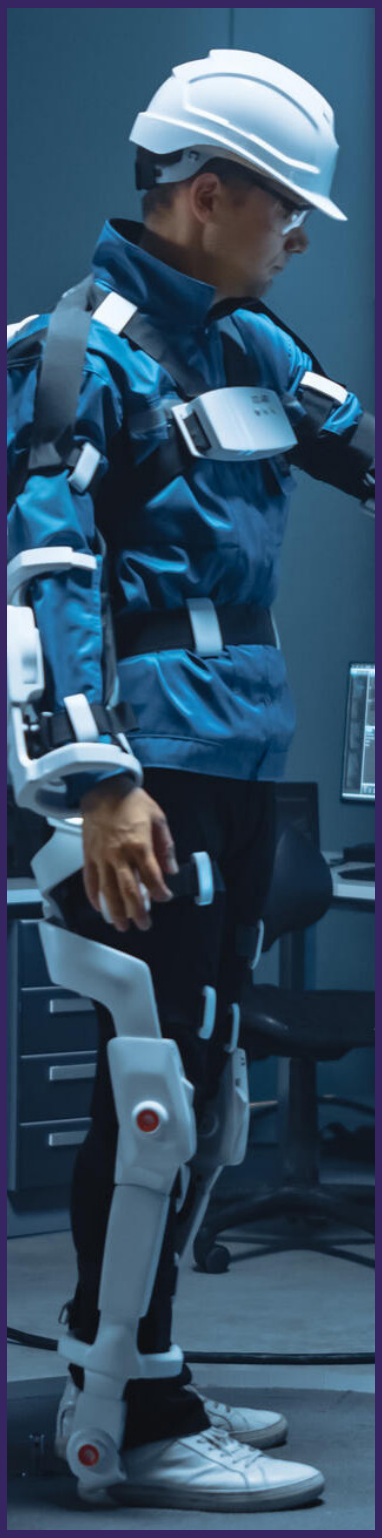
ROBOTICS & AI FOR GRID VIGILANCE AND WORKFORCE SAFETY



e·on

Infosys®
Navigate your next

Table of Contents

1. Executive Context and the Core Problem....3
2. Problem Statement....4
   - Cluster 6: Fortifying Grid Safety, Vigilance, and Resilience....4
   - Cluster 7: Targeted Automation for Workforce Safety and Augmentation....4
   - The Problem Space....4
   - Considerations/ Guardrails for the solution....5
   - Desired Outcomes....5
3. Expected Impact. How big is the problem....6
4. Criteria for All Challenges....7

Executive Context and the Core Problem

Improving Safety, Vigilance, and Resilience of Grids

Europe's energy networks are entering a phase of unprecedented operational stress. Grid expansion, renewable integration, and rising reliability expectations collide with structural constraints. In this context, vigilance, safety, and resilience are no longer optional improvements—they are prerequisites for maintaining secure and resilient network operations.

Emerging capabilities in robotics and Physical AI offer a promising pathway to address these challenges. By enabling intelligent machines to perceive, reason, and act within complex physical environments, these technologies can enhance inspection and monitoring capabilities across grid assets and improve the overall efficiency and resilience of energy network operations.

Targeted Automation to Improve Health and Safety of Field Workers and Augment Shrinking Technical Workforce

Structural workforce constraints are colliding with the increasing demands of modern energy networks. In this environment, targeted automation is a prerequisite for maintaining operations.

Robotics and Physical AI can automate high-risk and repetitive maintenance tasks, directly improving the health and safety of field workers. When strategically deployed, these technologies augment the existing workforce and reduce operational risk, providing a necessary solution to the shrinking technical labor pool.

Problem Statement

Design, develop, and evaluate autonomous systems—including Physical AI and robotics—to address one of the following two strategic pillars for European energy networks:

Cluster 6: Fortifying Grid Safety, Vigilance, and Resilience

We seek innovations that enhance the vigilance and resilience of grid infrastructure. Proposals should focus on providing a resilient shield against physical and cyber-physical attacks, improving asset and substation environment monitoring, and ensuring the continuous stability of the network under operational stress.

