Digitalization with Reliablity-Availability-Security

Agenda

- Brief Introduction – Phoenix Contact
- Digitalization in Power Industry
- Digitalization with Reliability, Availability and Security
- Cyber Security Trends in Power Sector

years of passion
for technology
and innovation

€ **3.6** Billion sales

10

Production sites

Germany | China | Taiwan | India | Poland | Sweden | Switzerland | Russia | Turkey Greece | USA

100.000

Products

22.000

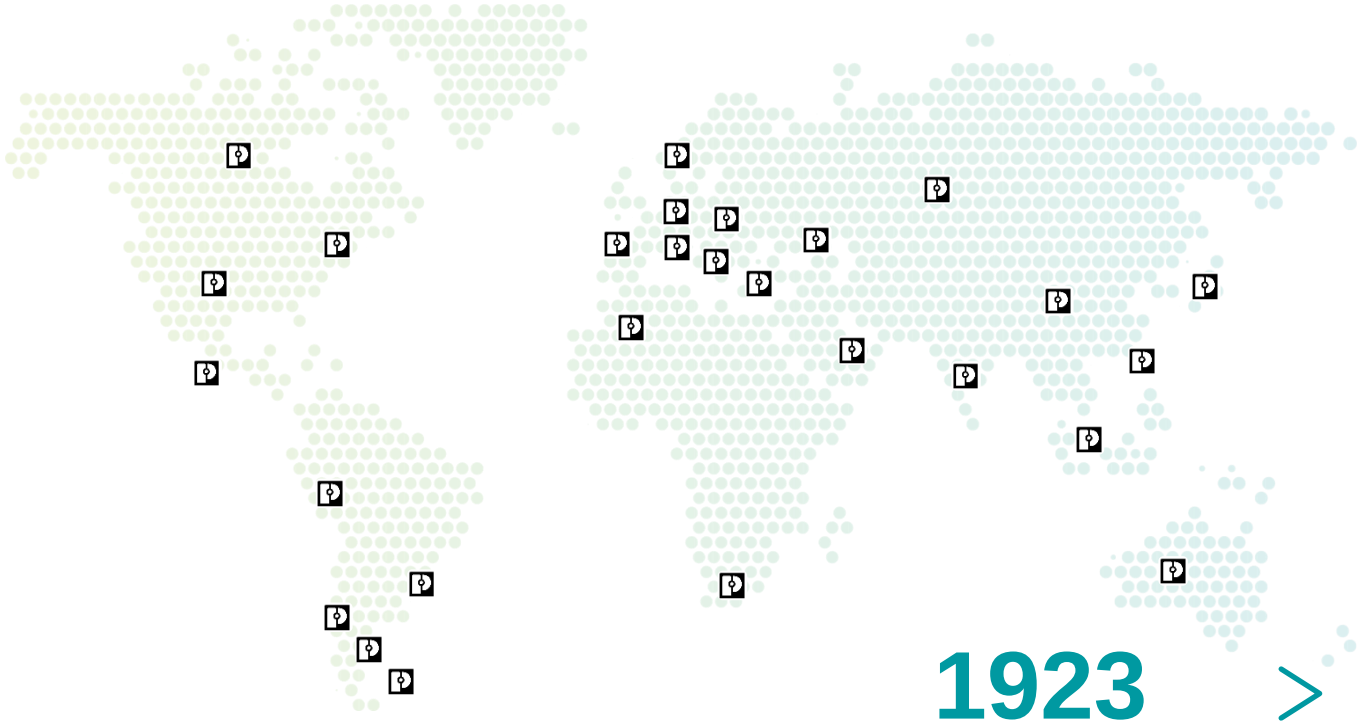
Employees worldwide

75%

Sales abroad

25%

Sales in Germany



9.100

Employees in Germany

1923

Founded in Germany

TODAY

Present in more than 100 countries

Group Executive Board:

Frank Stührenberg (CEO)
Axel Wachholz (CFO)
Frank Possel-Dölken (CDO)
Dirk Görlitzer (COO, President BA ICE)
Torsten Janwlecke (COO, President BA DC)
Ulrich Leidecker (COO, President BA IMA)

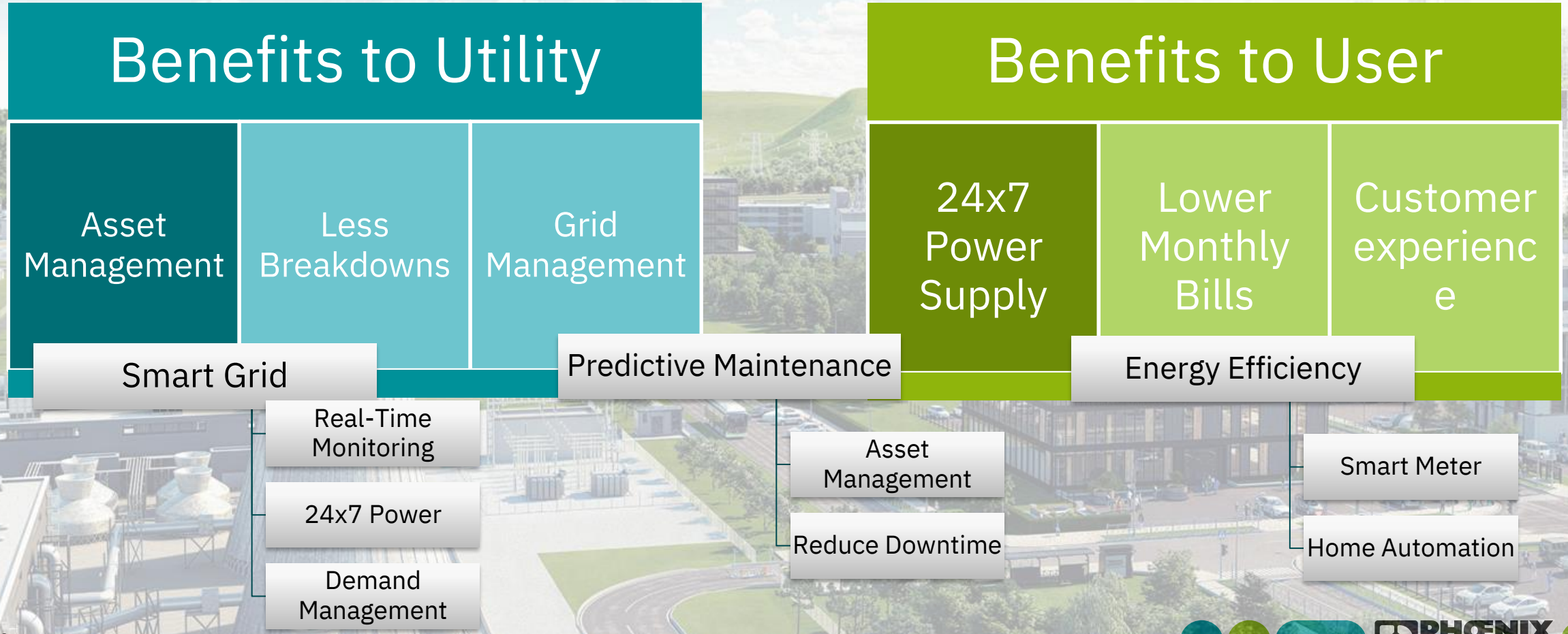
Agenda

- Brief Introduction – Phoenix Contact
- Digitalization in Power Industry
- Digitalization with Reliability, Availability and Security
- Cyber Security Trends in Power Sector

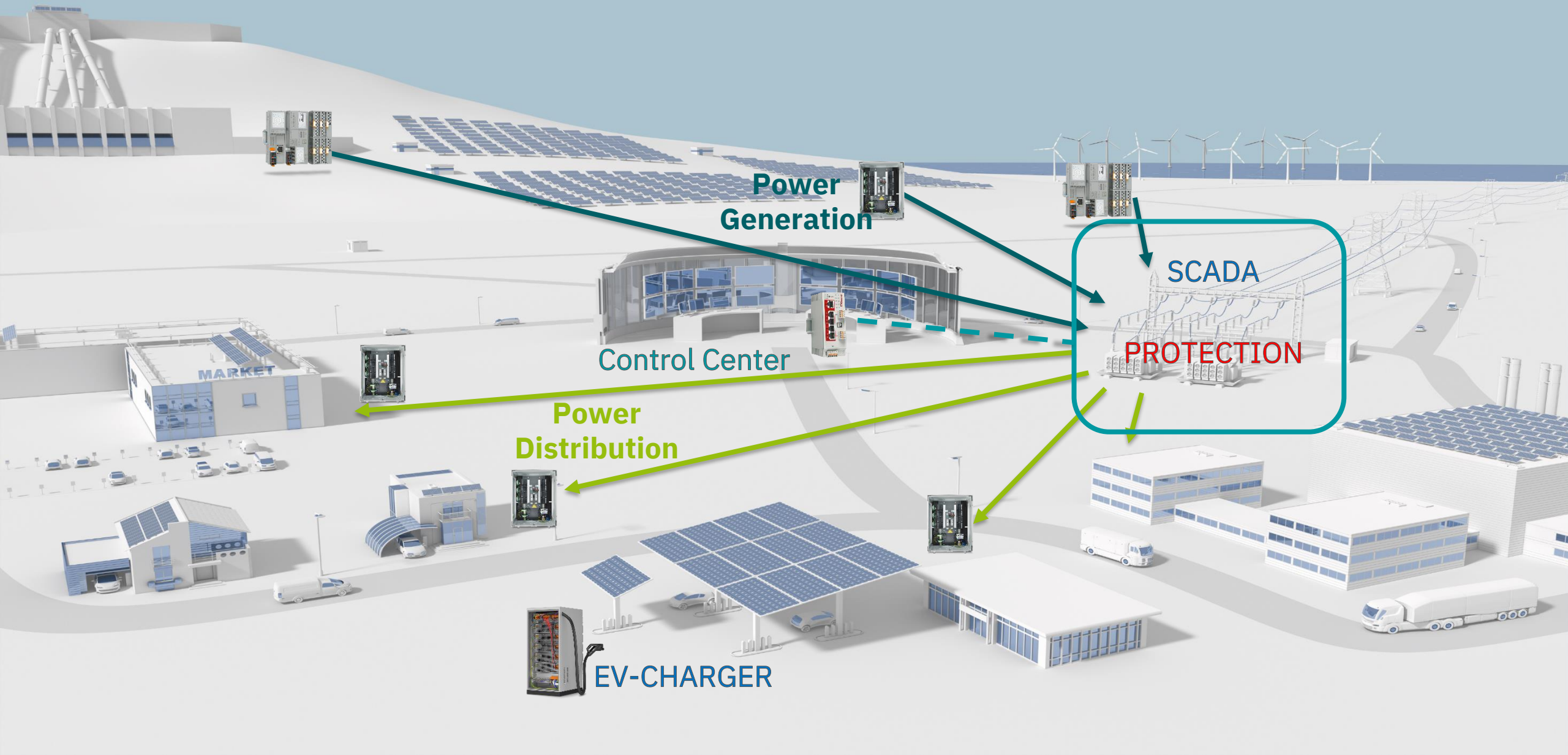
Digitalization in the energy sector is not just a trend but a critical enabler of Reliable, available, and secured energy systems

Digitalization in Power Sector

Digitalization in the energy sector is not just a trend but a critical enabler of Reliable, available, and secured energy systems



