Bezpečnost v oblasti MES systémů

-

kde začít?

Bezpečnost v oblasti MES systémů – kde začít?

Obsah

Bezpečnost v oblasti MES systémů – kde začít?

-Modelový příklad - Píšťalka a syn, s.r.o.
--Základní údaje

Výroba píšťalek

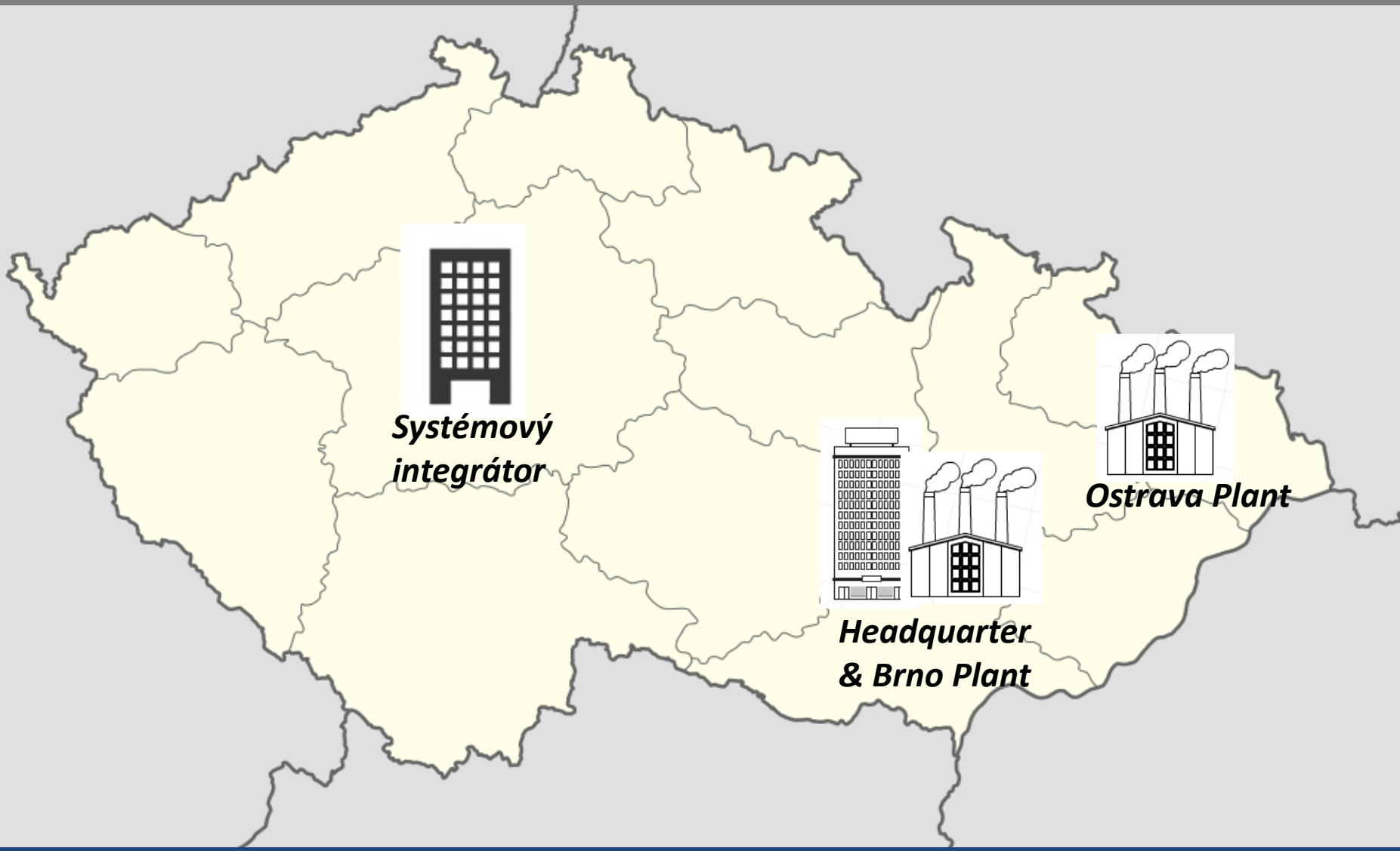
- Cca 20 druhů píšťalek
- Každá píšťalka se skládá z cca 7 komponent
- Každá píšťalka může být dodána až v 10 variantách
  - Barva kuličky
  - Druh pryžového obalu
  - Typ
  - Typ balení
- Možnost zákaznického vylisování loga
- …

Píšťalka a syn, s.r.o. a informační technologie

- Již několik let úspěšně používá lokální ERP systém
- Nově se rozhodla zavést MES systém

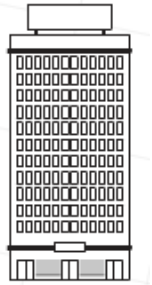
Bezpečnost v oblasti MES systémů – kde začít?

-Modelový příklad - Píšťalka a syn, s.r.o.
--Geografická lokace



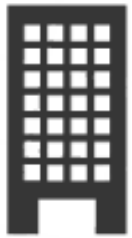
Bezpečnost v oblasti MES systémů – kde začít?

