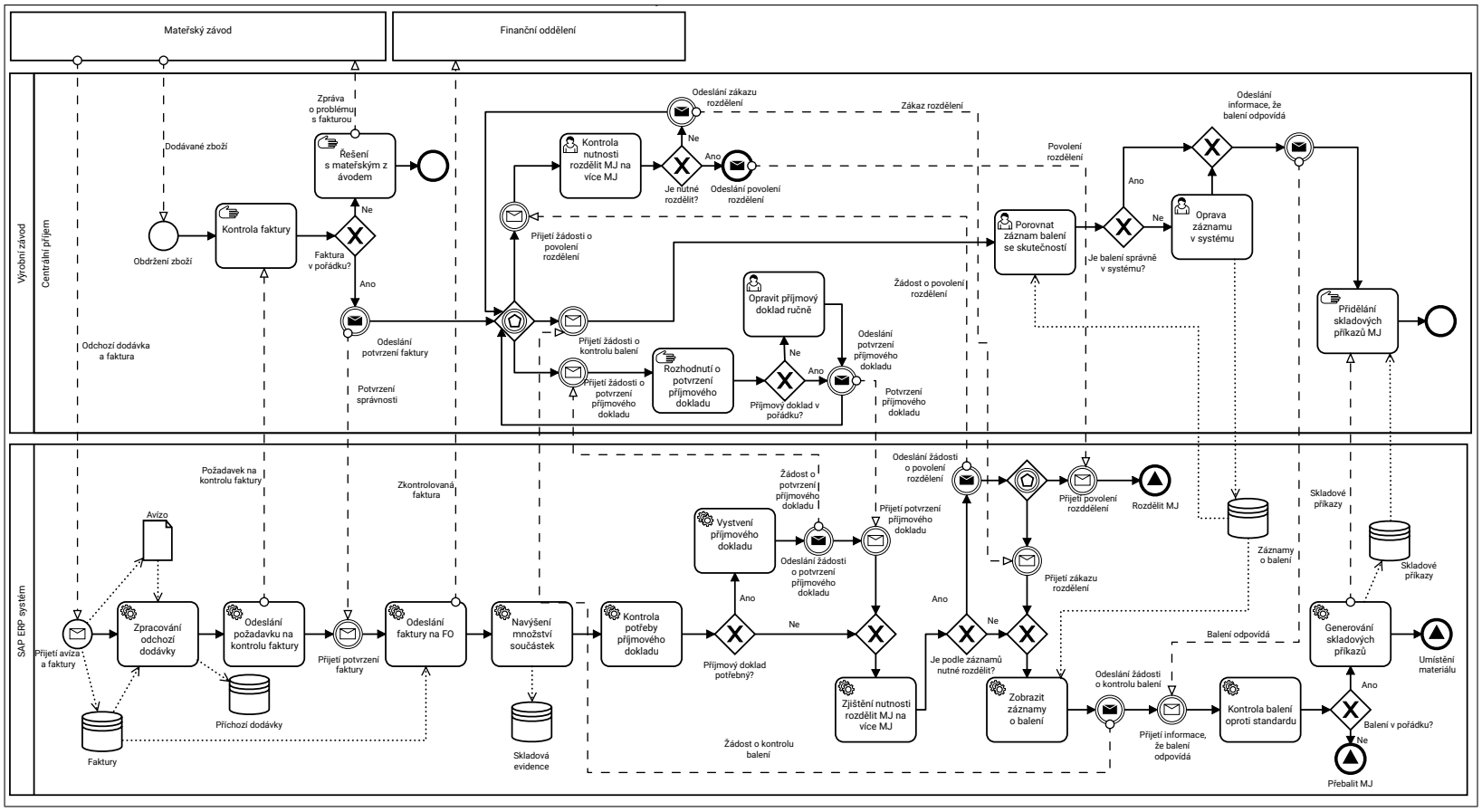
Obrázek B.5: Pořízení zboží od lokálního dodavatele bez použití plánu dodávek



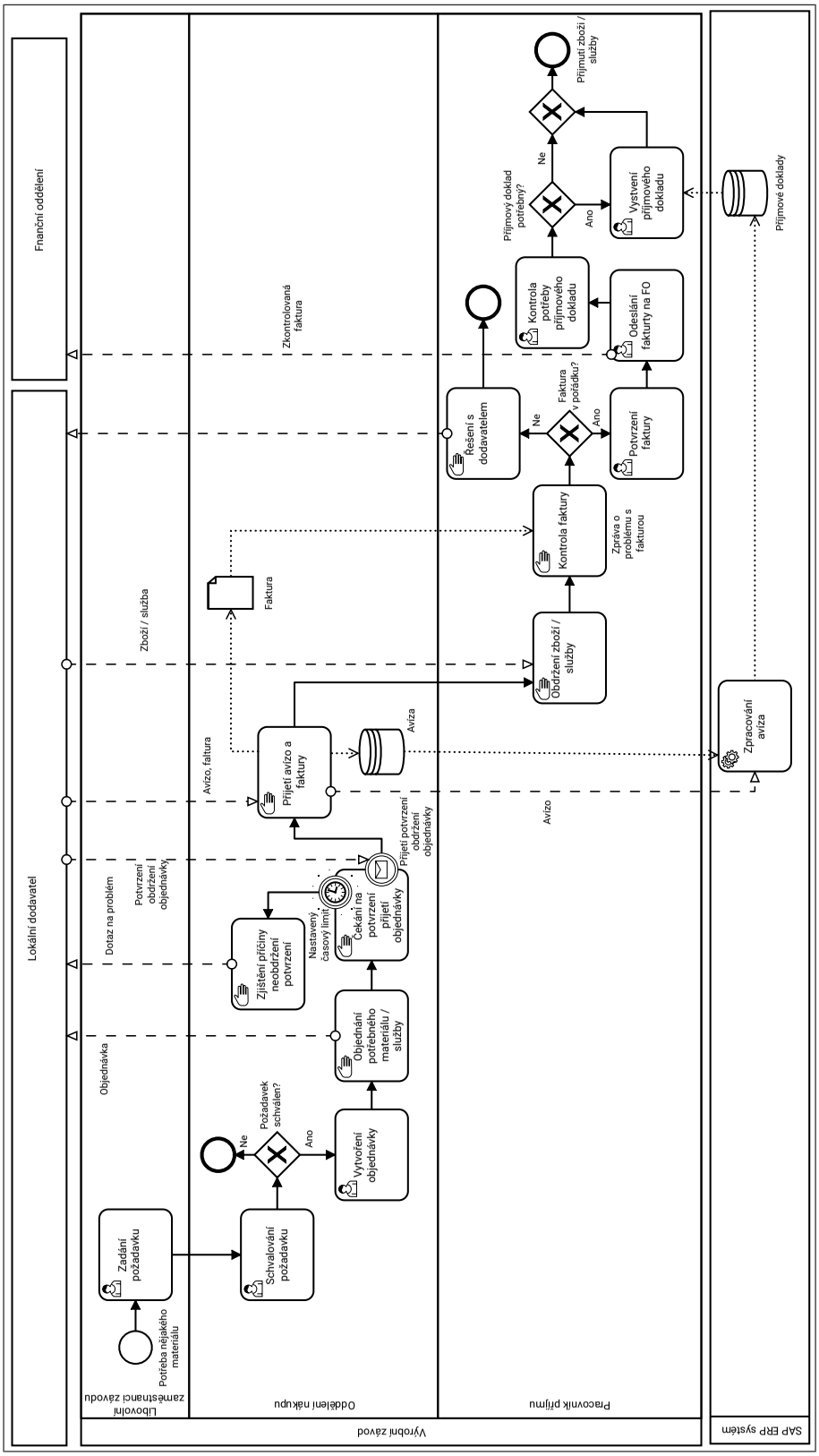
