

EDUCATION AND TRAINING

# CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



Co-funded by  
the European Union

# Cybersecurity Essentials and Management for Energy Sector

## CSP001\_C\_E

PRESENTATION BY:

**RUBEN RIOS**

UNIVERSITY OF MALAGA, SPAIN

EDUCATION AND TRAINING

# CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

## Next level cybersecurity education and training



Co-funded by  
the European Union

# Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

# Topic-3: Energy Sector Threats and Vulnerabilities

## Overview

- Identify and categorise common energy cybersecurity threats, such as malware, ransomware, phishing, and social engineering
- Recognise the specific vulnerabilities that energy systems face, including outdated software, weak passwords, and unpatched vulnerabilities
- Energy sector specific threats and vulnerabilities include targeted attacks on SCADA systems, smart grids, and other critical energy assets
- Understand the role of human error and insider threats in energy cybersecurity

# Topic-3: Energy Sector Threats and Vulnerabilities

## Overview

- **Identify and categorise common energy cybersecurity threats, such as malware, ransomware, phishing, and social engineering**
- Recognise the specific vulnerabilities that energy systems face, including outdated software, weak passwords, and unpatched vulnerabilities
- Energy sector specific threats and vulnerabilities include targeted attacks on SCADA systems, smart grids, and other critical energy assets
- Understand the role of human error and insider threats in energy cybersecurity

# Common threats in energy systems

- In 2013, ENISA launches the report “*Smart Grid Threat Landscape and Good Practice Guide*” with a comprehensive study about threats in Smart Grids
- However, the number of threats has risen sharply in recent years, as reflected both by
  - The attack matrix given by MITRE ATT&CK, and
  - ENISA annual reports about the threat landscape in the diverse fields

Source: ENISA, “Smart Grid Threat Landscape and Good Practice Guide”, December 2013  
URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>



# Common threats in energy systems

- In 2013, ENISA launches the report "*Smart Grid Threat Landscape and Good Practice Guide*" with a comprehensive study about threats in Smart Grids
- However, the number of threats has risen sharply in recent years, as reflected both by
  - The attack matrix given by MITRE ATT&CK, and
  - ENISA annual reports about the threat landscape in the diverse fields
- Based on these sources, we classify the threats in this sector using the traditional **AIC + A**
  - Availability
  - Integrity
  - Confidentiality
  - Authentication



Source: ENISA, "Smart Grid Threat Landscape and Good Practice Guide", December 2013  
URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>

# Common threats in energy systems

- More specifically, “**AIC + A**” threats refers to:
  - **(A) Availability**: Denial of Services (DoS) or lack of proper use of assets
  - **(I) Integrity**: Modification of legitimate assets of the system or generation of fake data or configurations
  - **(C) Confidentiality**: Unauthorized access to legitimate assets of a system, containing private or sensitive information
  - **(A) Authentication**: Theft of identity or impersonation of users

# Common threats in energy systems

- More specifically, “**AIC + A**” threats refers to:
  - **(A) Availability**: Denial of Services (DoS) or lack of proper use of assets
  - **(I) Integrity**: Modification of legitimate assets of the system or generation of fake data or configurations
  - **(C) Confidentiality**: Unauthorized access to legitimate assets of a system, containing private or sensitive information
  - **(A) Authentication**: Theft of identity or impersonation of users
- For AIC+A, we will explore three different trends
  - **Traditional threats** that still arise in power systems
  - **Recent threats** in power systems
  - **Future threats** in power systems

# Common threats in energy systems

- More specifically, “**AIC + A**” threats refers to:
  - **(A) Availability**: Denial of Services (DoS) or lack of proper use of assets
  - **(I) Integrity**: Modification of legitimate assets of the system or generation of fake data or configurations
  - **(C) Confidentiality**: Unauthorized access to legitimate assets of a system, containing private or sensitive information
  - **(A) Authentication**: Theft of identity or impersonation of users
- For AIC+A, we will explore three different trends
  - **Traditional threats** that still arise in power systems
  - **Recent threats** in power systems
  - **Future threats** in power systems
- The affected targets may be:
  - **Energy** - infrastructure / grid
  - **Control** – cyber-physical components
  - **User/organisation** – sensible information

Traditional threat trends  
in power systems

Current threat trends in  
power systems

Future threat trends in  
power systems

**Traditional threat trends  
in power systems**

Current threat trends in  
power systems

Future threat trends in  
power systems

# Common threats to AIC+A in power systems – *Traditional trends*

- Some of the most common and traditional threats in power systems are as follows:

Traditional threats	Description	Affects to / final impact						
		A	I	C	A	Energy	Control	User
<b>Causal threats</b>	Any unintentional threat caused by an unforeseen exploitation of a failure/error, natural disaster, or an <b>undeliberate human action</b>	X	X	X		X	X	X

- Given that human errors is seen as one of the most potential threats in the coming years, we will see in more detail in the point “**Understand the role of human error and insider threats in energy cybersecurity**”

Source: ENISA, “Smart Grid Threat Landscape and Good Practice Guide”, December 2013,  
 URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>



# Common threats to AIC+A in power systems – *Traditional trends*

- Some of the most common and traditional threats in power systems are as follows:

Traditional threats	Description	Affects to / final impact						
		A	I	C	A	Energy	Control	User
<b>Causal threats</b>	Any unintentional threat caused by an unforeseen exploitation of a failure/error, natural disaster, or an undeliberate human action	X	X	X		X	X	X
<b>Physical threats</b>	Any "deliberate" physical damage against the infrastructure and its resources such as sabotage or vandalism, theft of components, information leakage, etc.	X	X	X		X	X	X

# Common threats to AIC+A in power systems – *Traditional trends*

- Some of the most common and traditional threats in power systems are as follows:

Traditional threats	Description	Affects to / final impact						
		A	I	C	A	Energy	Control	User
<b>Causal threats</b>	Any unintentional threat caused by an unforeseen exploitation of a failure/error, natural disaster, or an undeliberate human action	X	X	X		X	X	X
<b>Physical threats</b>	Any "deliberate" physical damage against the infrastructure and its resources such as sabotage or vandalism, theft of components, information leakage, etc.	X	X	X		X	X	X
<b>Denial of Service (DoS) / outages</b>	Any lack to the availability of essential resources, such the grid and its energy, control resources or data	X				X	X	X

Source: ENISA, "Smart Grid Threat Landscape and Good Practice Guide", December 2013,  
URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>



# Common threats to AIC+A in power systems – *Traditional trends*

- Some of the most common and traditional threats in power systems are as follows:

