ezú elektrotechnický zkušební ústav

Ochrana osobních údajů a kybernetická bezpečnost v roce 2018

Ing. Michal Hager

Obsah

- **Ochrana osobních údajů ve světle obecného nařízení GDPR**
  - Propojení s dalšími nařízeními a směrnicemi EU
  - Základní principy nařízení GDPR
  - Vztah správce – zpracovatel(é)
  - Kodexy chování
  - Vydávání osvědčení
  - Školení
- **Kybernetická bezpečnost v roce 2018**
  - Zákon o kybernetické bezpečnosti a návazné právní předpisy
  - IECEE certifikační schéma pro kybernetickou bezpečnost

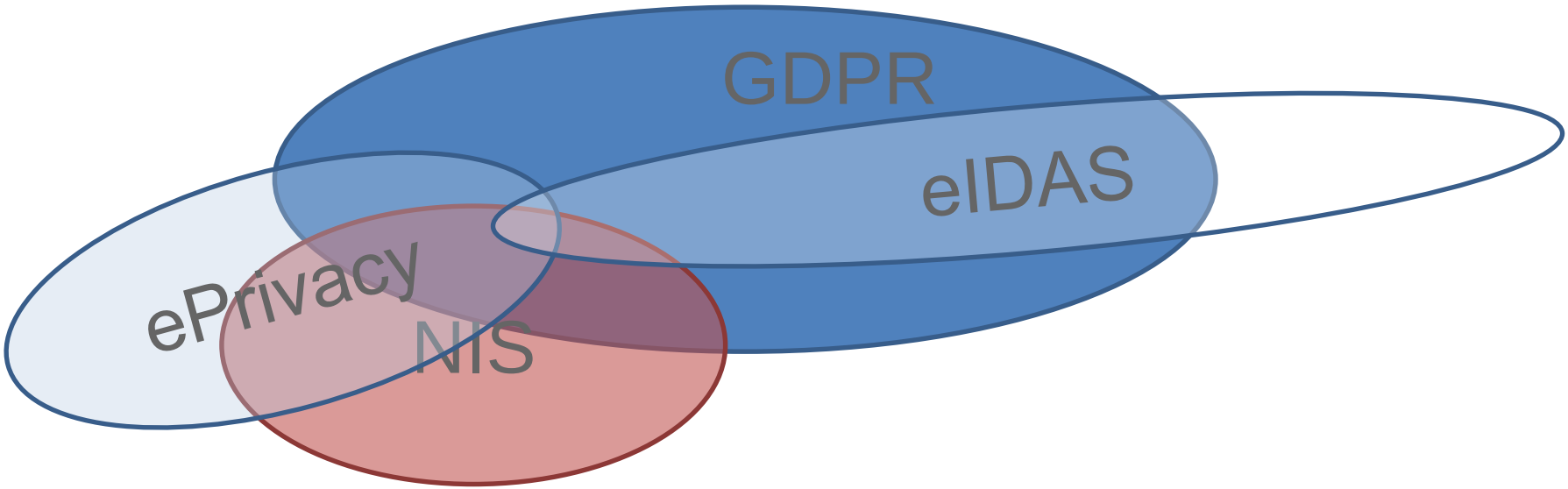
ezú elektrotechnický zkušební ústav

Ochrana osobních údajů ve světle obecného nařízení GDPR

Úvod

- Nařízení GDPR
  - NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- Účinnost
  - GDPR nabude účinnosti k 25. 5. 2018
- Koho se týká
  - Úplně všech
- Působnost
  - V rámci celé EU. Týká se i správců a zpracovatelů z třetích zemí, kteří zpracovávají osobní údaje občanů EU. Ti musí mít v EU stanoveného zástupce, který bude daný subjekt zastupovat.