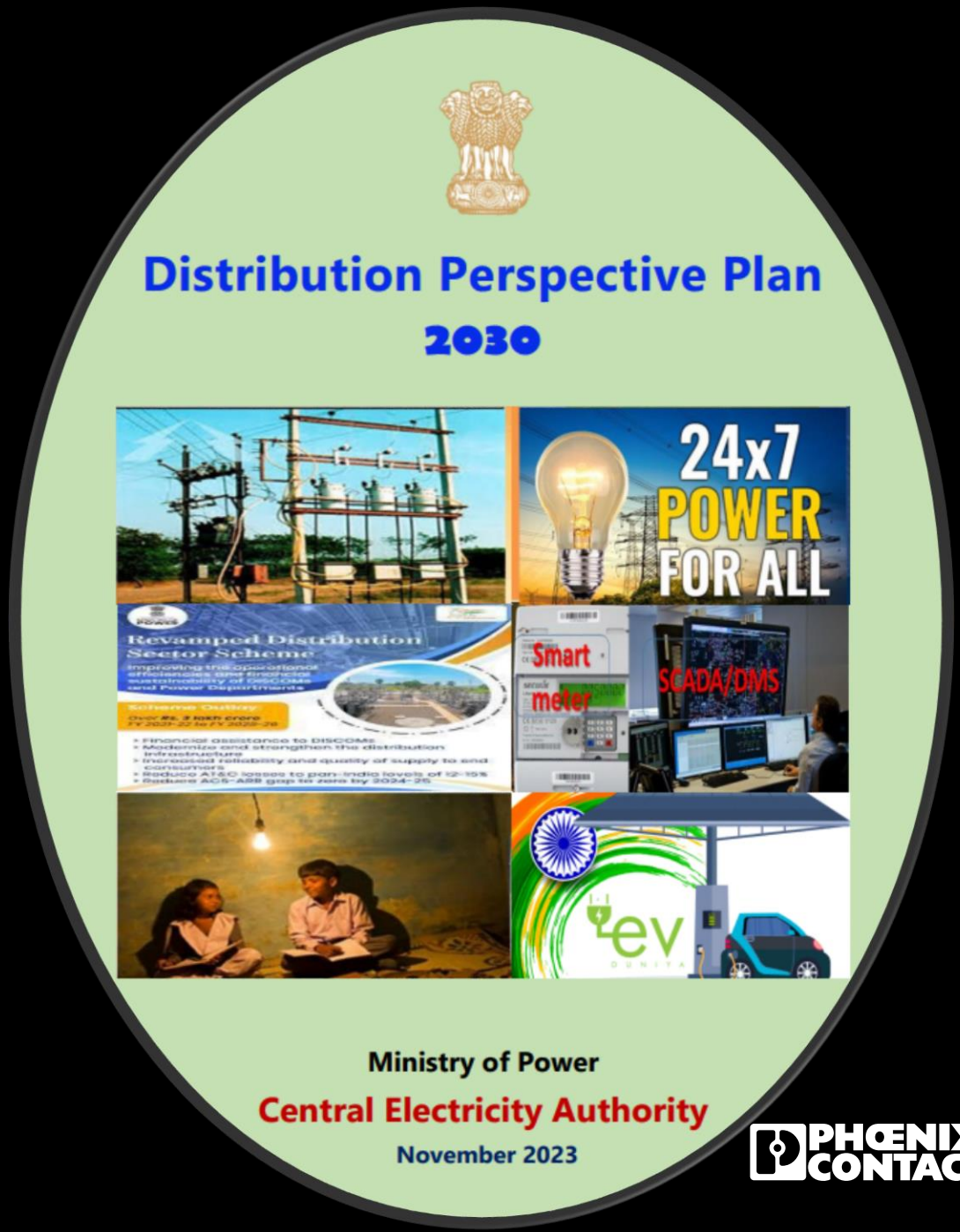
DIGITALIZATION FOR ALL



Agenda

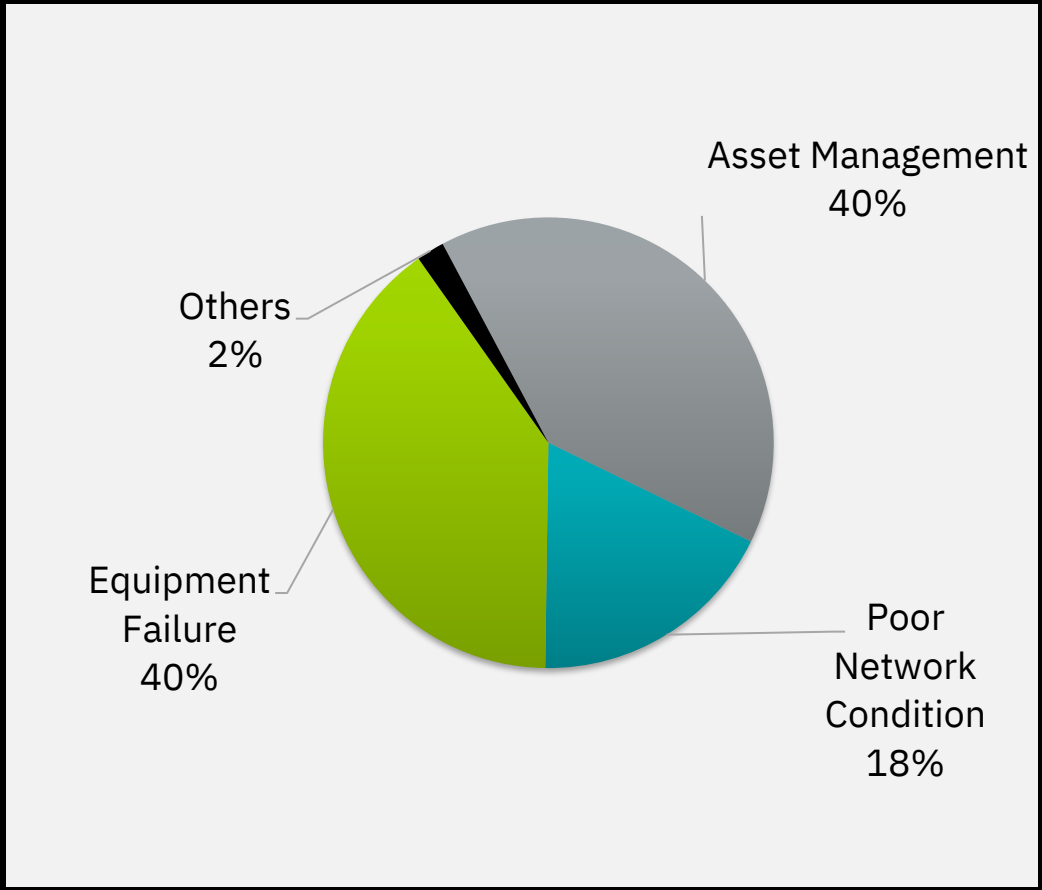
- Brief Introduction – Phoenix Contact
- Digitalization in Power Industry
- Digitalization with Reliability, Availability and Security
- Cyber Security Trends in Power Sector

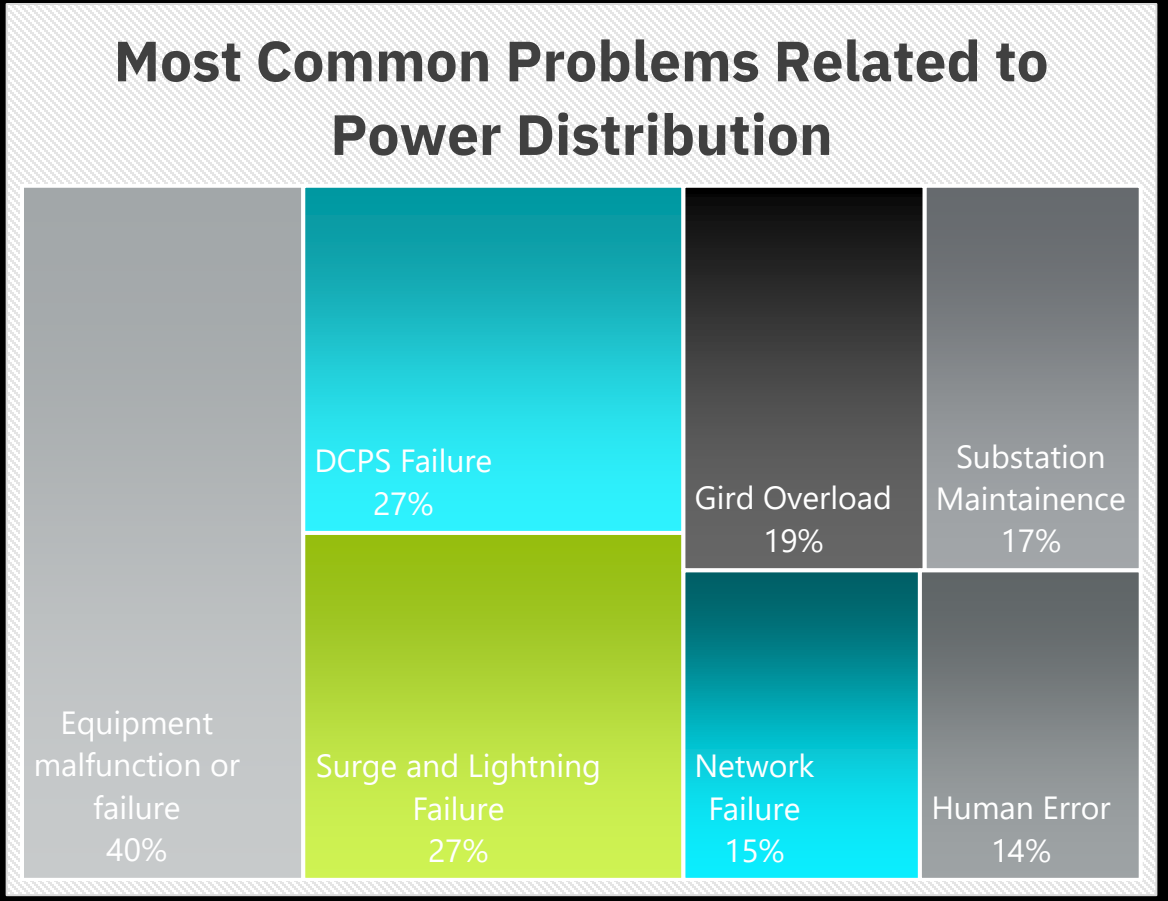
CEA, in 2023 prepared Distribution Perspective Plan for 2030, focusing on Best Practice to be followed by Discoms



Source: CEA

Common Problems with Power Distribution Sectors





With increasing electrification, networking and digitization of sectors, the dependence on reliability, availability and security of solutions is growing.

Everything for highest system availability

Key Requirement for System Reliability, Availability and Security

Protect
- ✓ Surges
- ✓ Short circuit
- ✓ Overcurrent

Supply
- ✓ 24 V
- ✓ High Power
- ✓ Decentral

Measure
- ✓ Energy consumption
- ✓ Switch-on and load management
- ✓ Key figures EnPI

Data
- ✓ Scalable
- ✓ Interoperable
- ✓ Futuristic

PHOENIX CONTACT

Power Outages & Uptime Challenges

Reduction of Downtime – Technical measures

RELIABILITY MEASURES

- Scalability
- Futuristic Approach
- Predictive Maintainence

AVAILABILITY MEASURES

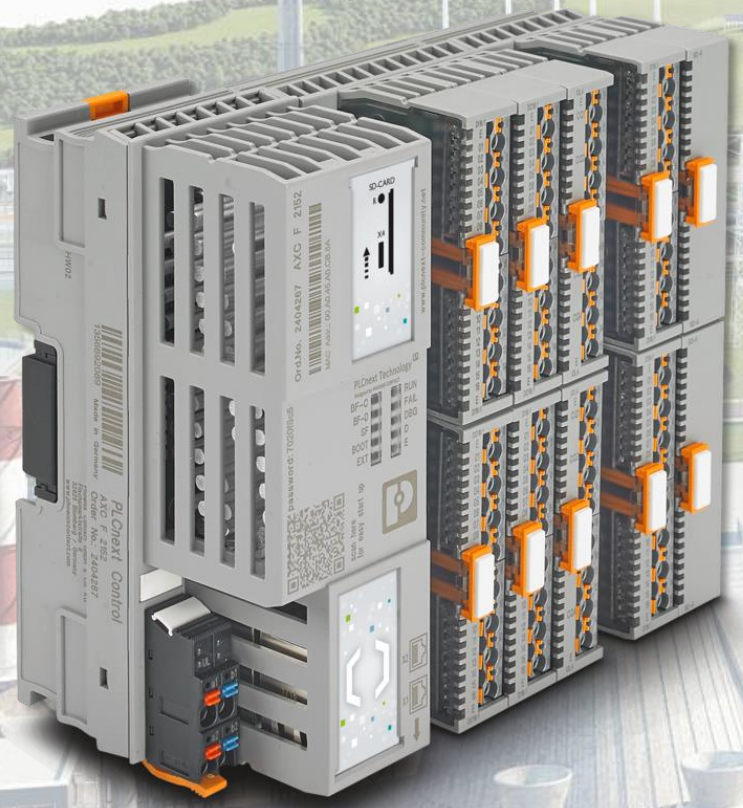
- Redundancy
- Lightning Protection
- Modularity