-Modelový příklad - Píšťalka a syn, s.r.o.
--Struktura společnosti



- BRNO - Headquarter
- Administrativní zázemí
- Centrální IT

- BRNO – Plant
- Lisovna plastů
- Výroba pryžových kuliček
- Finální montáž

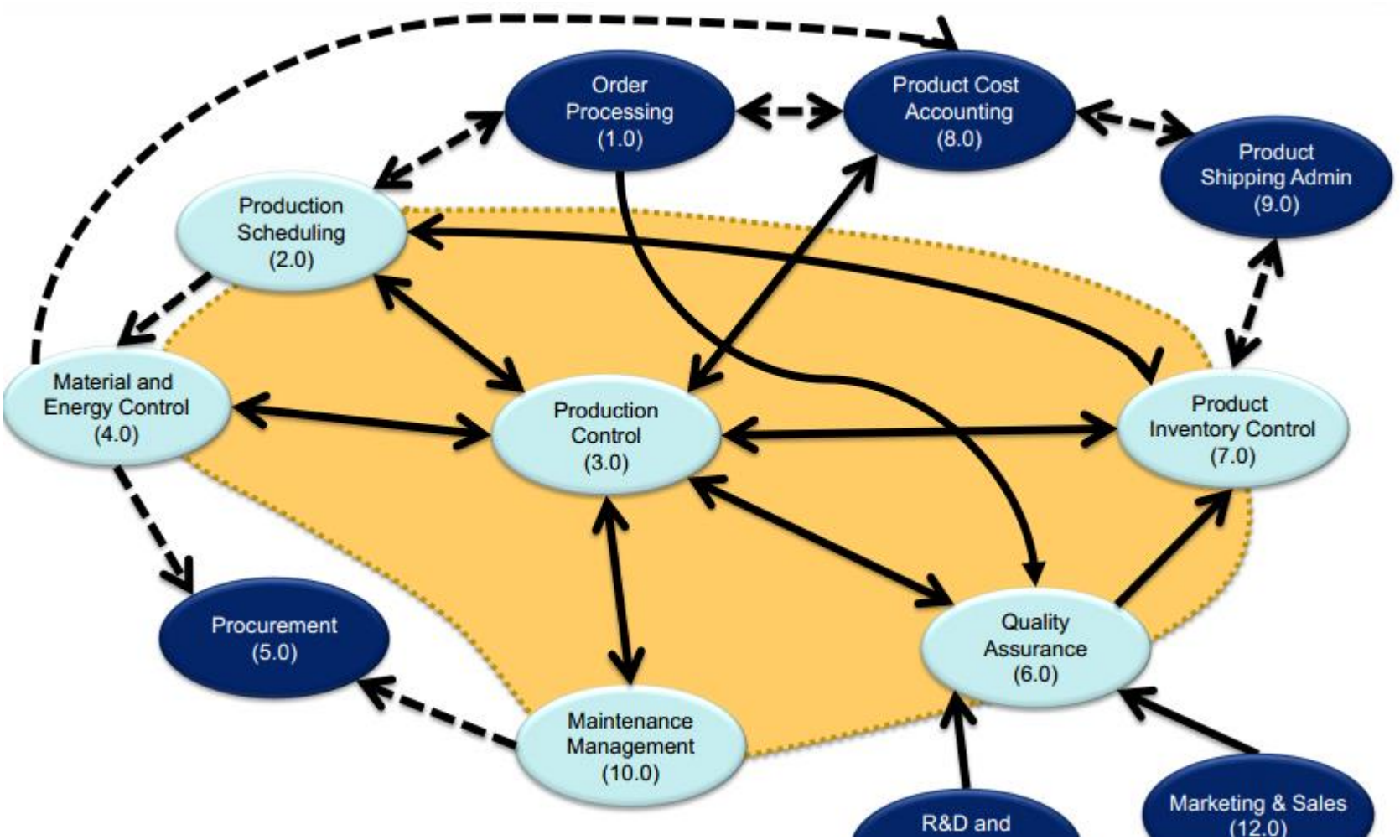


- PRAHA
- Systémový integrátor
- Servisní služby

- OSTRAVA - Plant
- Lisovna kovů
- Lokální IT

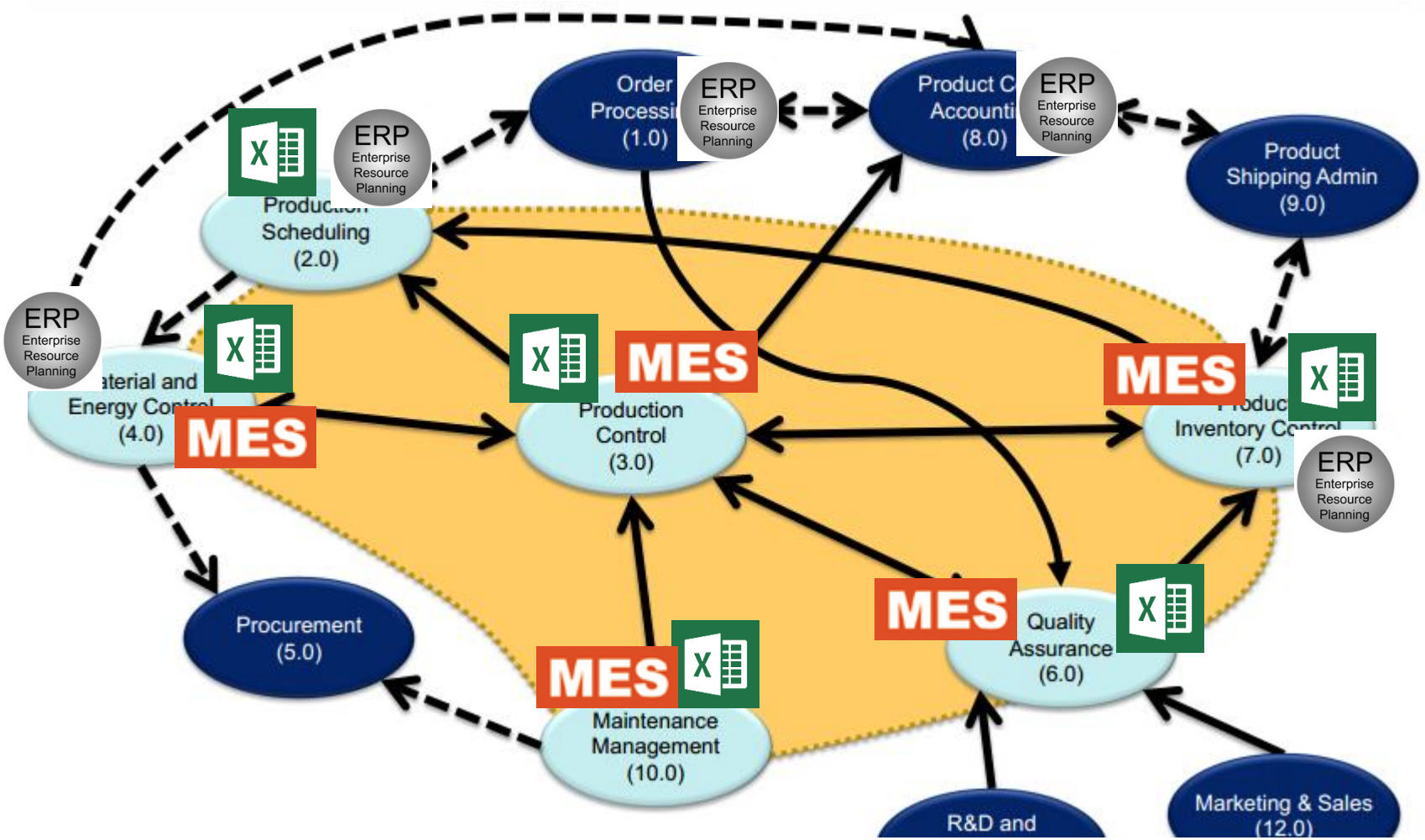
Bezpečnost v oblasti MES systémů – kde začít?

-Modelový příklad - Píšťalka a syn, s.r.o.
--Firemní procesy



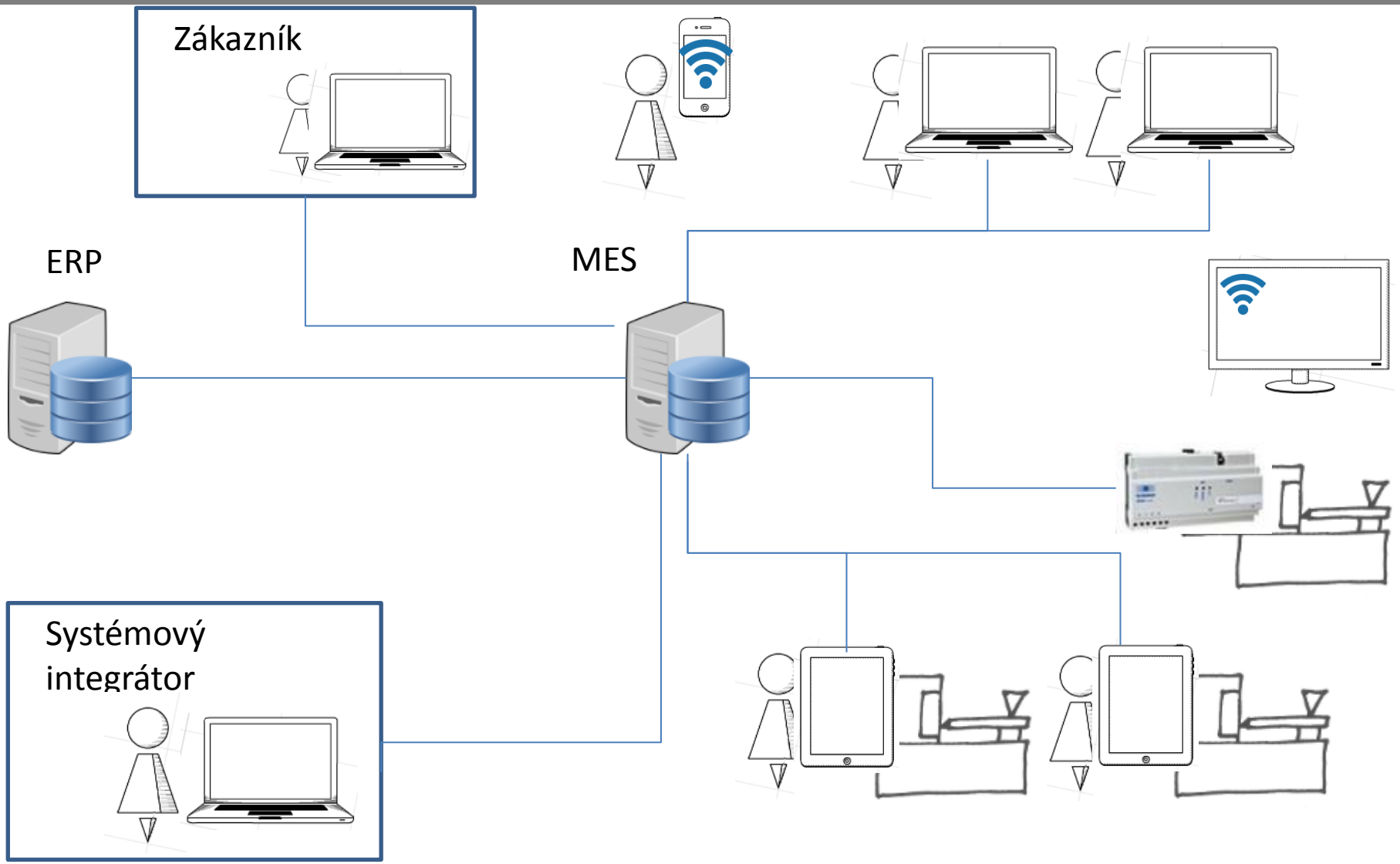
Bezpečnost v oblasti MES systémů – kde začít?

