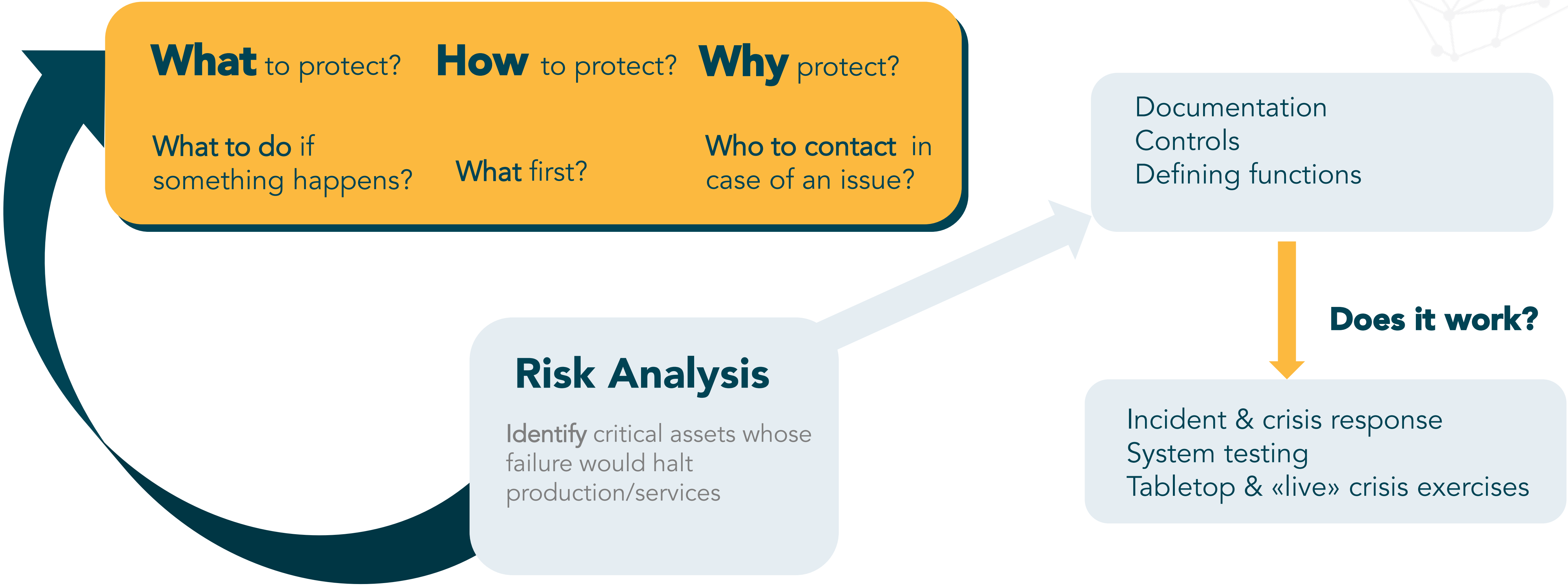
ADRONH
FUNDAMENTAL SECURITY

Cybersecurity & Resilience for Manufacturing Companies

Challenges & Recommendations

Desirée Alegre
Senior Cybersecurity Consultant

NIS2 is not just compliance
It is an opportunity to ensure resilience



What to protect? **How** to protect? **Why** protect?

What to do if something happens?

What first?

Who to contact in case of an issue?