Obrázek B.6: Pořízení zboží od lokálního dodavatele s použitím plánu dodávek



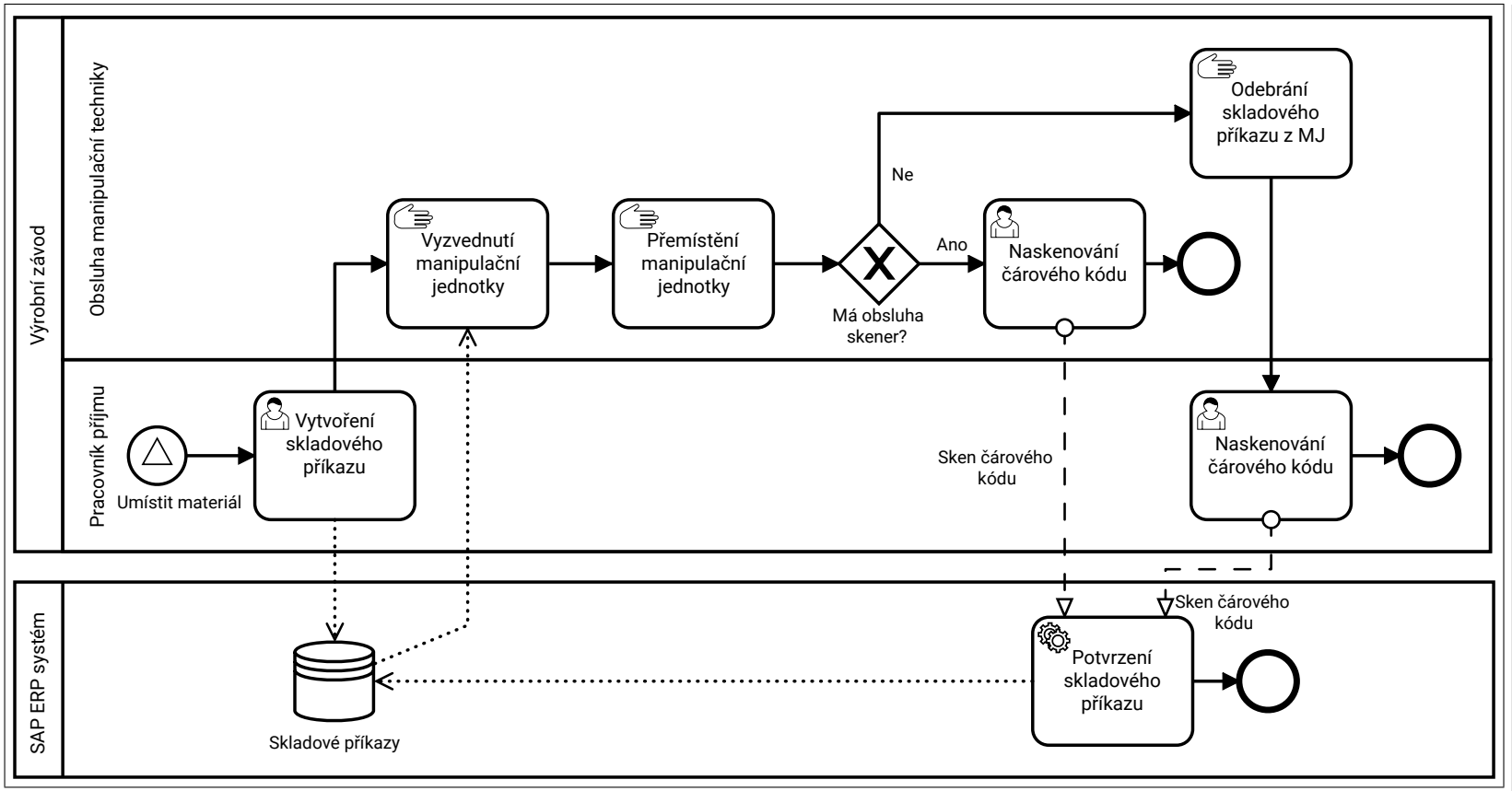
Obrázek B.7: Příjem zboží od lokálního dodavatele