-Modelový příklad - Píšťalka a syn, s.r.o.
--Aplikační podpora



Bezpečnost v oblasti MES systémů – kde začít?

-Modelový příklad - Píšťalka a syn, s.r.o.
--Základní prvky nově zavedeného MES systému



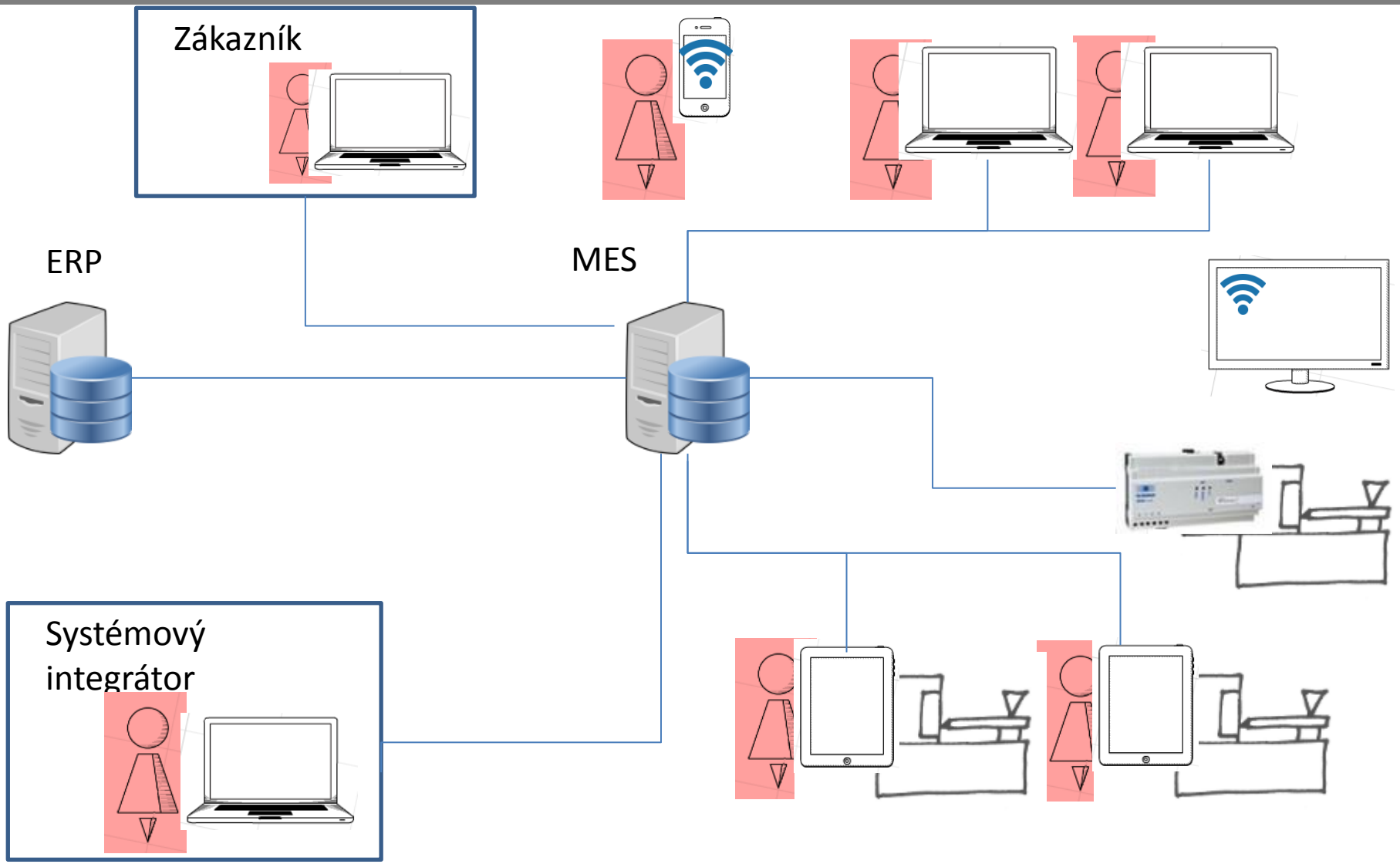
Bezpečnost MES systémů - kde začít?

identifikací rizik

Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik

---Lidé

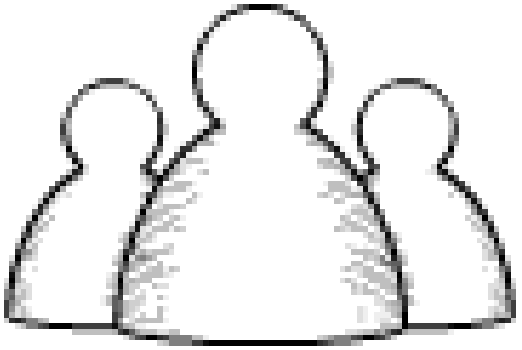


Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik
---Lidé

Uživatelské účty

- Definice jednorázových hesel
- Nutnost obnovy hesla po určité době
- Uzamknutí účtu po „n“ neúspěšných pokusech o přihlášení
- Alarmování v případě přihlášení osoby mimo definovanou pracovní dobu



Lidé jsou největším bezpečnostním rizikem

Přístupová oprávnění

- Informační systém musí disponovat velmi detailním členění přístupových práv
- Všechny přístupové práva musí být zamítnuté, dokud nejsou explicitně povolena

Bezpečnost v oblasti MES systémů – kde začít?

