Critical Infrastructure Protection and Resilience: Interdependencies and Essential Services

17 – 21 May 2027
London - Central London four-star



Critical Infrastructure Protection and Resilience: Interdependencies and Essential Services

Ref: 309_12390 **Date:** 17 – 21 May 2027 **Location:** London - Central London four-star **Fees:** 23000 SAR

Introduction:

Critical infrastructure protection fails at the seams between operators: a grid fault stops water pumping, a telecom outage blinds rail signalling, and a hospital loses both at once. Plans written for one site rarely see these cascades. This Core Concept course equips operators of energy, water, transport, telecom and health networks to map dependencies across sectors, assess risk on an all-hazards basis, locate single points of failure across networks, engineer redundancy and recovery, and coordinate with public bodies and peer operators. Participants build a Cross-Sector Interdependency Map and Essential Service Resilience Plan.

Course Objectives:

- Map upstream and downstream dependencies of an essential service across energy, water, transport, telecommunications and health networks and trace cascading failure paths
- Assess risk on an all-hazards basis covering natural, technical and malicious scenarios at the level of networks and services rather than single sites
- Rank network nodes and links by criticality and expose single points of failure and common-mode weaknesses shared with other operators
- Specify resilience engineering measures that combine redundancy, diversity, graceful degradation and recovery sequencing for a service network
- Structure public-private coordination, trusted information sharing and joint exercises with authorities and interdependent operators
- Define resilience indicators and a review cycle that show whether an essential service can withstand, absorb and recover from disruption

Target Audience:

- Resilience and emergency preparedness leads who coordinate protection arrangements for an essential service network
- Enterprise and operational risk leads who own the risk register of an infrastructure operator
- Security leads who oversee physical and cyber-physical protection across dispersed assets such as substations, pumping stations, exchanges and depots
- Network operations and control centre leads who manage service restoration after large-scale outages
- Coordinators in public bodies who liaise with operators on sector planning, information sharing and national exercises
- Asset and engineering leads who plan capital investment in redundancy, diversity and hardening

Course Outline:

Day 1: Critical Infrastructure Sectors, Essential Services and Interdependencies

- Critical Infrastructure Definitions and Sector Taxonomies Compared Across Jurisdictions
- Essential Service Catalogue: Outputs, Service Levels and Populations Served
- Physical, Cyber, Geographic and Logical Interdependency Types
- Cascading and Escalating Failure Patterns Between Power, Water, Telecom and Transport
- System-of-Systems Current-State Review of an Operator's Protection Arrangements

Day 2: All-Hazards Risk Assessment and Criticality Analysis for Networks

- All-Hazards Scenario Library: Natural, Technical, Human Error and Malicious Events for Defensive Planning
- Consequence Scaling by Population, Duration, Geography and Cross-Sector Spill-Over
- Network Criticality Scoring for Nodes, Links and Control Centres
- Single Point of Failure and Common-Mode Dependency Identification Across Operators
- Sector Risk Profile and Risk Heat Map Construction for a Service Network

Day 3: Protection Layers and Resilience Engineering

- Protection Overview for Dispersed Assets: Deter, Detect, Delay and Respond at Network Scale
- Cyber-Physical Convergence: Governance of Operational Technology and Control System Dependencies
- Redundancy, Diversity and Separation Design: N-1 Thinking, Alternate Routes and Diverse Suppliers
- Graceful Degradation and Load Shedding Priorities for Essential Users
- Restoration Sequencing, Black Start Dependencies and Mutual Aid Arrangements

Day 4: Public-Private Coordination, Information Sharing and Hard Cases

- Sector and Government Coordinating Council Model and Operator Security Plan Structure
- Trusted Information Sharing: Classification, Handling Rules and Early Warning Channels
- Compound and Concurrent Events: Heatwave With Grid Stress and Communications Loss
- Supply Chain and Third-Party Concentration Risk in Shared Infrastructure Services
- Resilience Indicators: Withstand, Absorb, Recover and Adapt Measures With Maturity Scales

Day 5: Cross-Sector Exercise and the Essential Service Resilience Plan

- Discussion-Based Tabletop Exercise: Regional Power Outage Cascading to Water and Health Services
- Operations-Based Drill Design: Objectives, Injects, Controllers and Evaluation Criteria
- After-Action Review and Improvement Plan Tracking Across Partner Operators
- Cross-Sector Interdependency Map and Essential Service Resilience Plan Drafting
- Peer Panel Challenge of Resilience Investment Priorities

Skills You Will Gain:

- Interdependency Mapping
- All-Hazards Scenario Development
- Network Criticality Analysis
- Common-Mode Failure Detection
- Resilience Engineering Design
- Restoration Priority Setting
- Cross-Sector Exercise Design
- Resilience Performance Measurement

Why Attend This Course:

- Return with a Cross-Sector Interdependency Map and Essential Service Resilience Plan for a service network you are responsible for
- See the cascades and shared weak points that single-site security studies and continuity plans leave out
- Rehearse a cross-sector outage under time pressure alongside peers from energy, water, transport, telecom and health
- Make a stronger case for investment in redundancy and diversity with criticality scores and resilience indicators

Conclusion:

Protecting critical infrastructure depends on seeing each service as part of a wider system whose failures travel across sector boundaries. The course moves from sector definitions and interdependency types, through all-hazards risk assessment and network criticality analysis, to protection layers, cyber-physical governance and resilience engineering. It then addresses coordination with public bodies, information sharing, compound events and resilience measurement. The final day runs a cross-sector exercise and produces a Cross-Sector Interdependency Map and Essential Service Resilience Plan.