The Future of Securing Intelligent Electronic Devices Using the IEC 62351-7 Standard for Monitoring

Andrea Carcano, Alessandro Di Pinto, Younes Dragoni

Who Are We?

ANDREA CARCANO

Co-founder and Chief Product Officer

andrea.carcano@nozominetworks.com

@andreacarcano

- PhD in industrial cyber security
- Sr. Security Engineer, major oil and gas company

ALESSANDRO DI PINTO

Security Research Manager

alessandro.dipinto@nozominetworks.com

@adipinto

- Co-authored TRITON research paper (BH18)
- Reverse-engineering addicted (SANS GREM)
- Interested in breaking things (OSCP)

YOUNES DRAGONI

Security Researcher

younes.dragoni@nozominetworks.com

@ydragoni

- Co-authored TRITON research paper (BH18)
- Enthusiastic White Hat reverse engineer
- Member of the Global Shapers Community (WEF)

Agenda

Line-up

- (In)Secure Smart Grids: State of the Industry
- WG15 and the IEC 62351 Standard
- DEMO: Active Monitoring in Action
- Future of the Threat Detection Landscape

(In)Secure Smart Grids: State of the Industry

(In)Secure Smart Grids: State of the Art Today

Technical Challenges:

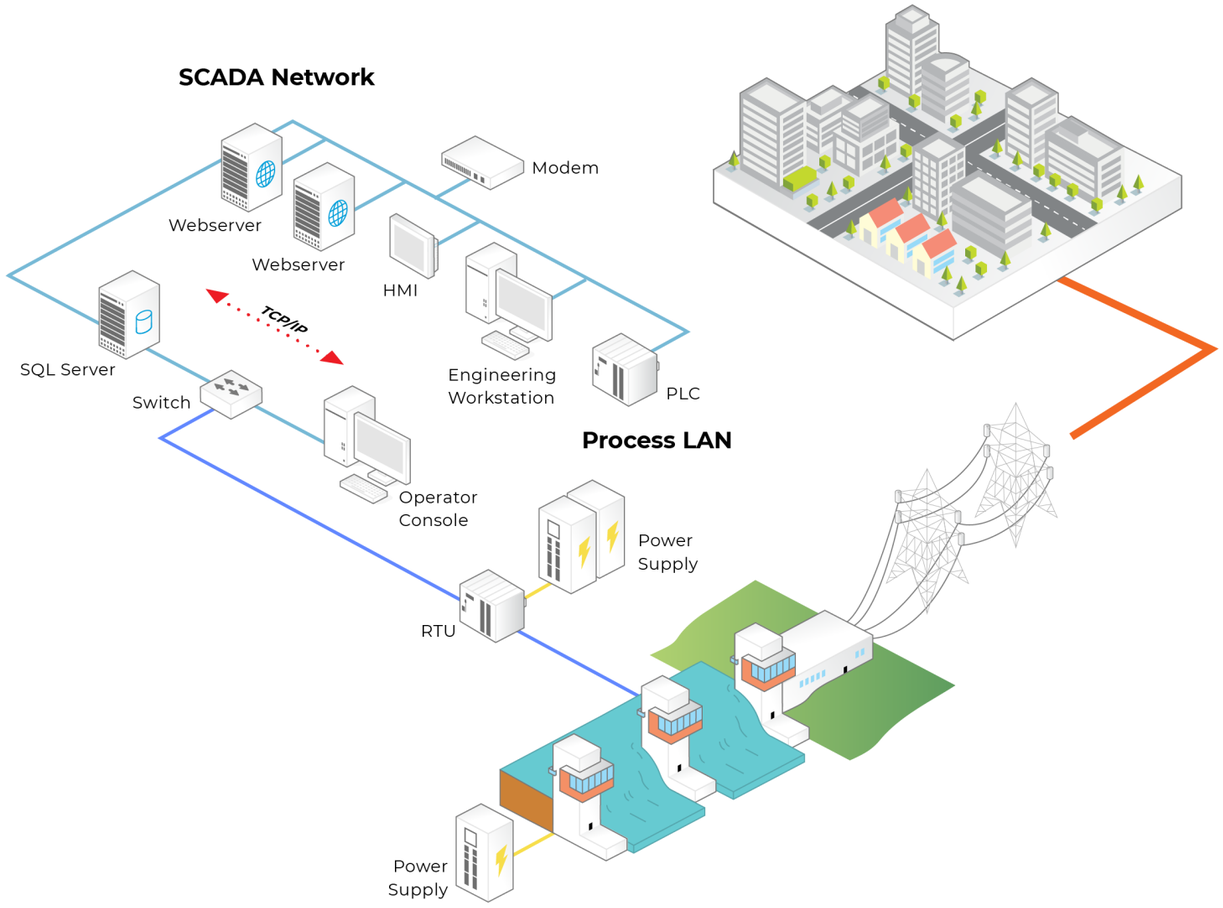
- Systems are “insecure-by-design”
- Passive network monitoring
- Limited asset health visibility