Documentation
Controls
Defining functions

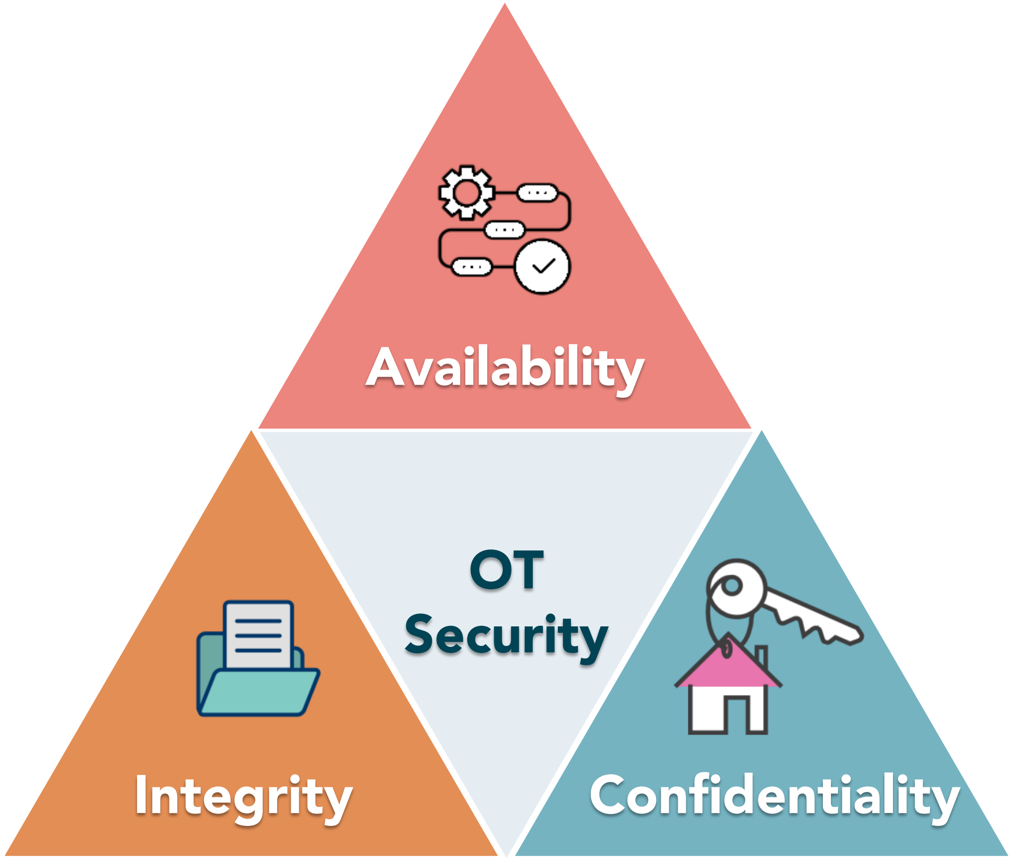
Does it work?

Incident & crisis response
System testing
Tabletop & «live» crisis exercises

Risk Analysis

Identify critical assets whose failure would halt production/services

Challenges in OT Security



ℹ *Manufacturing is the* ***#2*** *most targeted sector for cyberattacks* (IBM 2023)

From Cyber Attack to Production Setback:
a breach in security can halt productivity

Threat	Incident	Cost
Locked-down systems: operators lose visibility and control of equipment	Ransomware	$4.4M ransom $8M downtime
Confidential company data (intellectual property) stolen	Credential Theft	$3.1M in lost contracts R&D delays
Network saturation slowing down operations	Network congestion (DDoS)	A 12-hour DDoS can cost $500K–2M in logistical losses
Supplier unavailable due to a cyber incident	Malicious Supply Chain attack	24h shutdown of production

Processing chain in OT: cyber weaknesses and threats

Industrial control systems are classified based on their capabilities and security considerations.

