F. No. 353/65/2026-Green Hydrogen
Government of India
Ministry of New and Renewable Energy
(Hydrogen Division)

Atal Akshay Urja Bhavan, Lodhi Road,
New Delhi – 110 003
Date: 25th November, 2026

OFFICE MEMORANDUM

Subject: Cybersecurity of control and communication systems (SCADA/ICS) in electrolysers – circulation of concept note for preliminary stakeholder consultation – invitation for comments – regarding.

1. The undersigned is directed to circulate the enclosed concept note titled "Cybersecurity of Control and Communication Systems (SCADA/ICS) in Electrolysers", prepared by the Green Hydrogen Division of this Ministry, for preliminary stakeholder consultation.

2. No cybersecurity framework presently applies to electrolysers, or to the systems integral to their operation, as a category of equipment in their own right. The enclosed concept note sets out the current regulatory position, the considerations bearing on the need for a standard, and a set of principles on which the views of stakeholders are sought at this preliminary stage.

3. Stakeholders are requested to furnish written comments, addressing in particular the consultation questions at Annexure A to the concept note, within 30 days of the date of issue of this Office Memorandum, indicating the category of respondent and the principle or question to which each comment relates.

4. Comments may be forwarded by electronic mail to pmu-gh2@gov.in.

This issues with the approval of the competent authority.

(Dr. Prasad A. Chaphekar)
Director
Email: prasad.chaphekar@gov.in

Encl: Concept note, as above.

Copy for information to:

1. PPS to Secretary, MNRE

2. NIC Cell, MNRE – with a request to upload this Office Memorandum and the enclosed concept note on the Ministry's website.

ANNEXURE - I

Government of India
Ministry of New and Renewable Energy
Green Hydrogen Division

CONCEPT NOTE

Cybersecurity of Control and Communication Systems (SCADA/ICS) in Electrolysers

Preliminary Stakeholder Consultation

1. Background

The Central Electricity Authority has notified the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, in the Gazette of India on 31 July 2026, under section 177 read with section 73(c) of the Electricity Act, 2003, with the concurrence of the Ministry of Electronics and Information Technology. These regulations apply to entities owning, operating or managing operational technology infrastructure connected to the interconnected power system and interconnected information technology systems, and cover generating companies, captive generating plants and energy storage systems of fifty megawatts capacity or more, together with power exchanges and over-the-counter trading platforms. They establish requirements relating to governance, segregation of operational technology from information technology and public networks, supply chain security, control of vendor and third-party access, incident reporting to the Computer Security Incident Response Team for the Power Sector, auditing, and retention of data within India.

Electrolysers increasingly rely on supervisory control and data acquisition (SCADA) systems, programmable logic controllers and associated communication infrastructure for monitoring and control of process and electrical parameters, and are frequently connected to the grid. An electrolyser, being a consuming load, falls within the regulations referred to above only where it is co-located with generation or energy storage capacity meeting the applicable threshold. No cybersecurity framework presently applies to electrolysers, or to the power conversion, fire and gas, hydrogen detection and safety instrumented systems integral to their operation, as a category of equipment in their own right.

This note places that position before stakeholders and seeks preliminary views on the principles that would be relevant to a cybersecurity standard for electrolyser control and communication systems and directly associated systems, should such a standard be developed.

2. Purpose and Scope

This note seeks preliminary views from stakeholders on the principles that should inform a cybersecurity standard for control and communication systems used in electrolysers, comprising SCADA systems, distributed control systems, programmable logic controllers, human machine interfaces, engineering workstations, data historians, associated network infrastructure, and the interfaces of these systems with external parties.

This note extends also to systems ordinarily supplied and commissioned as part of the electrolyser package and integral to the safe production of hydrogen, namely power

conversion and rectification equipment, fire and gas detection systems, hydrogen detection instrumentation, and safety instrumented systems, to the extent that the cybersecurity of these systems is not addressed by the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026.

This note extends further to utilities and balance of plant systems associated with the electrolyser, including feedwater treatment, cooling, compressed air and diagnostic monitoring systems, to the extent that their compromise can affect the safe operation, safe shutdown or availability of the electrolyser.

This note does not constitute a draft standard or a draft regulation. Its purpose is limited to setting out the applicable regulatory position, the considerations bearing on the need for a standard, and a set of principles on which views are sought before further work is undertaken.

This note does not address the cybersecurity of electrical infrastructure, generation assets, energy storage systems or renewable energy assets to the extent that such infrastructure or assets fall within the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026. Where such infrastructure or assets are co-located with, or interface with, an electrolyser installation without falling within that framework, the interface between them and the electrolyser control system falls within the scope of this note and is addressed at Principle H.

This note is confined to electrolysers and the systems referred to above. Cybersecurity considerations relating to hydrogen storage, compression, transport and refuelling infrastructure raise related but distinct questions and are not addressed here.