Traditional threats	Description	Affects to / final impact							
		A	I	C	A	Energy	Control	User	
<b>Causal threats</b>	Any unintentional threat caused by an unforeseen exploitation of a failure/error, natural disaster, or an undeliberate human action	X	X	X		X	X	X	
<b>Physical threats</b>	Any "deliberate" physical damage against the infrastructure and its resources such as sabotage or vandalism, theft of components, information leakage, etc.	X	X	X		X	X	X	
<b>Denial of Service (DoS) / outages</b>	Any lack to the availability of essential resources, such the grid and its energy, control resources or data	X				X	X	X	
<b>Nefarious activity, abuse</b>	Any malicious action that may address penetration, intrusion, authorisation use/access to assets, impersonation, manipulation of assets, falsification of data, data leakage, DoS or infection	X	X	X	X	X	X	X	

Source: ENISA, "Smart Grid Threat Landscape and Good Practice Guide", December 2013,  
URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>



# Common threats to AIC+A in power systems – Traditional trends

- Some of the most common and traditional threats in power systems are as follows:

Traditional threats	Description	Affects to / final impact							
		A	I	C	A	Energy	Control	User	
<b>Causal threats</b>	Any unintentional threat caused by an unforeseen exploitation of a failure/error, natural disaster, or an undeliberate human action	X	X	X		X	X	X	
<b>Physical threats</b>	Any "deliberate" physical damage against the infrastructure and its resources such as sabotage or vandalism, theft of components, information leakage, etc.	X	X	X		X	X	X	
<b>Denial of Service (DoS) / outages</b>	Any lack to the availability of essential resources, such the grid and its energy, control resources or data	X				X	X	X	
<b>Nefarious activity, abuse</b>	Any malicious action that may address penetration, intrusion, authorisation use/access to assets, impersonation, manipulation of assets, falsification of data, data leakage, DoS or infection	X	X	X	X	X	X	X	
<b>Eavesdropping, interception, hijacking</b>	Any activity that entails interception in the communications, Man-in-the-Middle (MitM), reconnaissance, information gathering, relays of messages, etc.		X	X	X		X	X	

Source: ENISA, "Smart Grid Threat Landscape and Good Practice Guide", December 2013, URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>



Traditional threat trends  
in power systems

**Current threat trends in  
power systems**

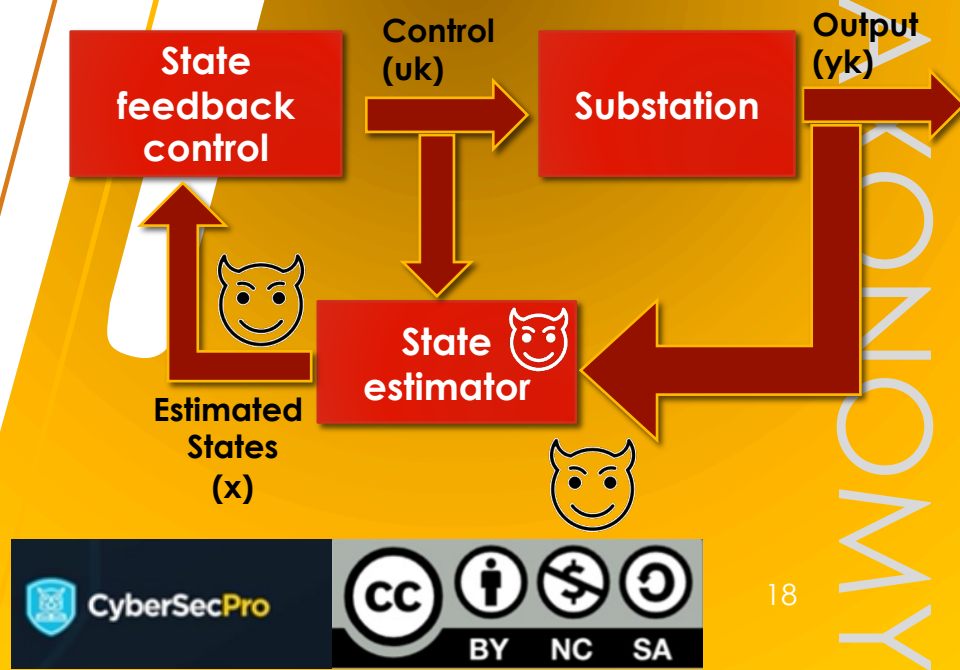
Future threat trends in  
power systems

# Common threats to AIC+A in power systems - *Current trends*

- More recent threats include:

Current threats	Description	Affects to / final impact						
		A	I	C	A	Energy	Control	User
<b>False Data Injection (FDI) attacks</b>	Any falsification about the control state to alter the performance of the infrastructure. This may range from the falsification of C&C packets to inject fake meter measurements to the state estimations		X			X	X	X
<b>Stealthy FDI attacks</b>	Any FDI action but in a stealthy manner		X			X	X	X

- There are some FDI attack strategies, which are based on:
  - **Power flow:** Attack models aim to change the linearity of the power flow
  - **Architecture:** FDI attacks modify measurements received and managed by state estimator/s. In centralized systems, the target is the state estimator (1 single element)
  - **Methodology:** Modification of measurements depending on the level of knowledge of the context, such as topology information, grid topology, or data models applied (e.g., ML and its inference)



Source: H. T. Reda, A. Anwar, A. N. Mahmood, Z. Tari, "A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids", ACM Computing Surveys, 55(14s), 1-37, 2023

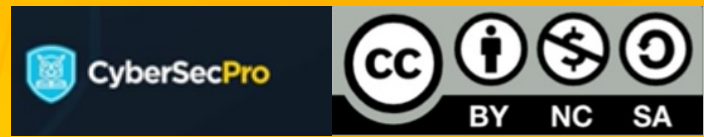
# Common threats to AIC+A in power systems – *Current trends*

- More recent threats include:

Current threats	Description	Affects to / final impact						
		A	I	C	A	Energy	Control	User
<b>False Data Injection (FDI) attacks</b>	Any falsification about the control state to alter the performance of the infrastructure. This may range from the falsification of C&C packets to inject fake meter measurements to the state estimations		X			X	X	X
<b>Stealthy FDI attacks</b>	Any FDI action but in a stealthy manner		X			X	X	X
<b>Malware</b>	Software intended to manipulate the normal operation of systems, without the knowledge or authorisation of the users who own those systems	X	X	X	X	X	X	X

- There are many types of malware: virus, worms, trojans, ransomware, ...
- The goals of the malware may be very varied, from the exfiltration/disclosure of sensitive information to isolation or destruction of critical assets (e.g., controllers)

Source: ENISA, "ENISA Threat Landscape 2023", 2023,  
URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>



