

JOB DESCRIPTION & PERSON SPECIFICATION



Job Title: Cyber Security Engineer	Location: Hunmanby / Mansfield
Department: Engineering	Contract: Permanent
Reports To: Senior Cyber Security Manager	Direct Reports: None

1.0 Job Summary & Role

Deep Sea Electronics Ltd (DSE) are a leading UK electronics manufacture specialising in development of advanced control and automation products for the power generation and off highway vehicle markets. Our range of solutions include connected devices that are subject to the latest cybersecurity standards.

The Cyber Security Engineer will support the cyber security aspects of our products, working under the guidance of the Senior Cyber Security Manager. They will work closely with cross functional teams including engineering, operations and commercial to help ensure products meet regulatory compliance and industry best practices.

2.0 Key Responsibilities & Main Duties

- Contribute to the development and maintenance of the cybersecurity strategy and policies for development of products within DSE product range
- Work cross functionally with other departments to ensure full coverage of the relevant cyber security regulations, including the EU Cyber Resiliency Act
- Support product management in progressing cyber security initiatives on the product road map
- Support the identification, assessment, and mitigation of cybersecurity risks associated with product development and deployment
- Assist in the preparation of necessary documentation for compliance with IEC 62443 and related regulatory requirements
- Ensure continuous alignment with industry regulations and frameworks related to industrial cybersecurity
- Collaborate with engineering teams to integrate security features into product design and architecture
- Advise on secure software development practices and secure by design principles
- Support vulnerability assessments, threat modelling, and penetration testing efforts for product solutions
- Support the implementation of secure remote access, network security, and secure communication protocols throughout the products
- Support the response to cybersecurity incidents within the product development lifecycle



- Work with internal teams to implement lessons learned from security incidents and continuously improve security measures
- Contribute to post-incident reviews and help develop preventative measures to mitigate future risks
- Develop and share cybersecurity subject matter knowledge with internal stakeholders
- Share cybersecurity best practice, emerging threats, and mitigation strategies with internal teams
- Support senior team members in engaging with customers and regulatory bodies on cybersecurity requirements and concerns

3.0 Internal & External Relationships

- Engineering Management team – assist with the implementation of cyber security projects
- Test and Approvals department – assist with training and in the development of test programs and procedures for functional safety
- Technical Support – assist technical support with more involved customer queries, and technical authoring support including review of security manuals
- Commercial sales team – Support customer faces sales literature and promotion of cyber security awareness at DSE

4.0 Key Performance Indicators

- Attention to detail, able to work both individually as a part of a team and self-discipline required for software developing and testing.
- Produce clear and concise software documentation.
- High quality software development.
- Ability to define and work to timescales.

5.0 Essential/Desirable Factors

Knowledge	
Essential: • Good level of knowledge in C/C++ for embedded systems • Cyber security development processes, including risk assessment techniques • Security protocols and techniques, encryption, key storage, secure boot and trust zones. • Knowledge of RED and CRA regulations • Automotive cyber security standards R155, R156 and ISO 21434	Desirable: • Embedded Linux operating systems • IoT systems • Electrical principles • Functional safety experience, alongside cyber security • Cyber security standards, IEC 62443, EN18031



JOB DESCRIPTION & PERSON SPECIFICATION



Skills & Attributes	
Essential: - Familiar with stage gated / agile development approaches - Comfortable collaborating and communicating with embedded systems engineers and company executives alike, bridging the gap between technical and management - Ability to contribute to cyber risk analysis, pragmatically - Use to work to working to high levels of quality and accuracy standards. - Ability to translate requirements into a technical product specification - Used to work in a high-pace environment - Enthusiastic and optimistic	Desirable:
Experience	
Essential: - Held a role focused on cyber security in embedded systems - Worked practice of the relevant standards - Contribution to risk analysis, mitigations and translation of requirements	Desirable: - Industrial protocols such as RS485, CAN - Background in industrial control and automation products
Qualifications	
Essential: BSC in computer science or related degree qualification	Desirable:

Created by	Dated Created
Technical Director	Sept 2026