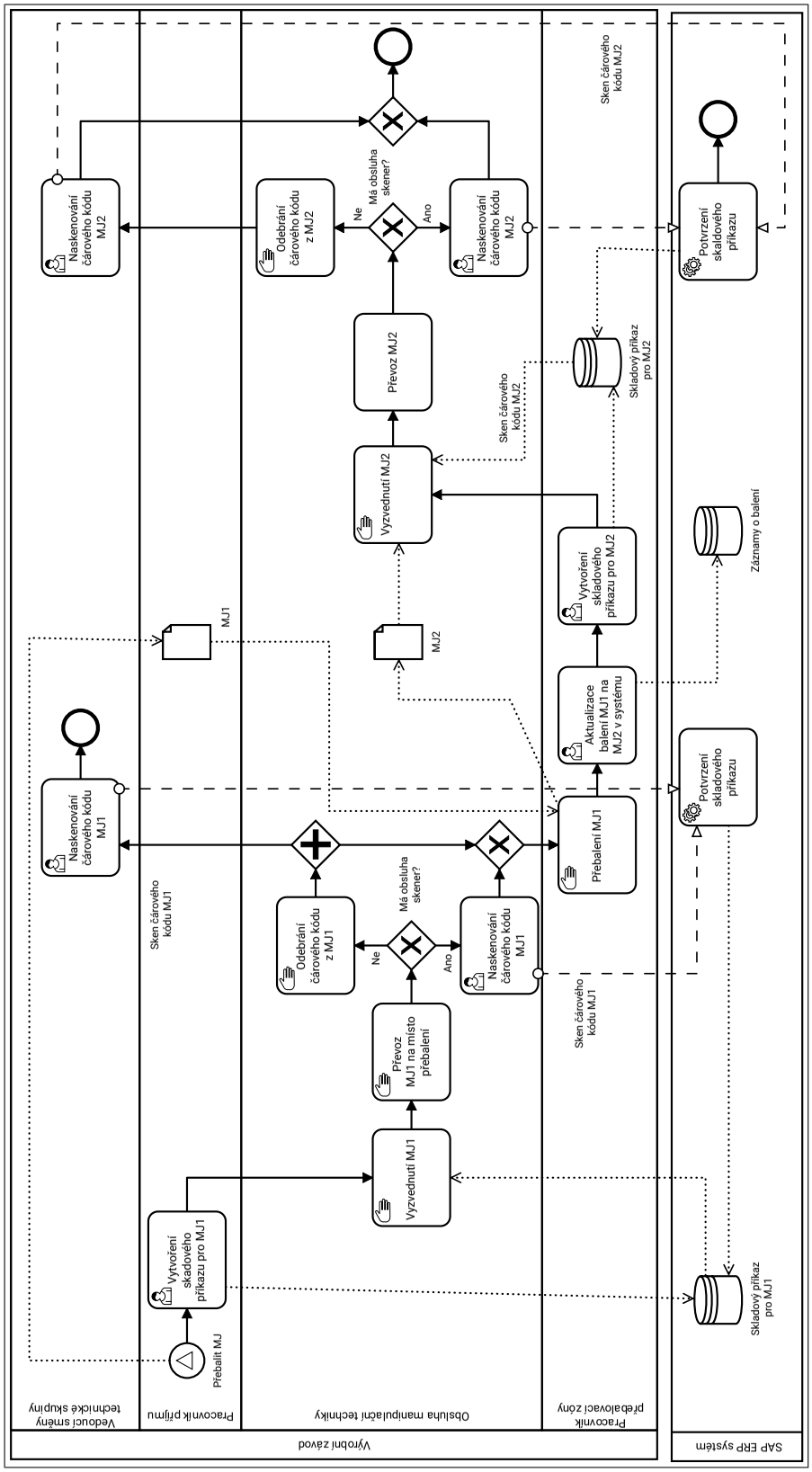
Obrázek B.8: Příjem zboží od mateřského závodu



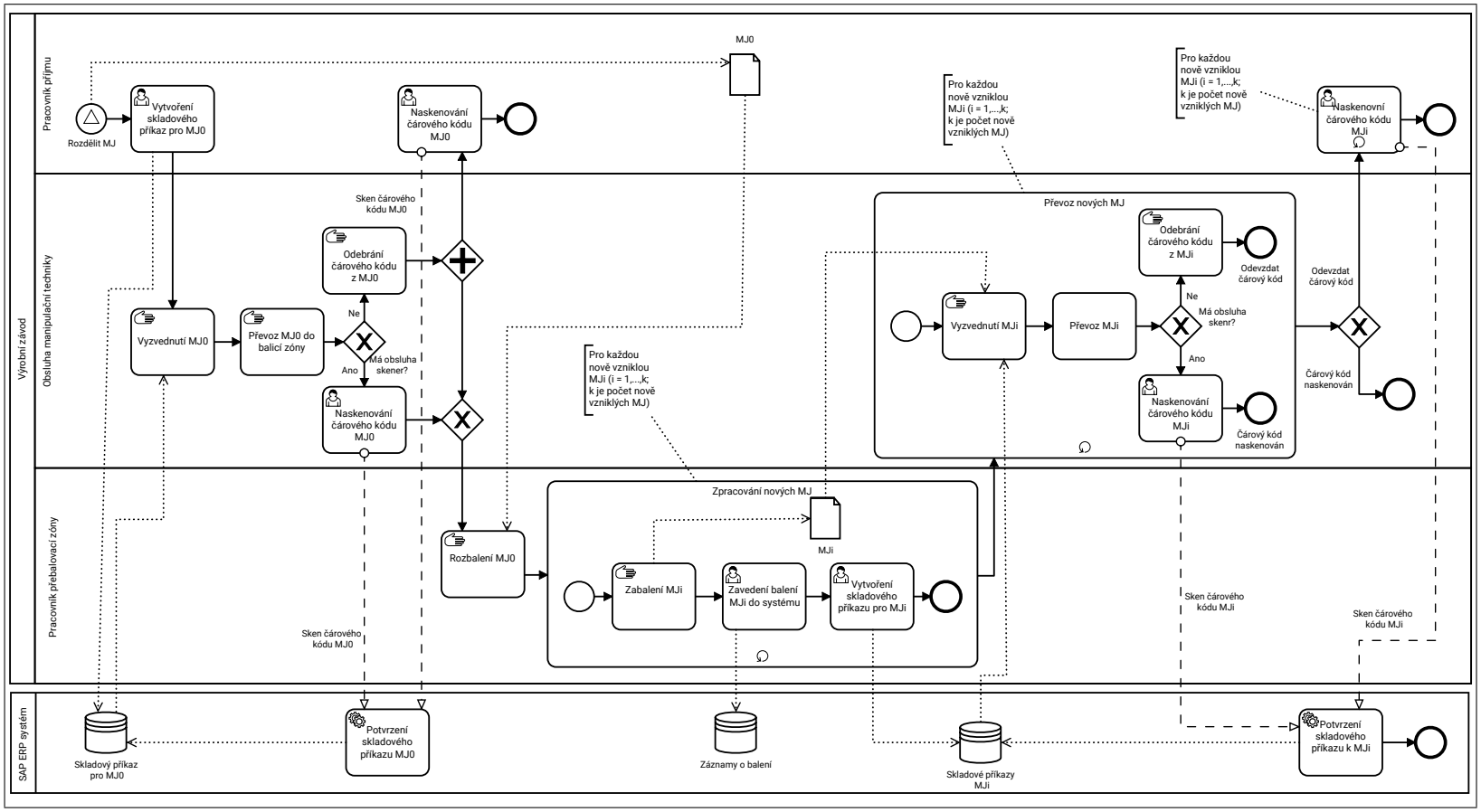