Cluster 7: Targeted Automation for Workforce Safety and Augmentation

We seek solutions that leverage targeted automation to improve the health and safety of field workers. Proposals should focus on augmenting the shrinking technical workforce by automating high-risk, repetitive maintenance tasks and supporting technicians navigating complex, high-risk power environments.

1. The Problem Space

Energy networks across Europe face a converging set of pressures in the areas as elaborated below:

Vigilance

Vigilance is the ability of a system to maintain persistent, high-fidelity observability and situational awareness across vast and often remote geographical areas. As grids become more decentralized with renewable inputs, the surface area for potential attacks expands, making it humanly impossible to monitor every node in real-time.

There is a "data-action gap": traditional monitoring relies on fragmented sensors or manual inspections that are too slow to detect sophisticated physical tampering or rapid cascading failures. Blind spots occur where physical or cyber-physical threats can go undetected for critical windows of time.

This is compounded by environmental complexity. High-risk energy environments are often "noisy" or hazardous, making it difficult for standard automated systems to differentiate between environmental interference and genuine security breaches. True vigilance, therefore, requires systems that can not only observe anomalies but also interpret them contextually - distinguishing between a routine equipment wear-and-tear and a coordinated strike on the network's integrity.

Resilience

Resilience refers specifically to the physical and operational ability of the grid to withstand external interference and sabotage. European energy infrastructure is often exposed and geographically dispersed, making them physically vulnerable for low-tech but high-impact attacks, such as the deliberate throwing of conductive objects onto overhead lines or the physical breaching of substations, as seen in recent incident 011 and incident 022 in Berlin. Attribution and response are also challenges, making it difficult to identify the source of a physical disruption in real-time to prevent "copycat" or coordinated multi-point attacks. True resilience would involve moving beyond fences and cameras toward autonomous systems that can actively patrol and protect high-risk assets.

Health & Safety of human workforce

Safety is the mandate to reduce or eliminate human exposure to high-risk tasks in energy networks. Field workers in Europe currently perform manual inspections and repairs in proximity to high-voltage equipment, often under extreme weather or operational stress, where a single oversight can be fatal.

Increasing safety would involve reducing hazardous proximity or the need for "hands-on" contact with energized components through remote manipulation, mitigating situational blindness eg. by providing field teams with real-time augmented means to detect invisible threats like gas leaks, structural fatigue, or electrical discharge and incorporating emergency response by using autonomous systems to assess damage before a human enters a potentially unstable site.

Targeted Automation

Targeted Automation refers to the strategic deployment of robotics and AI to address high-impact, repetitive, and precision-critical tasks that currently create operational bottlenecks in energy grid operations. Rather than focusing on broad, generic automation, this approach emphasizes the "surgical" integration of intelligent robotic systems into Europe's existing and aging energy infrastructure to help compensate for the shrinking technical workforce.

A key application is the automation of the "last mile" of maintenance activities—such as bolt tightening, debris removal, inspection, or cable handling—where high precision and reliability are required. These systems can execute tasks with sub-millimeter accuracy while operating consistently in challenging environments.

In addition, targeted automation eliminates or significantly reduces the need for human interaction with live energy systems, where operational risks are inherently high. By deploying robotic platforms designed with task-specific mobility, reach, and degrees of freedom, hazardous operations can be performed more safely, improving both workforce safety and operational efficiency.

2. Considerations/ Guardrails for the solution

All automation and assistance initiatives should align with the following guiding principles:

- Augment, not replace the workforce: Technology should support existing workers by enhancing their capabilities and productivity rather than replacing them. Automation should primarily serve as a safety and productivity enabler.
- Eliminate repetitive and inefficient tasks: Focus on automating routine, labour-intensive activities that consume valuable human resources.
- Reduce operational risk: Prioritize solutions that minimize human exposure to hazardous environments and high-risk operational tasks.

