

**Requisition Number:**


## Job Description. Principal Cybersecurity Engineer

Are you a Cybersecurity Engineer looking for your next challenge? Do you want to be part of a growing team that develop and deliver advanced engineering and test services for new vehicle technologies? Do you want to contribute to the future of global road transport solutions?

We are recruiting a Principal Cybersecurity Engineer to join our growing team and help us deliver consultancy and targeted research and development programmes to ensure that our customers are ready for the challenges ahead.

As off-board information relating to the current environment and position of a vehicle become key, and the role of the driver is progressively being removed from vehicle control; the electronic systems that replace the human inputs need to provide extremely high levels of dependability to ensure public acceptability of these technologies. The implications of new technologies for connectivity, autonomy and electromobility are driving significant changes in the way that the industry must engineer, test and verify next-generation transport solutions.

HORIBA MIRA is a world-class, independent engineering consultancy, operating in multiple locations around the world, to support vehicle manufacturers and their supply chain with cutting-edge engineering and testing expertise. We offer full-system design, test and integration expertise to automotive, defence, rail and transport industries and also specialise in developing low carbon and autonomous and co-operative driving technologies.

At our headquarters in the Midlands, we have access to one of the most comprehensive vehicle proving grounds which boasts 93km of test tracks and over 40 world-class test facilities and laboratories. Our facilities, combined with the engineering expertise of our 600 strong team makes MIRA Technology Park Europe 's number one location for transport sector R&D.

<b>Title of Job:</b>	Principal Cybersecurity Engineer		
<b>Department:</b>	Vehicle Resilience		
<b>Grade:</b>	Principal Engineer (5P)		
<b>Date Required:</b>	ASAP		
<b>Salary Range:</b>	Competitive		
<b>Number Required:</b>	1		
<b>Location:</b>	HORIBA MIRA, Nuneaton, UK		
<b>Reason for Vacancy:</b>	Team Expansion		
<b>Contract Type:</b>	<b>Permanent:</b>	Y	<b>Contractor:</b> N
<b>Responsible To:</b>	Team Leader (Vehicle Resilience)		
<b>Subordinates:</b>	None		

### Main Purpose of Job

MIRA is looking for a Principal Cybersecurity Engineer to join a unique and growing team within the Vehicle Resilience department. Based at the heart of the UK automotive industry, they will form part of the growth strategy within HORIBA MIRA. This role will include, but not be limited to, delivering and developing MIRA's trusted automotive cybersecurity service and product offerings, including:

- Delivery of cybersecurity engineering services with emphasis on a risk driven approach
- Research and development of new cybersecurity services and products
- Supporting the wider multi-disciplinary team of Cybersecurity, Electromagnetic Resilience and Functional Safety experts in developing and delivering integrated Vehicle Resilience services.

This technical role requires a highly motivated individual with experience in risk-driven engineering methods, security analysis and creative but structured problem resolution.

## Key Functions

The following activities cover the typical requirements of the role:

- Consultancy
  - Lead the technical delivery of consultancy projects carrying out cybersecurity engineering activities such as threat analysis, risk assessment, cybersecurity requirements, specification of cybersecurity controls, development of verification and validation plans and cybersecurity testing
  - Lead technical support in own area of expertise to cross-discipline team
- Research and Development
  - Lead research projects exploring the cybersecurity aspects of new technology including potential threats and vulnerabilities
  - Lead the development and validation of new cybersecurity engineering capabilities and services
  - Lead the optimisation of existing services through structured continuous improvement
  - Lead the development of cybersecurity engineering procedures
- Project Management
  - Support cross-discipline delivery across core programmes / projects
  - Lead the development of project proposals
  - Lead the training/coaching of other less experienced members of staff

Essential Qualifications	Preferred Qualifications
<ul style="list-style-type: none"> <li>• Bachelors degree (minimum 2:1) or equivalent qualification in electrical / electronic engineering, computer science, cybersecurity or other relevant discipline</li> </ul>	<ul style="list-style-type: none"> <li>• Relevant Masters Degree or PhD</li> <li>• Professional membership of a relevant engineering or computing institution for example Chartered Engineer</li> </ul>

Essential Experience	Preferred Experience
<p>8+ years of experience in a cybersecurity related field covering some combination of the key functions detailed previously.</p> <p>Experience in all of the following:</p> <ul style="list-style-type: none"> <li>• Security engineering including:               <ul style="list-style-type: none"> <li>○ Performing threat analysis and risk assessment</li> <li>○ Development of cybersecurity concepts and requirements</li> <li>○ Specification of cybersecurity controls</li> </ul> </li> </ul> <p>Knowledge of relevant automotive regulations</p>	<p>Experience in any of the following:</p> <ul style="list-style-type: none"> <li>• Security engineering for automotive or other cyber-physical systems</li> <li>• System level architectural design and technical review</li> <li>• SAE J3061, ISA/IEC 62443 or other appropriate cybersecurity standards</li> <li>• Automotive-relevant safety-related systems standards such as IEC 61508, MISRA SA and ISO 26262</li> <li>• Systems engineering</li> <li>• Cybersecurity testing</li> <li>• Cybersecurity assessments</li> </ul>

<p>and standards and their requirements, including:</p> <ul style="list-style-type: none"> <li>• ISO/SAE 21434</li> <li>• UN Regulations 155 and 156</li> </ul> <p>Experience in some combination of the following:</p> <ul style="list-style-type: none"> <li>• Wireless technologies (e.g. Wi-Fi, Bluetooth, NFC)</li> <li>• Wired networking technologies (e.g. CAN, Automotive Ethernet)</li> <li>• Embedded operating systems (e.g. QNX, Linux, Android)</li> <li>• Sensing technologies (e.g. RADAR, ultrasonic)</li> </ul>	<ul style="list-style-type: none"> <li>• Automotive software frameworks (e.g. AUTOSAR)</li> <li>• Cryptography principles, applications and implementation considerations</li> <li>• Developing and delivering training courses</li> </ul>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>What are the candidates likely to be doing now?</b>
<p>Cybersecurity engineer / analyst for an automotive OEM, Tier 1 or other supplier</p> <p>Cybersecurity engineering consultancy</p> <p>Cybersecurity research in an industrial or academic environment</p>

<b>Other information</b>
<p>The successful candidate should:</p> <ul style="list-style-type: none"> <li>• Be capable of delivering a high standard of technical writing</li> <li>• Be capable of presenting technical information confidently to customers</li> <li>• Be a self-starter and able to take ownership of and execute designated tasks accurately within timing and budget constraints</li> <li>• Have well-developed analytical skills – rigorous but pragmatic, being able to justify decisions with solid rationale</li> <li>• Have good interpersonal skills – a consensus-builder not confrontational</li> <li>• Be able to maintain discretion and confidentiality</li> <li>• Be capable of working under pressure, individually and as part of a team</li> <li>• Hold a full driving licence</li> <li>• Be willing to travel and work flexibly: The job is likely to involve trips or extended placements at customer facilities within the UK or overseas</li> <li>• Be willing to engage in the security clearance process and work on defence related projects</li> </ul>