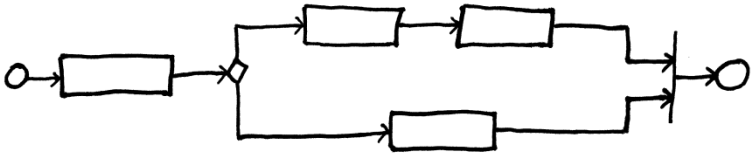
--Identifikace rizik
---Lidé

Zaškolování personálu

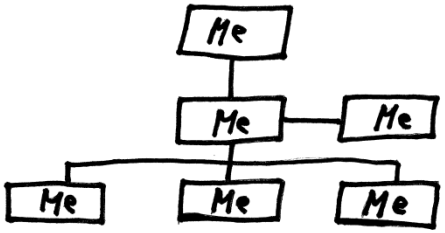
- Nesmíme zapomínat na jeden ze čtyřech základních kamenů při modernizaci našeho podniku – **Člověk**
- Neustálé investice do IT, stále se optimalizují procesy a struktury
- Člověk je nejvíce nebezpečným prvkem v bezpečnostní skládačce v oblasti MES systémů - a většinou ne záměrně

Manufacturing Maturity Level

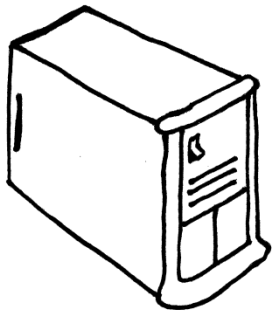
Lidé



Procesy



Struktura



IT

Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik

---Lidé

Rychlé přihlašování

- Použít pouze v případech velmi omezených přístupových práv
- RFID vs čárový kód
- Ošetřit zacházení s RFID kartou dostatečným školením a bezpečnostními předpisy

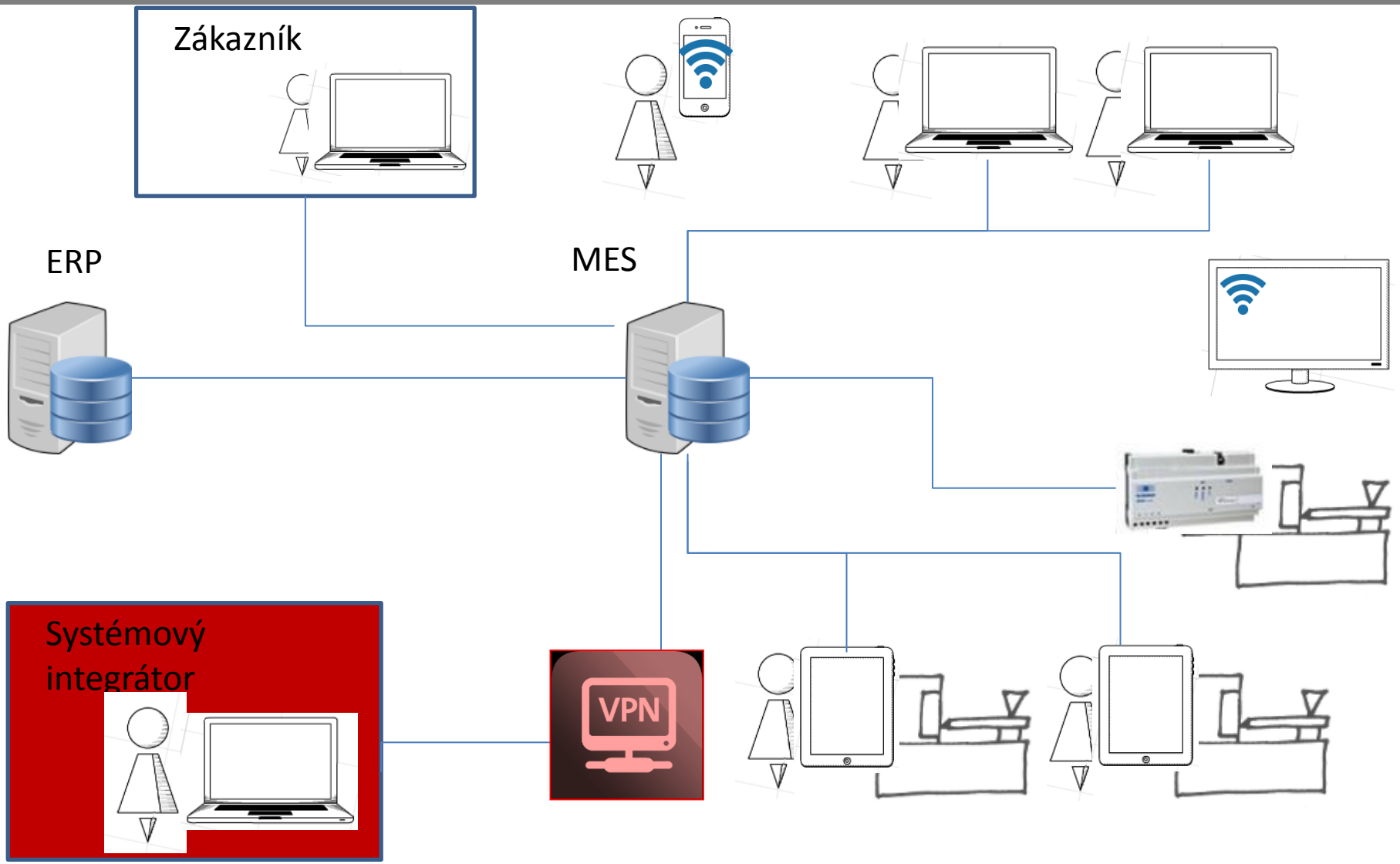
versus

Audittrail

- Automatické zaznamenání všech významných akcí, které jsou v systému provedeny
  - Nové záznamy
  - Editace
  - Odstranění
  - Schválení
  - Uvolnění
  - …
- Zaznamenání všech podstatných informací
  - IP adresa
  - Identifikace uživatele
  - Čas
  - Identifikace počítače
  - Změněné údaje
  - ¨
- Možnost automatické notifikace

Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik
---Vzdálená správa



Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik
---Vzdálená správa

Řídím kdy je přístup k mému serveru otevřený?

- Otevírání přístupu pouze na základě odůvodněné žádosti

Vím, kdo se k mému serveru skutečně připojuje?

- Povolení přístupu pouze pověřeným osobám, ne celé společnosti

Vím odkud se systémový integrátor připojuje?