3. Current Regulatory Position

Electrolyser operators are presently subject to the general cybersecurity obligations applicable to all body corporates under the Information Technology Act, 2000, administered through the Indian Computer Emergency Response Team. These obligations, under the directions issued by the Indian Computer Emergency Response Team on 28 April 2022, principally comprise reporting of specified cyber security incidents within six hours of their being noticed, maintenance of information and communication technology system logs within India for a rolling period of 180 days, and synchronisation of system clocks with the Network Time Protocol servers of the National Informatics Centre or the National Physical Laboratory.

These obligations are framed for information and communication technology systems generally. They address the reporting of incidents and the preservation of evidence after an incident has been detected. They do not address the architecture of control systems, segregation between control networks and enterprise networks, vetting of control system hardware and firmware, control of vendor access to control systems, or the interaction between cybersecurity measures and process safety systems.

The Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, referred to at paragraph 1 above, apply to entities owning, operating or managing operational technology and interconnected information technology systems in the power sector, including generating companies, captive generating plants and energy storage systems of fifty megawatts capacity or more. An electrolyser, being a consuming load, falls within that framework only where it is co-located with generation or storage capacity meeting the applicable threshold. Connection to the grid does not by itself bring an electrolyser within the scope of those regulations. Where a facility does fall within that framework, the cybersecurity of the co-located generation or storage capacity, and of the associated electrical infrastructure, is addressed by those regulations and is accordingly not further addressed in this note.

Requirements relating to the architecture, governance, supply chain and data handling of control and communication systems specific to electrolysers, and of the power conversion, fire and gas, hydrogen detection and safety instrumented systems integral to their operation, as a category of equipment, therefore remain to be defined.

4. International Practice

The following is set out for information and is not intended as a comparative assessment.

The Network and Information Security Directive of the European Union designates hydrogen production, storage and transmission as part of the energy sector, and subjects operators meeting defined thresholds to risk management and incident reporting obligations enforceable through administrative penalties.

The critical infrastructure framework of Germany extends resilience and associated cybersecurity obligations to power-to-gas facilities above a defined annual production threshold, applying the general critical infrastructure regime rather than a hydrogen specific instrument.

In the United States, guidance for operational technology security is issued on a voluntary basis and applies to industrial control systems generally. Mandatory cybersecurity requirements exist for certain pipeline and bulk power system entities, but do not presently extend to electrolysers. Published work on hydrogen infrastructure cybersecurity records the absence of hydrogen specific standards and identifies this as a gap.

The IEC 62443 series provides an international framework for the security of industrial automation and control systems, structured around zones and conduits, defined security levels, and seven foundational requirements covering identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events and resource availability. ISO/IEC 27019 addresses information security controls for process control systems in the energy sector. IEC 61511, the functional safety standard for the process industry, requires a security risk assessment to be carried out to identify security vulnerabilities of the safety instrumented system, and requires the design to provide resilience against the risks so identified. These standards are technology neutral and apply on a voluntary basis unless adopted through national law, regulation or contract.

No jurisdiction reviewed has issued a cybersecurity standard specific to electrolysers as a distinct category of equipment. The international committees responsible for hydrogen technologies and fuel cell technologies have not published a cybersecurity standard for electrolysers.

Preliminary stakeholder responses have indicated a preference for the IEC 62443 series as the principal reference framework for the cybersecurity of electrolyser control systems. Stakeholders may comment on the same.

5. Considerations Bearing on the Need for a Standard

Eight considerations are placed before stakeholders.

5.1 Process safety consequence. Electrolysis produces hydrogen and oxygen simultaneously, and the separation of the two streams is maintained by the control of pressure differentials, temperature, current density, purging sequences and the integrity of gas separation equipment. Manipulation of setpoints, interlock logic, valve actuation sequencing or instrument readings through the control system can result in conditions relevant to safety, including conditions bearing on the fire and gas detection and safety instrumented systems that provide protection against

such conditions. The consequence of a compromise is therefore not confined to loss of data or interruption of service.

5.2 Grid facing consequence. Large electrolysers constitute substantial controllable electrical loads, and are increasingly operated flexibly in response to renewable generation, price signals or system conditions. Coordinated, malicious or unauthorised alteration of load setpoints across a number of facilities, whether through direct compromise or through compromise of a scheduling or aggregation interface, can produce rapid aggregate demand variation of relevance to system operation. This consequence arises from the electrolyser as a load, and is distinct from the consequences addressed by the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026 applicable to generation, storage and network entities. Where an electrolyser is co-located with generation, storage or renewable energy assets, the interface between the electrolyser control system and those assets presents a related consequence distinct from the cybersecurity of the co-located assets themselves.

5.3 Connectivity and external dependency. Electrolyser control systems are commonly supplied with remote monitoring, diagnostic and performance optimisation functions operated by the equipment manufacturer or system integrator, in several cases hosted outside India. Guarantee and warranty arrangements frequently depend on continuity of such connectivity. This establishes a persistent external interface into the control system of the facility.