People and Process Challenges:

- Shortage of cyber security skills
- Immature cyber security processes
- Convergence of IT and OT

OT Solution Requirements:

- Safe, effective and efficient security



WG15 and the IEC 62351 Standard

(In)Secure Smart Grids: IEC Standards Improve Threat Detection

IEC 62351 Standard:

- Improves security
- Introduces secure network channels
- Utilizes network and system management

IEC 62351 – Part 7:

- Defines key data objects
- Uses SNMP-like protocols
- Increases asset visibility
- Improves threat and risk detection
- Applies to worldwide Smart Grid technologies (DNP3, IEC 61850, IEC 60870-5)

Passive vs. Active

- Threat detection based on passive indicators is not enough
- Cyber security experts now have deep knowledge of industrial protocols
- Industrial devices already expose SNMP
  - RTU, PLC, Switch, HMI
- Active threat detection covers additional scenarios

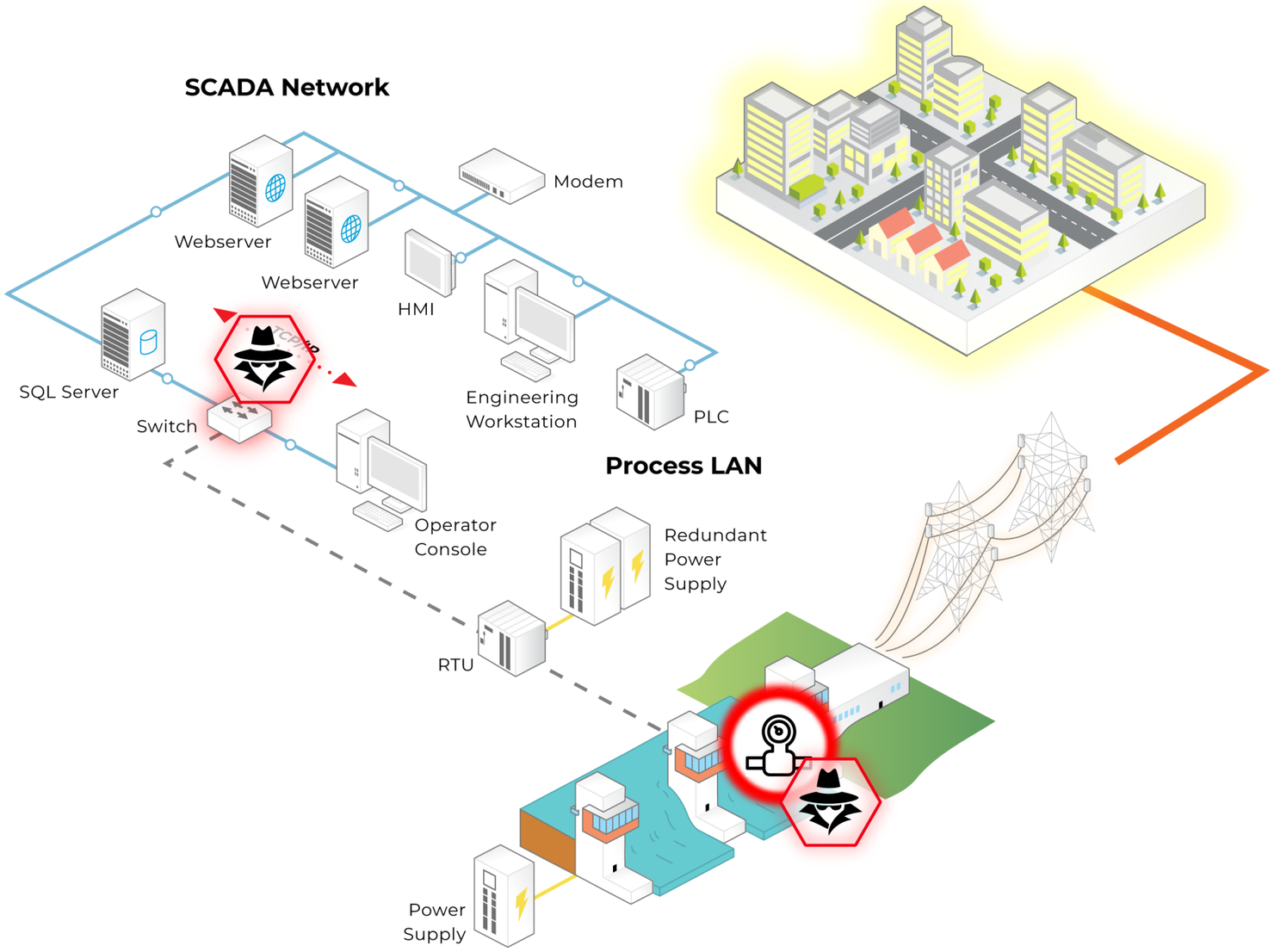
DEMOS:
Active Monitoring in Action

Demo – Real Industrial Process

Attack scenarios

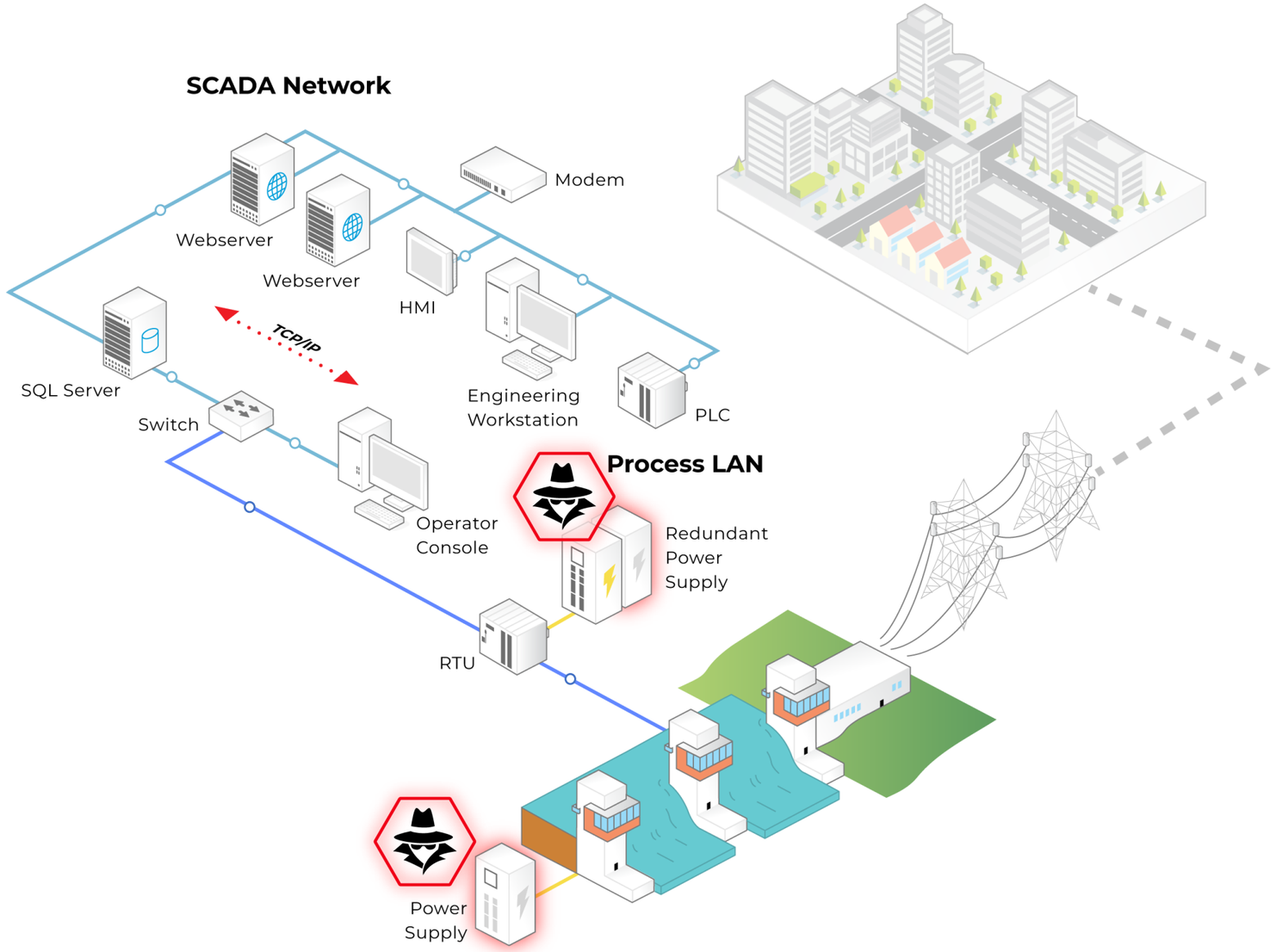
- Physical attacks
- Ladder-based attacks
- Power failure
- HMI malware detection

