



## KEY FIGURES

**5+** years in hospitals  
**60+** hospitals  
**4** industry certifications  
**720 h** OT security training

## SKILLS

### Cybersecurity

- ISA/IEC 62443, Purdue model
- Zones & conduits, IDMZ, VPN
- Industrial forensics
- Kali Linux, Nmap, Wireshark
- Metasploit (basic), OWASP

### Networking

- TCP/IP, DNS, DHCP, NAT
- VLAN, routing & switching
- VRRP, MRP/HRP

### Systems

- Windows Server, Windows
- Linux (Ubuntu, Kali), Bash
- Active Directory, Azure AD / MFA
- Docker, VMware, VirtualBox

### OT / Industrial

- SCALANCE, SINEMA RC, PROFINET
- S7-1200 PLC, TIA Portal
- Node-RED, OPC UA, SCADA

### Scripting

- Python, Bash, SQL, JSON

## LANGUAGES

**Spanish:** native

**English:** C1, fluent · full high school in Canada (3 years) and technical training in London

**Spanish Sign Language:** B1

# Santiago Ruiz Cajilema

## IT Systems & Network Specialist | IT/OT Cybersecurity

Lugo, Spain (CET) | EU citizen · Open to remote | +34 673 463 119 | [santiago\\_14\\_rj@icloud.com](mailto:santiago_14_rj@icloud.com)

LinkedIn: [linkedin.com/in/santiago-ruiz-cajilema](https://www.linkedin.com/in/santiago-ruiz-cajilema) | Portfolio & CV: [santiagoruiz.es](https://santiagoruiz.es)

## PROFILE

**5+ years of technical work in hospitals**, a critical infrastructure; the last 3 deploying and supporting clinical software on **large hospital networks** at 60+ sites across Spain.

Holder of an official **Specialisation in Operational Technology (OT) Cybersecurity** (720 h) and certified **Cisco CCST Cybersecurity, Cisco CCST Networking, IT Specialist – Cybersecurity** and **Network Security Support Technician**. Looking for my first dedicated cybersecurity role: SOC, OT security or systems. **Fluent English (C1)**: high school in Canada and technical training in London.

## CYBERSECURITY PROJECTS

### Final Project – OT Cybersecurity & High Availability

2026

CIFP Politécnico de Lugo · Defence in depth with Siemens SCALANCE for an industrial air-extraction plant

- Layered architecture (**Purdue model**) following **ISA/IEC 62443-3-2**: zones and conduits across 8 VLANs, **SCALANCE SC646-2C** perimeter firewall, **IDMZ** and cell micro-segmentation with **SCALANCE S615**.
- Secure remote access with **SINEMA Remote Connect** in the IDMZ: **VPN** tunnels (OpenVPN/IPsec) with **X.509** certificates; stateful firewall rules with default deny and **NAT/NETMAP** for cells with duplicate IP ranges.
- High availability: **HRP/MRP** ring (SCALANCE XM408-8C and XC208) validated with live cable cuts, **< 200 ms convergence** and zero packet loss, plus **VRRPv3** between two S615 units to remove single points of failure.
- Edge computing with **Node-RED** on SIMATIC IOT2000 (S7 Comm) and a web dashboard secured with HTTPS and tokens; process control with S7-1200 PLC, HMI and frequency drive.
- Test plan, secure operations manual and proposed improvements: industrial IDS, SIEM/Syslog, RADIUS and S7 Comm Plus with TLS.

Stack: ISA/IEC 62443 · Purdue · SCALANCE SC646-2C, S615, XM408, XC208 · SINEMA RC · VPN · VRRPv3 · HRP/MRP · NAT · Node-RED · PRONETA

## PROFESSIONAL EXPERIENCE

### INYCOM

Aug 2019 – Sep 2024

Instrumentación y Componentes S.A. · Zaragoza, Spain · Hospitals nationwide

### Cardiology Software Specialist · Implementation & Integration

2021 – 2024

- Deployed clinical software (Sentinel, Spacelabs) on **hospital infrastructures and networks** at 60+ hospitals; owned 40+ projects.
- Configured connectivity between applications, servers and devices: TCP/IP, **VPN**, **Windows Server**, SQL Server and **HL7** integration with the HIS.
- Diagnosed and resolved **communication and connectivity** issues, remotely and on site.
- Coordinated with hospital IT, the vendor and key users to ensure **service continuity**; trained 100+ staff.
- Supervised a junior technician** (training, task allocation and follow-up; escalation point for his work) and mentored an **intern**, later hired by the company.