SECURITY MEASURES

- Redundancy
- Lightning Protection
- Modularity

Digitalization: **Reliability**, Availability and Security

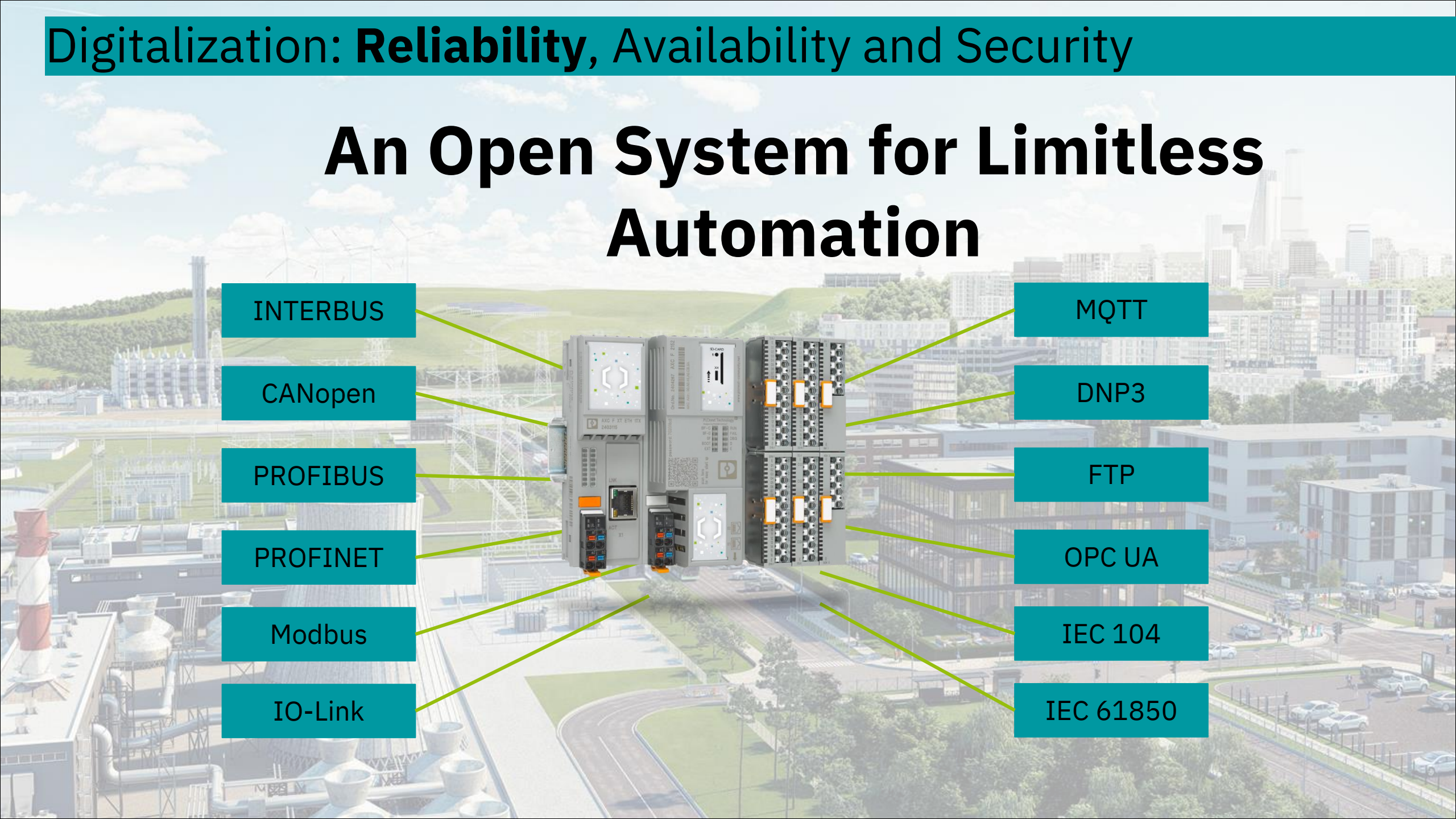
An Open System for Limitless Automation



- **The Openness of PLCnext Technology, IEC 61131 or high-level language**
- **OPC UA, Profinet, Modbus, Profibus, DNP, IEC 60870-5-104 etc.**
- **Support Cloud/IT Functions like MQTT, SQL, SNMP, Rest API for Digitalization**
- **Scalable and Future oriented, add upto 63 IOs**

Digitalization: **Reliability**, Availability and Security

An Open System for Limitless Automation



Digitalization: **Reliability**, Availability and Security

Futuristic Approach

- **Interoperable**
  - IEC 60870-5-104/101, DNP3.0, IEC 61850, Modbus supported

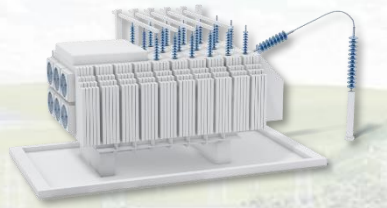
- **Futuristic Approach**
  - Upto 63 IOs can attached
  - Powerful processor

- **Secured Unit**
  - With in-built firewall
  - With TPM chip
  - With RBAC features

- **Modular Connection**
  - Reliable interconnection technology
  - Tool free connection

Digitalization: **Reliability**, Availability and Security

Predictive Maintenance



- Asset Health Tracking
- Timely Maintenance
- Demand Management
- Lower Outages

Power Outages & Uptime Challenges

Reduction of Downtime – Technical measures

RELIABILITY MEASURES

- Scalability
- Futuristic Approach
- Predictive Maintainence

AVAILABILITY MEASURES

- Redundancy
- Lightning Protection
- Modularity

SECURITY MEASURES

- Trends
- Standard

Digitalization: Reliability, **Availability** and Security

Power Redundancy

Power Supplies

Surge Protection

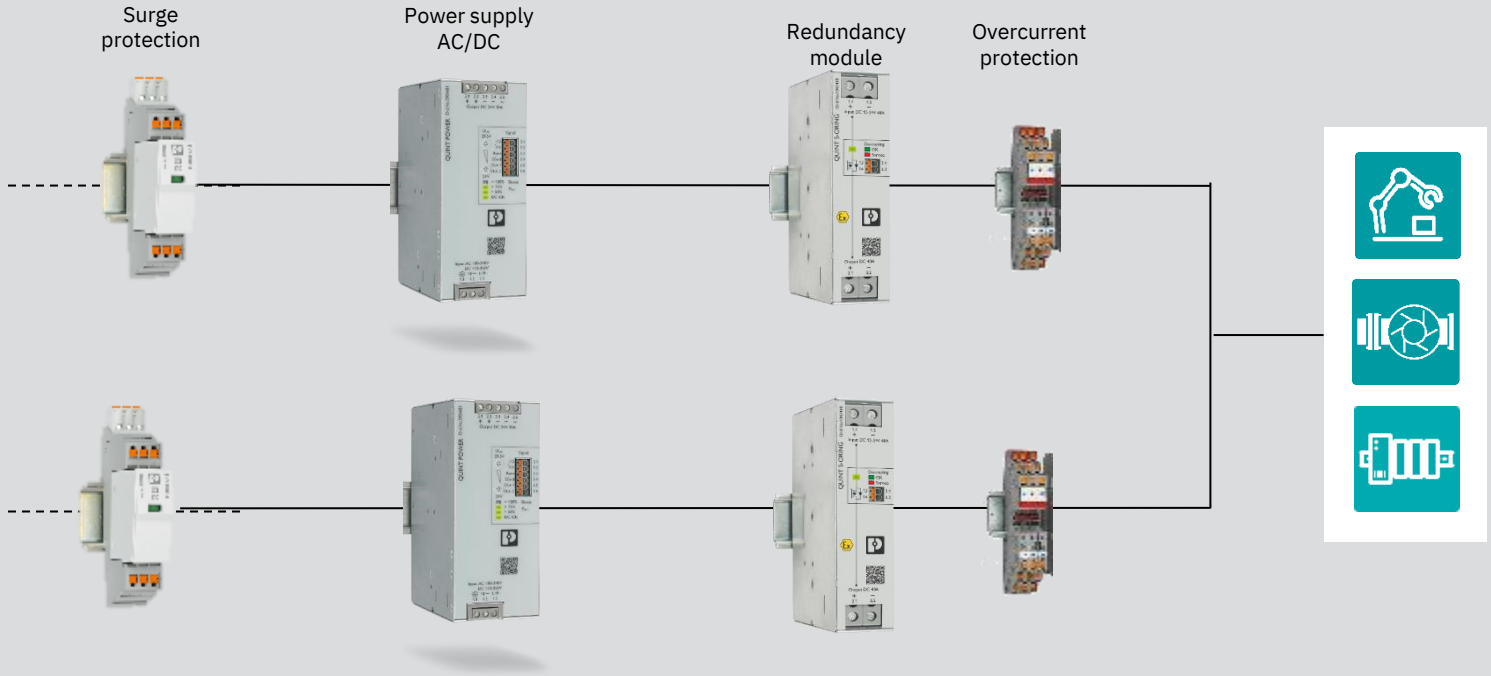
Modularity

Digitalization: Reliability, **Availability** and Security

Power Redundancy

Digitalization: Reliability, **Availability** and Security

Power Redundancy

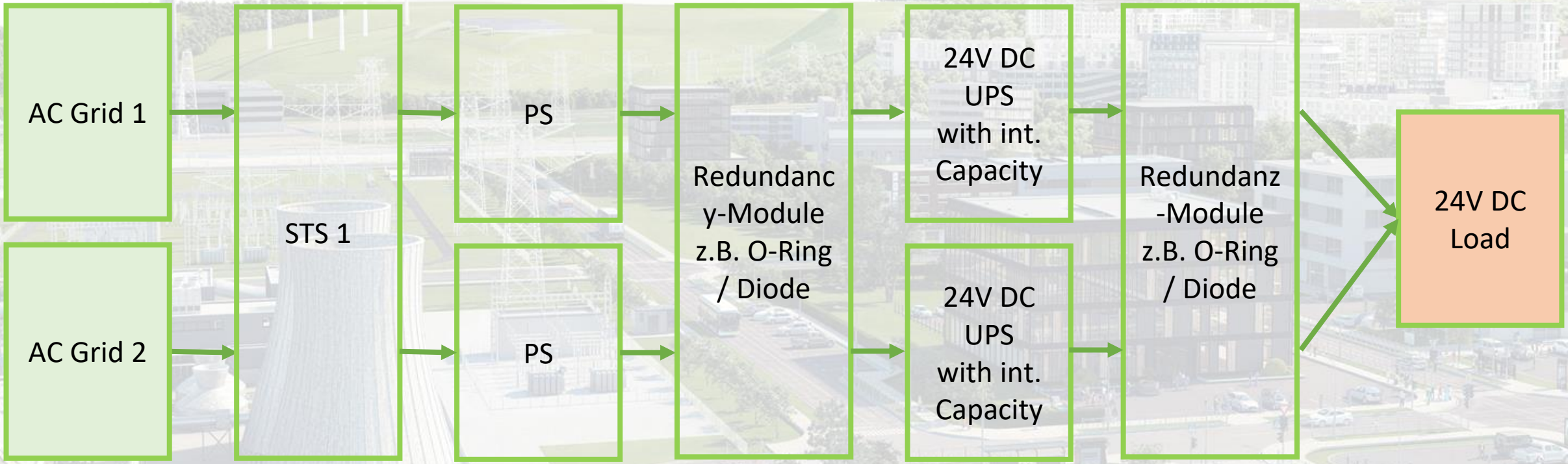


- QUINT POWER power supply
- QUINT S-ORING redundancy module
- Surge protection PLUGTRAB-SEC
- Electronic circuit breaker PTCB