5.4 Concentration of supply. A significant proportion of electrolyser stacks, power conversion equipment and control system components deployed in India is imported, and the associated firmware and software is developed outside India. The provenance of components and the integrity of firmware are therefore material to the security of the installed base.

5.5 Stage of deployment. Substantial electrolyser capacity is presently at the design, procurement and construction stage. Security requirements incorporated at the design stage are materially less costly to implement than those retrofitted to commissioned plant, particularly where control system architecture, network segregation and component selection are concerned.

5.6 Concentration of platform risk. Remote monitoring, diagnostic and optimisation functions referred to at paragraph 5.3 are frequently provided through infrastructure common to a number of electrolyser installations of the same manufacturer, system integrator or service provider. Compromise of such shared infrastructure is capable of producing simultaneous consequences across installations that are otherwise independent of one another, a consequence distinct in kind from compromise confined to a single facility.

5.7 Automated and model based optimisation. Electrolyser control systems increasingly incorporate automated, model based or artificial intelligence assisted functions for the optimisation of setpoints, dispatch and operating parameters. Erroneous or manipulated output from such functions is an additional pathway, distinct from direct compromise of the control system, by which the process safety and grid facing consequences described above may arise.

5.8 Cyber induced degradation of equipment. Manipulation of operating parameters, including current ramp rates, current pulsing, and temperature and pressure limits, within the thresholds at which alarms and trips operate, can accelerate the degradation of electrolyser stacks and associated components without producing an identifiable safety event. The consequence is loss of asset life and performance, including in electrolysers supported through public programmes.

6. Principles

The principles set out below are placed before stakeholders for comment. They are drawn in part from the power sector cybersecurity framework and from the general cybersecurity directions in force, adapted to the characteristics of electrolysers, and in part from established practice in industrial control system security and process safety. They are stated at the level of principle and are not intended as draft technical or legal provisions. Certain principles state a proposal, introduced by the words “it is proposed”, reflecting preferences indicated in preliminary stakeholder responses. These proposals are placed before stakeholders for comment, and views on them remain invited.

A. Governance, Accountability and Competence

A.1 Responsibility for the cybersecurity of control and communication systems should be assigned to an identified position within the operating organisation, distinguished from responsibility for enterprise information technology security, reflecting the different risk profile, operating constraints and consequence of failure of control systems.

A.2 Cybersecurity risk arising from control systems should be assessed and reviewed at a level of the organisation with authority to allocate resources for remediation, and should be recorded in a form that permits review.

A.3 Personnel with responsibilities relating to the operation, maintenance, engineering or security of control systems should possess demonstrated competence appropriate to industrial control system environments, and such competence should be maintained through periodic training.

A.4 Coordination should be maintained between the position or function assigned responsibility under Principle A.1 and the function responsible for the routine operation and maintenance of control and communication systems, so that the assignment of a distinct cybersecurity responsibility does not remove accountability from those routinely operating the systems concerned.

B. Risk Assessment and Assignment of Security Levels

B.1 Security requirements applicable to a facility should follow from a documented risk assessment addressing the consequences of compromise, rather than from a uniform prescription applied irrespective of the configuration and consequence profile of the facility.

B.2 The risk assessment should be conducted in conjunction with, and should take as input, the process hazard analysis for the facility, so that cybersecurity scenarios capable of defeating or degrading protective functions are identified against the hazards those functions address.

B.3 The risk assessment should be repeated on material modification to the control system, the process configuration or the external interfaces of the facility, and at a defined periodicity irrespective of modification.

C. Architecture and Network Segregation

C.1 Control and communication systems, including power conversion and rectification equipment forming part of the control system, should be segregated from enterprise information technology networks and from public networks. Any interconnection required for operational purposes should be routed through a defined, minimal and monitored boundary, and the interfaces so established should be documented.

C.2 Within the control system, further segmentation by function and criticality should be adopted, with communication between segments permitted only through defined pathways carrying only the traffic necessary for operation.

C.3 Data flows required for monitoring, reporting or analysis should so far as practicable be unidirectional outward from the control system, so that the existence of a monitoring interface does not by itself establish a path for the introduction of commands.

C.4 A current inventory of control system hardware, firmware, software, network components and external connections should be maintained, as a precondition for risk assessment, vulnerability management and incident response.

C.5 Components and systems that have reached the end of vendor support should be identified, and either replaced or subjected to compensating controls under a documented plan.

C.6 Physical access to control system equipment, including controllers, network equipment, engineering workstations and cabling, should be restricted and controlled, physical access being a means of defeating logical controls.

D. Identity, Access and Use Control

D.1 Every entity accessing the control system, whether a person, a device, a software process or an interfacing system, should be identified and authenticated before access is granted, and shared or generic credentials should be avoided for functions capable of altering process state.

