# CRA

dd picture

## EU Számháború 2.0

- Kis-Szabó András
- 2026

Kontron Hungary

- Kontron
- Áttekintő
- Linkek
- CRA helye, viszonya
- Feladatok
- Szabványok

# Kontron

Az ipari IoT úttörője világszerte

# Csoport

**~7,000**
Munkatárs

**1.7mrd**
Árbevétel*

**237m**
K+F kiadás*

**192m**
EBITDA*

**+20 ország**
Telephelyekkel

Az SDAX® agja
A TecDAX® tagja
HQ Ausztriában, tőzsdén jegyezve Németországban

* EUR-ban 2024-ben

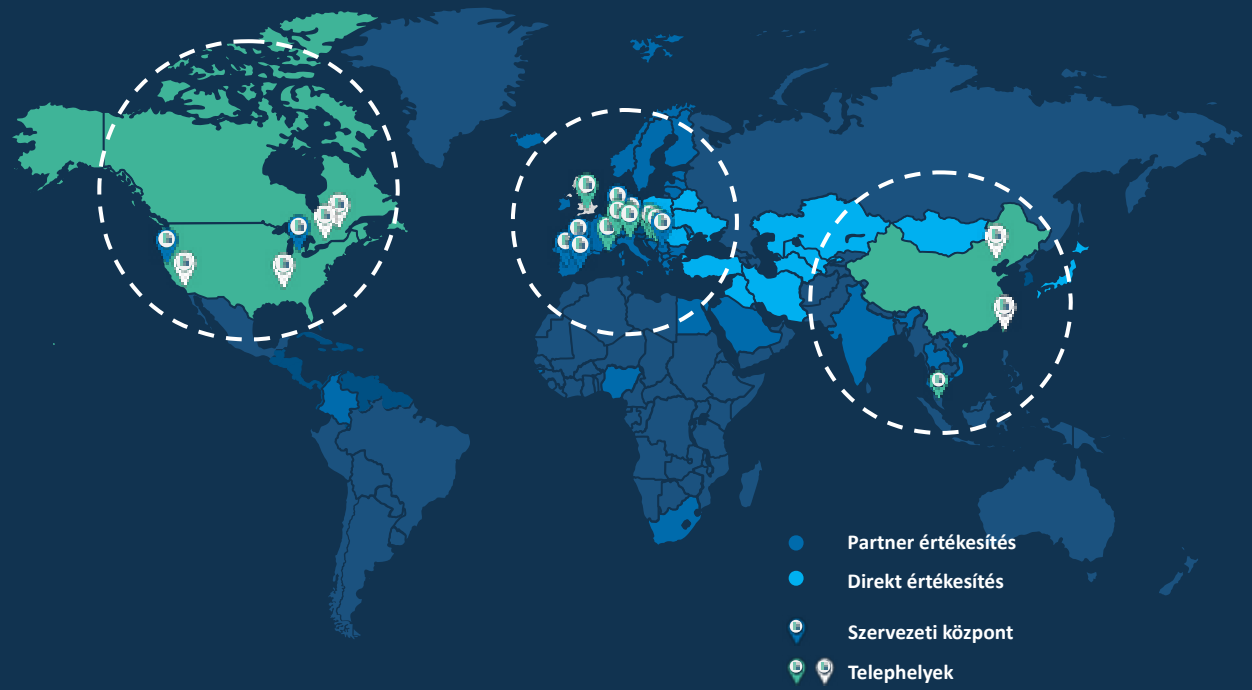
kontron
The Power of IoT

## Árbevétel

**Észak-Amerika**
~15%

**Európa**
~80%

**Ázsia**
~5%




**A legmodernebb technológiák fejlesztésére összpontosítunk.**
**Erős K+F tevékenységünk biztosítja technológiai előnyünket.**

