Role: Cyber Security Architect
Area: Business Services
Sub-Area: IT – Security & Operations Technology
Location: Cork/Dublin
Salary: Competitive
Duration: Permanent **Ref:** GNI024

Gas Networks Ireland operates and maintains Ireland's €3bn, 14,725km national gas network, which is considered one of the safest and most modern renewables-ready gas networks in the world.

Almost 725,000 Irish homes and businesses trust Ireland's gas network to provide efficient and reliable energy to meet their heating, cooking, manufacturing and transport needs.

The gas network is the cornerstone of Ireland's energy system, securely supplying more than 30% of Ireland's total energy and over 40% of the country's electricity generation.

Gas Networks Ireland is aiming to deliver a repurposed, resized and fully decarbonised gas network by 2045. Its "Pathway to a Net Zero Carbon Network" envisions transforming the existing gas network into two separate systems carrying 100% renewable gas, one dedicated to biomethane and the other to green hydrogen, with the potential to carry approximately 30% biomethane and 70% green hydrogen, as well as offering significant long term energy export opportunities.

Gas Networks is an organisation with a very strong legacy and a culture founded on pride in our purpose, to keep Irelands energy moving, and commitment to our vision, to be at the heart of Irelands energy future. Our organisational values demonstrate what is important across the organisation including building on our experience across our organisation to build towards our sustainable future, doing what's right for each other and for the people and communities that we serve and finally energised for the change of our future towards a renewable energy landscape. Throughout your career in Gas Networks Ireland, you will be part of an organisation that has a strong commitment to supporting and developing our workforce today and into the future. You will also have an opportunity to get involved in our ambitious iBelong programme ensuring a diverse, equitable and inclusive environment for us all to thrive. Finally, our Time to Talk Mental Health programme and our wellbeing initiatives ensure we provide support across many areas as you work in our organisation.

The Role:

Reporting to the Security Architecture & Deliver Manager, the Cyber Security Architect is responsible for defining, evolving, and governing the organisation's cyber security architecture strategy. This role ensures that security design decisions align with business objectives, regulatory obligations, and the ever-changing threat landscape. Acting as the authoritative voice on enterprise security, the architect embeds resilience and protection into the organisation's technology ecosystem.

Duties and Responsibilities:

1. **Security Architecture & Design**
   - Define, develop, and govern enterprise-wide security architecture across IT, OT, and ICS/SCADA environments.

- Establish architecture principles, standards, and reference security patterns aligned with IEC 62443, NIST CSF, NIS/NIS2, and EU/Irish critical infrastructure directives.
- Integrate secure-by-design approaches into technology, engineering, and delivery programmes.
- Lead and govern architecture reviews across major initiatives, acting as the final authority on security design decisions.
- Provide authoritative guidance on cloud security, network security, identity & access management, data protection, and secure infrastructure design.

2. **Standards & Compliance**
    - Own, maintain, and continuously refresh cybersecurity policies, standards, and governance frameworks.
    - Translate regulatory obligations into actionable technical and architectural controls.
    - Ensure compliance with external frameworks (IEC 62443, NIST CSF, Cyber Fundamentals) and alignment with CRU price control allowances.
    - Monitor and interpret emerging threats, vulnerabilities, and regulatory changes, translating them into strategic and architectural responses.
    - Promote cost consciousness and financial responsibility in cybersecurity decision-making.
3. **Cyber Strategy & Roadmap**
    - Define and evolve the enterprise cyber security architecture strategy, ensuring alignment with business objectives, regulatory obligations, and emerging threat landscapes.
    - Develop, maintain, and communicate a multi-year Cyber Security Strategy and risk-driven Cyber Roadmap.
    - Ensure roadmap delivery supports improved maturity, resilience, and compliance with external obligations.
    - Champion advanced security technologies, tools, and frameworks that strengthen the organisation’s security posture.
4. **Risk Assessment & Threat Modelling**
    - Lead comprehensive risk assessments and threat modelling across IT, OT, ICS, and critical systems.
    - Identify risks, propose mitigating controls, and ensure residual risk is understood and accepted appropriately.
    - Maintain and evolve threat models to guide mitigation strategies and architectural decisions.
5. **Technical Leadership & Collaboration**
    - Influence and collaborate with enterprise architects, solution architects, engineering leads, delivery managers, and vendors to embed security principles into blueprints and roadmaps.
    - Communicate security requirements in clear business language to senior stakeholders.
    - Support project delivery, architectural governance, and secure solution implementation.
6. **Resilience & Operational Security**
    - Ensure architecture supports incident detection, response, recovery, and forensic investigations.
    - Provide architectural insights to inform containment, recovery, and future prevention.
    - Safeguard operational availability and safety in ICS environments.
    - Enhance organisational resilience through secure infrastructure design and operational practices.