D.2 Access should be granted at the minimum privilege necessary for the function performed, and the ability to alter setpoints, control logic, interlock configuration or protective function parameters should be separately controlled from the ability to observe process state.

D.3 Default credentials supplied with equipment should be changed before the system is placed in service, and the design should not depend on credentials that cannot be changed by the operator.

D.4 The connection of removable media and transient devices, including maintenance laptops, portable programming devices and storage media, to the control system should be controlled, such devices being an established means by which segregation is defeated.

D.5 Programmable logic should be developed, configured and maintained under secure programming practice, including protection of the functions by which control logic is uploaded to or downloaded from a controller, controlled modification of safety interlock logic, and verification of control logic prior to deployment.

E. Supply Chain, External Access and Jurisdictional Control

E.1 Procurement of hardware, firmware and software forming part of control and communication systems should be preceded by a documented supply chain risk assessment, addressing the provenance of components, the security development and vulnerability disclosure practices of the supplier, the arrangements for support during the operating life of the equipment, and the arrangements for notification by the supplier of incidents and vulnerabilities affecting the supplied product. The assessment and its conclusions should be recorded, and should inform the terms on which the equipment is procured.

E.2 The integrity and authenticity of firmware and software, both as supplied at installation and as supplied by way of update during the operating life of the

equipment, should be verified before installation, by means established at the time of procurement. Where means of verification are not available in respect of a particular component, the limitation and the compensating controls applied should be recorded.

E.3 Remote access to control systems by equipment manufacturers, system integrators, service providers or other external parties, including for diagnostic, maintenance or optimization purposes, should be through defined, time bound, individually authenticated and logged channels employing multi factor authentication, subject to monitoring or recording of the session, initiated or authorized by the operator, and should not take the form of standing, unsupervised or persistently open access.

E.4 The capability to exercise control functions of the electrolyser, being the capability to alter setpoints, operating parameters, control logic or protective function configuration, should not be exercisable from outside India, whether directly or through a platform operated by a supplier, otherwise than under a defined and auditable mechanism of authorization by the operator within India.

E.5 Where control system functions, monitoring functions or process data processing are hosted on infrastructure not under the direct control of the operator, including infrastructure common to other installations of the same manufacturer, system integrator or service provider, the location of that infrastructure, the extent to which it is shared with other installations, and the legal regime governing access to it should be identified and addressed within the risk assessment of the facility.

E.6 Commercial arrangements, including warranty and performance guarantee arrangements, should not be structured so as to require the operator to maintain external connectivity or external access inconsistent with the principles above.

F. Data, Logging and Localisation

F.1 In addition to the log categories required generally under the law in force, records specific to control systems should be captured, including configuration and control logic changes, access to engineering workstations and human machine interfaces, alarm and interlock activations, setpoint changes, and firmware and software update events.

F.2 Process and control system data of an electrolyser should be stored within India, extending to control system records the localisation principle already applied to information and communication technology logs under the law in force.

F.3 Records should be time synchronized to a common and reliable time source, and should be retained in a manner resistant to alteration, so that the sequence of events preceding and during an incident can be reconstructed.

F.4 Retention periods should be sufficient to support investigation of incidents that are detected after an interval, incidents affecting control systems frequently being detected substantially after initial compromise.

G. Interface between Cybersecurity and Process Safety

G.1 Cybersecurity measures should be assessed jointly with the process safety arrangements of the facility, and should not degrade the availability or the response time of functions on which safety depends. Where a cybersecurity measure and a safety function are in tension, the resolution should be recorded and justified.

G.2 Safety instrumented systems performing shutdown, isolation, venting and hazard mitigation functions, including fire and gas detection systems and hydrogen

detection systems, should be independent of the control system used for routine operation, in respect of their logic solvers, communication paths and access arrangements, so that compromise of the control system does not by itself defeat the protective function.

G.3 Instrumentation on which protective functions depend, including hydrogen concentration measurement, differential pressure measurement, temperature measurement, cell voltage measurement and water conductivity measurement, should be protected against manipulation of the transmitted value, and the design should provide for detection of implausible or inconsistent readings. Protective functions dependent on such instrumentation, including cell voltage limits, reverse current protection, water conductivity thresholds and purge sequences, should be protected against unauthorised alteration.

G.4 The control system should be designed such that loss of communication, loss of supervisory control, a cyber induced fault, or receipt of an unauthorized or implausible command results in a predefined safe state rather than in continued operation on the last received instruction.

G.5 Rate of change limits and operating envelopes for parameters relevant to safety should be enforced locally within the control system, independently of the source of the command, so that a command outside the safe envelope is not executed irrespective of its apparent authorization.

G.6 Local, manual and emergency controls by which the electrolyser is brought to a safe state should be identified and protected against unauthorised operation, and cybersecurity measures should preserve their availability to authorised personnel in an emergency.