Digitalization: Reliability, **Availability** and Security

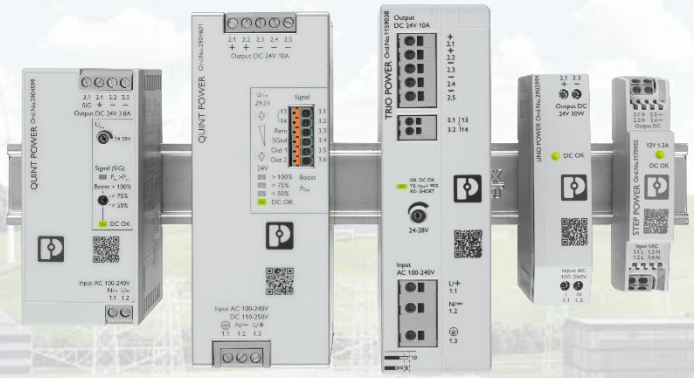
Power Redundancy

Tier III – redundancy



Digitalization: Reliability, **Availability** and Security

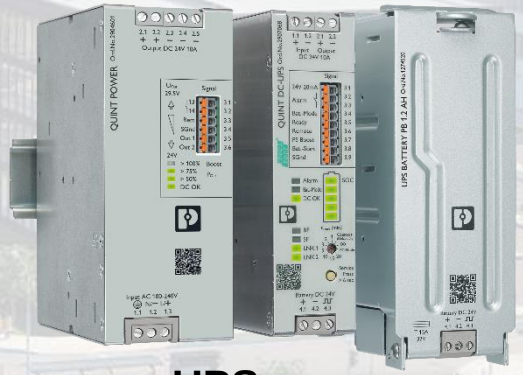
Power Redundancy



AC/DC Converters

DC/DC Converter

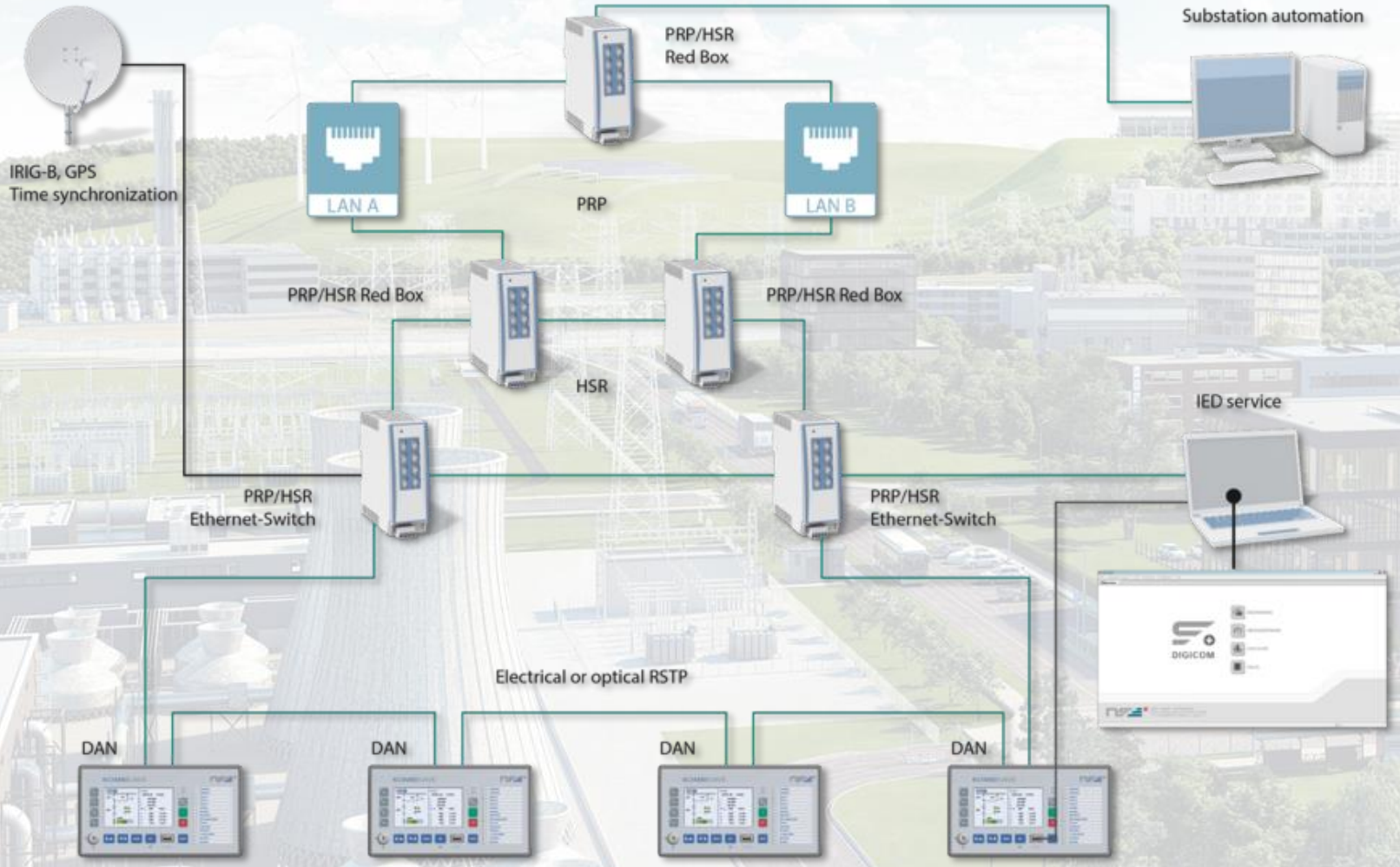
Redundancy Module



UPS

Digitalization: Reliability, **Availability** and Security

Network Redundancy



Industrial Ethernet Switch

- Managed and Unmanaged Switch
- IEC 61850 Complaint Switches
- HSR/PRP switches for Industrial Redundancy

Lightning Resilience

- Avoiding unplanned system failures and downtime
- Protection against risks include lightning and surge hazards that cause fires, outages and data loss

Solution:

- Supply concepts consisting of power supply in UPS systems, device protection and surge protection.
- Holistic and suitable protection zone concept and consideration of protective measures according to IEC

Digitalization: Reliability, **Availability** and Security

Lightning Protection

Surge protection for power supply
From the feed-in to the end device, our protective devices for power supply of type 1, type 2 and type 3 protect you against defects from lightning currents and overvoltage.