# Common threats to AIC+A in power systems – *Current trends*

- **Virus:** a self-replicating software code that, when executed, 'spreads' in the system, massively infecting other software components, mainly executables – it is required human intervention
- **Worm:** is also a self-replicating software code but without the need for human intervention
- **Trojan / backdoor:** a hidden malware, whose codes are not able to self-replicate their actions or infect other programs, but are executed and controlled remotely by malicious entities to achieve privilege escalation, information leakage, modification of services and data, etc.
- **Ransomware:** malicious code designed to block access to the system until a ransom is paid for it (obtaining the session key and encryption conditions)
  - The technique focuses on encrypting information on the system

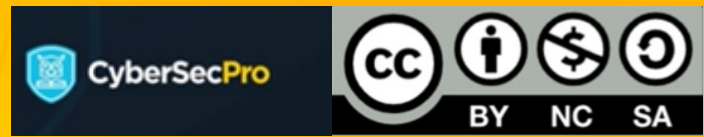
# Common threats to AIC+A in power systems – *Current trends*

- More recent threats include:

Current threats	Description	Affects to / final impact						
		A	I	C	A	Energy	Control	User
<b>False Data Injection (FDI) attacks</b>	Any falsification about the control state to alter the performance of the infrastructure. This may range from the falsification of C&C packets to inject fake meter measurements to the state estimations		X			X	X	X
<b>Stealthy FDI attacks</b>	Any FDI action but in a stealthy manner		X			X	X	X
<b>Malware</b>	Software intended to manipulate the normal operation of systems, without the knowledge or authorisation of the users who own those systems	X	X	X	X	X	X	X
<b>Social engineering</b>	Techniques to psychologically disclosure of sensitive information for penetration or intrusion such as security credentials or access mode			X	X		X	X

- There are many techniques to extract private information such as credentials: **phishing** / **spear phishing** (via the e-mail), **vishing** (via the phone), **HTTPS phishing** (forward to fake website), **pharming** (malware that forwards to the victim to a fake website), **angler phishing** (fake social media posts), etc.

Source: ENISA, "ENISA Threat Landscape 2023", 2023, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>  
 Source: FORTINET, "19 Types of Phishing Attacks, Different Types of Phishing Attacks", <https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks>, 2024



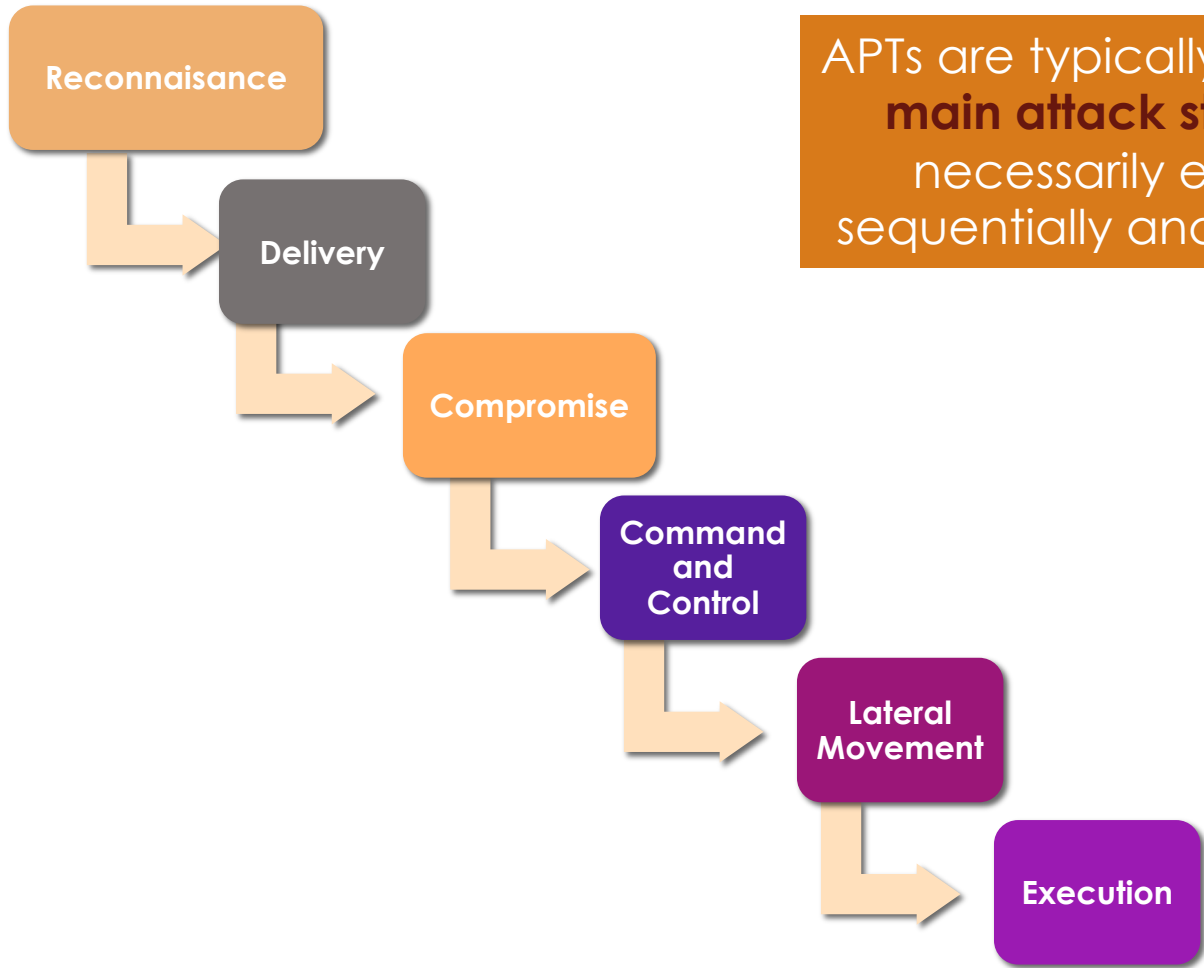
# Common threats to AIC+A in power systems – *Current trends*

- More recent threats include:

Current threats	Description	Affects to / final impact						
		A	I	C	A	Energy	Control	User
<b>False Data Injection (FDI) attacks</b>	Any falsification about the control state to alter the performance of the infrastructure. This may range from the falsification of C&C packets to inject fake meter measurements to the state estimations		X			X	X	X
<b>Stealthy FDI attacks</b>	Any FDI action but in a stealthy manner		X			X	X	X
<b>Malware</b>	Software intended to manipulate the normal operation of systems, without the knowledge or authorisation of the users who own those systems	X	X	X	X	X	X	X
<b>Social engineering</b>	Techniques to psychologically disclosure of sensitive information for penetration or intrusion such as security credentials or access mode			X	X		X	X
<b>Advanced persistent threats (APT)</b>	An APT is a sophisticated attack, normally executed by resourceful adversaries over a long time period; the aim is to destroy critical devices or exfiltrate sensitive data	X	X	X	X	X	X	X