G.7 The settings of power conversion and rectification equipment, including current and voltage references, operating limits, communication parameters and firmware, should be protected against unauthorised change, and the limits on which safe operation of the electrolyser and its electrical interface depend should be enforced locally within that equipment.

H. Grid, Storage and Renewable Interface Considerations

H.1 Interfaces through which external parties influence the electrical load of the electrolyser, including scheduling systems, aggregation platforms, energy management systems and demand response arrangements, and interfaces with co-located generation, energy storage or renewable energy management systems, should be treated as security boundaries and subjected to authentication, integrity protection and logging. The cybersecurity of a co-located generation, storage or renewable energy asset itself, where that asset falls within the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, is addressed by those regulations and is not further addressed in this note.

H.2 Limits on the magnitude and rate of change of electrical load setpoints should be enforced locally, so that an erroneous or unauthorized external instruction cannot produce load variation beyond the declared operating envelope of the facility.

H.3 The facility should be capable of continued safe operation, or of an orderly transition to a safe state, on loss of external scheduling or dispatch signals.

I. Change, Configuration and Patch Management

I.1 Changes to control system hardware, firmware, software, control logic and network configuration should be made under a documented change control

process, and the configuration in service should be recorded and verifiable.

I.2 Security updates should be assessed, tested in a representative environment and applied within defined maintenance arrangements. The requirement to apply updates should be reconciled with the operating constraints of control systems, in which the practices applicable to enterprise information technology, including immediate patching, automatic restart and intrusive scanning, may not be appropriate. Where an update cannot be applied, the residual risk should be recorded and compensating controls applied.

I.3 Backups of control system configuration, control logic and application software should be maintained, held separately from the operational system, verified for integrity, and tested for restoration at a defined periodicity. It is proposed that at least one such copy be held offline or otherwise protected against modification, including modification by ransomware.

J. Monitoring, Incident Response and Resilience

J.1 Control system networks should be monitored for anomalous communication, unauthorized devices and unexpected changes in configuration, by means appropriate to control system environments, passive observation being generally preferable to techniques that generate traffic or load.

J.2 Reporting of incidents under the law in force should, in the case of control systems, extend to the operational and safety consequence of the incident, including any effect on process parameters, protective functions or electrical load, and not be confined to the classification of the incident in information technology terms.

J.3 A documented incident response and crisis management plan specific to compromise of control systems should be maintained, addressing roles, decision authority for suspension of operations, communication with the system operator and relevant authorities, forensic preservation and restoration to a verified configuration, and should be tested periodically.

J.4 Independent assessment of control system cybersecurity should be conducted at a defined periodicity by assessors with demonstrated competence in industrial control system environments, such assessment being distinct in method and competence from an assessment of enterprise information technology systems. It is proposed that such assessment be conducted annually for installations of higher consequence, and at a periodicity determined by risk for other installations.

K. Lifecycle from Procurement to Decommissioning

K.1 Security requirements should be specified at the procurement and design stage, and should form part of the technical specification against which equipment and systems are offered and accepted.

K.2 Verification that security requirements have been met should form part of factory acceptance and site acceptance testing. It is proposed that this take the form of cybersecurity factory acceptance testing and cybersecurity site acceptance testing, conducted alongside conventional testing and covering secure configuration, credential management, network segmentation, remote access arrangements, programmable logic, logging, backup restoration, fail-safe behaviour and command validation, and that the system be placed in service only after the results are recorded.

K.3 On decommissioning, replacement or transfer of control system equipment,

configuration data, credentials, cryptographic material and process data resident on the equipment should be removed under a defined procedure.

K.4 It is proposed that conformity with requirements be assessed at three levels: the product or component as supplied, the integrated control system as commissioned, and the operating facility in service, since certification of a product verifies its capabilities but not its configuration, access control or operating practice after commissioning.

L. Allocation of Responsibility

L.1 The operator, being the entity in possession and control of the facility, should bear primary responsibility for implementation of these principles, irrespective of whether individual components or services are supplied or supported by third parties, and should not discharge that responsibility solely by contractual allocation to a supplier.

L.2 The operator should maintain documented evidence of implementation, in a form capable of being produced for verification. Such evidence would typically include, without limitation, a control system cybersecurity policy; network and system architecture diagrams; records of risk assessment and its periodic review; records of assigned responsibility, roles and competency; an asset and connectivity inventory; access control and remote access procedures; records of change, configuration and patch management; backup and restoration records, including records of restoration testing; a documented incident response and crisis management plan; records of the testing of that plan; records of security verification conducted at factory acceptance and site acceptance testing; records of periodic independent assessment of control system cybersecurity; vulnerability assessment reports; reports of controlled security testing; and a mapping of implemented controls to the applicable reference framework.