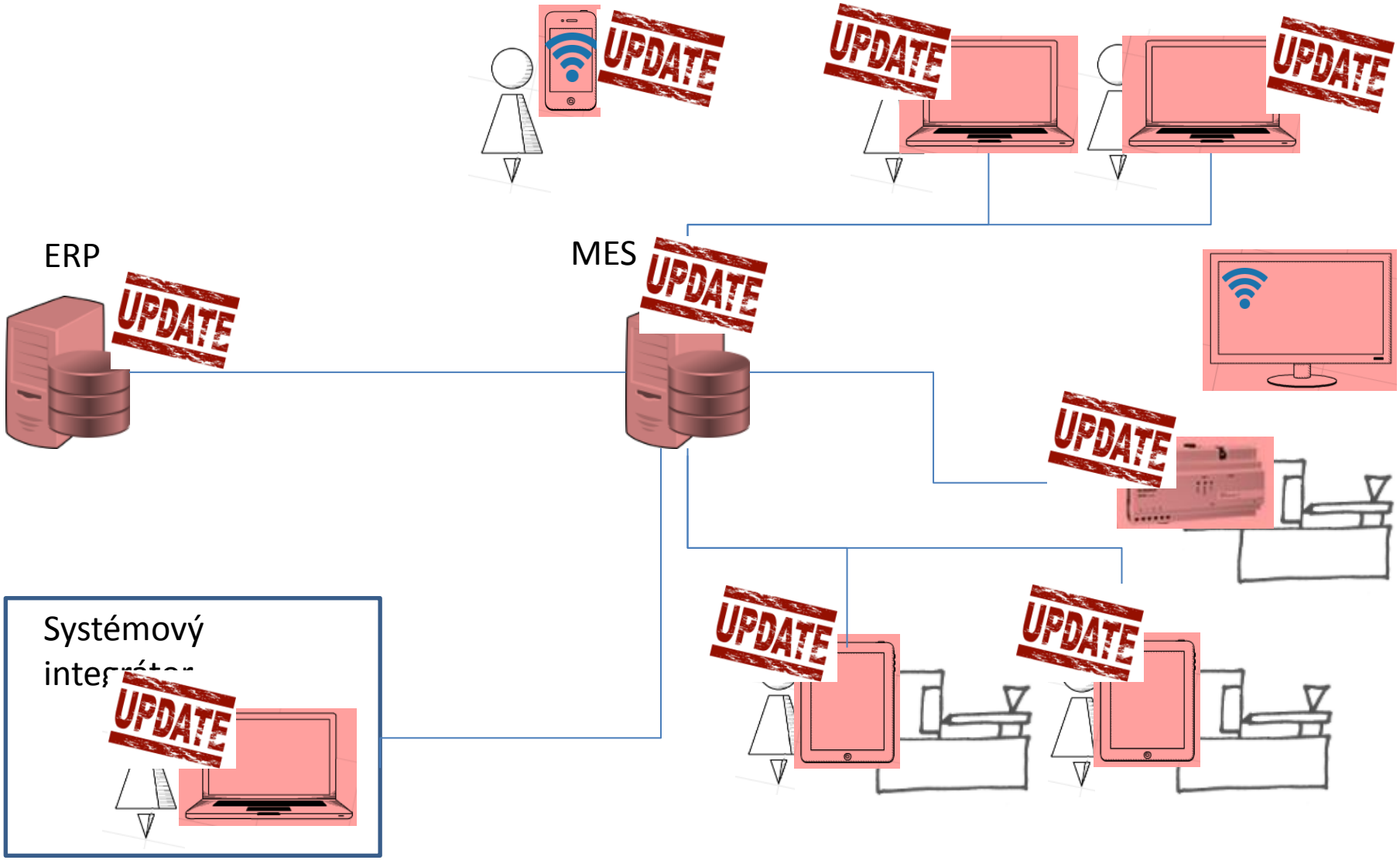
- Povolení přístupu pouze z definovaných lokalit => minimalizace rizika

Vyhodnocuji, co se na serveru dělo?

Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik

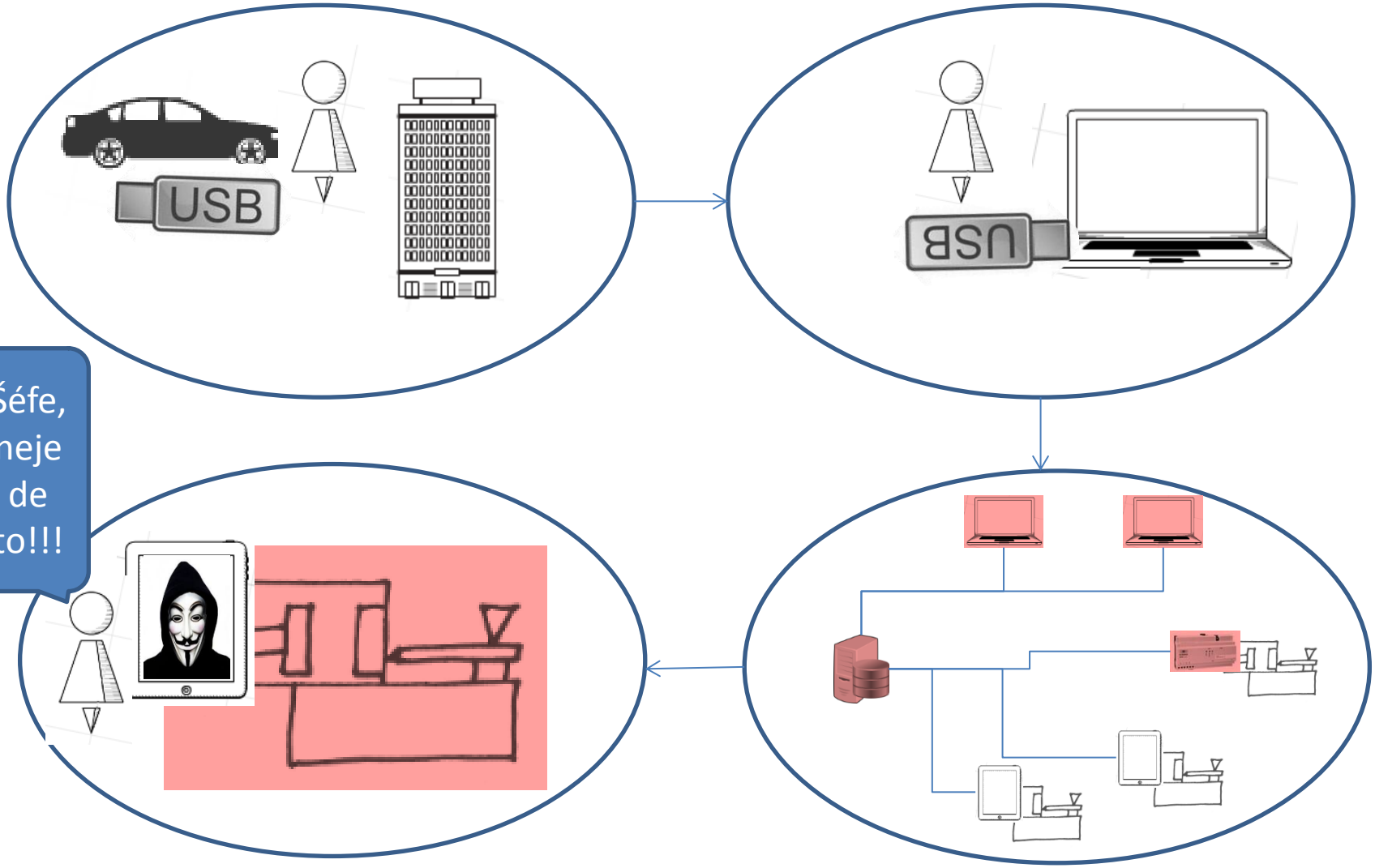
---Aktualizace, virová ochrana, …



Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik

---Aktualizace, virová ochrana, …



Bezpečnost v oblasti MES systémů – kde začít?