**~700**
Értékesítés

**~1,100**
Adminisztráció

**~2,100**
Gyártás és Logisztika

**~3,200**
Mérnök

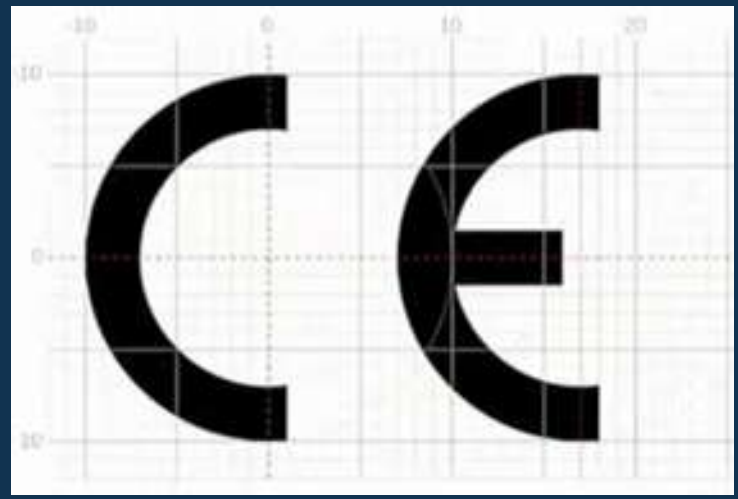
# The Power of IoT

- Solutions for connected ecosystems

# Maximális bírságok

- EU level

| Framework | Penalty € | Sum CY rev. % |
|---|---|---|
| GDPR | 20 000 000 € | 4 % |
| NIS2 | 10 000 000 € | 2 % |
| AI Act | 35 000 000 € | 7 % |
| CRA | 15 000 000 € | 2,5 % |



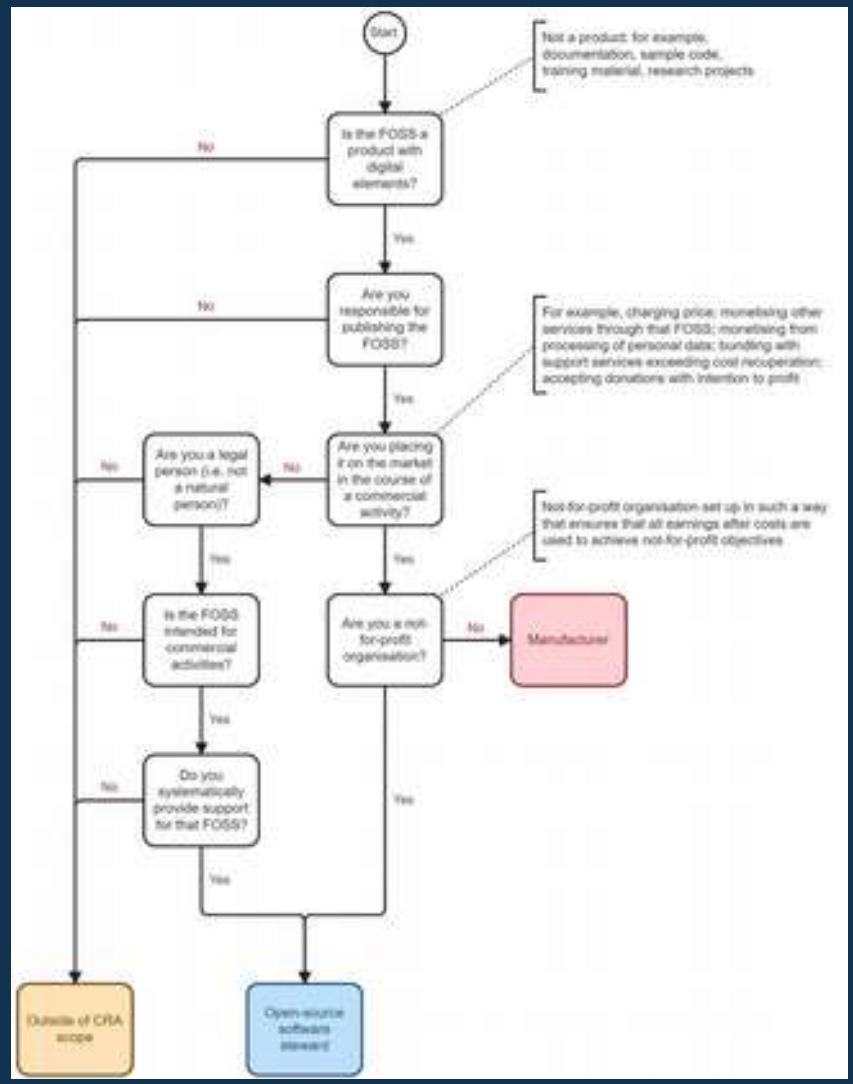
# Guidance of the Application of (EU) 2024/2847

- DRAFT, 2026.03.03ish

17. Article 3(1) of the CRA defines a product with digital elements as 'a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately'. Such products fall within the scope of the CRA where their intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.[6]

18. The CRA therefore can cover standalone software, such as (i) apps and computer programs; (ii) hardware with embedded software (e.g. Internet-of-Things devices); (iii) standalone hardware (e.g. integrated circuits, motherboards); and (iv) any combination of hardware and software supplied separately but intended to operate together.