L.3 Manufacturers and system integrators supplying control and communication systems should develop and maintain such systems under a documented secure development process, and should disclose to the operator the composition of the software and firmware supplied, in sufficient detail to permit the operator to assess exposure to disclosed vulnerabilities.

L.4 Manufacturers and system integrators should disclose known vulnerabilities affecting supplied systems, provide security updates for a defined minimum period following supply, and state that period at the time of supply.

L.5 Manufacturers and system integrators should support segregation, logging, authentication and access control by design, and should not supply systems whose architecture requires the operator to retrofit such controls externally or to disable them in order to obtain support.

L.6 Manufacturers, system integrators or service providers operating infrastructure common to multiple electrolyser installations should apply security measures proportionate to the aggregate consequence of compromise of that infrastructure across the installations served, and should disclose to each operator the extent to which functions relevant to that operator's installation depend on infrastructure shared with other installations.

M. Proportionality and Interface with Obligations in Force

M.1 A common minimum baseline of requirements should apply to all electrolyser installations, with additional requirements applied in proportion to the consequence profile of the facility. The consequence profile should be determined

having regard to installed capacity, grid connectivity, hydrogen inventory, process safety consequence, external connectivity, co-location with other installations, dependence on shared platforms and proximity to population, installed capacity alone being an insufficient basis. A pilot or demonstration scale electrolyser presents a materially different profile from a large facility integrated with downstream processing or with the grid.

M.2 Where an entity is separately subject to cybersecurity obligations under the law in force, whether by reason of grid interconnection under the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, designation, or general application, requirements applicable to the electrolyser should be capable of being read consistently with those obligations, and duplication of reporting and assessment should be avoided.

M.3 Requirements should so far as practicable be expressed in terms of outcomes and capabilities rather than named products or technologies, so as to remain applicable as technology changes.

M.4 It is proposed that requirements be applied in three tiers: installations in operation to undertake a gap and risk assessment, followed by phased remediation and compensating controls; installations under construction to apply requirements to the extent technically feasible, with justified deviations recorded; and installations yet to be procured to incorporate requirements in design, procurement, contractual specifications and acceptance testing.

N. Automated and Artificial Intelligence Assisted Optimisation

N.1 A command generated by an automated, model based or artificial intelligence assisted function, affecting a setpoint, protective function configuration or electrical load, should be subject to the same locally enforced operating limits as a command from any other source, and should not be executed where it falls outside those limits, irrespective of the function that generated it.

N.2 The basis on which such a function generated a command relevant to safety or electrical load should be capable of being recorded and reviewed, so that its output can be distinguished from a fault or an unauthorized instruction in the course of an investigation.

N.3 It is proposed that such functions operate in advisory mode, that a command affecting safety or electrical load be executed only on approval by the operator, closed loop operation being considered only where a deterministic fail-safe arrangement is established, and that such functions be isolated from safety instrumented systems. **It is important that such human-in-the-loop mechanism should allow for meaningful review and assessment, rather than just approval with a click of a button without sufficient time to review.**

7. Stakeholders

Views are proposed to be sought from the following, and the list may be expanded:

(1) Electrolyser manufacturers, including domestic manufacturers and entities importing electrolyser or electrolyser stacks

(2) Suppliers and system integrators of SCADA, distributed control system and industrial control system solutions deployed in electrolyser installations

(3) Suppliers of power conversion and rectifier equipment used in electrolyser installations

(4) Green hydrogen project developers and operators, including beneficiaries under

the Strategic Interventions for Green Hydrogen Transition scheme

(5) Bureau of Indian Standards

(6) Indian Computer Emergency Response Team

(7) National Critical Information Infrastructure Protection Centre

(8) Central Electricity Authority

(9) Petroleum and Explosives Safety Organization

(10) Central and State load dispatch centers and transmission utilities, in respect of interfaces with grid connected electrolyser installations

(11) Industry associations representing the hydrogen, chemical, fertilizer, refining and steel sectors

(12) Academic and research institutions working in industrial control system security and process safety

(13) Auditing and testing organizations with capability in operational technology security assessment

(14) Cybersecurity industry and professional bodies, including those engaged in operational technology and industrial control system security

8. Response Process

Respondents are requested to indicate the category of respondent under which they are responding, and to identify the principle or question to which each comment relates. Respondents may address questions listed under a category other than their own where they consider it appropriate. Comments not confined to the questions listed are also invited.

ANNEXURE A

Consultation Questions

The questions below are confined to technical and cybersecurity content. Questions relating to the authority by which any resulting standard should be issued, administered or enforced are not included at this stage.

Part I. Regulatory, Standard Setting and Technical Authorities

Addressed to the Bureau of Indian Standards, the Indian Computer Emergency Response Team, the National Critical Information Infrastructure Protection Centre, the Central Electricity Authority, the Petroleum and Explosives Safety Organisation, load despatch centres and transmission utilities, and cybersecurity industry and professional bodies.