Demo 1: Physical Attacks



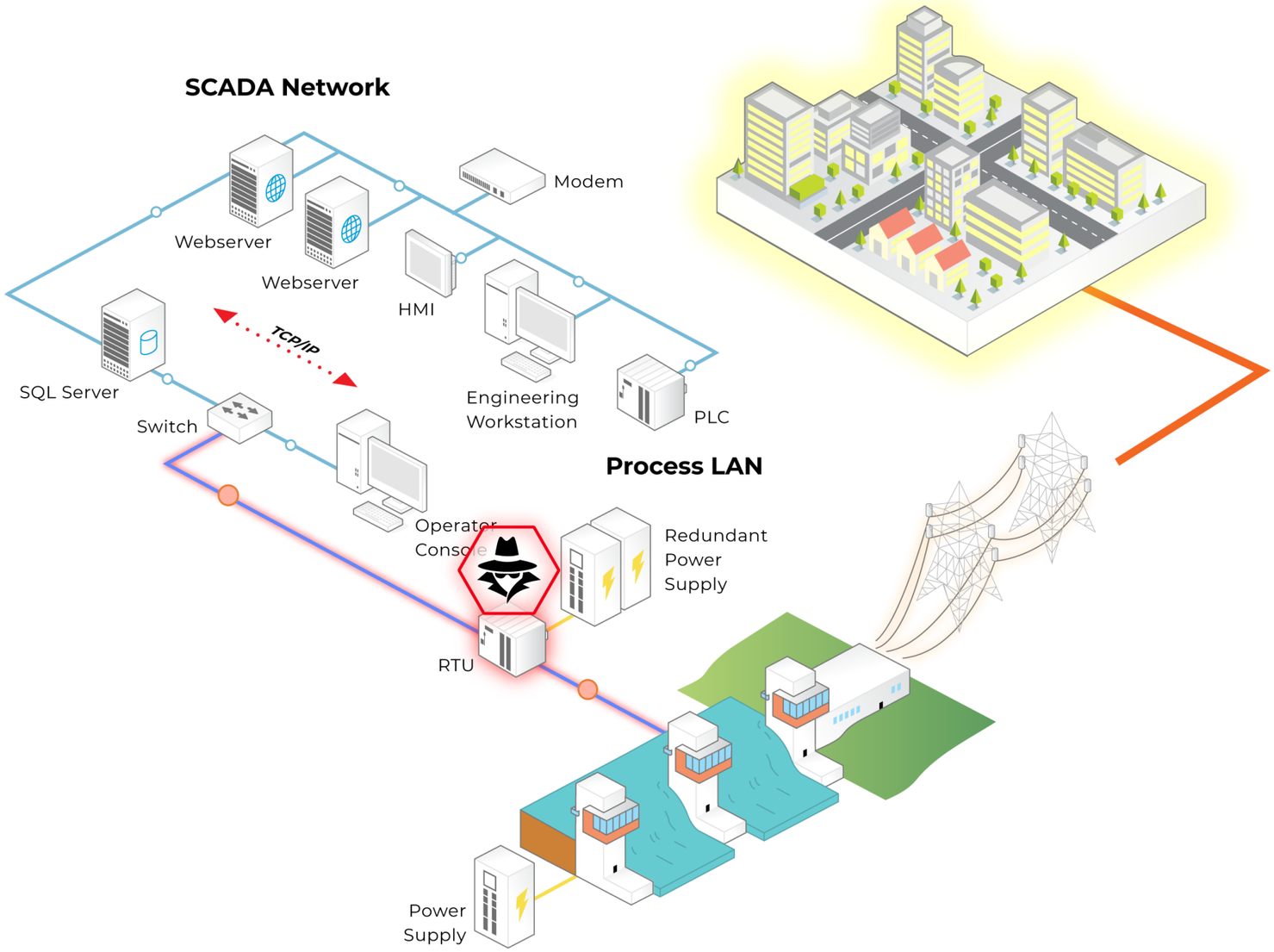
Demo 1: Physical Attacks

Demo 2: Power Failure



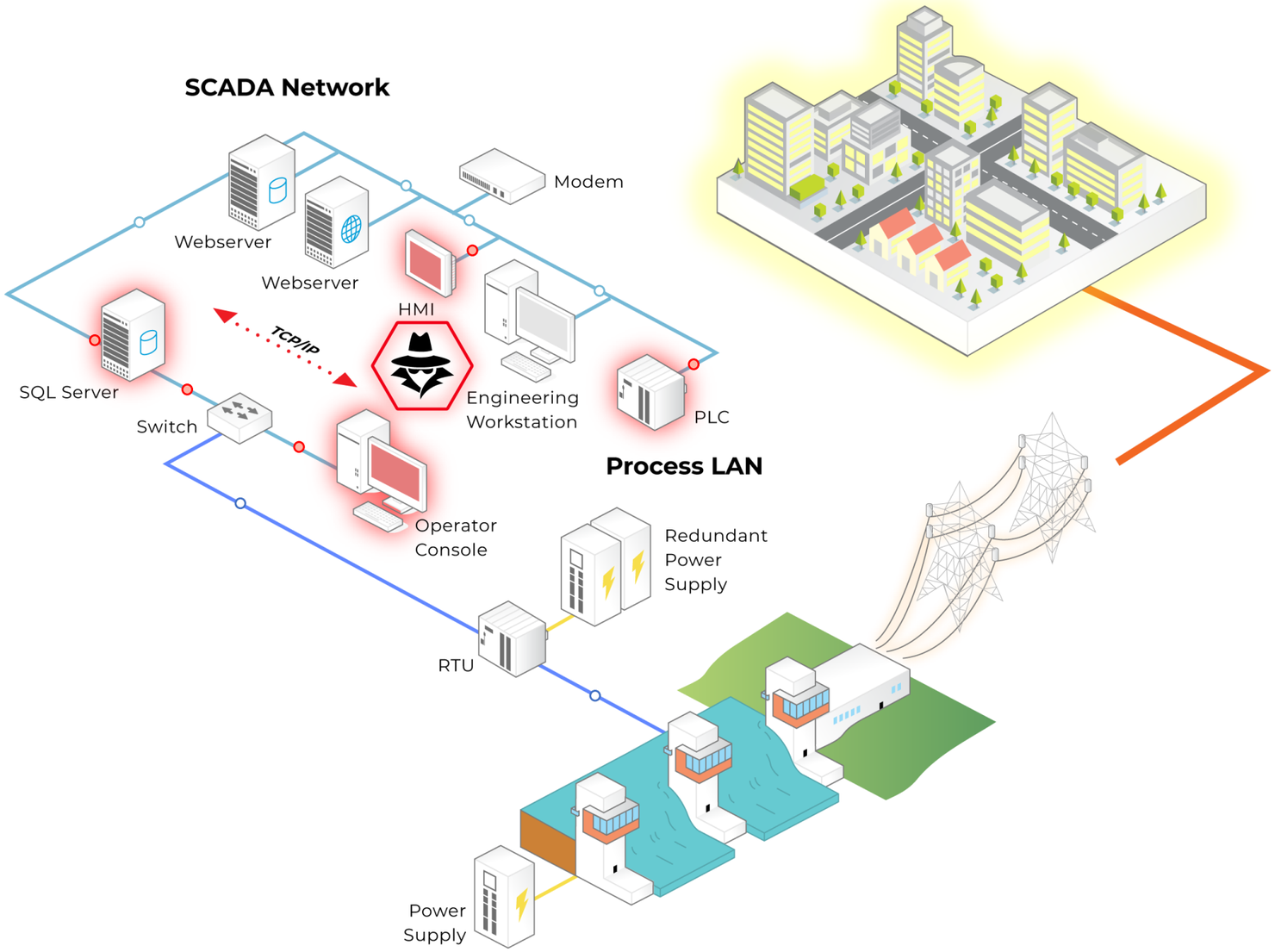
Demo 2: Power Failure

Demo 3: Ladder-based Attacks



Demo 3: Ladder-based Attacks

Demo 4: HMI Malware Detection



Demo 4: HMI Malware Detection

Future of Threat Detection Landscape

Black Hat Sound Bytes

- New approach to industrial network monitoring
- Real-world application of the IEC 62351 standard
- Identification of hard-to-detect threat scenarios

Q&A

ANDREA CARCANO

Co-founder and Chief Product Officer

andrea.carcano@nozominetworks.com

@andreacarcano

ALESSANDRO DI PINTO

Security Research Manager

alessandro.dipinto@nozominetworks.com

@adipinto

YOUNES DRAGONI

Security Researcher

younes.dragoni@nozominetworks.com

@ydragoni

NOZOMI NETWORKS LABS