19. Whether software forms part of a product should be determined not by how or when that software is delivered to the user, but by whether, in light of the product's intended purpose and reasonably foreseeable use, the software is necessary for the product to perform its intended functions. Where a hardware device is designed to operate together with specific software in order to perform its functions, the hardware and that software together constitute the product placed on the market. Software that is necessary to operate, configure, control or meaningfully use a device is therefore part of the product, even if it is obtained through a separate channel (e.g. an app store, a download link or another digital channel after the hardware has been placed on the market).



# CRA linkek

- Nyomtatott anyagba

- EU Startlap
  - https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation
- FAQ:
  - https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions
- Támogató projekt
  - https://cyberstand.eu/
- DigitalEU
  - CRAzy About Product Cybersecurity: From Compliance to Confidence
  - https://www.youtube.com/watch?v=QRLWcU_Yx18

- EU standardizáció: STAN4CR
  - https://www.stan4cra.eu/
- ETSI összefogással (work-in-rpogress)
  - https://labs.etsi.org/rep/stan4cra
  - https://docbox.etsi.org/CYBER/EUSR/Open

# EU CE termék AI+Menedzsment

- Van egy termékem, eladnám!

- CRA
  - Élesedés
    - 2026. június 11. / 2027. december. 11.
  - CE jelölés feltétele, alapfeltétel
  - (Szoftver) és szoftvert tartalmazó termék. Free szoftver is!
  - Viszonteladókra is van feltétel! (10 év retention)
- GDPR – PII, B2C, személy
- Data Act – B2B verziója a GDPR-nak

- CRA – CE feltétel (EU 2024/2847 + 2025/2392)
  - NIS2 – szolgáltatás, felhő
  - AI Act – MI felhasználás, funkció

- CRA módosítók
  - NIS2
  - AI Act – Kétirányú, minősítés
  - Termék-specifikus
    - RED – rádiós termékek (BT, WiFi, stb.)
  - Ágazat specifikus (CRA-ból olvasható!)
    - Orvosi, tenger, közlekedés és jármű, stb.

# Termékek

- EU level

| CRA kategória: | Alap | Fontos I | Fontos II | Kritikus |
|---|---|---|---|---|
| 3. Melléklet | | identity management, browsers, VPNs, operating systems, smart home devices, Wearables stb. | hypervisors, firewalls, IDS tamper-resistant microprocessors, industrial control systems stb. | HSM, smartcards/secure elements, smart meter gateways |
| Minősítés | Önbevallás | Harmonizált standard | Külső minősítés | EUCC minősítés |
| | „Egyszerű”, pár kötött tartalmú papír, mint most CE-hez | (Standard megfelelést igazolni kell! (audit) ) | | |