I.1 To what extent are the requirements presently applicable to electrolyser operators under the law in force adequate to address the risks identified at Section 5, and which of the principles at Section 6 fall outside those requirements?

I.2 Would adoption or adaptation of an existing international framework for industrial control system security, in preference to the framing of requirements independently, be appropriate for electrolysers, and if so which framework and with what modification for Indian conditions?

I.3 Should requirements be expressed as capabilities of the equipment, as obligations of the operating organisation, or as a combination, and what considerations bear on that choice in the case of electrolysers?

I.4 How should any requirements applicable to electrolysers be reconciled with the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, in respect of a facility that is grid connected or co-located with generation or storage capacity?

I.5 What conformity assessment arrangements would be appropriate for cybersecurity requirements relating to control systems, given that such requirements relate to configuration and operating practice in service as well as to the characteristics of the equipment as supplied?

I.6 In respect of grid facing risk at Principle H, what interfaces between electrolyser installations and system operation are presently in use or anticipated, and what requirements would be appropriate at those interfaces?

I.7 Does the process safety regulatory framework applicable to hydrogen installations presently address, or contemplate addressing, security risk to the safety instrumented systems of such installations?

I.8 What capability presently exists within India to conduct independent assessment of industrial control system cybersecurity, and what would be required to establish sufficient capability for the anticipated deployment?

I.9 Does the boundary drawn at Section 2 and Section 3, excluding matters that fall within the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, correctly identify the systems and interfaces that remain unaddressed by existing regulation, particularly in respect of facilities co-located with generation, storage or renewable energy assets?

I.10 Views are invited on the preference indicated in preliminary stakeholder responses for the IEC 62443 series as the principal reference framework, and on the supporting role of IEC 61511, ISO/IEC 27019 and NIST SP 800-82.

I.11 Views are invited on the proposal at Principle K.4 for assessment of conformity at three levels, and on the methods and evidence appropriate at each level.

I.12 What arrangements would be appropriate for sharing threat and vulnerability information among electrolyser operators and with the authorities concerned?

Part II. Electrolyser Manufacturers, Control System Suppliers and System Integrators

II.1 What control system architecture is typically supplied with electrolyser installations, including the degree of segregation between control networks, enterprise networks and external connections, and what variation exists across technologies and scales?

II.2 What remote monitoring, diagnostic, optimisation or maintenance functions are provided with supplied systems; where are these functions hosted; what categories of data are transmitted; and what capability, if any, exists through these functions to alter setpoints, control logic or protective function configuration?

II.3 Are warranty, performance guarantee or service arrangements presently conditioned on the maintenance of external connectivity or on a specified level of external access, and if so on what terms?

II.4 What technical or commercial constraints would arise from Principle E.4, restricting the exercise of control functions from outside India, and what arrangements would permit the associated functions to be performed while observing that principle?

II.5 Are supplied control systems presently developed under a documented secure development process, and is composition information for the software and firmware supplied made available to operators?

II.6 For what period following supply are security updates presently provided, and by what means is the integrity and authenticity of updates established at the point of installation?

II.7 To what extent do supplied systems presently permit the operator to change all credentials, to obtain logs in a usable form, and to implement segmentation and access control without loss of vendor support?

II.8 How is independence between the safety instrumented system and the control system presently established in supplied installations, in respect of logic solvers, communication paths and access arrangements?

II.9 Are rate of change limits and operating envelopes for parameters relevant to safety and for electrical load presently enforced locally within the supplied control system, independently of the source of the command?

II.10 To what extent are the controllers, human machine interfaces, network components and drives used in electrolyser installations the same as those deployed in other process industries, and what considerations arise from applying requirements to such equipment by reference to its use in electrolysers rather than by reference to the equipment itself?

II.11 In respect of Principles E.1 and E.2, what supply chain assessment is presently conducted at procurement, and for which categories of component are means presently available to verify the integrity and authenticity of firmware and software before installation?

II.12 What lead time and what cost implication would arise from incorporating the principles at Section 6 into equipment presently offered, and how would this differ between new supply and installed equipment?

II.13 What cybersecurity vulnerabilities and protective measures are specific to power conversion and rectification equipment supplied with electrolyser installations, and are these presently addressed within the same control system architecture as the electrolyser process control, or separately?

II.14 Where control, monitoring or optimisation functions for multiple electrolyser installations are hosted on shared or common supplier infrastructure, what measures are presently applied to prevent or contain a compromise of that infrastructure from affecting more than one installation?

II.15 Should certification of the development process of manufacturers under IEC 62443-4-1, and of control system components under IEC 62443-4-2, be required; if so, at what security level; and what is its feasibility for domestically manufactured and imported products?

II.16 What minimum period should be specified for the provision of security updates and technical support following supply, and how should that period relate to the operating life of the stack?