Type 1/2

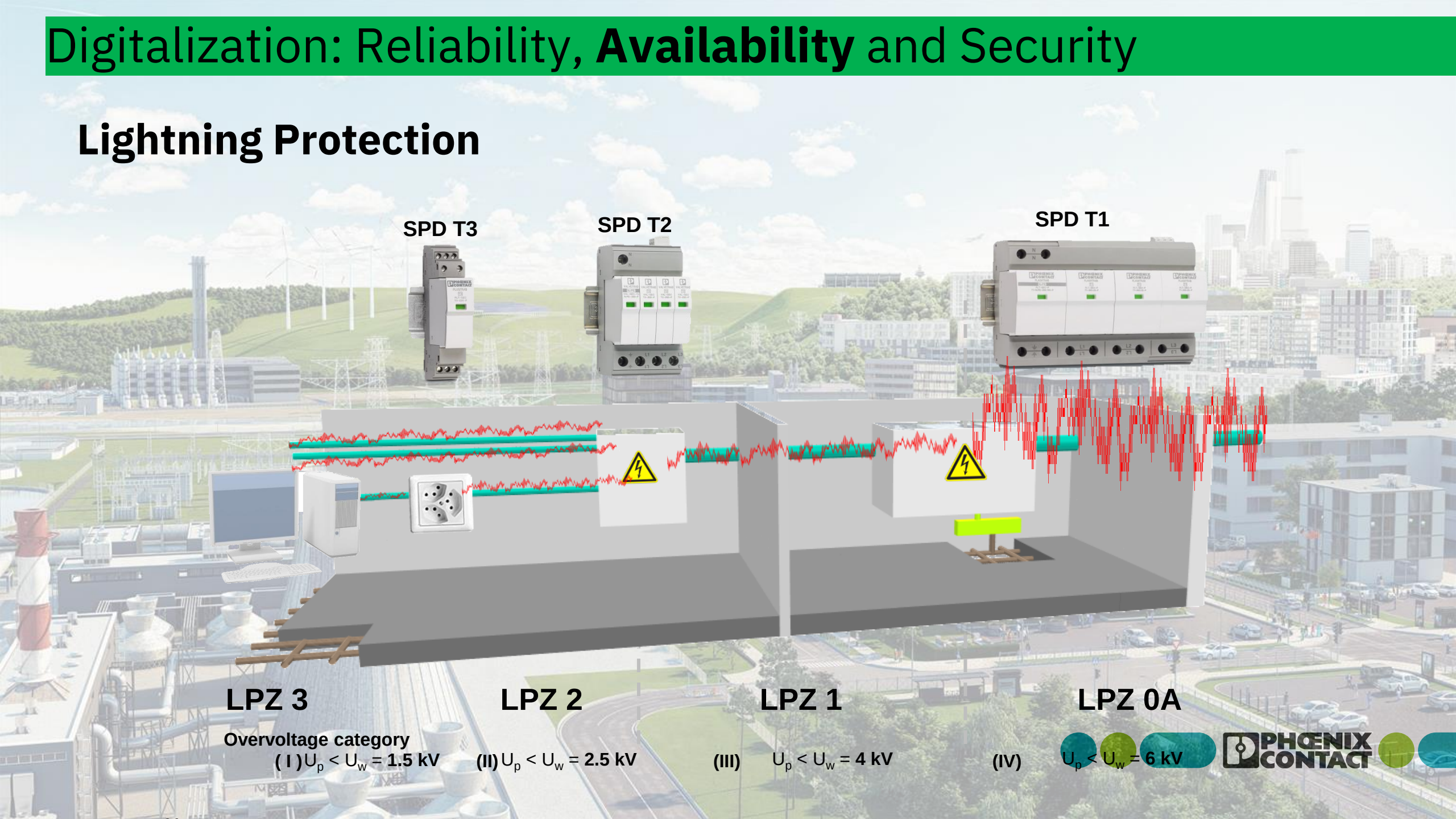
Type 1+2

Type 2

Type 3

Digitalization: Reliability, **Availability** and Security

Lightning Protection



Digitalization: Reliability, **Availability** and Security

Holistic solutions with Modular Solutions

Smart Services

Protect | Power | Measure | Data

PHOENIX CONTACT

Power Outages & Uptime Challenges

Reduction of Downtime – Technical measures

RELIABILITY MEASURES

- Scalability
- Futuristic Approach
- Predictive Maintainence

AVAILABILITY MEASURES

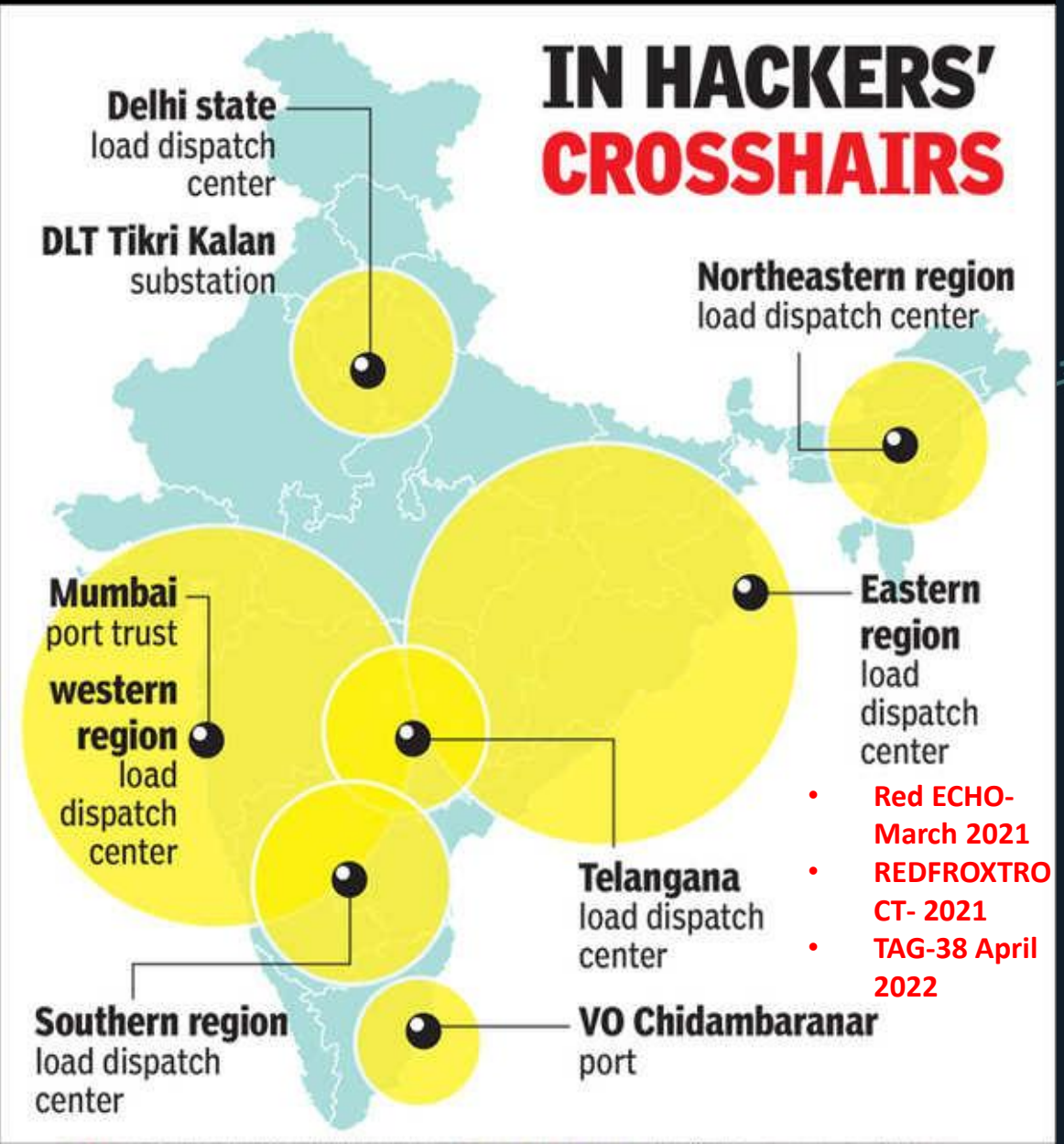
- Redundancy
- Lightning Protection
- Modularity

SECURITY MEASURES

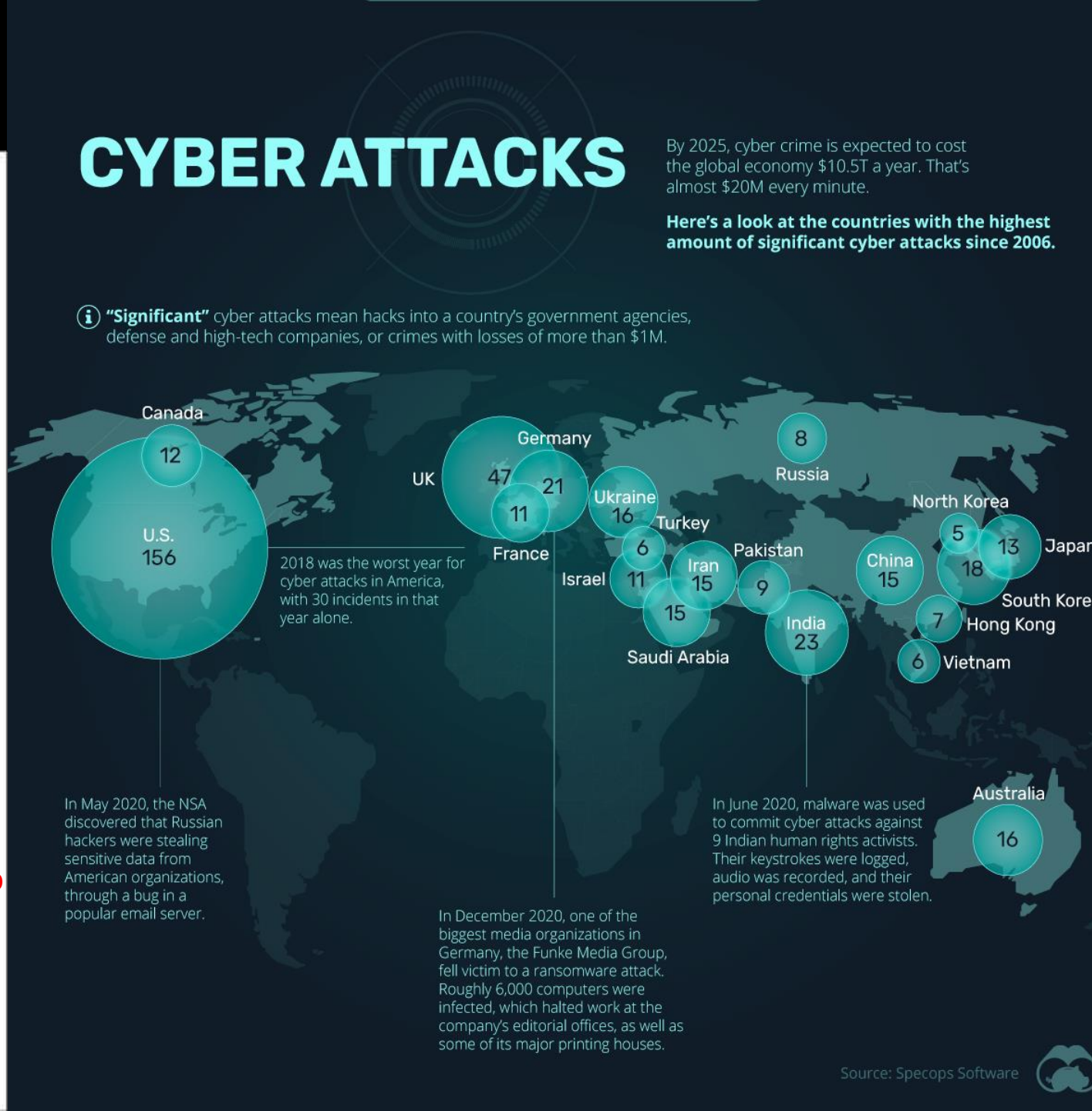
- Trends
- Standard

CYBER SECURITY

Cyber Attacks across Globe



- Red ECHO- March 2021
- REDFROXTROCT- 2021
- TAG-38 April 2022



Cyber Attacks across Globe

Cyber crime cases go from 25 to 155 in two months

Action follows suspension of a woman PI from Kasturba Marg police station for not registering one

FAIZAN KHAN
faizan.khan@mid-day.com

At Andheri police station alone, around 41 FIRs were registered against cyber crimes. PIC/ISTOCK

THE suspension of a police inspector for not registering a cyber crime spurred police across the city to register around 155 of the cases in past two months. Before the departmental action, the Mumbai police had registered only 25 cases. The statistics about online FIR details in past two months (May 1 to June 30) that were accessed by mid-day from Maharashtra police's online FIR facility, also suggest that few police stations have been updating the records in Mumbai. The figures will go up if every police station updates the system on a daily basis.

During the first week of March this year a woman approached Kasturba Marg police to register an FIR regarding a debit card related fraud. When there was no response, the complainant reached out to the Joint Commissioner (law and order), who suspended PSI Varsha Gavit who was the duty officer. She had allegedly kept the complaint letter with her for two months instead of forwarding it to the concerned officer.

"Cyber fraud needs to be addressed with extreme seriousness and should always be taken as a challenge. Most police stations don't register FIRs in cyber crimes as it requires expertise and skill to crack the cases, which sometimes takes a lot of effort and time. In Mumbai the police are burdened with festivals, patrolling, action against traffic violators etc. But cyber crimes need to be addressed separately, because in future they are going to escalate and emerge as a big challenge," a senior IPS officer told mid-day.

After the PSI's suspension, at Andheri police station alone, around 41 FIRs were registered in past two months.

Vinay Choubey, Jt Commissioner (law and order) said they are registering cyber crimes on priority. "We have been getting several complaints from citizens regarding cyber fraud. Complaints are also made to us on Twitter. We have also been doing several initiatives for awareness so that people understand they should not share sensitive information."

"It's good to know that more and more FIRs are being registered, because earlier it would take months to get an FIR registered. This way cops can make the public aware of trending cyber crimes. Cyber criminals are adopting new methods of committing fraud and citizens should know them so that they are well equipped to protect themselves. Many people are not yet aware of the modus operandi behind frauds on matrimonial sites, digital wallets, etc. It's extremely important that cyber cops not only register the FIRs but also inform the public about cyber crimes," said Ritesh Bhatia, a cyber crime investigator.

India's No 2 victim of cyber crime

Report says impact of attacks is immense, with many feeling cheated

Divyesh Singh

With increasing use of computers and the Internet through broadband penetration, the risk of being a victim of cyber crime has increased. Indian net users have been one of the most favourite targets of cyber criminals. In fact, a recent research report by global e-security solutions provider Norton has shown that 56% Indian web users have been victims of cyber crime.

The report pointed out that India is the second most victimised nation after China in terms of cyber attacks or cyber crime. It includes virus attacks, botnet attacks, online credit card frauds, lottery frauds, identity thefts, hacking attacks and attacks through social networking sites on personal profiles, which could include sexual harassment online and cyber-bullying.

Around 65% Internet users worldwide have been victims of cyber crime, but in India it is greater.

The report revealed that the impact of such attacks has been immense on victims who feel ripped off or cheated. High emotional impact has affected their personal and professional lives.

Around 38% victims feel angry, while 31% have been left feeling annoyed and cheated and 46% among them are upset. Eighty-eight percent victims feel they are themselves to blame for the attack.

Only 8% Indian users think it will not happen to them and that they cannot be victims of cyber crime.

Most Indians believe cyber criminals cannot be brought to justice as police and other agencies cannot go beyond borders to take action against those who easily swindle money out of people's accounts.

The next time you surf the net, consider this. You may be a click away from becoming the next cyber crime victim.

The study by Norton revealed the staggering prevalence of cyber crime. Two-thirds (65%) Internet users globally, and over three-quarters (76%) Indian web surfers have fallen victim to cyber crimes, including computer viruses, online credit card fraud and identity theft.

Despite being left with a feeling of helplessness, only 80% Indian adults think that they will charge their behaviour and take action legally when targeted.

Surprisingly, only 37% victims of cyber crime have reported it to the police.

"We all pay for cyber crime, either directly or through pass-along costs from financial institutions," said Adam Palmer, Norton lead cyber security advisor.

Delhi registered 1850% rise in cyber crime cases

Jatin Anand
jatin.anand@hindustantimes.com

VIRTUAL ASSAULT

NEW DELHI: Statistics prove that the Capital is on the receiving end of a bitter onslaught in cyber space as the Delhi Police, in particular, and the security establishment, in general, struggle to confront the challenge.

While the police face a debilitating manpower crunch in its cyber cells, other security agencies still prefer to view cyber attacks from an obsolete perspective.

"In a day and age where American government-sponsored hackers are targeting Iran's nuclear programme and terror outfits such as the Indian Mujahideen (IM) are conducting recruitment drives over the internet, our security agencies still take weeks to trace creators of fake profiles on Facebook," said a Delhi-based hacker, who wished to remain anonymous.

"Just two weeks ago, the official webpage of Delhi University's (DU) English department was hacked by a Pakistan-based group. If you look at official estimates, hacking in India is now done like never before," said another hacker, who is pursuing his engineering from a private college.

The hacker's claim, when viewed with arrested Lashkar-e-Toiba (LeT) commander Syed Zabiuddin Ansari's admission that he was operating nine email accounts post 26/11 attacks, may not be entirely off the mark.

According to figures compiled by the National Crime Records Bureau (NCRB), cases of hacking registered an increase of 1850% — from just two cases in the year 2010 to 39 in 2011.

June 22: DU's English department's website was hacked by a Pakistan-based hacker, 'Anon CIOJP' as revenge for India's 'transgressions into Pakistan's cyberspace'

May 12: Shubham Kansal, 22, was arrested for uploading his former classmates' phone number on a fictitious Facebook page replete with provocative pictures

March 5: Two foreign nationals were arrested for hacking into the bank account of a company and subsequently siphoning off ₹16 lakh

The sheer volume of such cases, registered under Section 66(2) of the Information Technology (IT) Act, seems to make Delhi the most vulnerable Indian city when it comes to cyber attacks. Not even a single case of hacking was registered in other metropolitan cities such as Mumbai and Kolkata or even Chennai and Hyderabad in 2011.