- APTs are focused on combining multiple attack vectors that include the exploitation of **zero-day vulnerabilities**, together with “**stealthy**” and evasive techniques

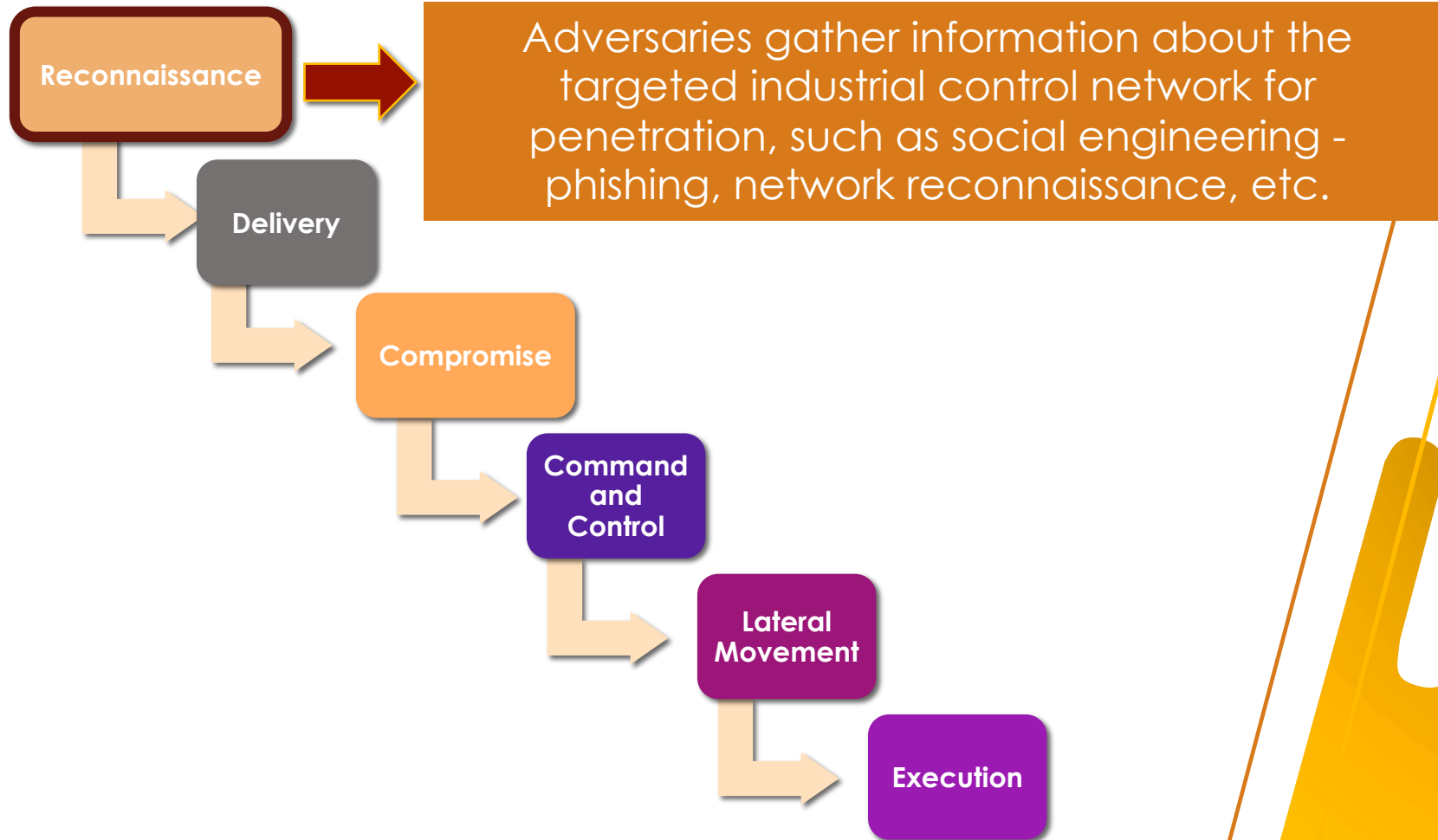
# Common threats to AIC+A in power systems – *Current trends*



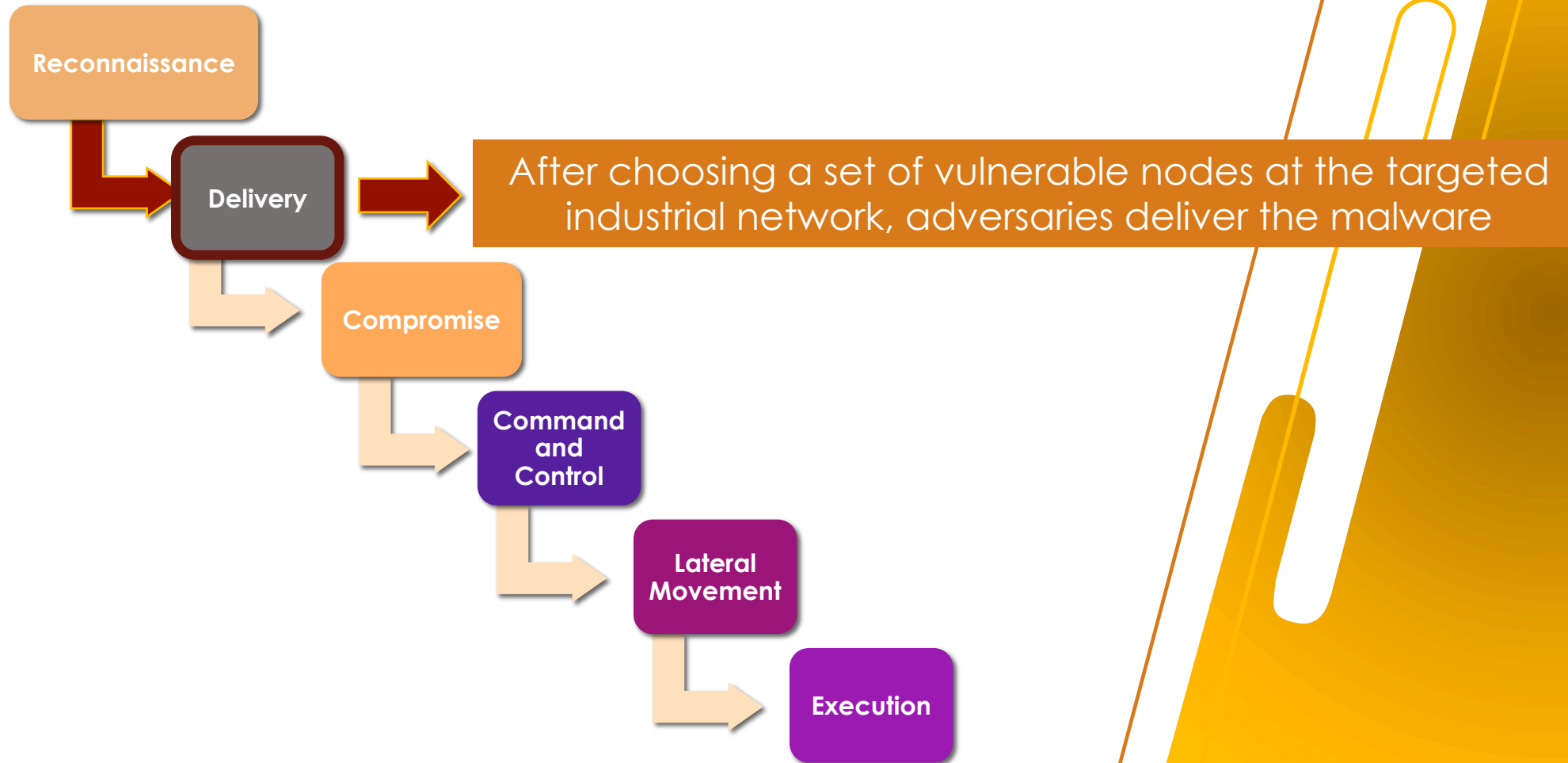
APTs are typically based on **6 main attack stages**, not necessarily executed sequentially and all of them

