

26745 - Senior Solution Engineer

Location: Braine-l'Alleud, Belgium.

Period: 300 (start on 14 Dec. 2026)

Deadline: 02 Nov. 2026

Duties/Roles:

1. System and Solution Engineering

- Analyse operational, functional & project requirements & translate them into implementable DCIS solutions;
- Define the overall technical solution and system architecture using the established DCIS Node, Module & Service taxonomies;
- Ensure that the resulting system delivers the required end-to-end functionality & emergent behaviour;
- Perform technical trade-off analyses considering performance, interoperability, security, deployability, resilience, maintainability, cost, schedule & technological maturity.

2. Model Based Systems Engineering

- Apply MBSE throughout the engineering lifecycle;
- Map project requirements against existing Requirement Models, Implementation Guidelines & Implementation Constraints;
- Maximise reuse of approved Modules, Services, architectures & engineering patterns;
- Identify gaps where existing Requirement Models or standardized building blocks cannot satisfy project requirements.

3. Complex Systems Product Ownership – Operational Nodes

- For designated Nodes already introduced into operational service, act as the Complex Systems Product Owner:
- Maintain technical ownership and system-level design responsibility for assigned operational Nodes throughout their lifecycle;
- Maintain an authoritative understanding of the Node architecture, configuration, interfaces, dependencies, capabilities & design constraints;
- Ensure that modifications to individual Modules or Services do not compromise the overall coherence, interoperability, performance, security or operational capability of the Node;
- Assess operational technical issues from an end-to-end system perspective & coordinate their resolution with the appropriate SMEs, Model Custodians & service organizations;

- Analyse requests for change, obsolescence issues, technology refreshes, security changes & evolving operational requirements to determine their impact on the complete Node;
- Define & maintain the technical evolution path & Node roadmap, aligned with Module & Service roadmaps & the wider DCIS Target Architecture;
- Identify technical debt, architectural divergence, lifecycle risks & emerging obsolescence before they become operational constraints;
- Initiate or recommend engineering activities required to maintain the technical viability of the Node;
- Provide system-level technical guidance to operations, maintenance & service-management organizations where issues require design-level knowledge;
- Ensure that operational experience & lessons identified are fed back into the Modularity Framework, Requirement Models & future system designs;
- Maintain consistency between the as-designed, as-built and as-operated technical baselines of the Node;
- Support configuration & change-control processes by assessing the system-level impact of proposed changes.

4. Multi-Domain Technical Integration

- Integrate engineering contributions across DCIS technical domains, including as applicable: Network & Communication Access;
- WAN/LAN and network services;
- SATCOM & tactical communications; Radio systems; Infrastructure & Platform services;
- compute, virtualization & cloud technologies; storage & data services; cybersecurity & security services;
- identity & access management; Business Support Services; automation, orchestration & Infrastructure-as-Code;
- physical deployable infrastructure & associated supporting systems.

5. Technical Coordination

- Act as the primary technical focal point for assigned projects & operational Nodes;
- Coordinate the engineering contributions required from the different technical domains;
- Translate system-level requirements & operational issues into clear engineering tasks & technical questions for the appropriate SMEs & Model Custodians;
- Integrate the outputs produced by the different engineering disciplines into a single coherent solution;

- Identify conflicting requirements, assumptions or design decisions & drive their technical resolution.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO SECRET security clearance
- University degree in Systems Engineering, Telecommunications Engineering, Computer Engineering, Electronic Engineering, Computer Science or another relevant discipline.
- 10 years of relevant professional engineering experience, including significant experience with complex ICT/CIS, defence, aerospace, telecommunications or other highly integrated technical systems.
- Experience in Systems Engineering and/or Solution Architecture applied to complex systems.
- Professional working proficiency in English, including the ability to produce and review complex technical documentation

Essential Professional Experience

- Complex Systems Engineering: Significant experience in the architecture, design, integration, verification or lifecycle management of complex systems involving multiple technical domains;
- Demonstrated ability to translate operational or business needs into system requirements, architectures and implementable technical solutions;
- Experience defining and managing system boundaries; functional decomposition; interfaces; dependencies; constraints; non-functional requirements; system-level performance
- Technical Leadership: Experience as a Technical Lead, Lead Systems Engineer, Solution Architect, System Architect or equivalent senior engineering role;
- Experience technically coordinating multidisciplinary engineering teams and SMEs
- Ability to provide clear technical direction: Experience resolving technical disagreements and driving engineering decisions across organizational and technical boundaries.
- System Integration: Significant experience integrating systems composed of multiple technologies, products or engineering disciplines. Strong

understanding of system interfaces, dependencies and emergent behaviour.

- Experience identifying and resolving integration problems spanning multiple technical domains. Experience planning or supporting system integration, verification, validation and acceptance activities. Demonstrated ability to perform structured root-cause analysis
- Lifecycle Engineering / Product Ownership: Experience supporting complex systems after their transition into operational service;
- Understanding of the relationship between: design authority; configuration management; change management; obsolescence; technology refresh; technical debt; operational support; system evolution;
- Experience assessing the system-level impact of changes to individual components, subsystems or services.

Essential Technical Expertise

- Broad technical understanding across ICT/CIS domains, rather than being specialists exclusively within one technology.
- Strong knowledge of several of the following areas is expected: IP networking and routing;
- LAN/WAN architectures; network security and firewalls; compute and server infrastructure; virtualization and hyperconverged infrastructure; storage technologies; identity and access management; cybersecurity architectures; enterprise and infrastructure services; cloud and hybrid-cloud technologies; automation and orchestration; monitoring and management systems; telecommunications; SATCOM and/or radio communications; deployable or mobile ICT infrastructure.
- The candidate is not expected to be the SME in all these domains. However, they must have sufficient technical breadth to understand how these technologies interact.

Essential Systems Engineering Expertise:

- Strong understanding of requirements engineering, including functional and non-functional requirements.
- Ability to decompose complex systems into manageable subsystems and components while preserving understanding of the complete system.
- Strong understanding of interfaces and Interface Control.
- Experience with requirements traceability from operational need through implementation and verification.

- Understanding of architecture versus detailed design & the appropriate allocation of responsibilities between system-level & domain engineers.
- Experience performing engineering trade-off analyses.

Required Level of Security Clearance:

NATO SECRET.