Obrázek B.9: Pořízení A-materiálu a služeb



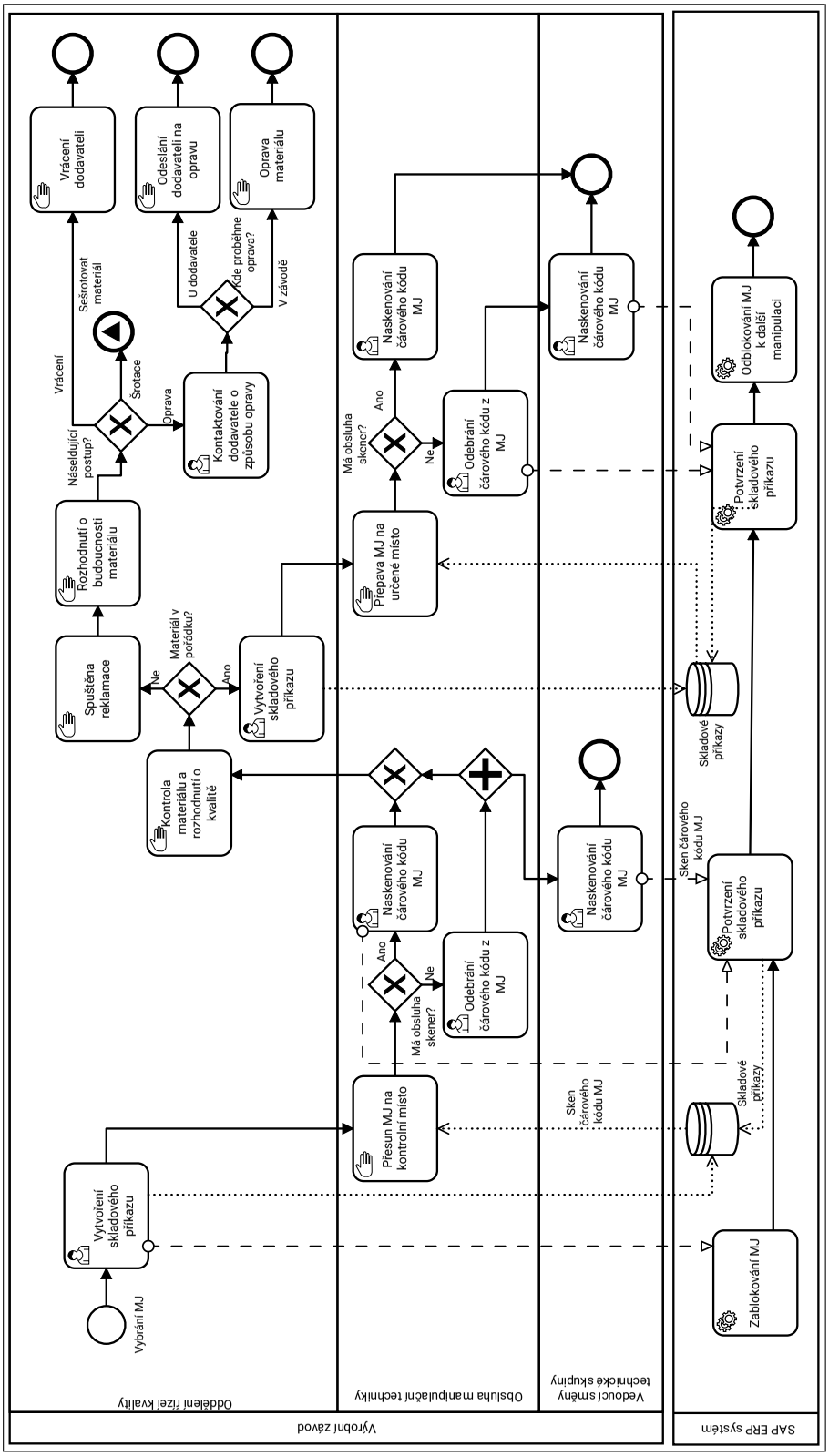
Obrázek B.10: Umístění materiálu



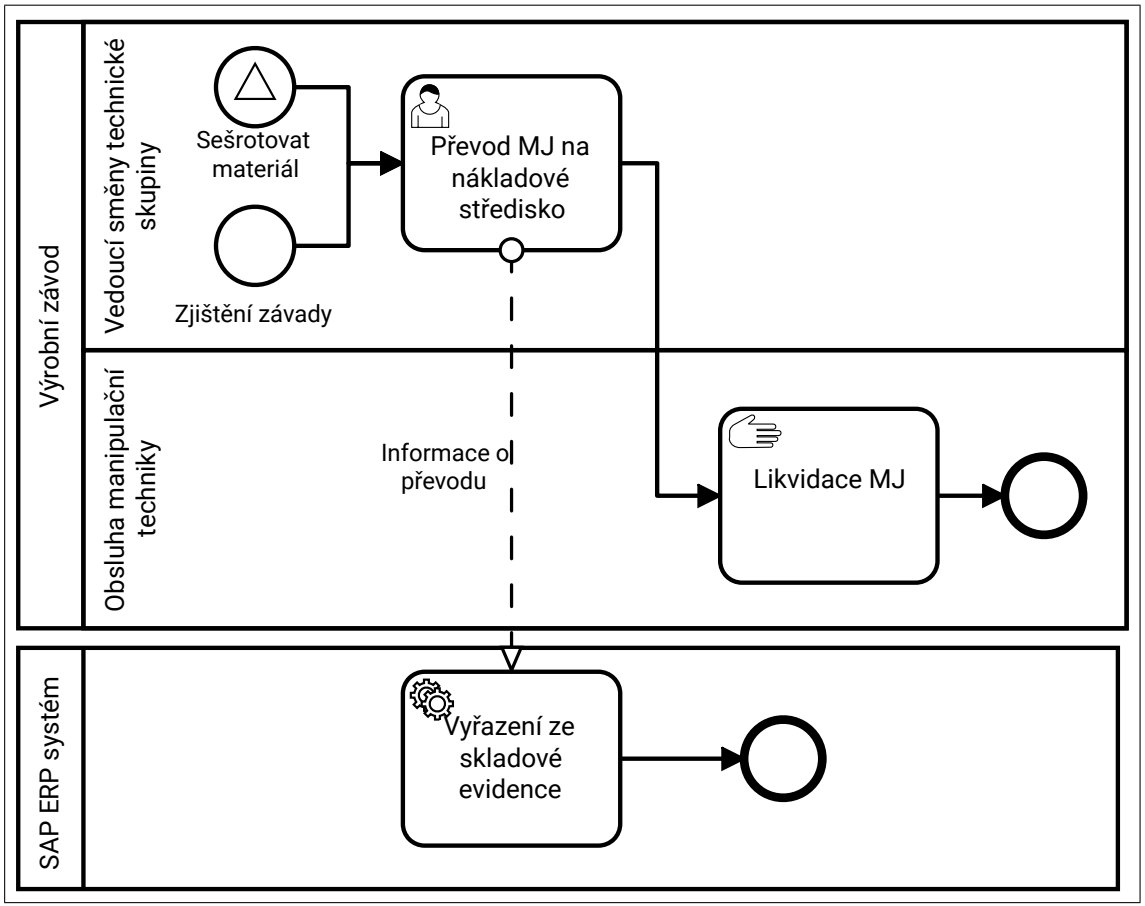