Propojení s dalšími nařízeními a směrnicemi EU



Co přináší GDPR nového

- **Je jednotně aplikovatelné v celé EU**
- Rozšiřuje pojem osobních údajů – nově též např. biometrické prvky
- Zpřesňuje souhlas se zpracováním osobních údajů
- **Vyžaduje vyšší technickou a organizační bezpečnost správců a zpracovatelů**
- Při rozsáhlém a systematickém zpracování osobních údajů požaduje jmenování **pověřence na ochranu osobních údajů**
- Zavádí novou povinnost - vést záznamy o činnostech zpracování a ruší oznamovací povinnost
- Při rizikových zpracováních osobních údajů požaduje předchozí provedení posouzení vlivu na ochranu osobních údajů a případně též konzultaci s Úřadem na ochranu osobních údajů
- Posiluje stávající práva fyzických osob (občanů, zákazníků) a zakládá práva nová – právo být zapomenut či právo na přenositelnost údajů
- Ochrana „by design“ a „by default“
- **Porušení ochrany dat musí být oznámeno do 72 h**
- Nová pravidla pro předávání osobních údajů do zahraničí
- **Nepoměrně vyšší sankce**

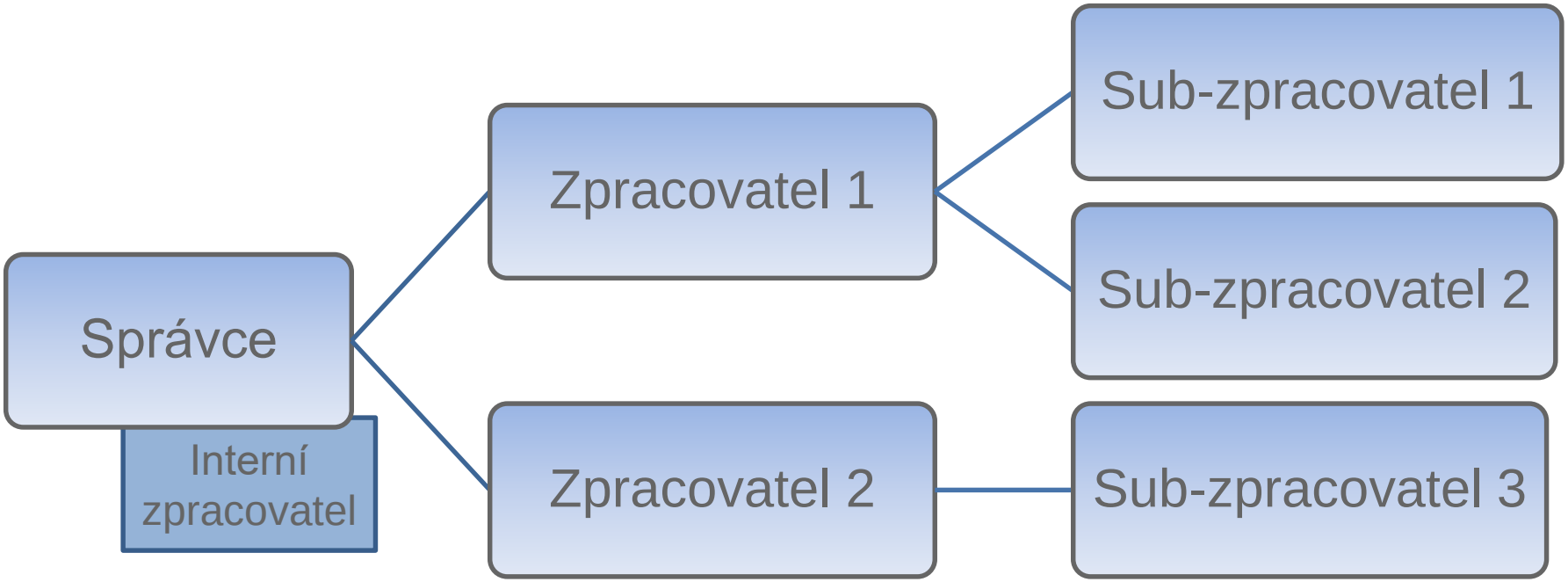
Základní principy nařízení GDPR

1) Zákonnost
2) Omezení účelem
3) Minimalizace údajů a omezení uložení
4) Přesnost
5) Transparentnost
6) Integrita a důvěrnost
7) Odpovědnost

Základní principy nařízení GDPR

1) Zákonnost
2) Omezení účelem
3) Minimalizace údajů a omezení uložení
4) Přesnost
5) Transparentnost
6) Integrita a důvěrnost
7) Odpovědnost

Vztah správce – zpracovatel(é)



Vztah správce – zpracovatel(é)