3. Desired Outcomes:

Level One (TRL 2 – Technology Concept Formulated):

The concept must be defined through a problem statement, planned solution with clear basic architecture, including block and/ or state diagrams. Where feasible, the idea should be evaluated using simulation tools (backed by Robot learning/AI algorithms) to validate first feasibility and core assumptions. Based on the nature of your solution (hardware, pure software, or AI algorithm-based), please consider the following listed parameters and constraints as guidance:

1. **Technical Parameters and Success Metrices:** Please describe the specific technical parameters and KPIs your solution aims to achieve

- Detection Performance: Detect anomalies within <5–10s with >90% target accuracy and <10% false positives (simulation-based at TRL-2).
- AI & Edge Processing: Enable real-time edge AI (<2s latency) with >70% local decision-making and contextual threat classification.
- Robotics & Autonomy: Operate with supervised autonomy, achieving >85% mission success and >95% obstacle avoidance (simulated).
- Grid Interaction: Safely operate near HV assets (IEC-compliant), detecting thermal deviations and intrusions, improving inspection frequency by 3–5x.
- Communication: Ensure <1–2s alert latency via hybrid connectivity (4G/5G + edge fallback) with secure data handling.
- Reliability: Target >95% availability with robust performance under simulated environmental and EMI conditions.

2. **Operational Constraints:**

- Electrical Environment: The system must operate safely across LV (<1 kV), MV (1–60 kV), and HV (>60 kV) environments, withstanding strong electromagnetic interference (EMI), partial discharge, corona effects, and ground potential rise risks.
- Environmental Conditions: The solution must function reliably in outdoor conditions ranging from –20°C to +50°C, including exposure to rain, snow, fog, ice, dust, and vegetation, with capability for night operations and (for aerial systems) wind tolerance up to ~10–15 m/s.
- Physical Infrastructure Constraints: The system must navigate and operate within complex grid environments including dense substations, remote overhead lines, and constrained underground assets, handling narrow access zones, obstacles, and signal reflections from metallic structures.
- Connectivity Constraints: The solution must handle limited or no network coverage by enabling edge autonomy (offline operation), intermittent synchronization with central systems, and integration with legacy SCADA infrastructure.
- Safety & Regulatory Constraints: The system must comply with IEC standards for high-voltage proximity and HSE "Vision Zero" principles, ensuring fail-safe behavior including safe shutdown near humans, emergency stop functionality, and zero interference with grid operations.

- Cyber & Physical Security Constraints: The solution must ensure secure communication (protection against spoofing/hacking), resilience against physical tampering, and robust identity and access control for remote operation.
- Level Two (TRL 4 – Technology Validated in Lab):
  The concept must be realised through initial or rapid prototype components that demonstrate the core functionality and validate key technical principles.
- Level Three (TRL 5 + – Technology Demonstrated in Relevant Environment)**:** A prototype must be developed and tested in a relevant operational or field environment that closely reflects the intended real world use case and be ready for deployment at the end of testing.
- Cross-cutting requirement: Across all maturity levels, solutions must be designed with European energy grid requirements and standards as the primary reference, while ensuring compatibility with global energy system standards where applicable.
- Business impact and viability requirements:

To demonstrate the viability and value of your solution, please address the following:

- Commercial Potential: Present a robust business case, including market sizing and scalability for Distribution System Operator (DSO) adoption in Europe.
- Value Proposition: Detail the quantitative (e.g., cost savings, efficiency gains) and qualitative (e.g., regulatory compliance) benefits for the DSO.
- Scalability:

Solutions must be scalable and "interoperable by design," ensuring that robotic hardware and AI models can be deployed across diverse European grid architectures without requiring bespoke re-engineering for each Member State. Ideas should ensure:

- Standardized Interfaces: Using open communication protocols (like IEC 61850, MODBUS, etc) so the AI can "talk" and interact to different brands of grid hardware.
- Environmental Adaptability: Ensuring robotics can operate in varying climates—from Arctic humidity to Mediterranean heat.
- Regulatory Compliance: Designing for the "highest common denominator" of safety and data privacy laws (GDPR/AI Act) to ensure the solution is legally scalable across borders.

Resource Estimate: A rough breakdown of the hardware, software, and personnel required to move from concept to a functional prototype(TRL 06).