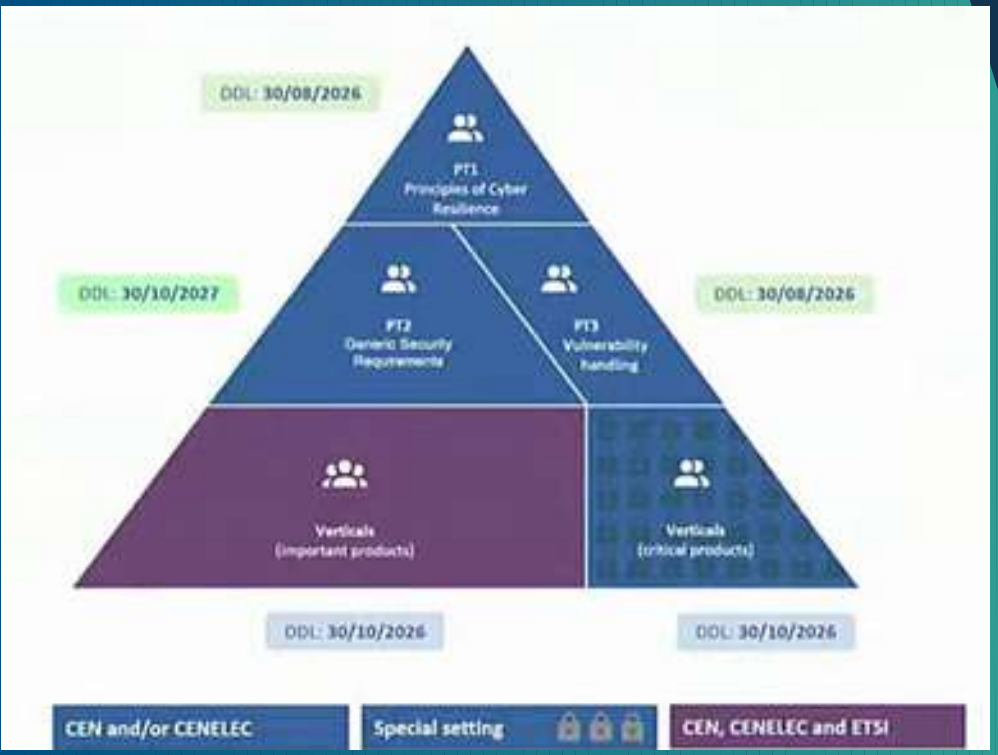
Kockázatértékelés, mint AI Act-nál: mellékletben kijelölve…

# Műszaki leírás minták

- Operációs rendszerek
  - Digitális elemeket tartalmazó szoftvertermékek, amelyek absztrakt interfészt biztosítanak az alapul szolgáló hardverhez, és ellenőrzik a szoftver végrehajtását, és amelyek olyan szolgáltatásokat nyújthatnak, mint például a számítástechnikai erőforrás-gazdálkodás és -konfiguráció, az ütemezés, a bemeneti-kimeneti vezérlés, az adatok kezelése, valamint olyan interfész biztosítása, amelyen keresztül az alkalmazások kapcsolatba lépnek a rendszer erőforrásaival és perifériáival.
- Tűzfalak, behatolásérzékelő és megelőző rendszerek
  - A tűzfalak olyan, digitális elemeket tartalmazó termékek, amelyek a hálózatra irányuló és onnan kiinduló adatátviteli forgalom nyomon követése és korlátozása révén védik az összekapcsolt hálózatot vagy rendszert a jogosulatlan hozzáféréssel szemben.
  - Ebbe a kategóriába tartoznak többek között a hálózati tűzfalak és az alkalmazásszintű tűzfalak, például webalkalmazások tűzfalai vagy szűrői és a kéretlen üzenetek elleni átjárók.
  - A behatolásérzékelő rendszerek olyan, digitális elemeket tartalmazó termékek, amelyek figyelik a forgalmat, miután az gyanús tevékenység céljából belépett a hálózati környezetbe, és észlelik vagy azonosítják, hogy behatolást kíséreltek meg, behatolás történt vagy történik egy csatlakoztatott hálózaton vagy rendszerben.
  - Ebbe a kategóriába tartoznak többek között a hálózatalapú behatolásérzékelő rendszerek és a gazdagépalapú behatolásérzékelő rendszerek.

# Standard?

- ISO? EN? EN!