- Vztah mezi správcem a zpracovatelem je vždy třeba smluvně upravit
  (nové požadavky na smlouvy)
  - Smlouva musí jasně nastavit povinnosti a odpovědnost za případnou škodu každé ze smluvních stran
- Zákaz pověření dalšího zpracovatele bez souhlasu správce (při obecném souhlasu povinnost informovat)
- Správce odpovídá za výběr zpracovatele, který dodržuje nařízení GDPR
  - Měl by tedy ověřit zda vybraný zpracovatel splňuje požadavky GDPR (audit druhou stranou)
- Pro někoho zpracovatel může sám být také správcem

Kodexy chování a vydávání osvědčení

- Jedná se o nástroj, jehož prostřednictvím mohu správci a zpracovatelé **doložit soulad s nařízením** a naplnit tak jednu z klíčových zásad celého nařízení – **zásadu odpovědnosti**
- Jednotné uplatňování nařízení a posílení ochrany osobních údajů v celé EU
- Pro správce i zpracovatele
- Posouzení a monitorování souladu provádí:
  - Dozorový úřad
  - Akreditovaný subjekt posuzování shody
- Dobrovolná báze
- Ani jeden z těchto institutů zatím není nastaven
  - Připravovány mechanismy pro vydávání osvědčení

Kodexy chování

- Sdružení nebo jiné subjekty zastupující různé kategorie správců nebo zpracovatelů mohou vypracovávat kodexy chování nebo tyto kodexy upravovat či rozšiřovat, a to s cílem upřesnit uplatňování ustanovení tohoto nařízení
- Jsou nástrojem, který **zohledňuje specifika různých odvětví**
  - upřesnění povinností správců a zpracovatelů
- Netýká se zpracování prováděného orgány veřejné moci a veřejnými subjekty

Vydávání osvědčení

- **Osvědčení** (certifikát) o ochraně osobních údajů je dokument vydaný subjektem pro vydávání osvědčení (certifikačním orgánem), kterým subjekt (správce, zpracovatel, výrobce atd.) prokazuje zajištění souladu s požadavky nařízení 2016/679
- Rozdíl oproti kodexům chování tkví v tom, že necílí na jednotlivá odvětví, resp. neřeší specifika zpracování osobních údajů v rámci konkrétních odvětví
- **Zaměřeno přímo na konkrétní produkty, procesy a služby**
- **Platnost 3 roky**

Vydávání osvědčení – předmět certifikace

Předmětem posouzení (certifikace) mohou být:

1. **Hmotné produkty:**
   a) **Programové produkty** - software (pro účely zpracování osobních údajů)
   b) **Výpočetní technika** - hardware (pro účely zpracování osobních údajů)
2. **Procesy a služby:**
   a) **Jednotlivá zpracování osobních údajů** (proces) správce nebo zpracovatele
   b) **Systém řízení ochrany osobních údajů** u správce nebo zpracovatele (zahrnuje více zpracování osobních údajů)
   c) **Služby**

Kodexy chování a vydávání osvědčení - hlavní přínosy

- Schválené kodexy chování a osvědčení (certifikáty) se zohlední při rozhodování, zda Dozorový úřad udělí správní pokutu, případně v jaké výši (viz Článek 83 nařízení)
- V oblasti předávání do třetích zemí jsou vedle závazných podnikových pravidel nebo standardních smluvních doložek dalším vhodným nástrojem zajišťujícím bezpečný přenos osobních údajů do třetích zemí (viz Článek 46 nařízení)
- Pro subjekty údajů jsou schválené kodexy chování a osvědčení (certifikáty) signálem toho, že zpracování jejich osobních údajů je pravidelně posuzováno a kontrolováno způsobilou a nezávislou třetí stranou
- Zvýšení transparentnosti a možnost rychle vyhodnotit úroveň ochrany údajů relevantních výrobků a služeb
- Konkurenční výhoda na trhu

Školení nařízení GDPR

- Školení nařízení GDPR a jeho implementace je rozděleno do tří bloků, které na sebe navazují:
  - **Blok I. (1.den): GDPR – OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ**
  - **Blok II. (2.den): IMPLEMENTACE NAŘÍZENÍ GDPR PRAKTICKY (SVÉPOMOCÍ) I. ČÁST**
  - **Blok III. (3.den): IMPLEMENTACE NAŘÍZENÍ GDPR PRAKTICKY (SVÉPOMOCÍ) II. ČÁST ANALÝZA RIZIK + DPIA**

Školení nařízení GDPR

- Nejbližší možný termín školení **4. - 6. 4. 2018**
- Další termíny najdete na našich webových stránkách www.ezuedu.cz
- Cena za **kompletní školení** je **10.950,- Kč**, ovšem můžete se zúčastnit pouze Vámi vybraného bloku.