4. Expected Impact. How big is the problem.

The scale of the crisis facing Europe's energy networks is defined by a "triple threat" of aging infrastructure, a critical workforce deficit, and an escalating landscape of hybrid warfare. Over 30% of Europe's power lines and transformers are now more than 45 years old3. In 2025 alone, "grey zone" attacks on energy infrastructure—such as the severance of subsea interconnectors and physical incursions—resulted in over €17 billion in damages4.

Furthermore, the industry is hitting a "demographic wall": for every new entrant into the grid technical workforce, 2.4 experienced workers5 are approaching retirement. This talent gap directly threatens the reliability of the grid as it integrates decentralized renewables.

The Expected Impact if Solved: Successfully deploying autonomous vigilance and targeted automation would transform the grid from a passive, fragile network into a self-defending, resilient ecosystem.

Economic Security: Enhancing grid resilience to prevent large-scale outages safeguards the European economy against billions of Euros in direct damages, systemic productivity losses, and the prohibitive 'Value of Lost Load' (VoLL) incurred by energy-intensive industries.

Workforce Multiplier: Targeted robotics would allow a shrinking pool of specialists to supervise ten times the current maintenance volume while achieving a zero-harm environment by removing humans from live-energy interfaces.

Geopolitical Resilience: Proactive AI-driven vigilance could detect and neutralize physical sabotage in the "critical first minutes," preventing localized incidents from spiralling into continent-wide systemic failures.

Criteria for All Challenges

1. Transferability and Scalability in Europe and Globally

The proposal must be transferable and scaleable to Europe and globally. Scalability within India is nice-to-have but not mandatory.

a. Explicit transferability to Europe (mandatory)

- Clear explanation of how the solution can be adapted to European regulatory[1], market, and customer contexts
- Identification of required modifications (e.g. standards, cost structure, integration)

b. Global scalability potential (mandatory)

- Core concept is not India-specific in its fundamentals
- Demonstrates relevance to other markets facing similar constraints

c. Scalable within India (good to have)

- Clear pathway from pilot to large-scale deployment
- Addressable market size and adoption drivers identified
- Key customer(s)/segments identified

2. Leverages Strengths of the Indian Innovation Landscape

Proposals must demonstrate a strong alignment with India's proven innovation strengths:

- **Cost efficient engineering:** The idea leverages engineering approaches that minimize cost without compromising essential functionality.
- **Frugal innovation mindset:** The solution delivers high value with limited resources and avoids unnecessary complexity.
- **Constraint-driven creativity:** The proposal explicitly shows how constraints related to cost, infrastructure, skills, or system complexity have informed the design.

3. Practicality and Rapid Deployability

The idea must be suitable for rapid validation and deployment in the coming 12 to 18 months in a large, diverse markets in the EU and globally, and as a good-to-have, India:

- Addresses a clearly identifiable real-world problem.
- Demonstrates usability in environments with varying levels of infrastructure maturity.
- Shows evidence that the solution can be tested, piloted, or scaled without long development cycles.

4. Solution Quality Requirements

All submitted solutions must meet the following non-negotiable design principles:

a. Simple

- Clear core functionality
- Minimal dependencies
- Easy to understand, use, and maintain

b. Robust

- Reliable under variable operating conditions
- Tolerant to imperfect infrastructure or user behavior
- Low maintenance requirements

c. Affordable

- Cost structure suitable for price-sensitive markets for EU and global markets and optionally, Indian markets
- Transparent assumptions on production, deployment, and operating costs, presented in the form of estimates for Total Cost of Ownership (TCOs) or techno-economic assessments

Overall proposed ideas will be measured on how they fare on three "I's"

- **Innovation:** novelty, competitive differentiation, translation across markets (EU, global, India)
- **Implementation:** adoption risks, co-innovation risks, regulatory hurdles, time to deploy, time to mature market
- **Impact:**
  - how much you can make - serviceable addressable market size (% of TAM)
  - how much you can save – resilience, robustness, reliability

Participants should ensure ideas are in broad alignment with European regulations. Guidance can be provided by E.ON on request on more specific details of European regulations.

For more information, contact askus@infosys.com

Navigate your next