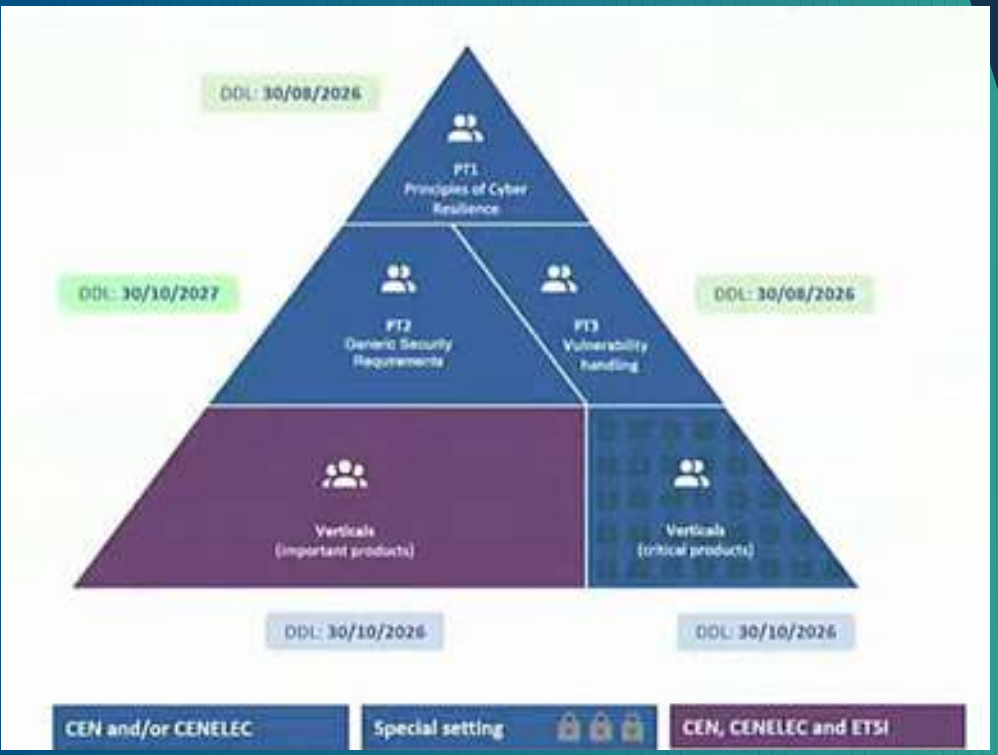

EN 304 633 – Internet connected toys
EN 304 634 – Personal wearable products
EN 304 635 – Hypervisors and container runtime systems

- PT1 – PT2 – PT3: átfogó. Önértékelést segíti
  - EN 40000-1-1 Vocabulary
- PT1: EN 40000-1-2 Principles for Cyber Resilience (risk, lifecycle)
- PT2: EN 40000-1-4 Security Controls (EN 18031:2024 series)
- PT3: EN 40000-1-3 Vulnerability handling
- Verticals: 18 CRA termékspecifikáció: EN 304 6xx (617-642)
- „Harmonizált standardok”: Fontos I, Fontos II, Kritikus
  - CC PP-k valójában

- „CLC/TC 65X” – OT előírások, mert NIS2-ben keresi mindenki!
  - EN IEC 62443-4-1 Security product development lifecycle requirements
  - EN IEC 62443-4-2 Technical security requirements for IACS components

# Standard?

- ISO? EN? EN!




EN 304 633 – Internet connected toys
EN 304 634 – Personal wearable products
EN 304 635 – Hypervisors and container runtime systems

- PT1 – PT2 – PT3: general, mandatory for the organization
  - EN 40000-1-1 Vocabulary
- PT1: EN 40000-1-2 Principles for Cyber Resilience (risk, lifecycle)
- PT2: EN 40000-1-4 Security Controls (EN 18031:2024 series)
- PT3: EN 40000-1-3 Vulnerability handling
- Verticals: 18 CRA product standards: EN 304 6xx (617-642)
- „EU harmonized standards”: Important I, Important II, Critical
  - CC PPs at real life

„CLC/TC 65X” – OT standards

- EN IEC 62443-4-1 Security product development lifecycle requirements
- EN IEC 62443-4-2 Technical security requirements for IACS components

# EN 304 635

- Virtualisation and Container Execution Systems

- Termékjellemző – Type II
  - A konténeres futtatókörnyezetek olyan, digitális elemeket tartalmazó szoftvertermékek, amelyek elszigetelt folyamatokként kezelik az egy gazdagépes operációs rendszeren futó konténerek végrehajtását és életciklusát, elosztják az erőforrásokat, és lehetővé teszik az egyes konténerek kezelését és szervezését.
  - E termékkategóriával összefüggésben a konténer olyan szoftveralapú végrehajtási környezet, amely egy vagy több szoftver alkotóelemét és azok függőségeit egyetlen csomagba foglalja, lehetővé téve számukra, hogy függetlenül és következetesen működjenek.
- V0.0.10 = 249 oldal!
  - **T-CE-INTEG-COMP:** Integrity compromise of container engine and managed images
    - An attacker tampers with the container engine's binaries, configuration files, or locally cached container images. The compromised engine can then execute manipulated workloads or disable controls, while still appearing healthy to the orchestrator.
  - REQ-CRS-CN-ISO-002: The CRS shall support configuration of strong separation between containers and the host operating system by restricting container access to kernel interfaces, privileged operations, and system resources outside their assigned execution context.
- FOSS → ADCO

# EN 304 635

- Virtualisation and Container Execution Systems

**1. Assessment Reference**
Requirement: REQ-CRS-B-INT-002 (Elevated)

**2. Assessment Objective**
Verify that:

1) The CRS implements mechanisms to participate in a verifiable chain of trust for CRS startup components delivered as part of the CRS product and executed before container execution services are enabled.