Obrázek B.11: Přebalení materiální jednotky



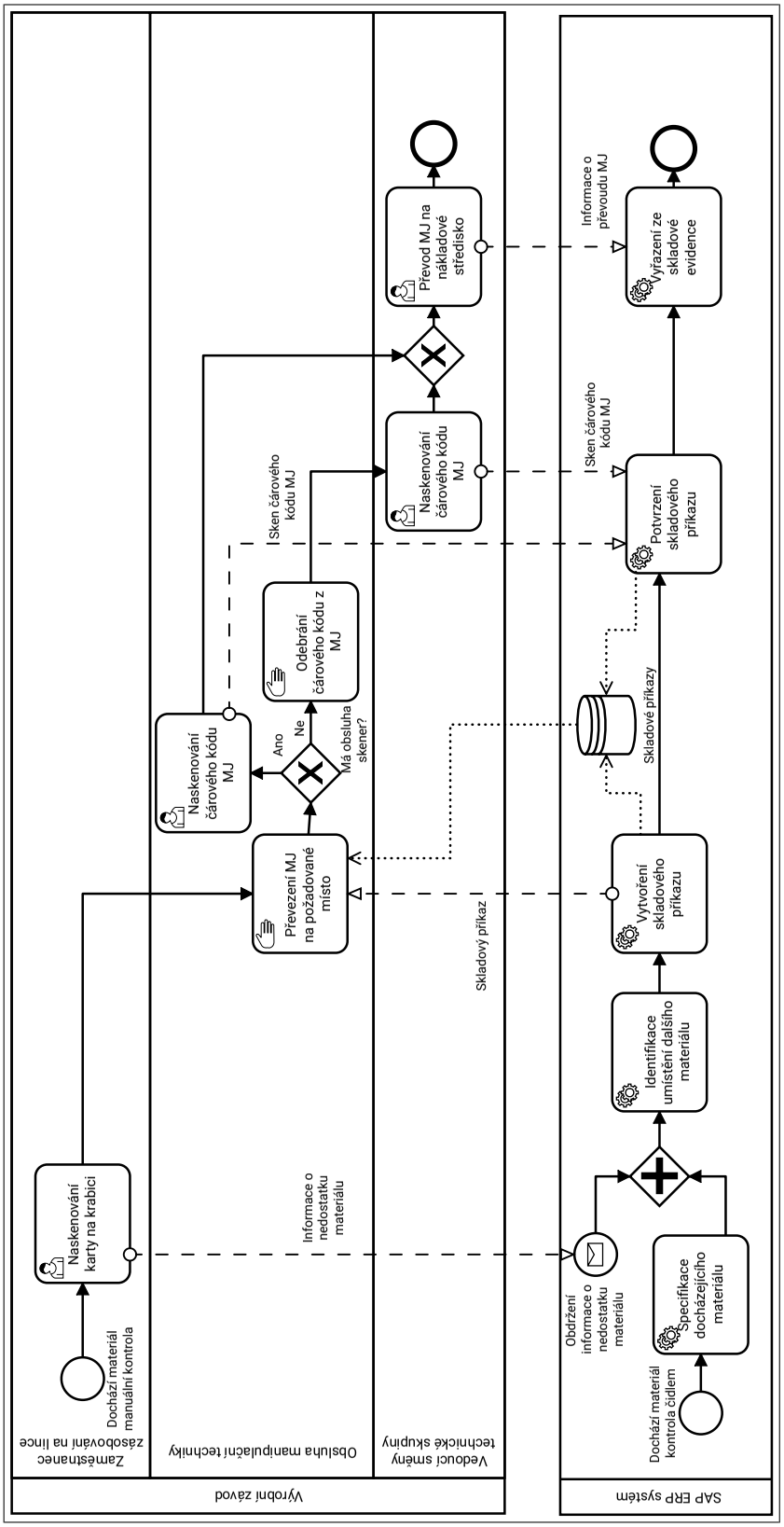
Obrázek B.12: Rozdělení materiální



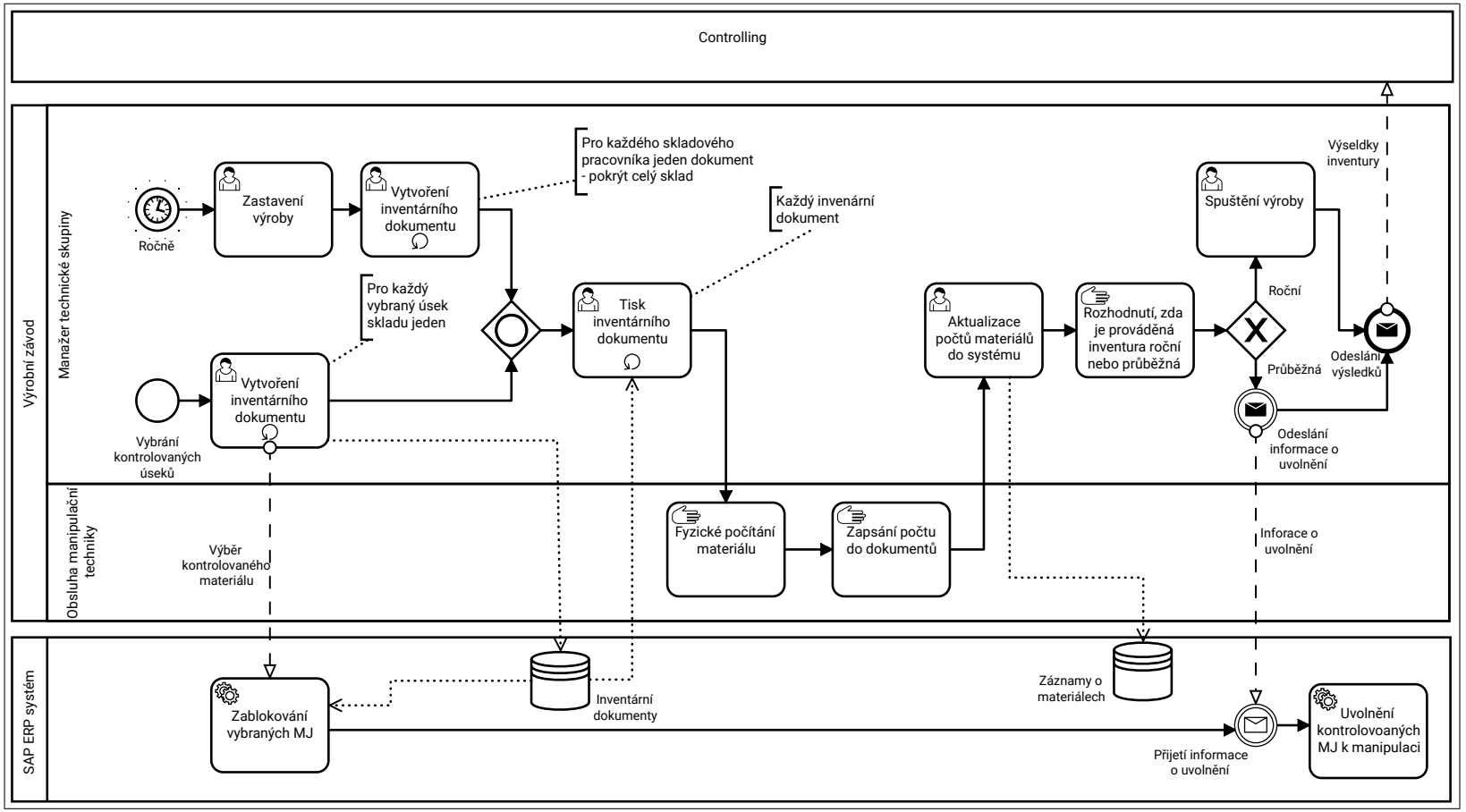