Source: J. E. Rubio, R. Roman, C. Alcaraz, and Y. Zhang, "Tracking Advanced Persistent Threats in Critical Infrastructures through Opinion Dynamics", European Symposium on Research in Computer Security (ESORICS 2018) vol. 11098, pp. 555-574, 2018

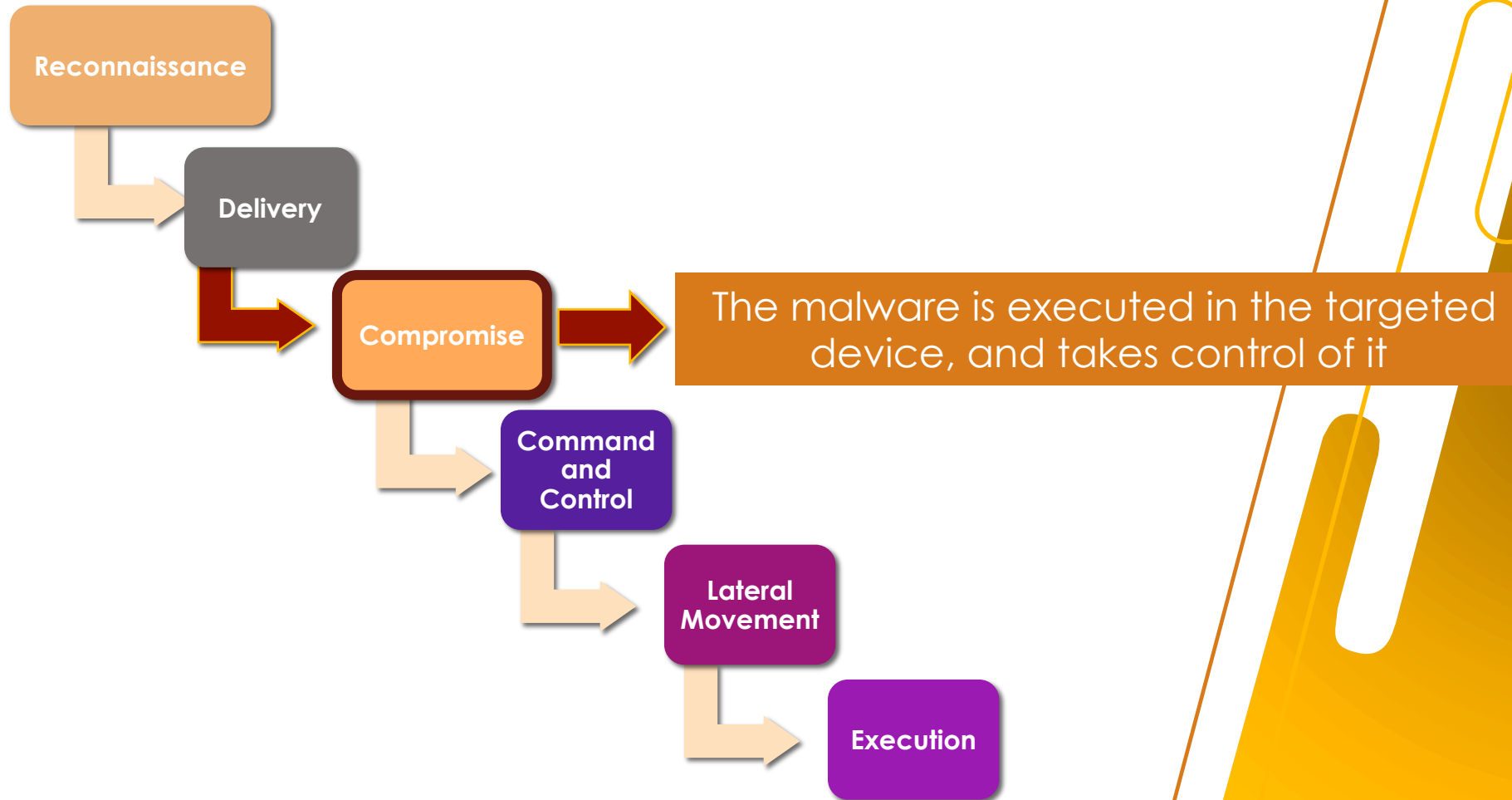
# Common threats to AIC+A in power systems – *Current trends*