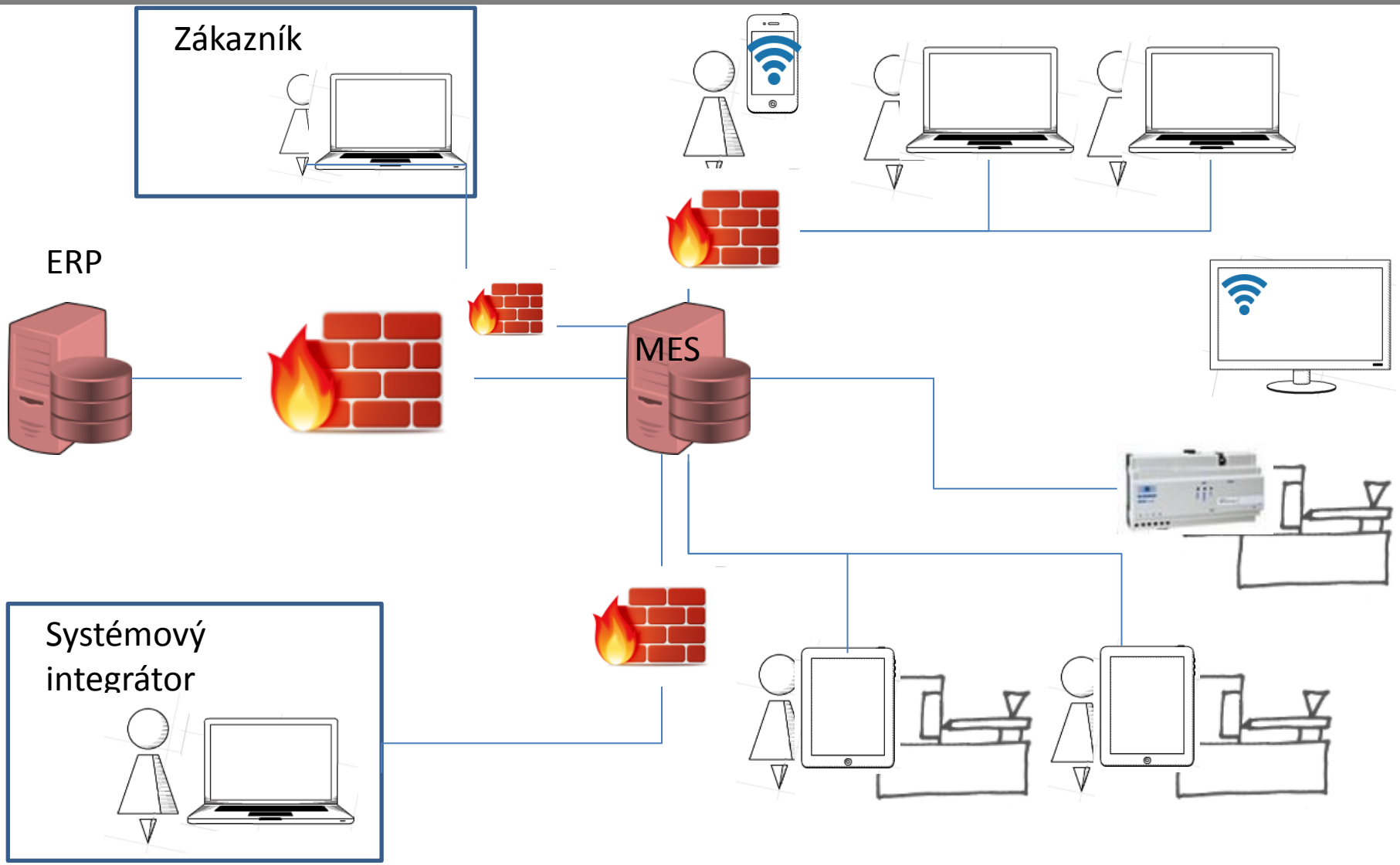
--Identifikace rizik

---Aktualizace, virová ochrana, …

Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik

---Oddělení síťových segmentů



Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik
---Oddělení síťových segmentů