Kontakty: **Ing. Lucie Rainová**

manažer produktu pro školení

M: +420 603 223 412

E: lrainova@ezu.cz

ezú elektrotechnický zkušební ústav

Kybernetická bezpečnost v roce 2018

Kybernetická bezpečnost - novinky v legislativě

- Novela zákona o kybernetické bezpečnosti (zákona č. 181/2014 Sb.)
  - Nabyla účinnosti 1. 8. 2017
  - Transponována evropská směrnice pro zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS)
  - Zřízení nového ústředního správního úřadu pro oblast kybernetické bezpečnosti (NÚKIB)
  - Rozšíření působnosti zákona o správce a provozovatele informačního systému základní služby a poskytovatele digitálních služeb

Návazné právní předpisy k zákonu o KB

- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (novelizována v 01/2015)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích (novelizována v 07/2016)
- Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti (bude novelizováno v 2018)
  - Poslední návrh nové vyhlášky o kybernetické bezpečnosti je ze dne 19. 1. 2018
  - Řada vylepšení a aktualizovaných bezpečnostních opatření
  - V něm se počítá s účinností od 9. 5. 2018
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby
  - Vydána dne 15. 12. 2017 a účinná od 1. 2. 2018

Zákon o kybernetické bezpečnosti – kontrola a audit

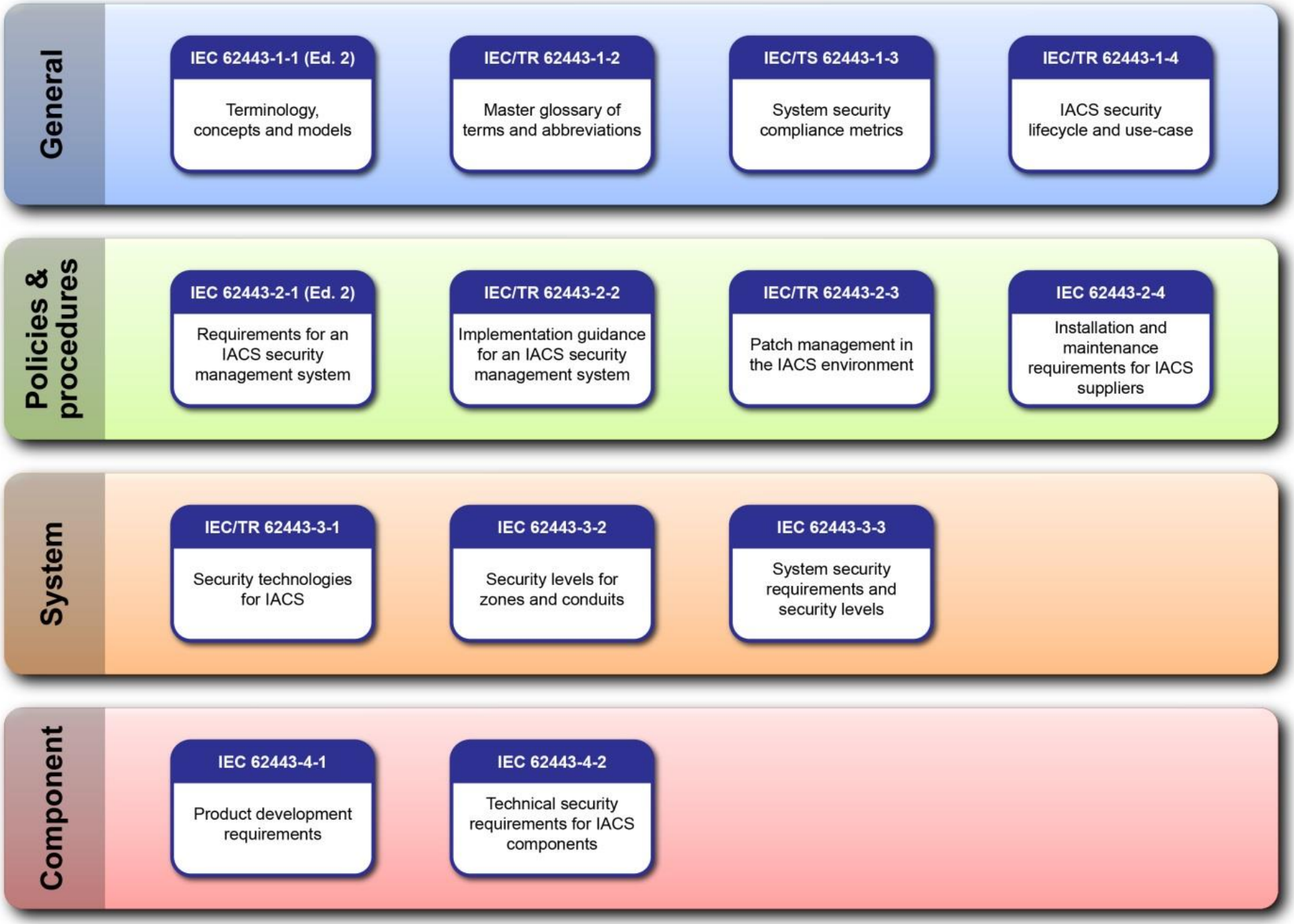
- Kontrolu souladu provádí sám NÚKIB

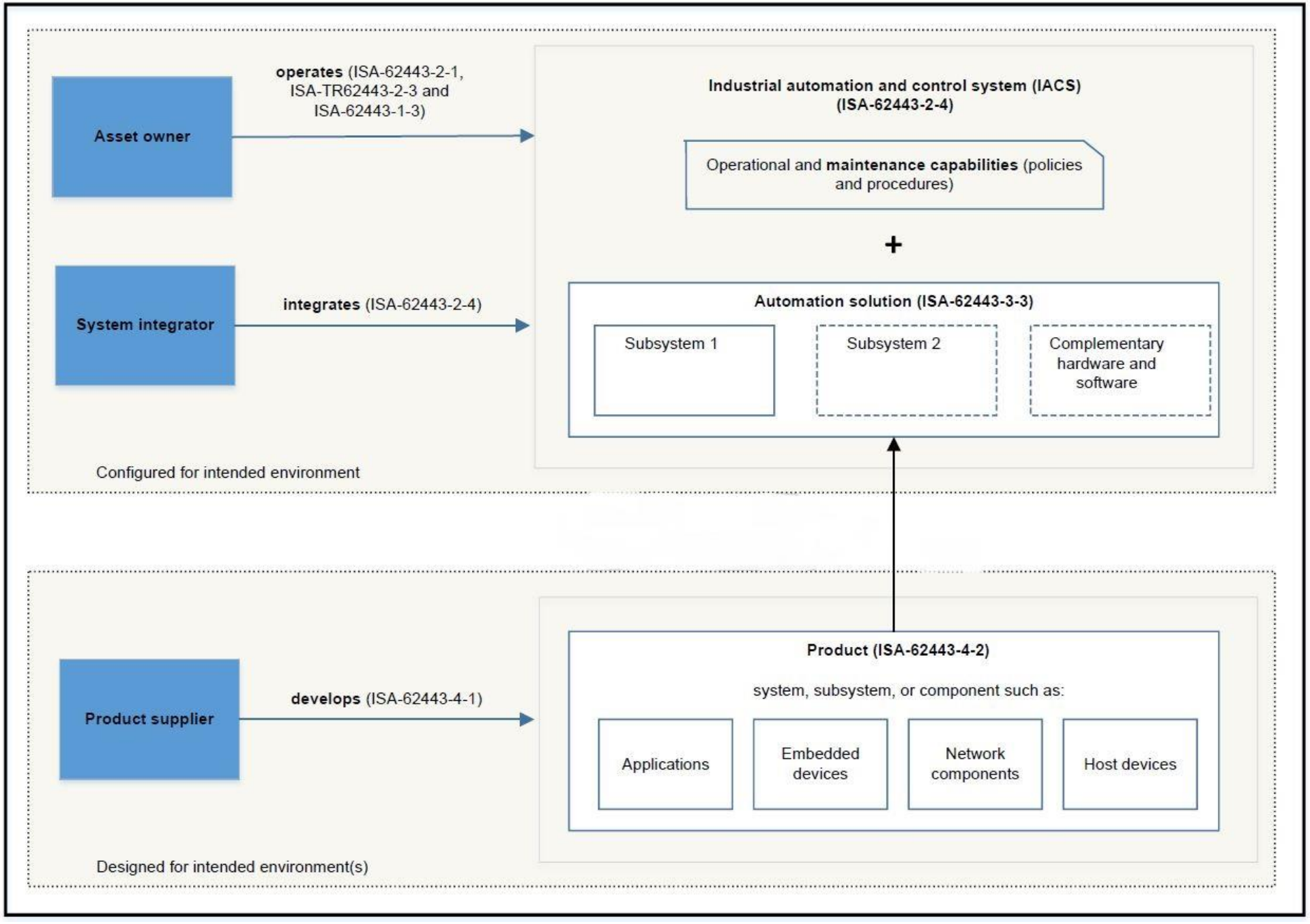
- Přístup A:
  - Interní audit
  - Zajištění role interního auditora kybernetické bezpečnosti