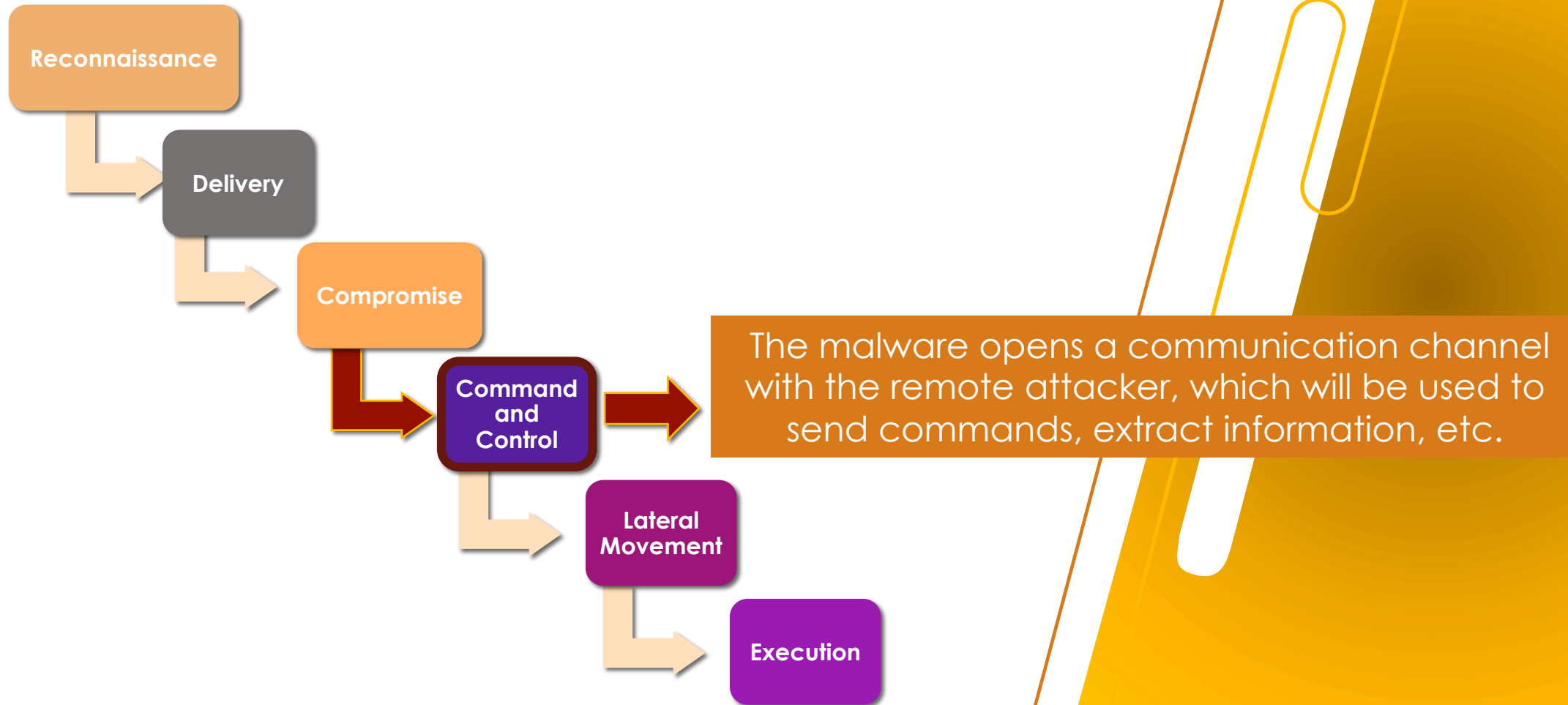
# Common threats to AIC+A in power systems - *Current trends*



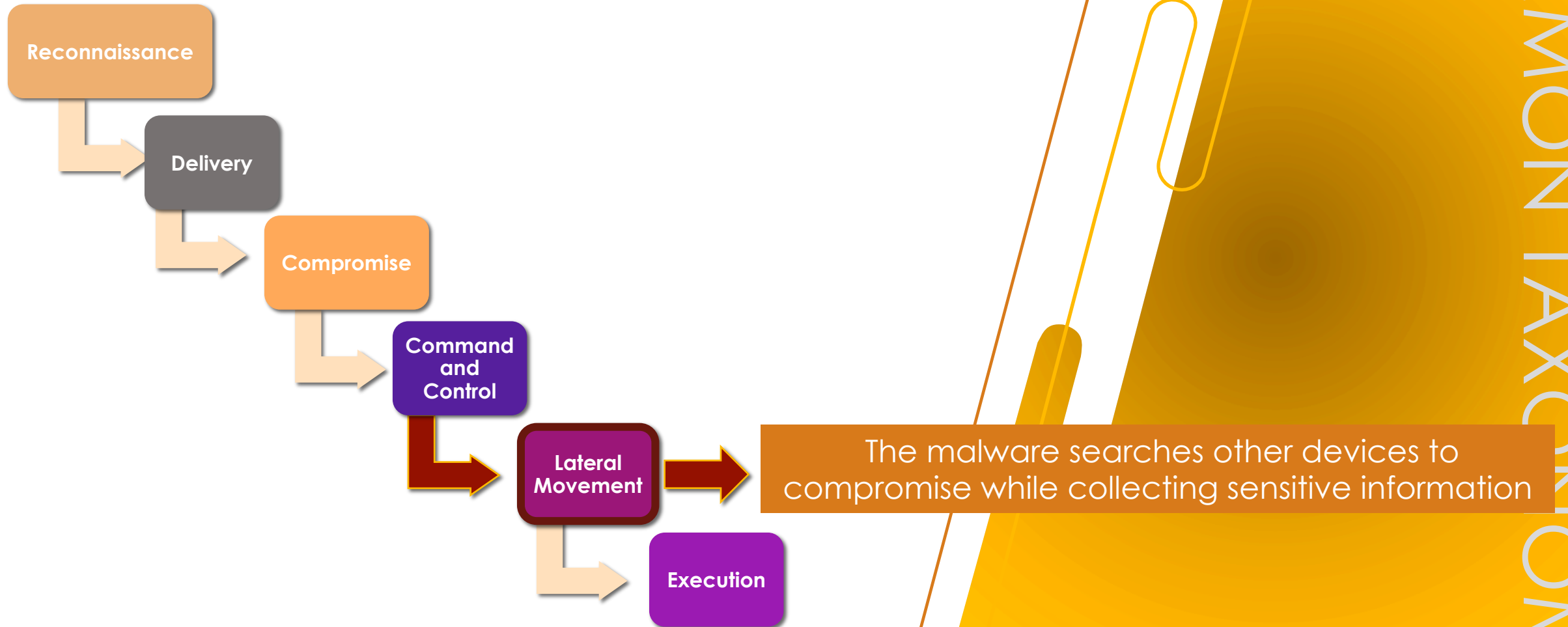
# Common threats to AIC+A in power systems - *Current trends*