"It's about time that the word 'hacking' stopped being a negative term for our security establishment," said Jiten Jain, a cyber security analyst, who wants to bring hackers and security agency officials together at The Hackers' Conference later this month.

"There is a tremendous pool of talent, in the form of young hobbyist hackers. Cyber security can't be left to salaried government officials working nine-to-five shifts," Jain said.

दलाल इंजीनियरिंग कॉलेज संचालकों को बेच रहे हैं ब्योरा, सीबीएसई ने जांच कराने का लिया फैसला

जेईई मेन का गोपनीय डाटा लीक

हिन्दुस्तान एक्सक्लूसिव

नोएडा | प्रभात उपाध्याय

13 लाख छात्रों का डाटा कंसल्टेंसी फर्म और दलालों के पास

03 साल की सजा हो सकती है डाटा लीक करने पर

छात्रों का ब्योरा पूरी तरह गोपनीय होता है। यदि कोई पैसा लेकर इसे बेच रहा है तो यह अपराध है। डाटा बाहर कैसे पहुंचा, इसकी जांच की जाएगी। -राजबीर सिंह, कार्यकारी निदेशक, जेईई मेन (जैब)

जेईई मेन (ज्वाइंट इंट्रेंस एग्जामिनेशन) के परीक्षार्थियों का गोपनीय डाटा लीक हो गया है। कंसल्टेंसी फर्म चलाने वाले इसे प्राइवेट इंजीनियरिंग कॉलेजों को पैसे लेकर बेच रहे हैं। 'हिन्दुस्तान' द्वारा मामला उजागर करने के बाद सीबीएसई ने मामले की जांच कराने का फैसला किया है।

आईआईटी, एनआईटी और देश के प्रमुख इंजीनियरिंग कॉलेजों में दाखिले के लिए जेईई-मेन 2015 की परीक्षा में शामिल 13 लाख छात्रों का डाटा कंसलटेंसी फर्म और दलालों के पास है। इस डाटा में छात्र का नाम, माता-पिता का नाम, पंजीकरण नंबर, जन्म-तिथि, मोबाइल नंबर, ई-मेल आईडी, राज्य का नाम और पिन कोड मौजूद है। दलाल प्राइवेट इंजीनियरिंग कॉलेज संचालकों को ई-मेल और फोन पर पैसे लेकर छात्रों का ब्योरा देने को कह रहे हैं। एक छात्र के ब्योरे के लिए 5 रुपये मांगा जा रहा है। यदि कोई सारे छात्रों का डाटा लेना चाहता है तो उसे 65,000 रुपये देने होंगे। वहीं दिल्ली-एनसीआर के छात्रों के डाटा के लिए 7 हजार रुपये की मांग की जा रही है।

5 लाख रुपये जुर्माना भी हो सकता है: आईटी एक्ट की धारा 43-बी के अनुसार यदि कोई भी गोपनीय डाटा को बेचता या खरीदता है तो उसे 3 साल की कैद और 5 लाख तक का जुर्माना हो सकता है। इसके अलावा, जिसके पास डाटा को संरक्षित और रखरखाव करने की जिम्मेदारी है उसे आईटी एक्ट की धारा 67-सी के तहत तीन साल की सजा हो सकती है।

साइबर विशेषज्ञ व कम्प्यूटर सोसायटी ऑफ इंडिया के नोएडा चैप्टर के चेयरमैन अनुज अग्रवाल कहते हैं कि लीक डाटा में छात्र का मोबाइल नंबर भी है। ऐसे में यह छात्र की निजता से भी जुड़ा है। आईटी एक्ट के तहत निजता के ब्योरे को सार्वजनिक करने पर 3 साल की सजा और 2 लाख के जुर्माने का प्रावधान है।

डाटा लीक होने से क्या होगा नुकसान

जेईई मेन में शामिल अभ्यर्थियों का ब्योरा प्राइवेट इंजीनियरिंग कॉलेजों के हाथ लगने पर वे इसका फायदा उठा सकते हैं। उत्तर प्रदेश समेत कई राज्यों के प्राइवेट इंजीनियरिंग कॉलेजों में जेईई मेन के स्कोर के आधार पर दाखिले के लिए सीटें आरक्षित हैं। दाखिला प्रक्रिया काउंसलिंग के बाद ही शुरू होती है। पर डाटा हाथ लगने के बाद कॉलेज पहले से ही छात्रों को संपर्क कर अपने संस्थान में दाखिले का प्रलोभन देना शुरू कर देते हैं।

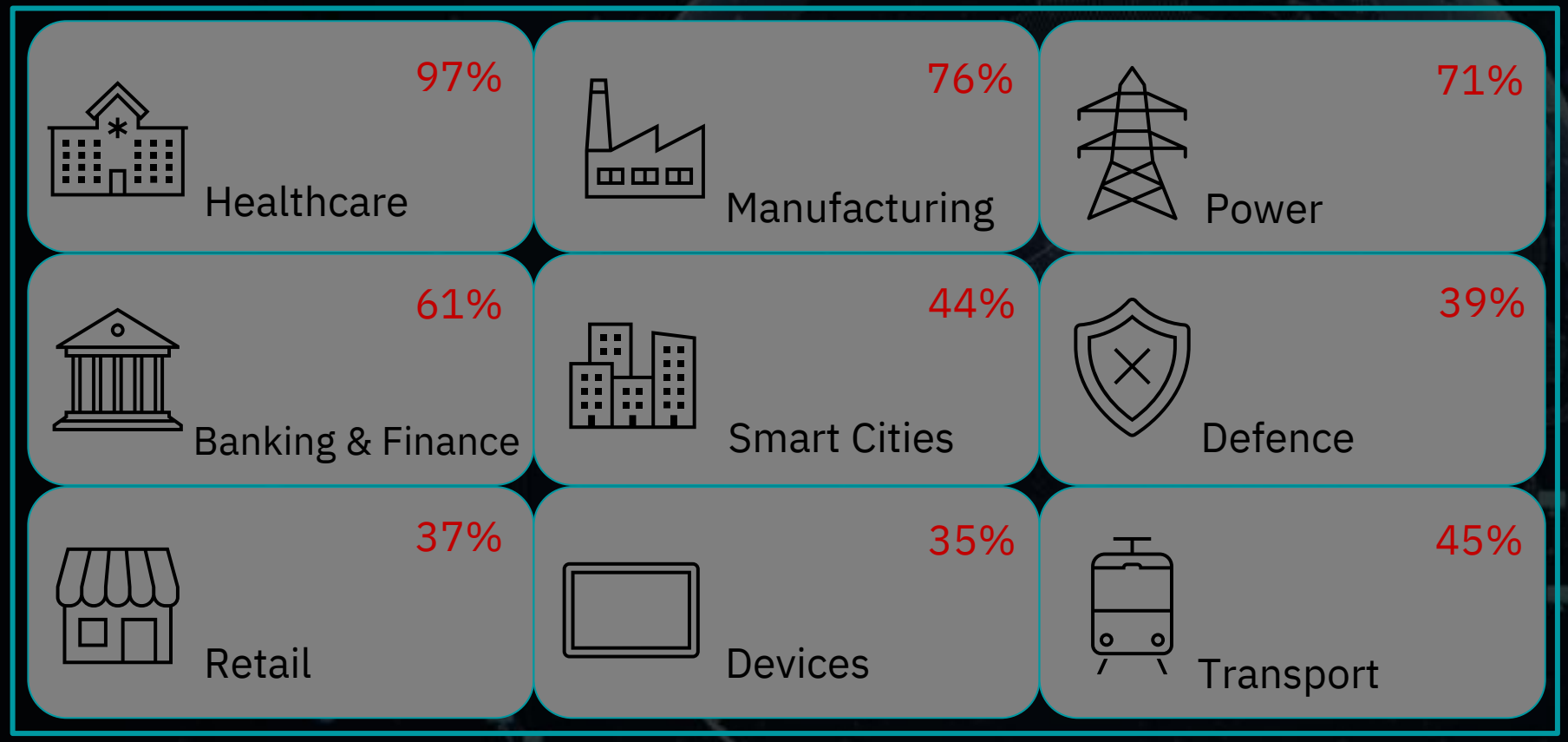
न्यूनतम तीन साल तक डाटा गोपनीय रखना होता है

छात्रों से संबंधित डाटा को न्यूनतम तीन साल तक गोपनीय रखना होता है। कई मामलों में यह अवधि न्यूनतम 8 साल भी है। ऐसे में परीक्षा के दो महीने के अंदर ही छात्रों का ब्योरा लीक होने पर विशेषज्ञों ने सवाल उठाया है।

यूपीएसईई का डाटा भी हो चुका है लीक

उत्तर प्रदेश के इंजीनियरिंग और प्रबंधन कॉलेजों में दाखिले के लिए आयोजित राज्य प्रवेश परीक्षा (यूपीएसईई) का डाटा भी लीक हो चुका है। छात्रों का ब्योरा कॉलेज के पास पहुंचने के बाद उन्होंने छात्रों को प्रलोभन देना भी शुरू कर दिया है। यूपीटीयू इस मामले की जांच करवा रहा है।

Risk of Cyber Security across All Sectors

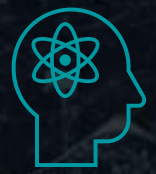


Rising attacks on OT installations across key sectors

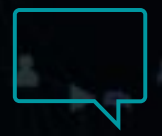
- Healthcare with 97% risk
- Manufacturing with 76% risk
- Critical Infra with 71% risk includes Water Industry, Energy Industry, Process Industry

Possible consequences of a security incident

Data loss



Loss of know-how



Reputation damage

System downtime

Extortion with ransomware

Personnel costs

PHOENIX CONTACT

Cyber Security Trends in Power Sector

Cyber Security Regulations 2024

GOVERNMENT OF INDIA
CENTRAL ELECTRICITY AUTHORITY
(MINISTRY OF POWER)
Sewa Bhawan (North Wing), Room No. 622, 6th Floor,
R. K. Puram, New Delhi-110066
Tel. Fax -011-26103246, email: celegal-cea@gov.in
Website: www.cea.nic.in

PUBLIC NOTICE

In accordance with the Section 177 of the Electricity Act, 2003, the Central Electricity Authority (CEA), proposes to notify the **draft Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024.** The proposed draft regulations are available on the CEA Website www.cea.nic.in for inviting public comments. The Regulations can also be inspected in the office of Chief Engineer (Legal), Sewa Bhawan (North Wing), Room No. 622, 6th Floor, R. K. Puram, New Delhi-110066 on any working day till **10th September, 2024** between 1100 hrs to 1600 hrs.

2. All the Stakeholders including the public are requested to send their comments on the draft regulations to Chief Engineer (Legal), Sewa Bhawan (North Wing), Room No. 622, 6th Floor, R. K. Puram, New Delhi-110066 by post or through e-mail (celegal-cea@gov.in) latest by **10th September, 2024.**

(Rakesh Kumar)
Secretary, CEA

CHAPTER-9: TECHNICAL REQUIREMENTS OF RTU

9.0 General

The Remote Terminal Unit (RTU) shall be installed at primary substation to acquire data from Multifunction Transducers (MFTs), discrete transducers & status input devices such as CMRs etc. RTU & shall also be used for control of Substation devices from Master station(s). The supplied RTUs shall be interfaced with the substation equipment, communication equipment, power supply distribution boards; for which all the interface cables, TBs, wires, lugs, glands etc. shall be supplied, installed & terminated by the Contractor. Further , the equipments indicated in the MoP order no 12/34/2020-T&R dtd 08.06.21 & CEA /PLG/R&D/MII/2021 dtd 11.6.21 and any amendment from time to time shall be adhered to. This chapter is applicableto Group A,B,C & new RTUs of Group U as per functional requirements

9.1 Design Standards

The RTUs shall be designed in accordance with applicable International Electro- technical Commission (IEC), Institute of Electrical and Electronics Engineer (IEEE), American National Standards Institute (ANSI), and National Equipment Manufacturers association (NEMA) standards, unless otherwise specified in this Technical specification. In all cases the provisions of the latest edition or revision of the applicable standards in effect shall apply.