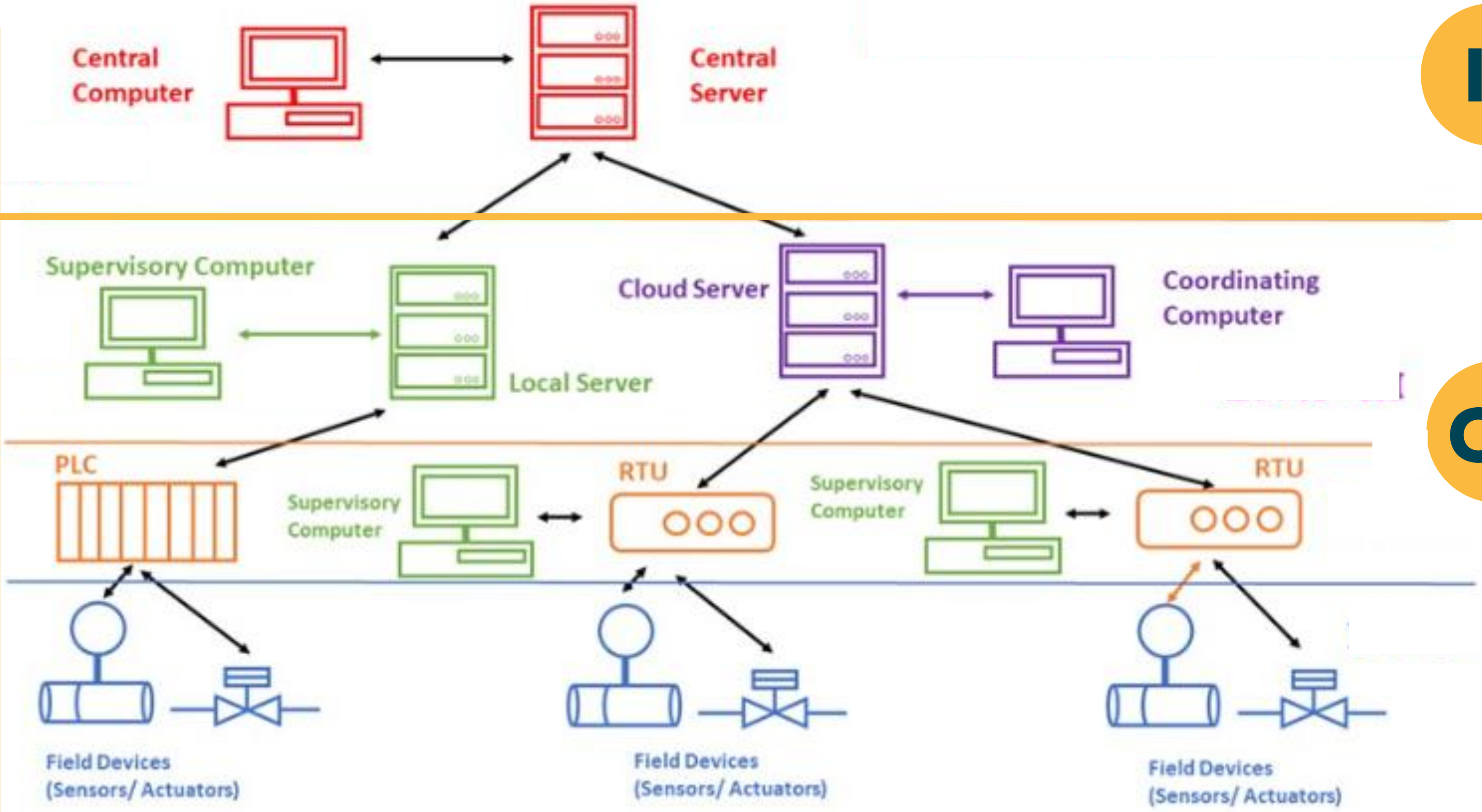
Business planning & logistics

Manufacturing operations & controls

Supervision

Programming device

Sensors, probes

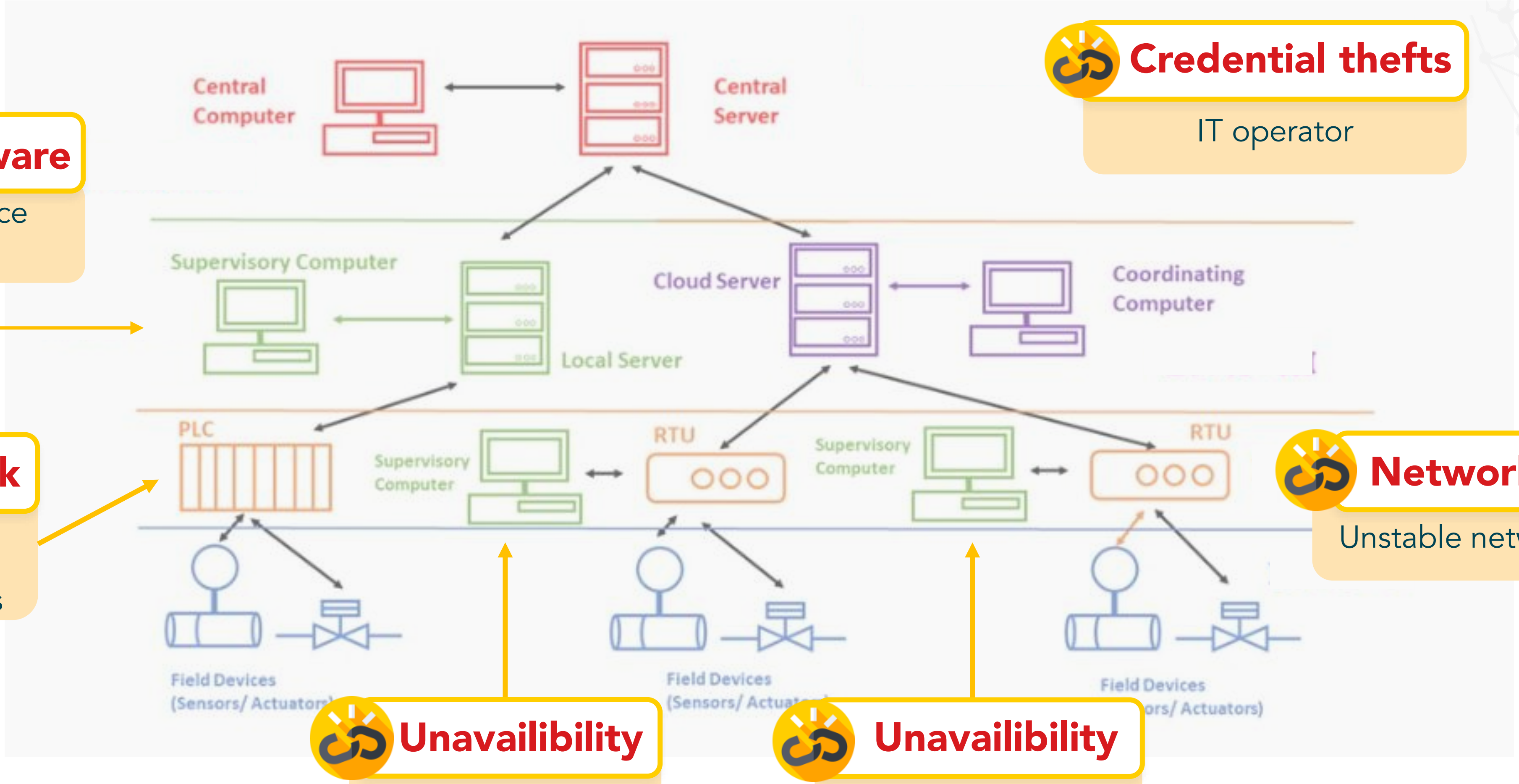


IT

OT

Different Types of SCADA System Architecture

Processing chain in OT: cyber weaknesses and threats



Ransomware
Mobile device access

Credential thefts
IT operator

Malicious attack
Vendor's remote access for maintenance/updates

Network congestion
Unstable network connection

Unavailibility
Disk backup
Hardware spare

Unavailibility
Outdated system

Risk analysis: Key challenges & Remediations

Risk analysis in itself

Start Small,
Scale Smart

No consensus on what's critical

Establish easy definitions, ex. "critical" as:
">X hours downtime = production stops"
>1h downtime = Breaches NIS2 SLA

Unclear risk ownership

Assign RACI matrix
per asset/scenario

Human factor

Identification of skills and
documentation of knowledge

NIS2 Gym Membership: Drills for Your Security Six-Pack

From 'paperwork' to 'bulletproof': Bridging Risk Analysis to Action with Crisis & Tabletop Exercises

Exercises

- Tabletop Tales: Where Hypothetical Disasters Meet Real Coffee.
- System Testing: has the Back up tested? Critical app restauration?
- Crisis Exercises – Because 'Oops' Isn't an NIS2 Compliance Strategy?

＋ Advantages

- Eye-opener
- Revise documents
- Adjust RACI
- Update controls
- Define real costs

> "*Our crisis exercises must mirror real-world chaos—not just test controls, but human instincts. The goal isn't perfection but exposing gaps before attackers do.*"

