

Kybernetická bezpečnost v OT, technické normy ISA



Martin Fábry, Accura s.r.o
CISSP, GICSP, CISA, CSSA, GRID, IEC 62443 Expert

ISA/IEC 62443 Series of Standards



Úvod

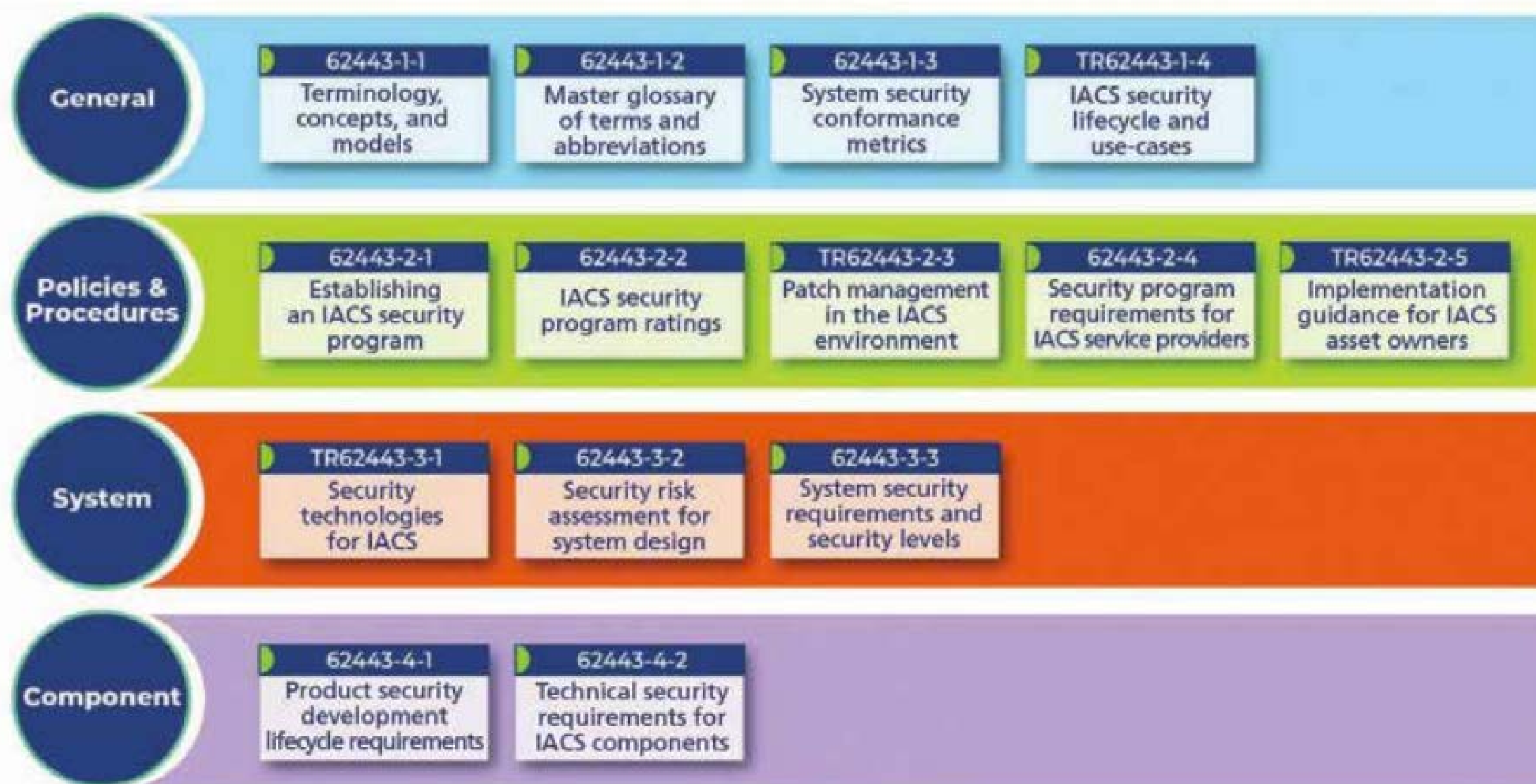
- Sada 14tich dokumentov vytvorená (2007) primárne ISA99 výborom pre industriálne prostredie za účelom adresácie kybernetickej bezpečnosti
- De facto je „zlatý cyber štandard“ vo svete OT/ICS
- Adoptovaný tiež BAC (Building Automation Systems), dopravou a medicínskymi zariadeniami (Medical IoT)
- Cieľom je posilniť ICS bezpečnosť aby nedochádzalo ku kyberneticko-fyzickým dopadom spôsobenými kybernetickými incidentami ako napríklad explóziám, stratou na životoch, alebo environmentálnym škodám
- Hlavné priority: functional safety (priemyselná bezpečnosť), integrita, dostupnosť a spoľahlivosť procesu