The RTU shall be designed around microprocessor technology. For easy maintenance the architecture shall support pluggable modules on backplane. The field wiring shall be terminated such that these are easily detachable from the I/O module. **The RTU shall comply to IEC62351- 3 for cyber security in communication between RTU and master station and IEC62443-4-2 for cyber security for product** including testing requirement as per MoP order no. 12/34/2020-T&R dtd 08.06.21 & CEA /PLG/R&D/MII/2021 dtd 11.6.21 and any amendment from time to time.

9.2 RTU Functions

All functional capability described herein shall be provided by the Contractor even if a function is not initially implemented.

As a minimum, the RTU shall be capable of performing the following functions:

(a) Acquiring analog values from Multifunction Transducers or alternatively through transducer- less modules and the status inputs of devices from the substation, processing and transmitting to Master stations. Capability to acquireanalog inputs from analog input cards receiving standard signals viz current loops 4-20Ma standard signals such as 0-5vdc etc.for RTD , transducer etc.

(b) Receiving and processing digital commands from the master station(s)

(c) Data transmission rates - 300 to 19200 bps for Serial ports for MODBUS. and 10/100 mbps for TCP/IP Ethernet ports

(d) IEC 60870-5-104 protocol to communicate with the Master station(s) at least 2, IEC 60870-5-101 for slave devices & MODBUS protocol over RS485 interface to communicate with the MFTs. If considered as a part of RTDAS/SCADA solution to use IEC20922 for real time monitoring/control using IEC20922 can be additionally and optionally , used with GPRS also subject to meeting

Cyber Security Trends in Power Sector

NPCL

NOIDA POWER COMPANY LIMITED

Technical Specification of FRTU

1. The FRTU shall comply to IEC62351-3 for cyber security in communication between FRTU & master station & IEC62443-4-2 for cyber security for product testing.
2. FRTU Cyber security shall be in complaint & tested with 3rd party agency such as TUV etc.
3. The FRTU shall compliance the security features as per the NERC / CIP recommendations.
4. The FRTU shall comply with cyber security guidelines as notified from time to time by CERT-in, NCIIPC and Ministry of Power during the warranty period and also support provided after post warranty period including new firmware if required.
5. There shall be provision in FRTU to block, unused physical ports through software and remote accessibility protocols like HTTPS, SSH V2 and Telnet. User shall be able to revive and revoke these feature upon need basis.
6. For above requirement FRTU shall maintain proper audit trail for logging user, services and access activities.
7. Any traffic flowing in the network or access mechanism i.e., using webserver, access through protocols like SSH, Telnet, FTP, RSH, SNTP etc. should be in encrypted form and hence should use secured SSL, HTTPS etc. methods with strong encryption level (AES128) and standards and updated with latest certificates
8. All firmware and patches should be maintained at the latest version during the warranty period and support provided after the expiration of warranty.
9. The support shall also provide to compliance / upgrade the FRTU features in accordance with the guidelines as prescribed by NCIIPC, Cert-D and Ministry of Power on time to time during the warranty period as per below requirements as minimum:

- Access to services restricted to authenticated and authorized users.
- Management of users, roles and associated permissions.
- Capability to integrate with a centralised credentials system like LDAP/AAA (centralised, role-based access control - RBAC).
- RADIUS Authentication for centralize access management.
- SNMPv3 Encryption for secure centralize monitoring.
- Backup and Restore facilities, for managing configuration data.
- Log all security events and send security alarms to central log system if necessary.
- Authentication of messages received over protocols supporting such mechanisms (IEC104).

10. Blocking connection to specific ports & interfaces.
11. Define blacklist IP addresses from which all incoming and outgoing connections will be rejected.
12. Define whitelists IP addresses authorised to connect to the CPU.
13. The supplier has to comply for cybersecurity requirements raised during VA/PT audits conducted by Utility during the warranty period at no extra cost. The supplier has to provide solution for any vulnerability discovered even after expiry of warranty period.

WBSEDCL

dimension. The RTU I/O card shall exchange data from the substation equipments/ IED panel using hardwired equipment TB and using TCP/IP ports in case of Other IED. For extending the IEDs, ethernet switches shall be used and ethernet to RTUs-OFC shall be used. Wherever the equipment's/ IEDs don't have this provision, these shall be hardwired directly to the RTU. If there is requirement of LIU same shall be used.

5.4.Cyber Security :

The offered RTU shall comply to IEC62351-3 for cyber security in communication between RTU and MCC/BCC and IEC62443-4-2 for cyber security for product including testing requirement as per MOP order no 12/34/2020-T&R dt 08/06/2021 & CEA /PLG/R&D/MII/2021 dtd 11/06/2021 and any amendment from time to time

5.5.RTU Functions

All functional capability described herein shall be provided by the bidder even if a function is not initially implemented.

RTUs shall provide a reliable system for acquisition of required information from the RTUs, BCPUs, Numerical relays, Multifunction meters, Condition Monitoring Devices, and other communicable devices as well as hardware signal through I/O cards. All functional capability described herein shall be provided by the bidder even if a function is not initially implemented. As a minimum, the RTU shall be capable of performing the following functions:

As a minimum, the RTU shall be capable of performing the following functions:

1. Acquiring analog values from Multifunction Transducers or alternatively through transducer- less modules and the status inputs of devices from the substation, processing and transmitting to Master stations. Capability to acquire analog inputs from analog input cards receiving standard signals viz current loops 4-20mA 0-10 V RTD, etc. This includes all type of MFTs. weather transducers, DC transducers etc.

BSES

N D

SOUTHERN POWER
DISTRIBUTION COMPANY OF T.S. LTD.
Lighting up your lives

PHOENIX CONTACT

Cyber Security Trends in Power Sector

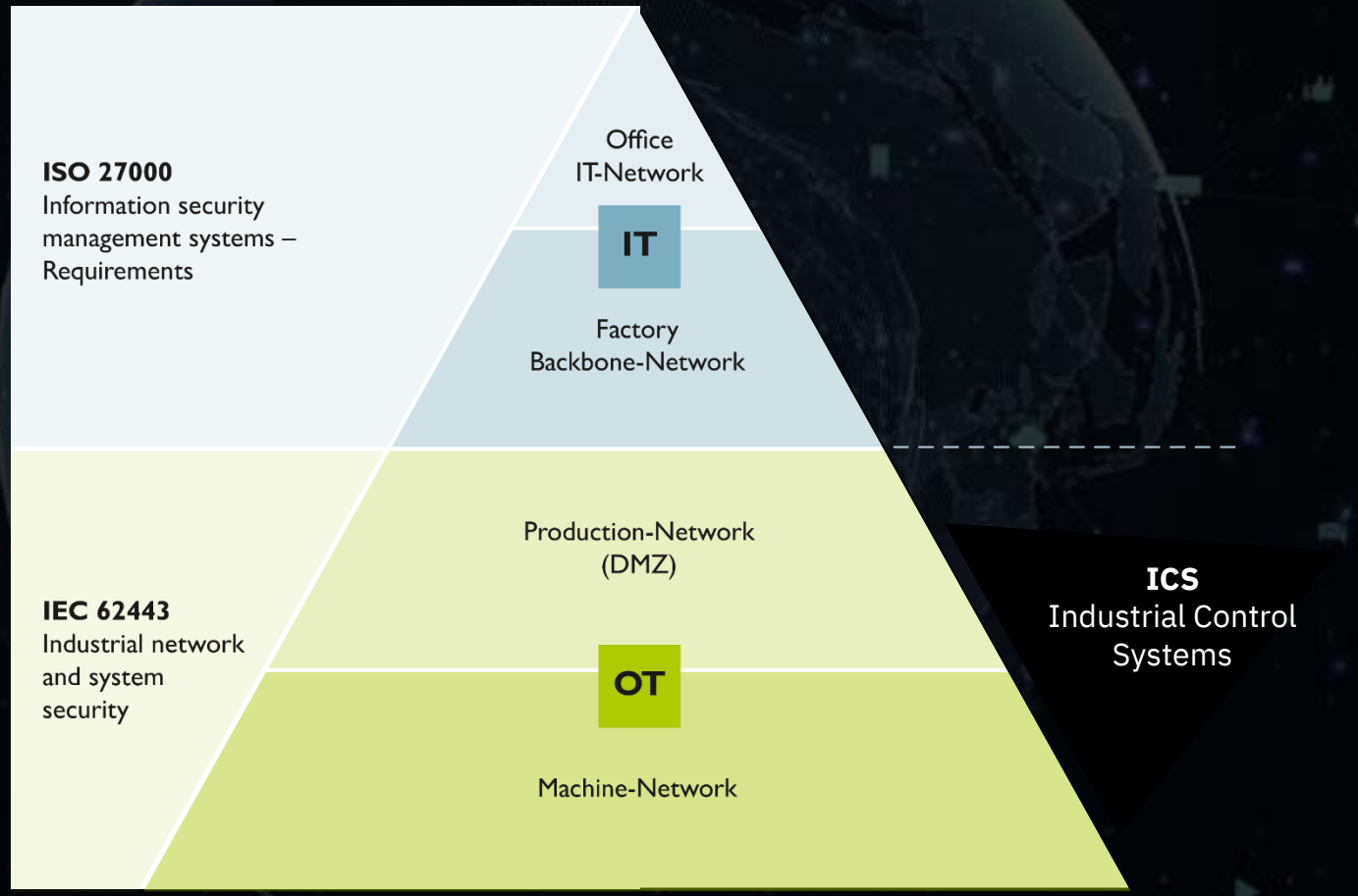
"RTU AND FRTU SHALL COMPLY TO IEC 62351-3 FOR COMMUNICATION CYBER SECURITY BETWEEN RTU AND MASTER STATION (SCADA, DMS) AND IEC 62443-4-2 FOR PRODUCT CYBER SECURITY"

IEC 62443 Standard for Power System

IEC 62443 – IT-Security for Industrial Automation Control Systems

- International series of standards
- Aims to provide support for the secure operation of industrial automation systems (ICS systems) – from design through implementation to management
- Affects component manufacturers, system integrators, and operators
- Builds on standard ISO 27001, which mainly consists of rules for IT security

ISO 27000 vs. IEC 62443



IEC 62443 structure and systematics

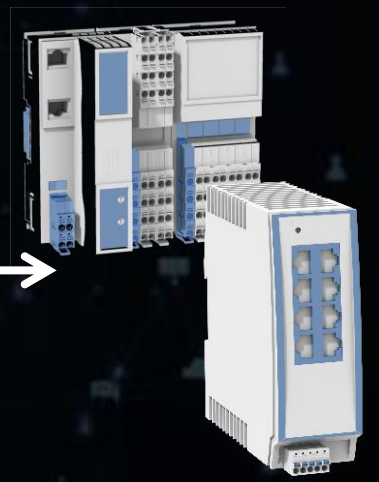
IEC 62443 structure and systematics

Protection

requirements

(Functional)