- Přístup B:
  - Certifikace dle ČSN ISO/IEC 27001:2014

IECEE certifikační schéma pro kybernetickou bezpečnost

- Nové certifikační schéma pro kybernetickou bezpečnost (zejména pro oblast průmyslu)
- Založeno na fungování základních pravidel CB schématu
  - To znamená, že výsledné výstupy (protokoly a certifikáty) jsou uznatelné po celém světě
- Postaveno na standardech ze série IEC 62443
- Specifická vlastnost: žadatel o certifikaci si sám určuje požadavky, vůči kterým bude posuzováno a certifikováno


General
IEC 62443-1-1 (Ed. 2)
Terminology, concepts and models
IEC/TR 62443-1-2
Master glossary of terms and abbreviations
IEC/TS 62443-1-3
System security compliance metrics
IEC/TR 62443-1-4
IACS security lifecycle and use-case
Policies & procedures
IEC 62443-2-1 (Ed. 2)
Requirements for an IACS security management system
IEC/TR 62443-2-2
Implementation guidance for an IACS security management system
IEC/TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Installation and maintenance requirements for IACS suppliers
System
IEC/TR 62443-3-1
Security technologies for IACS
IEC 62443-3-2
Security levels for zones and conduits
IEC 62443-3-3
System security requirements and security levels
Component
IEC 62443-4-1
Product development requirements
IEC 62443-4-2
Technical security requirements for IACS components


Asset owner
operates (ISA-62443-2-1, ISA-TR62443-2-3 and ISA-62443-1-3)
Industrial automation and control system (IACS) (ISA-62443-2-4)
Operational and maintenance capabilities (policies and procedures)
+
System integrator
integrates (ISA-62443-2-4)
Automation solution (ISA-62443-3-3)
Subsystem 1
Subsystem 2
Complementary hardware and software
Configured for intended environment
Product supplier
develops (ISA-62443-4-1)
Product (ISA-62443-4-2)
system, subsystem, or component such as:
Applications
Embedded devices
Network components
Host devices
Designed for intended environment(s)

Konkrétní standardy a možné scénáře pro certifikaci

- IEC 62443-2-4
  - Process Capability Assessment
  - Product Capability Assessment
  - Solution Application Capability Assessment
- IEC 62443-4-1 (připravuje se)
  - Process Capability Assessment
  - Product Application Capability Assessment
- IEC 62443-3-3 (připravuje se)
  - Product Capability Assessment
- IEC 62443-4-2 (připravuje se)
  - Product Capability Assessment

Závěrem

- **Nařízení GDPR**
  - Kodexy chování
  - Vydávání osvědčení
- **Zákon o kybernetické bezpečnosti**
  - Interní audity
  - Zajištění role interního auditora kybernetické bezpečnosti
  - ISO/IEC 27001
- **Certifikační schéma pro IEC 62443 standardy**
  - Certifikace kybernetické bezpečnosti v oblasti průmyslu

ezú elektrotechnický zkušební ústav

Děkuji za pozornost!

Ing. Michal Hager
mhager@ezu.cz
www.ezu.cz