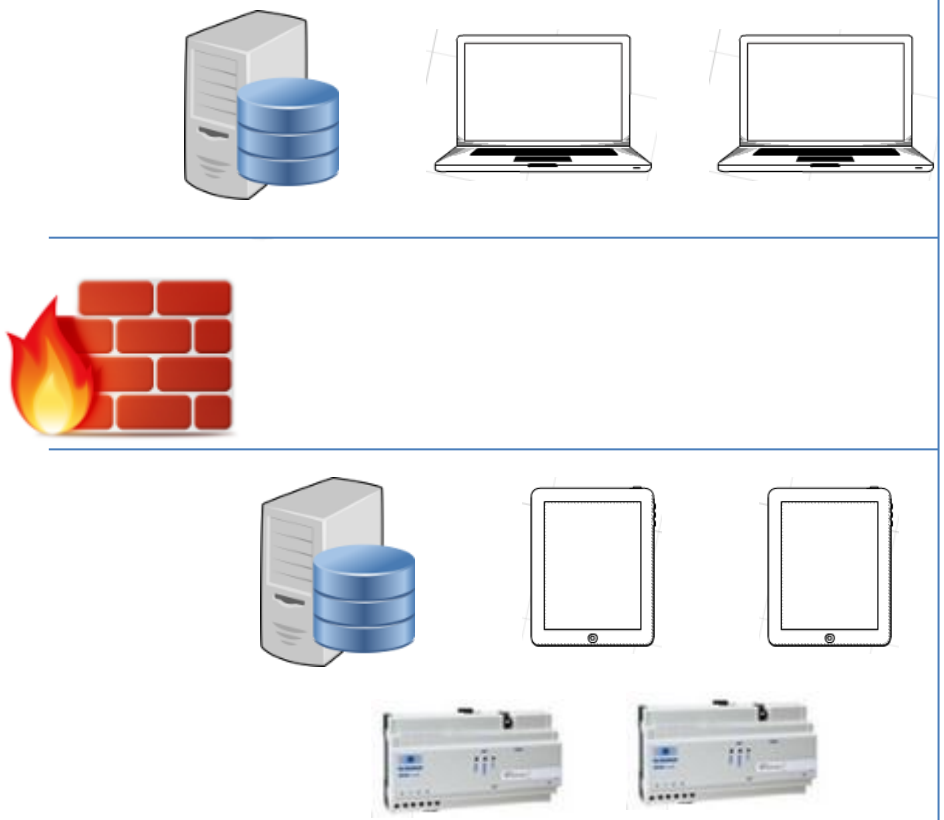
Level 4

Level 3

Level 2

Level 1

Level 0

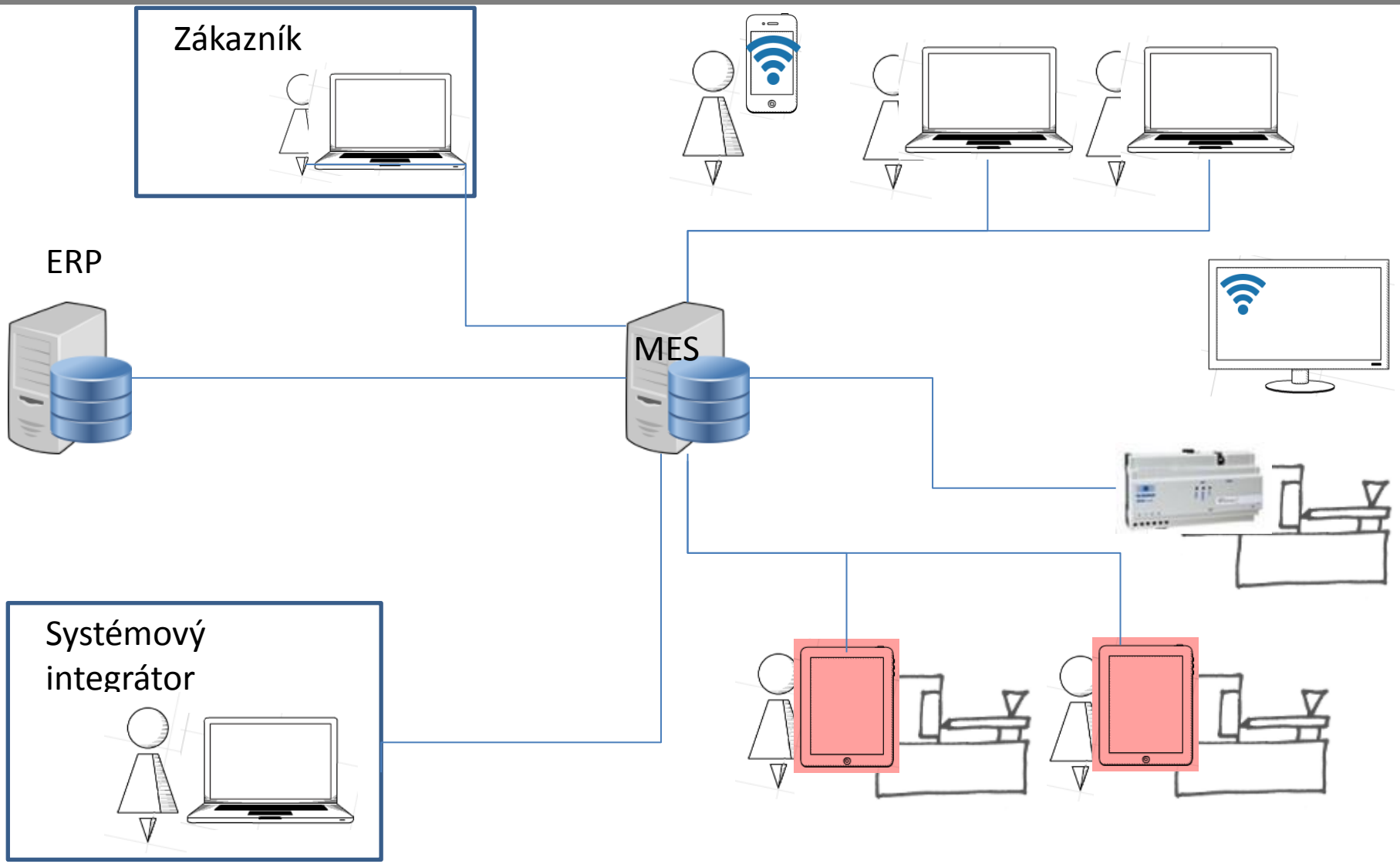


- **Oddělené segmenty sítě**
- **Všechny komunikační cesty musí být definovány a kontrolovány**
- **ISA 99 – Industrial Automation and Control Systems Security**

Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik

---Operátorské terminály

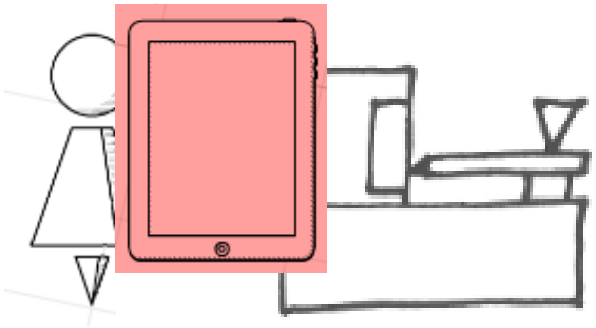


Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik
---Operátorské terminály

Důležitá fakta

- Operátoři jsou velmi nadaní hackeři a
- Velmi často mají chuť dokázat, že systém je špatně nastaven

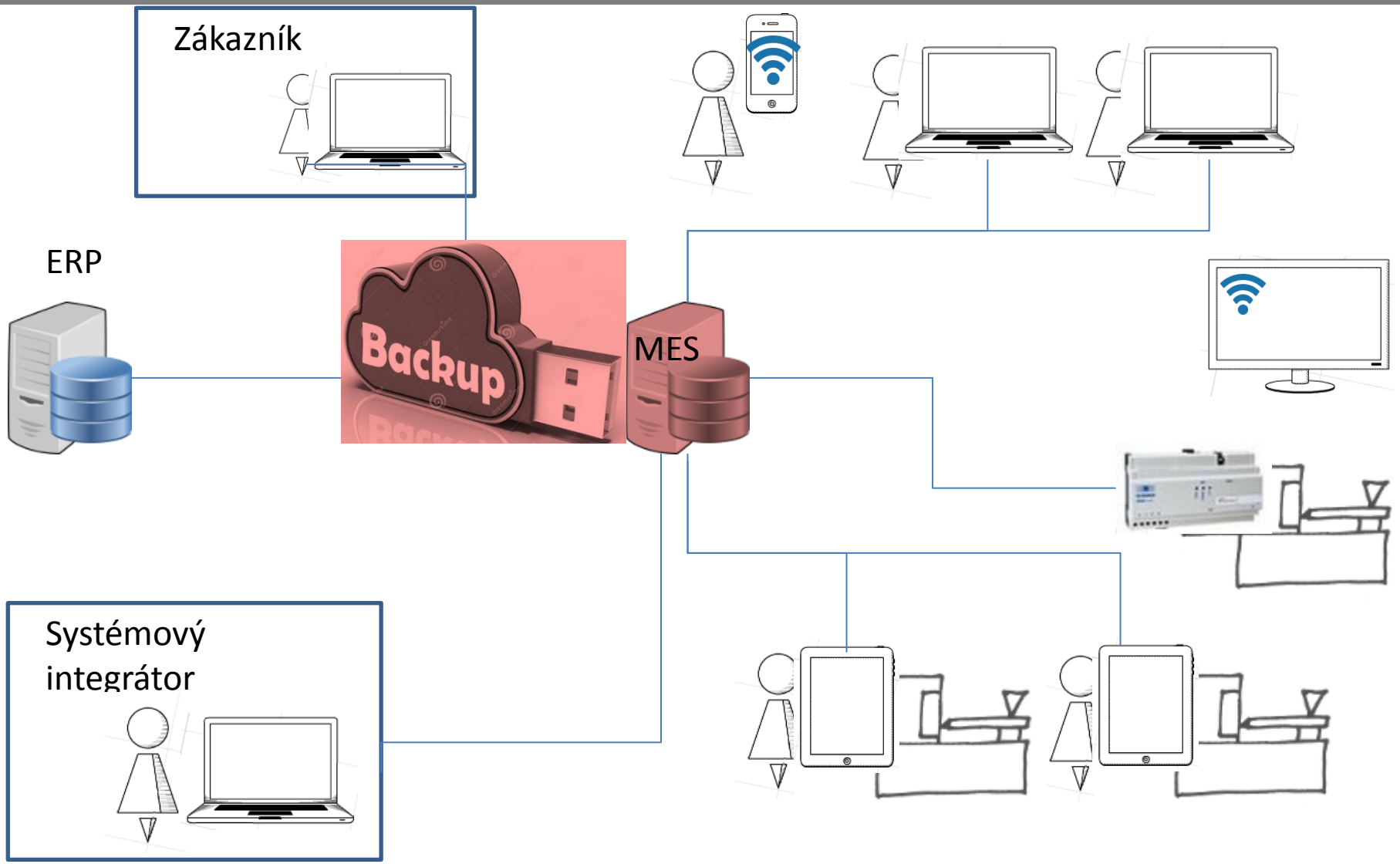


Doporučení

- Využívat upravené OS, které jsou budovány stylem „white listu“
  - Vše je zakázáno kromě toho, co je explicitně povoleno
- Využívat antivir
  - Opět forma „white list“
  - Na terminálu nesmí běžet nic jiného, než je jasně předdefinováno
- Využívat standardizované operátorské terminály

Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik
---Plán obnovy



Bezpečnost v oblasti MES systémů – kde začít?

--Identifikace rizik
---Plán obnovy

Zálohování

- Zálohuje se vůbec? ☺
- Jak často?
- Kam?