security requirement



Asset

System

Product

IEC 62351 Standard for Power System

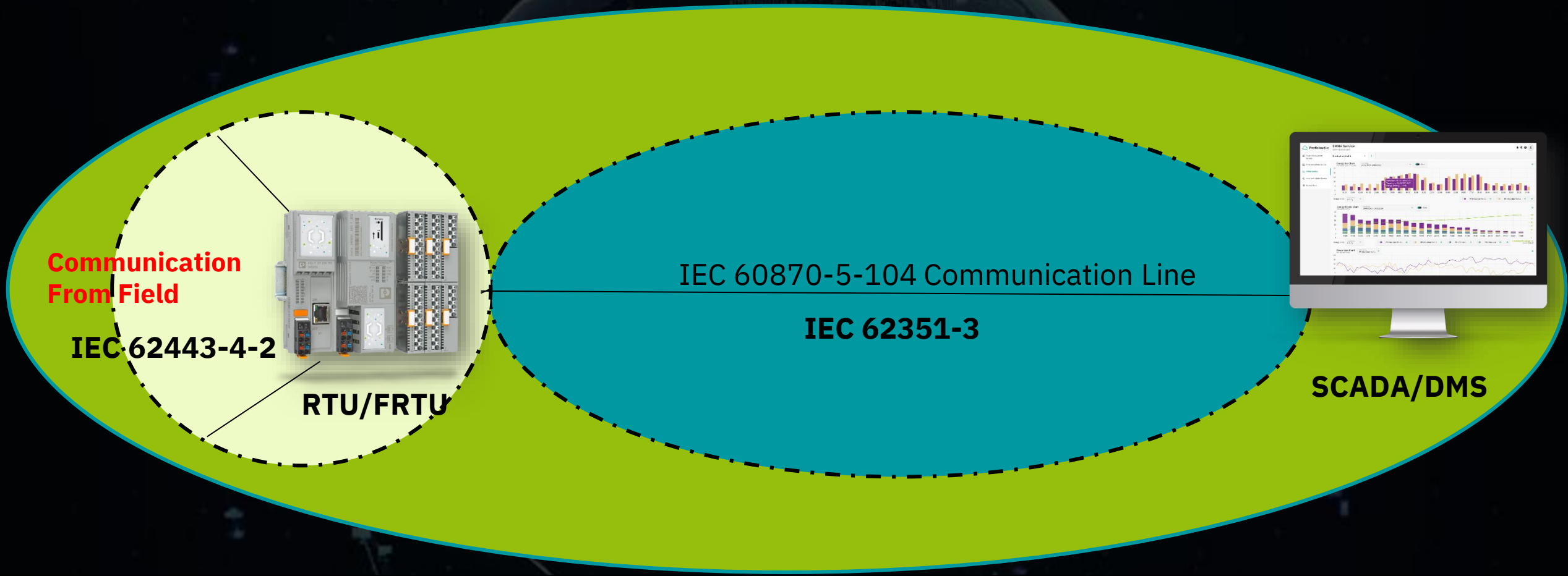
IEC 62351- Cyber Security Standard for Power System

The Scope of IEC62351 series is information security for Power System Control Operation

Standard	Part
IEC 62351-1	Introduction
IEC 62351-2	Glossary of Terms
IEC 62351-3	Security for profiles including TCP/IP
IEC 62351-4	Security for profiles including MMS
IEC 62351-5	Security for IEC 60870-5 and derivatives
IEC 62351-6	Security for IEC 61850 profiles: Goose &SV

PHOENIX CONTACT

Cyber Security: IEC 62443-4-2 and IEC 62351-3



To achieve comprehensive protection against all possible Cyber threats/attacks RTU and FRTU shall comply to **IEC 62351-3 and IEC 62443-4-2** standard for Cyber Security

Phoenix Contact Solutions for Cyber Secured Solutions

Certification according to

- IEC 62443-4-1: Secure product development
- IEC 62443-4-2: Technical Security Requirements
- IEC 62351-3: TLS Encryption

Industrial IT Security
TÜV SÜD
IACS Component

Secure Product Development Lifecycle assessed & monitored according to IEC 62443-4-1

Technical Security Requirements assessed according to IEC 62443-4-2

PHOENIX CONTACT

Cyber Security Certificates

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. IITS2 029429 0027 Rev. 00

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Product: IACS components

Model(s): PLCnext Control
(Configuration: Security Profil active)
AXC F 1152, AXC F 2152, AXC F 3152

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 21CR03S047
Valid until: 2024-10-20

Date, 2021-11-19 (Nadia Patricia Stefan)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

DNV

ATTESTATION OF CONFORMITY

No. 10484600-DSO 24-4043

Issued to:
PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
Germany

For the server product:
AXC F 3152 PLCnext Control
Software version: PLCnext IEC 61850 V1.1.0
Firmware version: 2023.9.0
Hardware version: 06 | S/N: 1368266346

The server product has not been shown to be non-conforming to:

IEC 62351-3 Ed.1.2

Communication network and system security - Profiles including TCP/IP

Security extension applied on IEC 61850-8-1 Edition 2

The conformance test has been performed according to IEC 62351-100-3:2020 Ed.1, in combination with IEC 61850-8-1 edition 2.1, with server product protocol, model and implementation conformance statements: "Protocol Implementation Description (PICS/P10T) v1.0, Date: 29-January-2024".

The IEC 62351 test cases related to the following conformance requirements have been verified with a positive result:

Conformance to selected TLS protocol features:	Conformance to certificate support:	Conformance to cryptographic algorithm support:
TLS versions: 1.2 TLS Resumption using HelloRequest TLS Resumption at least every 24 hours TLS Resumption using session tickets TLS Renegotiation at least every 24 hours TLS Renegotiation using HelloRequest TLS Renegotiation extension	Support of multiple CA Maximum supported certificate size is 8.192 bytes Follow certificate validation rules according to RFC 5280 Certification revocation state validation using CRL Acceptance of any certificate from an authorized CA Simple chain of trust PKI Complex chain of trust PKI	RSA 1024, 2048, 3076, 4098, ECDSA with 256-bit keys Curve secp256r1 SHA-256 SHA-1

This attestation is granted on account of conformance test cases carried out at DNV in The Netherlands and performed with DNV UniGrid Telecontrol Simulator version 2.5.0 (2023). This attestation has been issued for information purposes only, and the archived DNV Verification report no. 10484600-DSO 24-4044, including remarks and limitations, will prevail.

The test has been carried out on one single specimen of the server product as referred above and submitted to DNV by PHOENIX CONTACT GmbH & Co. KG. The manufacturer's production process has not been assessed. This attestation does not imply that DNV has verified any server product other than the specimen tested.

Arnhem, February 5, 2024

Issued by:

K. Lazaridis
Test Engineer

DNV

O. Serban
Team Leader & Principal Consultant
Interoperability of Power Systems

IMPORTANT: Remarks apply to this implementation. See the resulting report for full details. Publication of this document is allowed. Publication in total or in part and/or reproduction in whatsoever way of the contents of the above-mentioned report(s) is not allowed unless permission has been explicitly given either in the report(s) or by previous letter.

Page 1 of 1

DNV Netherlands B.V.
Utrechtseweg 310-B50, 6812 AR ARNHEM, The Netherlands
P.O. Box 9035, 6800 ET ARNHEM, The Netherlands
Tel. +31 26 356 9111
Fax. +31 26 351 3683
www.dnv.com
contact@dnv.com

DNV

ATTESTATION OF CONFORMITY

No. 10484600-DSO 24-4041

Issued to:
PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
Germany

For the server product:
AXC F 2152 PLCnext Control
Software version: PLCnext IEC 61850 V1.1.0
Firmware version: 2023.6.1
Hardware version: 06 | S/N: 1371972989

The server product has not been shown to be non-conforming to:

IEC 62351-3 Ed.1.2

Communication network and system security - Profiles including TCP/IP

Security extension applied on IEC 61850-8-1 Edition 2

The conformance test has been performed according to IEC 62351-100-3:2020 Ed.1, in combination with IEC 61850-8-1 edition 2.1, with server product protocol, model and implementation conformance statements: "Protocol Implementation Description (PICS/P10T) v1.3, Date: 29-January-2024".

The IEC 62351 test cases related to the following conformance requirements have been verified with a positive result:

Conformance to selected TLS protocol features:	Conformance to certificate support:	Conformance to cryptographic algorithm support:
TLS versions: 1.2 TLS Resumption using HelloRequest TLS Resumption at least every 24 hours TLS Resumption using session tickets TLS Renegotiation at least every 24 hours TLS Renegotiation using HelloRequest TLS Renegotiation extension	Support of multiple CA Maximum supported certificate size is 8.192 bytes Follow certificate validation rules according to RFC 5280 Certification revocation state validation using CRL Acceptance of any certificate from an authorized CA Simple chain of trust PKI Complex chain of trust PKI	RSA 1024, 2048, 3076, 4098, ECDSA with 256-bit keys Curve secp256r1 SHA-256 SHA-1

This attestation is granted on account of conformance test cases carried out at DNV in The Netherlands and performed with DNV UniGrid Telecontrol Simulator version 2.5.0 (2023). This attestation has been issued for information purposes only, and the archived DNV Verification report no. 10484600-DSO 24-4042, including remarks and limitations, will prevail.

The test has been carried out on one single specimen of the server product as referred above and submitted to DNV by PHOENIX CONTACT GmbH & Co. KG. The manufacturer's production process has not been assessed. This attestation does not imply that DNV has verified any server product other than the specimen tested.

Arnhem, February 5, 2024

Issued by:

K. Lazaridis
Test Engineer

DNV

O. Serban
Team Leader & Principal Consultant
Interoperability of Power Systems

IMPORTANT: Remarks apply to this implementation. See the resulting report for full details. Publication of this document is allowed. Publication in total or in part and/or reproduction in whatsoever way of the contents of the above-mentioned report(s) is not allowed unless permission has been explicitly given either in the report(s) or by previous letter.

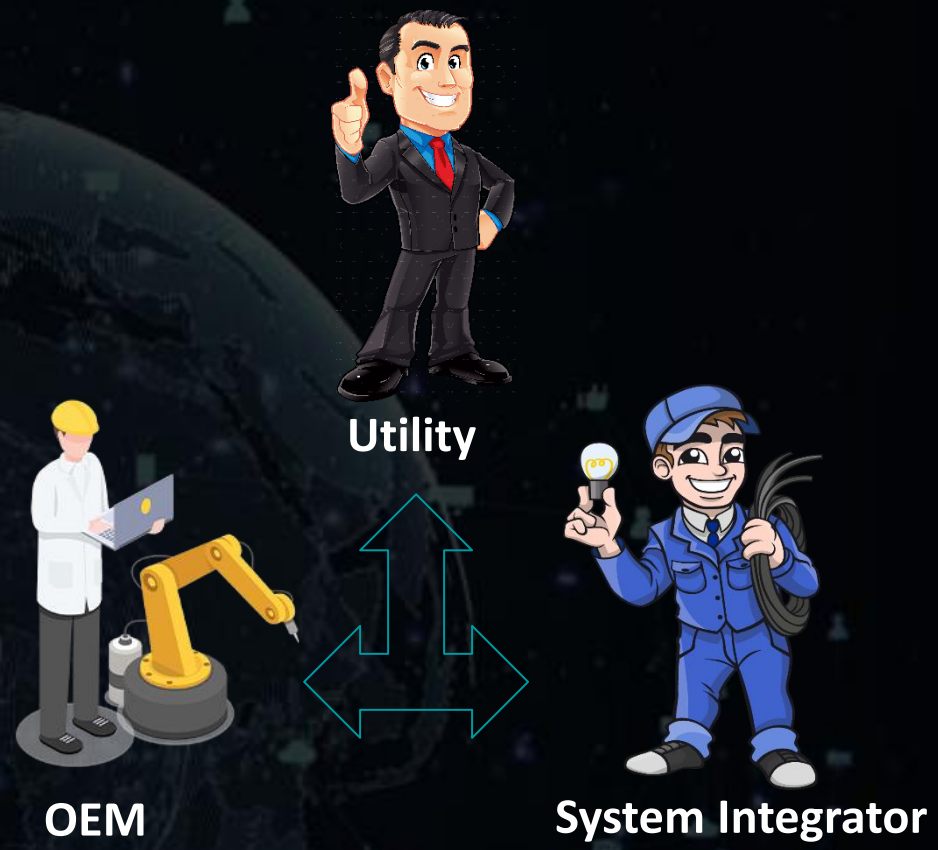
Page 1 of 1

DNV Netherlands B.V.
Utrechtseweg 310-B50, 6812 AR ARNHEM, The Netherlands
P.O. Box 9035, 6800 ET ARNHEM, The Netherlands
Tel. +31 26 356 9111
Fax. +31 26 351 3683
www.dnv.com
contact@dnv.com

PHOENIX CONTACT

Cyber Security Need of an Hour

By Simply putting the specification will not solve the purpose of secured system



Collaboration of all 3 major stakeholder (Utilities, System Integration and OEM) in implementing the specification is must in making our grids secured and powerful

PHOENIX CONTACT

Cyber Security Need of an Hour

Meet our Cyber Warriors on Booth no 4 & discuss how we can mitigate and protect our Grids

PHOENIX CONTACT