Date	Target	Method
2000	Australian Sewage Plant	Insider
2010	Iran Uranium Enrichment	Stuxnet
2013	ICS Supply Chain attack	Havex
2014	German Steel Mill	
2015	Ukraine Power Grid	BlackEnergy, KillDisk
2016	Ukraine Substation	CrashOverride
2017	Global shipping company	NotPetya
2017	IoT DDos attack	BrickerBot
2017	Health care, Automotive, many others	WannaCry
2017	Saudi Arabia Petrochemical	TRITON/TRISIS
2019	Norwegian Aluminum Company	LockerGaga

Zdroj: ISA

ISA/IEC 62443 Series of Standards

Sada štandardov

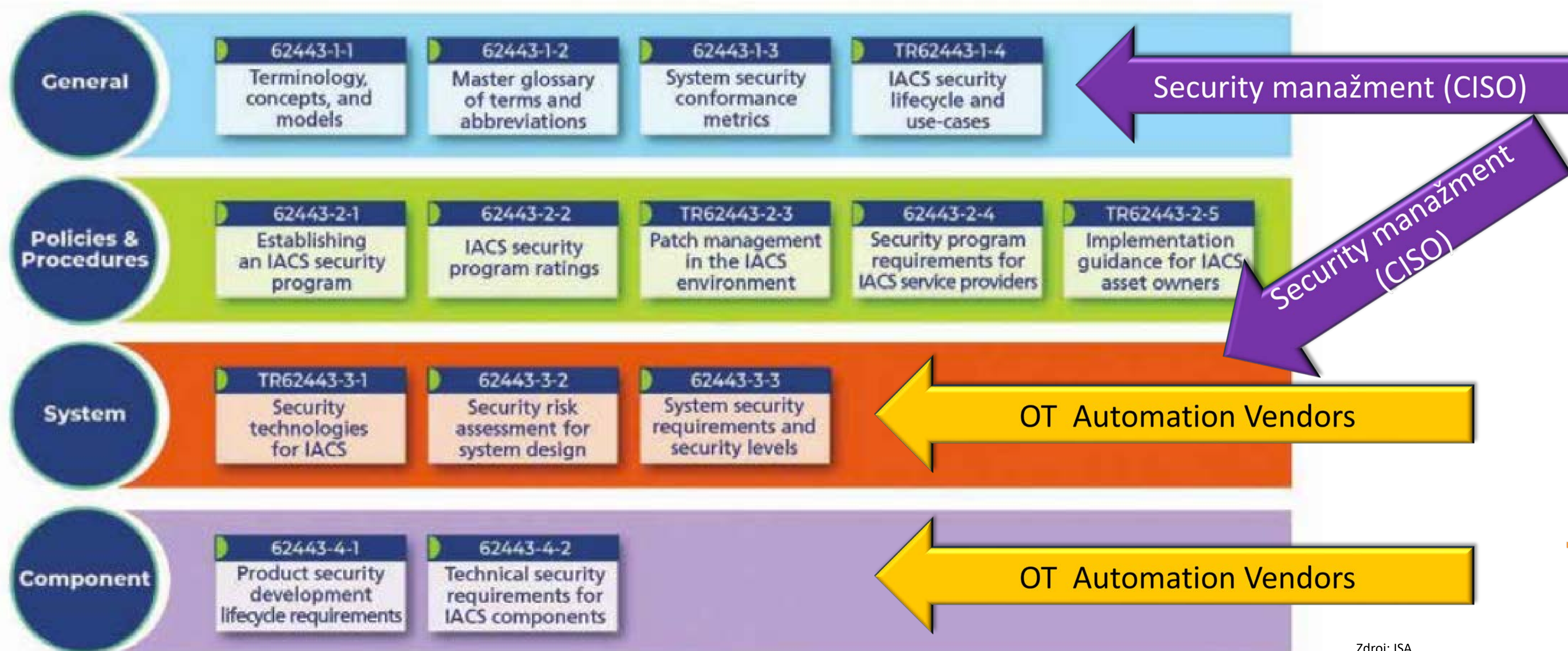


Zdroj: ISA



ISA/IEC 62443 Series of Standards

Komu daný štandard adresovať



Zdroj: ISA

ISA/IEC 62443 Security Levels

Špecifiká 62443 a fundamentálne koncepty

Security level (Úroveň bezpečnosti) je definovaný ako miera dôvery, že posudzovaný systém (SuC), zóna, alebo prechod je bez zraniteľností a funguje zamýšľaným spôsobom.