2) Each CRS startup stage delivered with the product and executed prior to exposing container execution interfaces validates the integrity and authenticity of the subsequent CRS stage before transferring control.

3) If validation fails for any such startup stage, the CRS prevents startup of container execution services and generates a security-relevant event.

**3. Assessment Preparation**
The assessment shall have access to:

- Documentation of the CRS startup chain for components delivered with the product (e.g. CRS launchers, shims, daemons that initialize container execution services).
- Documentation describing how each CRS startup stage validates the integrity and authenticity of the next CRS stage (e.g. signature checks, hash verification) and how this can integrate with a platform or CRS-defined chain of trust.
- A test configuration where:
  - normal startup with valid CRS startup components is possible;
  - a controlled validation failure can be induced for at least one CRS startup stage (e.g. modified or unsigned binary, untrusted key), consistent with vendor guidance.

**4. Assessment Activities**
The assessment shall at least:

1) Review documentation to identify all CRS startup stages delivered with the product that execute before container execution services are enabled, and the validation performed at each stage.

2) Perform a normal CRS startup and verify, using logs or diagnostic outputs, that:
   - each CRS startup stage validates the integrity/authenticity of the next stage before passing control;
   - container execution services are enabled only after successful validation of all such stages.

3) Introduce a controlled integrity/authenticity failure in one CRS startup stage and restart the CRS. Verify that:
   - the validation failure at that stage is detected;
   - container execution services are not started;
   - a security-relevant event is generated and recorded.

- Felkészül: NIS 2.1 + CSA 2.0

**Table 4.6.3-1: Relevant CRA harmonised standards for OE components**

| OE Component | Relevant CRA Reference |
|---|---|
| Boot Manager | ETSI EN 304 623 [i.4] (CRA for Boot Manager) |
| Host Operating System | ETSI EN 304 626 [i.5] (CRA for Operating System) |
| Network Infrastructure (Virtual / Physical / SDN) | ETSI EN 304 625 [i.6] (CRA Network Interfaces) |
| Identity & Access Management / PKI | ETSI EN 304 624 [i.7] (CRA PKI) |
| Image Registry / Artifact Repository | NA |
| External Logging / SIEM | ETSI EN 304 622 [i.8] (CRA SIEM) |
| External Attestation System | NA |
| Trust Anchors | CEN xxx xxx (CRA Security Modules) |
| Firewall / Intrusion Prevention System | ETSI EN 304 636 [i.9] (CRA Network Security Appliances) |
| Storage Systems | NA |

| Threat ID | Basic Requirements | Elevated Requirements | Advanced Requirements |
|---|---|---|---|
| Associated Risk Level | Low | Medium | High |
| T-CRS-INTF-ESC | REQ-CRS-CN-ISO-001<br>REQ-CRS-CP-ISO-001<br>REQ-CRS-NP-ISO-001 | REQ-CRS-CN-ISO-002<br>REQ-CRS-CP-ISO-002<br>REQ-CRS-NP-ISO-002 | REQ-CRS-CN-ISO-003<br>REQ-CRS-CP-ISO-003<br>REQ-CRS-NP-ISO-003 |
| T-CRS-INTEG-COMP | REQ-CRS-B-INT-001<br>REQ-CRS-IMG-INT-001 | REQ-CRS-B-INT-002<br>REQ-CRS-IMG-INT-002<br>REQ-CRS-RP-INT-002 | REQ-CRS-B-INT-003<br>REQ-CRS-B-INT-004<br>REQ-CRS-IMG-INT-003<br>REQ-CRS-IMG-INT-004<br>REQ-CRS-RP-INT-003<br>REQ-CRS-RP-INT-004<br>REQ-CRS-RA-INT-003<br>REQ-CRS-RA-INT-004 |

# Your contact to success

Köszönöm a figyelmetek!


- Kis-Szabó András
- Andras.Kis-Szabo@kontron.hu

- Kontron AG