Obrázek B.13: Kontrola kvality



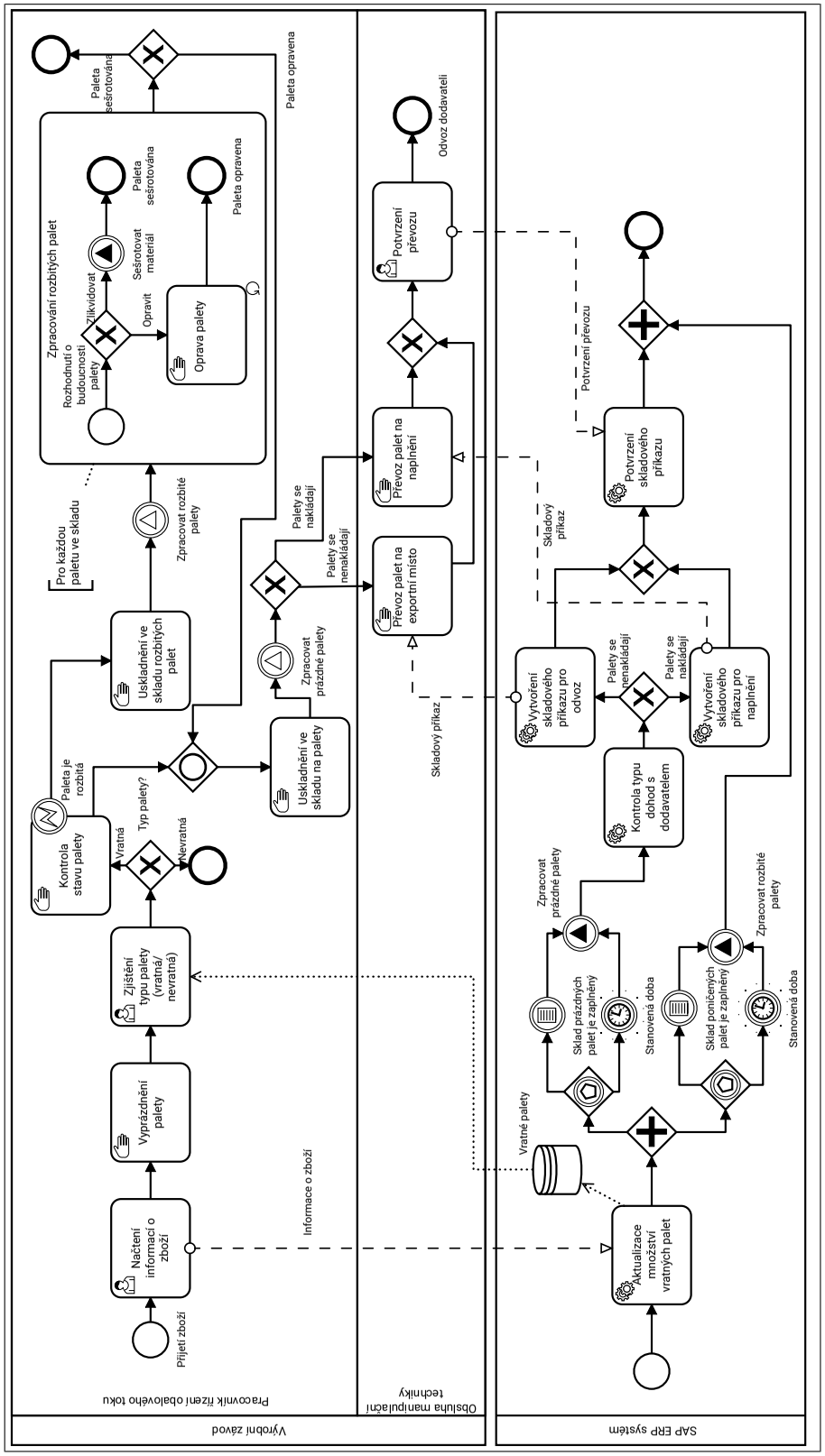
Obrázek B.14: Šrotace



Obrázek B.15: Zásobování montážní linky



Obrázek B.16: Fyzická inventura materiálu



Obrázek B.17: Řízení toku palet

Příloha C

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `diagrams` ..... diagramy vytvořené v analytické a v praktické části práce
- `src` ..... zdrojová forma práce ve formátu LaTeX
- `BP_Obermajerová_Lenka_2019.pdf` ..... text práce ve formátu pdf