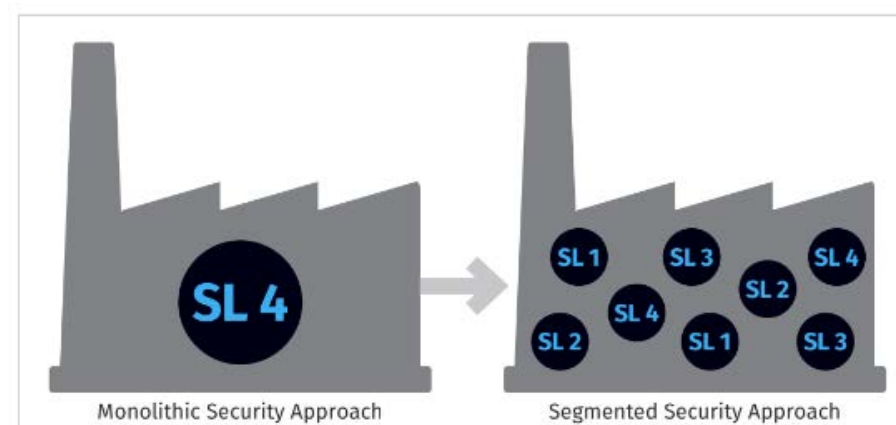
Security Level	Definition	Means	Resources	Skills	Motivation
1	Protection against casual or coincidental violation				
2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation	simple	low	generic	low
3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation	sophisticated	moderate	IACS-specific	moderate
4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation	sophisticated	extended	IACS-specific	high

3 typy Security Levels:

1. Target (SL-T) cielená úroveň bezpečnosti na základe analýzy rizík pre IACS. Napr. vhodným výberom produktov.

2. Capability SL (SL-C) hovorí, že systém, alebo komponent je schopný natívne splniť SL-T bez kompenzačných opatrení.

3. Achieved SL (SL-A) dosiahnutá úroveň bezp. Systému v prevádzke sprevádzaná politikami a procedúrami (CSMS)



SRs and REs				SL 1	SL 2	SL 3	SL 4
FR 1	Identification and authentication control (IAC)						
SR 1.1	Human user identification and authentication			5.3	✓	✓	✓
SR 1.1 RE 1	Unique identification and authentication			5.3.3.1		✓	✓
SR 1.1 RE 2	Multifactor authentication for untrusted networks			5.3.3.2			✓
SR 1.1 RE 3	Multifactor authentication for all networks			5.3.3.3			✓
SR 1.2	Software process and device identification and authentication			5.4		✓	✓
SR 1.2 RE 1	Unique identification and authentication			5.4.3.1			✓
SR 1.3	Account management			5.5	✓	✓	✓
SR 1.3 RE 1	Unified account management			5.5.3.1			✓
SR 1.4	Identifier management			5.6	✓	✓	✓

Functional and System Requirements :

Základné stavebné bloky. Na ich základe sa určujú požiadavky na daný systém alebo zónu.

Zdroj: ISA a SANS

ISASecure Certification – non profit organizácia, ktorá certifikuje program a komponenty ICS <https://isasecure.org/>

Kategórie certifikácií:

1. ISA/IEC 62443-3-3 Certified Systems – certifikuje produkty, ktoré spĺňajú požiadavky štandardu Part 3-3 podľa (System Security Assurance)



Picture	Supplier ▾	Type	Model	Version	Certificate	Certification Date
	ABB	System	Ability System 800xA	6.1.1.x	SSA 4.0.0 Level 1	4/26/2022

2. IEC 62443-4-1 Certified Development Organizations – výrobné prevádzky, ktoré dosiahli SDLA (Security Development Lifecycle Assurance) certifikáciu



Picture	Supplier ▾	Company SDL Name	Scope	Specification Version	Certificate	Certification Date
	Yokogawa Electric Corporation	Secure Development Life Cycle	Musashino, Tokyo, Japan	SDLA 3.0.0	View Certificate	12/20/2022

3. ISA/IEC 62443-4-2 Certified Components – Certifikované produkty na základe Component Security Assurance (CSA) ktoré spĺňajú štandard Part 4-2 a boli vyrobené podľa SDLA



Picture	Supplier ▾	Type	Model	Version	Certificate	Certification Date
	Honeywell Process Solutions	DCS Controller	Experion Experion C300 with CF9	R500	EDSA 2.0.0 Level 1	8/23/2018

ISA/IEC 62443 Certifikáty

Certifikácie osôb



ISA ponúka nasledujúce certifikáty kybernetickej bezpečnosti pre študentov, ktorí **absolvovali školenia a kurzy**. Certifikáty nemajú byť zamieňané s certifikáciami produktov.

- ☐ ISA/IEC 62443 Cybersecurity Fundamentals Specialist
- ☐ ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
- ☐ ISA/IEC 62443 Cybersecurity Design Specialist
- ☐ ISA/IEC 62443 Cybersecurity Maintenance Specialist
- ☐ ISA/IEC 62443 Cybersecurity Expert



Certificate 1



Certificate 2



Certificate 3



Certificate 4



Expert



Ďakujem za pozornosť



Accura s.r.o
Mileticova 500/1
821 08
Bratislava
Slovakia
accura@accura.io