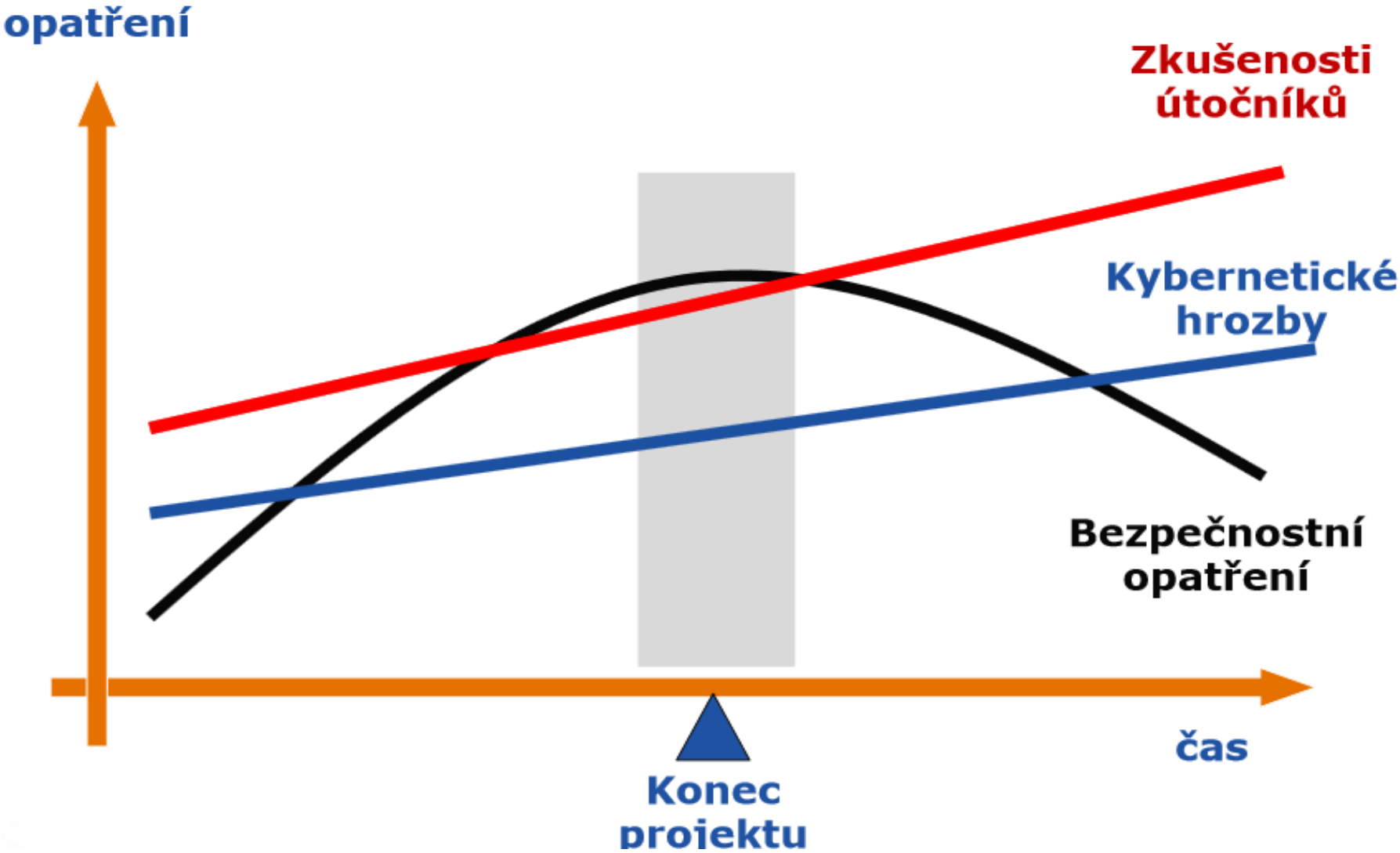
Krizové plány obnovy

- Umíme vůbec obnovit systém do funkčního stavu?
  - Máme to někde zdokumentováno?
  - Vyzkoušel někdo, jestli jde záloha obnovit? !!!!!!!
  - Máme na to proškolené zaměstnance?
- Za jak dlouho se dokážu k záloze dostat?
- Kdy je poslední bod platných dat v záloze?
- Za jak dlouho dokážu zálohu obnovit? (včetně všechny potřebné infrastruktury)
- O kolik dat a času jsem tedy vlastně přišel? **A kolik mě to bude stát???**

Bezpečnost v oblasti MES systémů – kde začít?

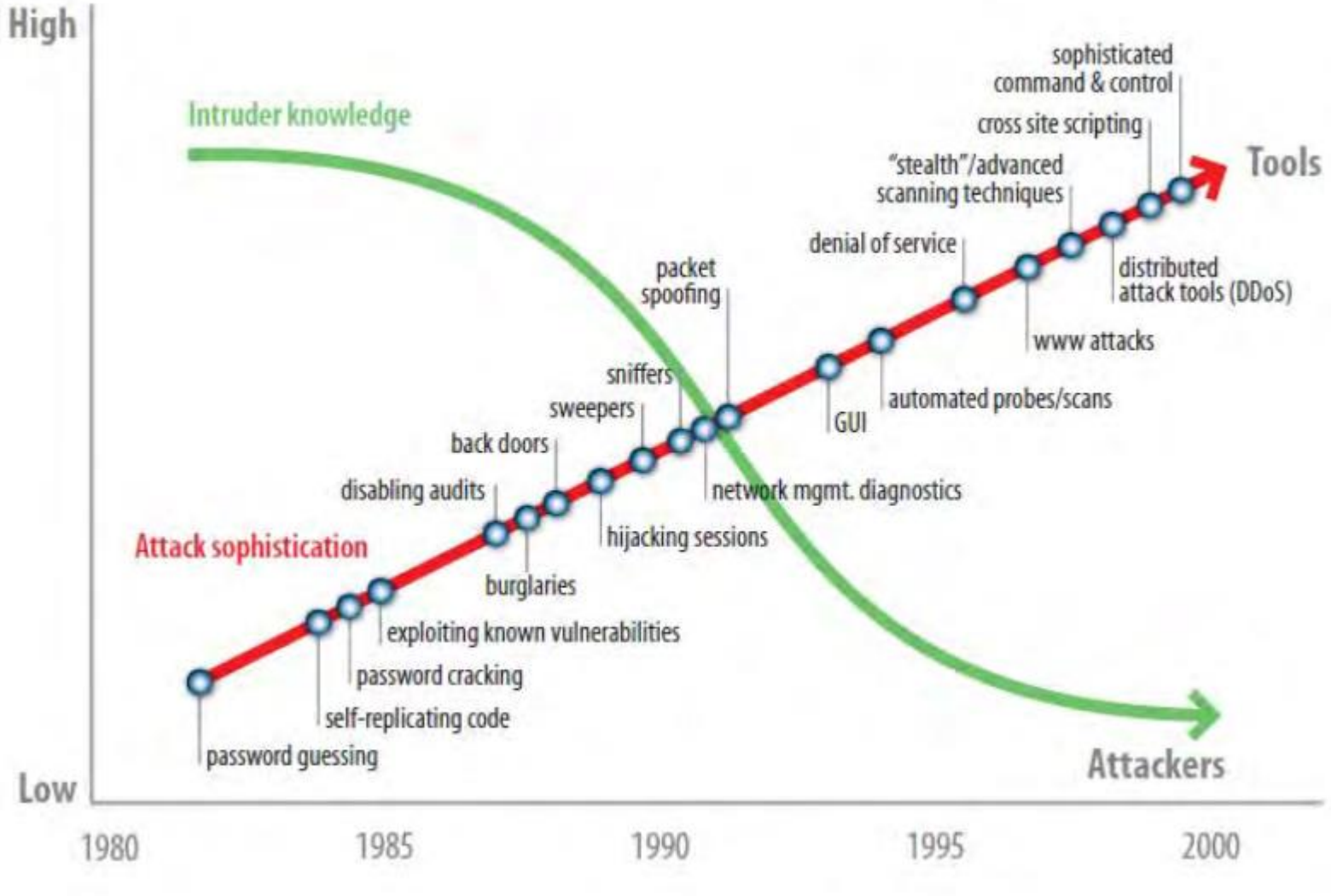
-Něco na závěr

--Jak je obvykle kladen důraz na bezpečnost v rámci implementace MES systému



Bezpečnost v oblasti MES systémů – kde začít?

-Něco na závěr
--Znalosti potřebné pro útok klesají



Děkuji