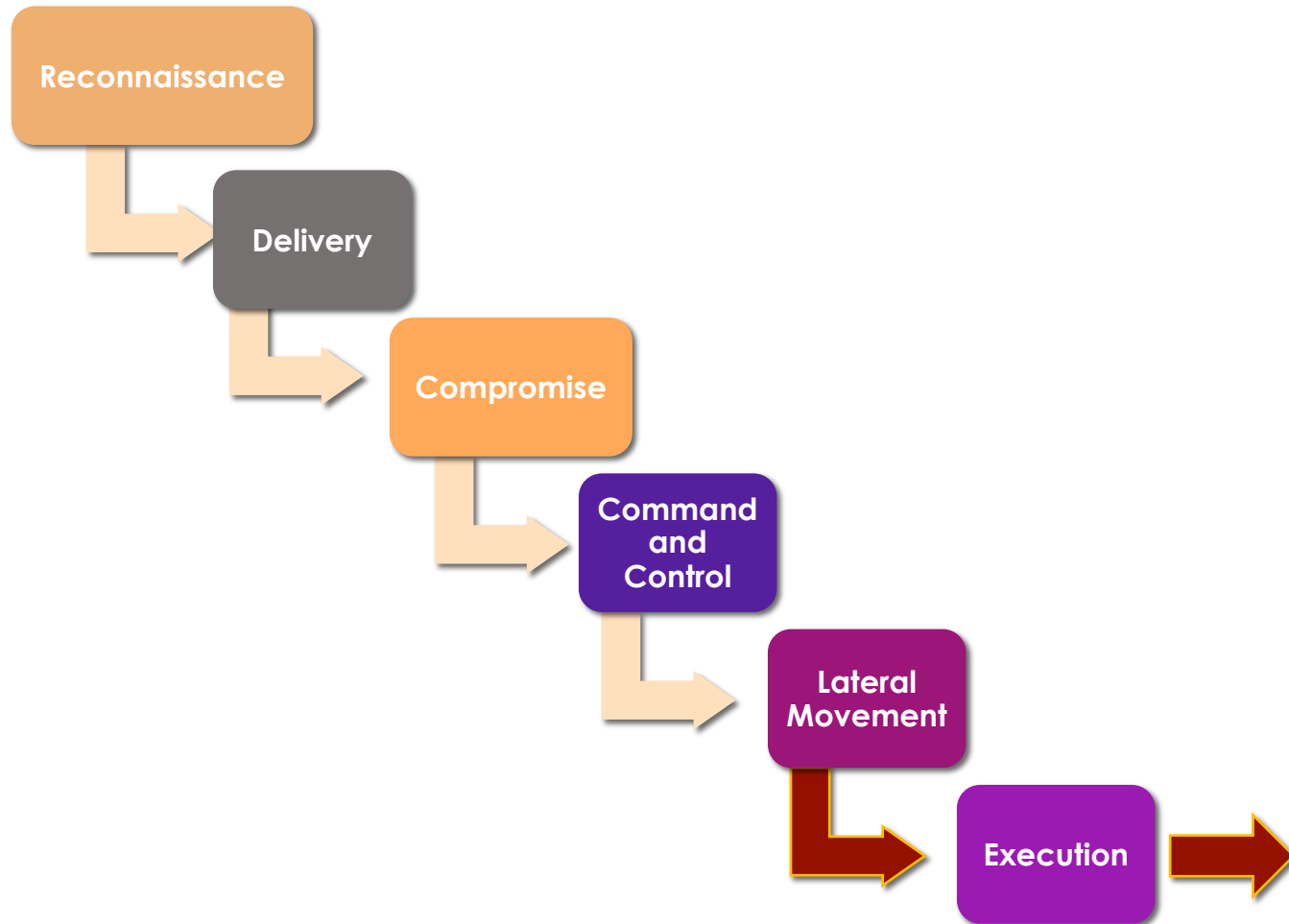
# Common threats to AIC+A in power systems - *Current trends*



# Common threats to AIC+A in power systems - *Current trends*



# Common threats to AIC+A in power systems - *Current trends*



The malware finally performs the attack against the industrial network, which involves the **extraction of sensitive data or the destruction of resources**

# Common threats to AIC+A in power systems – *Current trends*

- In order to keep the persistence, the **movements and actions** (e.g., C&C) must be performed **from a stealthy manner**
  - Keeping patience, avoiding abrupt actions/movements, hiding malicious actions/data,...
- There are many attack techniques that disclose information, recognise the environment, or exfiltrate information to other external sites, such as:
  - **Side channel:** analyse data signals in communication channels to physically derive sensitive information transmitted from a network peer to another one
  - **Covert channel:** manipulate targets (e.g., via a malware) and camouflage C&C orders in packets or signals in order to exfiltrate information such as sensor measurements, or send commands to actuators

# Common threats to AIC+A in power systems – *Current trends*

- MITRE ATT&CK also provides the tactics and techniques corresponding to MITRE ATT&CK® Matrix for ICS
- As illustrated in the figure, the attack tactics coincide (in the majority) with the kill chain of an APT-type attack

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog ↗ Search

MATRICES

Enterprise ▾  
Mobile ▾  
ICS

Home > Matrices > ICS

## ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

[View on the ATT&CK® Navigator ↗](#)

[Version Permalink](#)

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Spoof Reporting Message	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking					Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

# Common threats to AIC+A in power systems – *Current trends*

- More recent threats include:

Current threats	Description	Affects to / final impact						
		A	I	C	A	Energy	Control	User
<b>False Data Injection (FDI) attacks</b>	Any falsification about the control state to alter the performance of the infrastructure. This may range from the falsification of C&C packets to inject fake meter measurements to the state estimations		X			X	X	X
<b>Stealthy FDI attacks</b>	Any FDI action but in a stealthy manner		X			X	X	X
<b>Malware</b>	Software intended to manipulate the normal operation of systems, without the knowledge or authorisation of the users who own those systems	X	X	X	X	X	X	X
<b>Social engineering</b>	Techniques to psychologically disclosure of sensitive information for penetration or intrusion such as security credentials or access mode			X	X		X	X
<b>Advanced persistent threats (APT)</b>	An APT is a sophisticated attack, normally executed by resourceful adversaries over a long time period; the aim is to destroy critical devices or exfiltrate sensitive data	X	X	X	X	X	X	X
<b>Supply chain compromise</b>	Any corruption in the supply chain may compromise the integrity of the software and hardware dependencies, and their trustworthy	X	X	X	X	X	X	X

Traditional threat trends  
in power systems

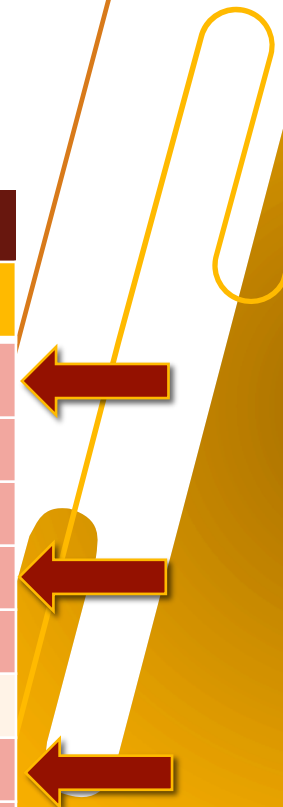
Current threat trends in  
power systems

