Kwalifikacja cząstkowa na poziomie szóstym Polskiej Ramy Kwalifikacji i europejskich ram kwalifikacji

Reliability and cyber security management for equipment and technology in industry

Status: włączona funkcjonująca

Rodzaj: cząstkowa

Kategoria: wolnorynkowe

Krótka charakterystyka kwalifikacji

The holder of the qualification "Reliability and cyber security management for equipment and technology in industry" independently implements a risk prevention plan for equipment and technology in the enterprise. Has knowledge of reliability and cybersecurity as well as national and European legal regulations in these areas. Uses techniques of hazard analysis and risk analysis, e.g. HAZOP (Hazard and Operability Study), FMEA. Uses IT and OT systems in the company"s business and operational processes. Develops elements of the IT / OT diagram. Defines requirements for technical solution providers. Identifies the location of a security breach in the technological area after an effective cyber attack. Draws up a record of the effects of a cyber attack in hardware. Creates scenarios for corrective action and restoration of hardware operation.

Informacje o kwalifikacji

Informacje dodatkowe

Kod ISCED

0714 - Elektronika i automatyka

Kod kwalifikacji (od 2020 roku)

40869

Efekty uczenia się

Syntetyczna charakterystyka efektów uczenia się

The holder of the qualification "Reliability and cyber security management for equipment and technology in industry" independently implements a risk prevention plan for equipment and technology in the enterprise. Has knowledge of reliability and cybersecurity as well as national and European legal regulations in these areas. Uses techniques of hazard analysis and risk analysis, e.g. HAZOP (Hazard and Operability Study), FMEA. Uses IT and OT systems in the company"s business and operational processes. Develops elements of the IT / OT diagram. Defines requirements for technical solution providers. Identifies the location of a security breach in the technological area after an effective cyber attack. Draws up a record of the effects of a cyber attack in hardware. Creates scenarios for corrective action and restoration of hardware operation.