Stack: Hospital networks · TCP/IP · VPN · Windows Server · SQL Server · HL7 · OPC UA · Remote support

CERTIFICATIONS

Cisco CCST Cybersecurity  
Cisco · 2025 · valid until 2030

Cisco CCST Networking  
Cisco · 2025 · valid until 2025

IT Specialist – Cybersecurity  
Certiport / Pearson VUE · 2025

Network Security Support Technician  
Certiport / Pearson VUE · 2025

Cisco Networking Academy  
Junior Cybersecurity Analyst Career Path ·  
Cyber Threat Management · 2025  
Verify on Credly: [credly.com/users/santy-r](https://credly.com/users/santy-r)

ADDITIONAL TRAINING

Cybersecurity in Logistics & Transport  
Networks, VLAN, VPN, firewalls, SCADA, risk  
management · 150 h · 2025

IT Security Management  
Policies, auditing, cryptography · 100 h ·  
2022

Introduction to Ethical Hacking  
Nmap, Metasploit, iptables · 12 h · 2022

Web Hacking  
SQLi, XSS, LFI · 6 h · 2022

TCP/IP Networking · Azure AD (AZ-  
500)  
OpenWebinars · 2022

Advanced Python Programming  
Official Python Institute course · 150 h ·  
2026

CURRENTLY LEARNING

AI agents & automation  
MKT Hackers · 2026 · n8n, AI APIs

REFERENCES

Letter of recommendation  
Director of Operations, Service (INYCOM) ·  
available on request

INYCOM — Biomedical Equipment Technician Aug 2019 – Jan 2021  
Zaragoza, Spain · Role before moving to software implementation in the same company

- Installed, commissioned and maintained medical equipment in hospitals; fault diagnosis and technical documentation.

ARALUX — Industrial Maintenance Technician Oct 2018 – Feb 2019  
Zaragoza, Spain

- Maintained automated installations: KUKA and ABB robots, Siemens S7-1200 PLC and TIA Portal; diagnosed faults together with production.

PERSONAL LAB

Systems & security lab 2025 – present  
Personal project

- Kali Linux and Ubuntu virtual machines for reconnaissance with Nmap and traffic analysis with Wireshark.
- Linux command-line administration (permissions, services, ports), Bash scripting and services on Docker / Docker Compose.

CYBERSECURITY CASE STUDIES

Cybersecurity for Transport & Logistics Networks 2025  
150-hour course (Mainjobs) · Scenario: public transport operator running buses and trains

- Risk assessment of critical assets (traffic control and electronic payments): threats, impact, likelihood and mitigation.
- Incident Response Plan: preparation, detection with SIEM and IDS/IPS, containment, recovery and coordination with national CERTs (INCIBE, CCN-CERT).
- Real-world incident report: NotPetya attack on Maersk and the Port of Rotterdam (2017), with resilience recommendations.
- Secure network design: segmentation, firewall and ACLs, DHCP/DNS and NAT/PAT, and WAN connectivity to stations and fleet.

EDUCATION

Specialisation in Operational Technology (OT) Cybersecurity 2025 – 2026  
CIFP Politécnico de Lugo · Official Spanish qualification · Advanced vocational programme (post-Higher VET) · 720 h

- Cybersecurity in industrial projects · Secure industrial control systems · Secure industrial communication networks · Industrial cybersecurity forensics · Integrated security

Higher Technician Diploma in Industrial Automation & Robotics 2016 – 2018  
CPIFP La Salle Santo Ángel, Zaragoza · Industrial communications, industrial computing

Alberta High School Diploma 2013 – 2015  
Ross Sheppard High School, Edmonton, Canada · Taught in English