**Future threat trends in  
power systems  
(Threats 2030)**

# Common threats to AIC+A in power systems – Future trends

- ENISA's report on "Identifying Emerging Cyber Security Threats and Challenges for 2030" forecasts some potential threat trends for 20230

Foreseen threats	A	I	C	A	Affects to / final impact		
					Energy	Control	User
Supply chain compromise	X	X	X	X	X	X	X
Disinformation campaigns		X		X			X
Loss of privacy			X				X
Human error	X	X	X		X	X	X
Targeted attacks (led by smart devices)	X	X	X	X	X	X	X
Lack of analysis and control	X	X			X	X	
Advanced hybrid threats	X	X	X	X	X	X	X
AI Abuse	X	X	X	X	X	X	X



Source: ENISA, "Identifying Emerging Cyber Security Threats and Challenges for 2030", 2023, <https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>

## Final remarks

Threat trends	A	I	C	A	Energy	Control	User
Traditional	4	4	4	2	4	5	5
Current	3	5	4	4	5	6	6
Future	6	7	6	5	6	6	7

- We have seen "how" the number of threats in power systems trends to grow, providing a clear overview of:
  - **Traditional** (but persistent) threat trends
  - **Current** trends
  - **Possible** and future trends
- For all of them, we have also explored their impact, and particularly on:
  - **Energy** and its respective infrastructures
  - **Control** including its components and networks
  - **User or organisation**
- In most of cases, "control" may be the most attractive target for attackers
  - Why? Because through control, attackers may lead subsequent attacks against the energy and its resources

# References and sources

1. ENISA, "Smart Grid Threat Landscape and Good Practice Guide", December 2013  
URL: <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>
2. H. T. Reda, A. Anwar, A. N. Mahmood, Z. Tari, "A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids", ACM Computing Surveys, 55(14s), 1-37, 2023
3. J. E. Rubio, R. Roman, C. Alcaraz, and Y. Zhang, "Tracking Advanced Persistent Threats in Critical Infrastructures through Opinion Dynamics", European Symposium on Research in Computer Security (ESORICS 2018) vol. 11098, pp. 555-574, 2018.
4. ENISA, "ENISA Threat Landscape 2023", 2023,  
URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
5. FORTINET, "19 Types of Phishing Attacks, Different Types of Phishing Attacks",  
URL: <https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks>, 2024
6. ENISA, "Identifying Emerging Cyber Security Threats and Challenges for 2030", 2023  
URL: <https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>
7. DeepL Translator for Proofreading.  
URL: <https://www.deepl.com/translator>



# Connect with CyberSecPro: How to register and other practical information

1. Website:  
[www.cybersecpro-project.eu](http://www.cybersecpro-project.eu)
2. X (Twitter):  
[https://twitter.com/CyberSecPro\\_eu](https://twitter.com/CyberSecPro_eu)
3. LinkedIn:  
<https://www.linkedin.com/company/cybersecpro-euproject/>



**Co-funded by  
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

 ACEEU ACCREDITATION COUNCIL FOR ENTREPRENEURIAL & ENGAGED UNIVERSITIES	 AIT AUSTRIAN INSTITUTE OF TECHNOLOGY	 APIROPLUS SOLUTIONS	 SINTEF	 SOCIAL ENGINEERING ACADEMY	 TAL TECH
ACEEU GmbH Germany <a href="#">Visit Website</a>	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Austria <a href="#">Visit Website</a>	APIROPLUS SOLUTIONS LTD Cyprus <a href="#">Visit Website</a>	SINTEF AS Norway <a href="#">Visit Website</a>	Social Engineering Academy GmbH Germany <a href="#">Visit Website</a>	Tallin University of Technology Estonia <a href="#">Visit Website</a>
Logo missing	 COFAC COOPERATIVA DE FORMAÇÃO E ANIMACÃO CULTURAL C.R.L.	 Consiglio Nazionale delle Ricerche	 Technische Universität Braunschweig	 TECHNICAL UNIVERSITY OF CRETE	 trustilio Enhance your Trustworthiness
C2B CONSULTING Portugal <a href="#">Visit Website</a>	COFAC Portugal <a href="#">Visit Website</a>	Consiglio Nazionale delle Ricerche Italy <a href="#">Visit Website</a>	Technical University of Braunschweig Germany <a href="#">Visit Website</a>	Technical University of Crete Greece <a href="#">Visit Website</a>	trustilio B.V. The Netherlands <a href="#">Visit Website</a>
 focal point Cyber Defence Exercises as a Service	 GOETHE UNIVERSITÄT FRANKFURT AM MAIN	 ITML	 UNINOVA	 UNIVERSIDAD DE MÁLAGA	 NOVA UNIVERSIDADE NOVA DE LISBOA
FOCAL POINT Belgium <a href="#">Visit Website</a>	Goethe University Frankfurt Germany <a href="#">Visit Website</a>	Information Technology for Market Leadership Greece <a href="#">Visit Website</a>	Uninova Portugal <a href="#">Visit Website</a>	Universidad de Malaga Spain <a href="#">Visit Website</a>	Universidade Nova De Lisboa Portugal <a href="#">Visit Website</a>
 Institut Mines-Télécom	 LAUREA	 GRUPPO Maggioli	 University of Cyprus	 FACULTY OF SCIENCES NOVI SAD SERBIA	 UNIVERSITY OF PIRAEUS RESEARCH CENTER
Institut Mines-Télecom France <a href="#">Visit Website</a>	Laurea University of Applied Sciences Finland <a href="#">Visit Website</a>	Maggioli S.p.A. Italy <a href="#">Visit Website</a>	University of Cyprus Cyprus <a href="#">Visit Website</a>	University of Novi Sad Faculty of Sciences Serbia <a href="#">Visit Website</a>	University of Piraeus Research Center Greece <a href="#">Visit Website</a>
 PDMFC	 Security Labs Consulting Ltd	 SGI	 Zelus		
PDMFC Portugal <a href="#">Visit Website</a>	Security Labs Consulting Ltd Ireland (Republic) <a href="#">Visit Website</a>	Serious Games Interactive Denmark <a href="#">Visit Website</a>	ZELUS P.C. Greece <a href="#">Visit Website</a>		

# Thank you

If you have any questions, please do not hesitate to contact:

- Ruben Rios  
Associate Professor  
University of Malaga  
[ruben.rdp@uma.es](mailto:ruben.rdp@uma.es)