II.17 What arrangements would permit commissioning, specialist troubleshooting and software support by manufacturers while observing Principle E.4, including engineering presence in India, sessions supervised by the operator, and read-only diagnostics from outside India, and what is the impact of each on time and cost?

II.18 Views are invited on the proposal at Principle K.2 for cybersecurity factory and site acceptance testing, including its scope, the party by whom it should be

conducted, and the availability of competent testing capacity.

Part III. Project Developers and Operators

III.1 What arrangements presently exist within operating organisations for responsibility, competence and review in respect of control system cybersecurity, and how are these distinguished from arrangements for enterprise information technology security?

III.2 What external access to control systems is presently permitted, to which parties, on what terms, and by what means is such access authorised, restricted in time and recorded?

III.3 What control system records are presently captured and retained, over what period, and in what location?

III.4 Is a security risk assessment presently conducted for the control system and the safety instrumented system, and is it conducted in conjunction with the process hazard analysis of the facility?

III.5 What arrangements presently exist for the assessment, testing and application of security updates to control systems, and what operating constraints limit those arrangements?

III.6 What arrangements exist for backup and verified restoration of control system configuration and control logic?

III.7 Where the facility participates in scheduling, aggregation or flexible operation arrangements, what interfaces exist for external influence over electrical load, and what safeguards are applied at those interfaces?

III.8 Which of the principles at Section 6 would present material difficulty in implementation at existing or committed installations, and what transitional arrangements would be required?

III.9 On what basis should proportionality under Principle M.1 be determined, whether by installed capacity, by grid connection status, by hydrogen inventory, by proximity to population or other installations, or by other criteria?

III.10 What fire and gas detection, hydrogen detection and other safety instrumented systems are presently integrated with the electrolyser control system, and by what means is their independence from the routine control system presently maintained?

III.11 To what extent do presently deployed or planned control systems employ automated, model based or artificial intelligence assisted optimisation of setpoints, dispatch or operating parameters, and what verification is applied to the commands such systems generate before execution?

III.12 How should existing warranty, performance guarantee and service contracts that depend on external connectivity be treated in implementing Principles E.4 and E.6?

III.13 Views are invited on the proposal at Principle M.4 for transition in three tiers. What time would be required for gap assessment and remediation at installations in operation, and what would be the cost of retrofit as a proportion of control system value?

III.14 Which operating parameters could be manipulated to induce degradation of stacks and associated equipment without triggering alarms, do present protective arrangements detect gradual degradation, and what is the order of financial loss

that could result?

III.15 What minimum retention period should apply to control system records, and what arrangements for on-premises and cloud based historians would be consistent with Principle F.2?

III.16 Views are invited on the proposals at Principles I.3 and J.4 for a protected offline backup copy and for annual independent assessment of installations of higher consequence, including the criteria by which higher consequence should be determined.

III.17 Views are invited on the proposal at Principle N.3 for advisory mode operation of automated and artificial intelligence assisted functions, and for operator approval of commands affecting safety or electrical load.

Part IV. Research, Academic, Testing and Assessment Organisations

IV.1 Which attack scenarios against electrolyser control systems warrant particular attention, having regard to the process characteristics of alkaline, proton exchange membrane, anion exchange membrane and solid oxide technologies, and do these differ materially between technologies?

IV.2 What methods are appropriate for the assessment of security risk to control systems in installations where process hazard and functional safety analyses have also been conducted, and how should the two be integrated?

IV.3 What monitoring and detection techniques are appropriate to electrolyser control system environments, having regard to the constraints on techniques that generate network traffic or processing load?

IV.4 What testing and assessment capability, in terms of facilities, methods and personnel, would be required to support conformity assessment against principles of the kind set out at Section 6?

IV.5 Are there vulnerabilities specific to the power conversion and rectifier equipment of electrolyser installations that warrant treatment distinct from that of the process control system?

IV.6 What testing and assessment approaches are appropriate to verify that commands generated by automated or artificial intelligence assisted optimisation systems remain within locally enforced operating limits?

Part V. All Respondents

V.1 Are the considerations at Section 5 an accurate statement of the risks presented by electrolyser control and communication systems, and are there material considerations not stated?

V.2 Are there principles relevant to the cybersecurity of electrolyser control and communication systems that are not addressed at Section 6 and that should be included?

V.3 Are any of the principles at Section 6 considered inappropriate, disproportionate or impracticable, and on what grounds?

V.4 Should any resulting requirements apply uniformly to all electrolyser installations, or be differentiated, and on what criteria?

V.5 What transitional arrangements would be appropriate as between installations in operation, installations under construction, and installations yet to be procured?

V.6 Should cybersecurity requirements for hydrogen storage, compression, transport and refuelling infrastructure be considered separately, and if so what considerations distinguish those categories from electrolysers?

V.7 Does the exclusion from this note of matters falling within the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026 leave any material gap, particularly at the interface between the electrolyser and co-located generation, storage or renewable energy assets?