Lessons from the Trenches: Key Takeaways

> *Because ‘hoping for the best’ is not a cybersecurity strategy*

Risk Analysis	Focus on Impact, Not Just Compliance	A risk matrix won’t stop an attack—but prioritizing might
Responsibilities	Who Does What When Chaos Hits?	In a crisis, ‘someone should handle that’ means no one will
Vendor Communication	No Blind Trust	Your vendors’ security is your security—until it isn’t
Exercise	Is your six-pack strong enough?	If your tabletop exercise feels easy, you’re doing it wrong

Know Your Allies	No IR team on standby? Enjoy your breach chaos	Finding your incident response team during an attack is like Googling ‘fire department’ while your kitchen is burning

Thank you for your time!

Appendix

NIS2 art 18 - Cybersecurity risk management measures	OT List of Controls
a) risk analysis and information system security policies;	Touch all controls
(b) incident handling (prevention, detection, and response to incidents);	Incident response Personnel training Breach monitoring Asset Vulnerability Management Log Management
(c) business continuity and crisis management;	Backup and recovery
(d) supply chain security including security related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;	Secure remote access Device Security Change Control Update systems Asset inventory
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Network Security Update systems Secure remote access Asset inventory Malware protection Device Security Change Control Access Management
(f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;	At all controls
(g) the use of cryptography and encryption	