Knowledge, Skills and Experience:

Required Skills & Experience:

- **Cybersecurity Architecture Expertise:**
  - Proven experience designing and governing enterprise cybersecurity architecture across IT, OT, ICS/SCADA, and complex enterprise environments.
  - Strong understanding of secure network architecture, segmentation, zero trust principles, identity/security controls, and secure by design practices.
  - Expertise in cloud platforms (Azure, AWS, GCP) and associated security controls.
  - Solid grasp of endpoint protection, IAM, encryption, secure SDLC, and modern security tooling (SIEM, DLP, EDR, vulnerability management).
- **Frameworks & Standards Mastery:**
  - Deep knowledge of IEC 62443, NIST Cyber Security Framework (CSF), NIS/NIS2 Directive, Cyber Fundamentals, ISO 27001, SABSA, and TOGAF.
  - Ability to translate these standards into practical architectural patterns and security controls.
- **Regulatory & Compliance Experience:**
  - Experience working with EU and Irish critical infrastructure regulations.
  - Understanding of CRU oversight, price control cycles, evidence based investment, and cost efficient design decisions.
  - Ability to align cybersecurity architecture and spending with regulatory and compliance obligations.
- **Strategy & Roadmap Leadership:**
  - Experience developing or contributing to Cyber Security Strategy and multi year Cyber Roadmaps.
  - Ability to link architecture decisions to maturity improvement, regulatory compliance, and risk reduction.
- **Risk & Threat Modelling:**
  - Strong experience performing architectural risk assessments and threat modelling across IT, OT, ICS, and enterprise systems.
  - Ability to evaluate operational impact and clearly communicate residual risk to senior stakeholders.
- **Collaboration & Influence:**
  - Skilled at engaging engineering, operations, IT, and project teams in secure delivery.
  - Ability to translate complex cyber concepts into clear business focused language for technical and non technical audiences.
  - Strong influence and leadership within architectural governance processes.
- **Operational & Resilience Awareness:**
  - Understanding of how cybersecurity impacts system availability, safety, and operational continuity in ICS/OT contexts.
  - Experience designing architectures that enable monitoring, detection, response, recovery, and forensic investigations.
- **Professional Background & Certifications (Preferred):**
  - 7–10+ years in cybersecurity, with 3–5+ years in architecture or senior technical leadership.

- Experience in regulated industries (energy, utilities, transport, pharma, critical infrastructure).
- Relevant certifications such as GICSP, ISA/IEC 62443, CISSP, CISM, CCSP, SABSA, TOGAF, or similar.

Preferred Qualifications:

- Bachelor's or Master's degree in Cyber Security, Computer Science, or related field.
- Experience in regulated industries (e.g., financial services, healthcare).
- Familiarity with DevSecOps practices and automation tools.

Applications, including current Curriculum Vitae, should be emailed to the following address stating the job title and reference number in the subject line of your email:
recruit@gasnetworks.ie

The closing date for receipt of applications for this vacancy is the 28th January 2026.

Please note that applications submitted after this closing date will not be accepted.

Gas Networks Ireland is an equal opportunities employer

We are committed to providing a diverse and inclusive place of work and have a robust strategy and framework called ibelong to enable this. We are an equal opportunity employer and through our recruitment process we welcome and encourage applications from interested and suitably qualified individuals regardless of gender, age, racial or ethnic origin, membership of the traveller community, religion or beliefs, family or civil status, sexual orientation/gender identity or disability.

GNI will only hold your data for as long as necessary. By providing a CV to GNI you are agreeing for GNI to process this information about you. If you have any question about how GNI processes your data, please see our Privacy Notice. If you have further questions, you can contact us at DataProtection@gasnetworks.ie