1. []{#_Toc212194842 .anchor}QPLANT Control System

    1. []{#_Toc200492240 .anchor}Overview

The QPLANT Control System (QPLANT:CIS) is the dedicated system for the local control of the QPLANT, ensuring all on-site cryogenic processes operate safely and efficiently. To function within the wider facility, the QPLANT:CIS integrates with the MCS, the MIT platform, and the MIS.

The integration with the MCS is designed to:

- Exchange all necessary data between the QPLANT:CIS and the QCELLs.
- Provide operators with a single, unified interface to seamlessly monitor and control the QPLANT alongside other primary systems.

The integration with the MIT platform is designed to:

- Connect to centralized networking
- Utilize centralized infrastructure like data storage, backups, and user authentication.

Within the overall safety framework, the QPLANT:CIS has a clearly defined role:

- It manages the dedicated local protection of the QPLANT, executing immediate safety functions such as automated shutdowns in response to internal faults.
- It defers to the MIS for all global safety functions, particularly when the QPLANT interacts with other facility systems

        1. Reference Architecture

Figure 9 illustrates the reference architecture of the complete cryogenic control system, identifying the QPLANT:CIS as a key sub-system.

Refer to §9.2.2 for detailed signal and interface mapping shown in Figure 9

2. Architecture, Autonomy, and Scope

238. The QPLANT:CIS shall include all components identified in green within Figure 9 (Reference Architecture). The QPLANT:CIS shall include any additional systems or subsystems required to meet overall cryogenic system performance, functional, and safety objectives.

239. The QPLANT:CIS shall use a commercially available, industrial-grade control platform with documented lifecycle support and vendor independence. It shall meet applicable safety, performance, and reliability standards and shall comply with all relevant regulatory frameworks.

240. The QPLANT:CIS shall enable autonomous operation of the QPLANT across all defined operational scenarios and transitions, without requiring operator intervention.

241. The QPLANT:CIS shall support real-time monitoring of instrument health (e.g.: drift, dropout, deviation from expected range) with alarms and diagnostic flags for early fault detection.

    1. Test System for Functional Verification

242. The Contractor shall deliver a dedicated, fit-for-purpose Test System for functional testing, validation, and commissioning of the System Under Test (SUT), specifically the QPLANT and its QPLANT:CIS

243. The Test System shall emulate key operational states including normal start-up, shutdown, transients, degraded modes, and fallback conditions.

244. The Test System shall enable alarm logic verification, interlock testing, and diagnostic evaluation without reliance on the live operational system.

- In the Offer, the Applicant shall:
- Describe proposed SUT/Test System architecture.

    1. Digital Process Model

A complete digital process model (transient simulation or digital twin) is not mandatory. However, if the Contractor proposes one, the following requirements shall apply:

245. Any proposed model shall use certified, validated, or standards-compliant toolsets (e.g., Simulink®, SimCryogenics, or validated statistical/ML models).

246. The model shall support operator training, failure simulation, diagnostics, and maintenance planning.

247. The model shall enable future integration into the control system to support virtual sensors, inference algorithms, and predictive diagnostics.

- In the Offer, the Applicant shall:
- State if they will provide a digital process model and motivate it the decision by a cost-benefit analysis.
- If it is not provided, the Applicant shall describe alternative approach for commissioning, fault simulation, diagnostics, training.
- Provide supporting documentation for training and validation strategy.

    1. Cryogenic System Control and MCS Integration

248. The QPLANT:CIS shall regulate the mass flow rate and supply temperature at the QPLANT–QCELL interface (via QINFRA to QRB in the coldbox room), such that the temperature change rate - during cool-down and

warm-up - of each QCELL remains within predefined and controlled limits. The temperature change rate is defined as the maximum allowable rate of change of the internal QCELL temperature, expressed in K/h (e.g., 4 K/h).

249. The QPLANT:CIS shall allow the adjustment of these limits depending on the thermal inertia of each QCELL and the operational mode to form part of process design and general control methodologies

250. The QPLANT:CIS shall support bidirectional communication with the Concentrator PLC (refer to Figure 9 and items 20 and 33), exchanging real-time operational and control signals at an update rate of 1 Hz. This will be used by the Concentrator PLC, implemented within MCS, to actively control and enforce this temperature change rate by issuing setpoints and operational constraints to the QPLANT.

251. The QPLANT:CIS shall route all control commands, system status updates, and alerts related to cryogenic operation via MIT to ensure centralized visibility and unified supervision across QPLANT and QCELL domains.

252. The QPLANT:CIS shall enable autonomous operation (without operator intervention) of the QPLANT across all specified scenarios and transitions between them.

    1. General Software and Hardware Requirements

253. The Contractor shall follow the applicable sections from the General Software and Hardware Requirements for Contractors (GSHRC) containing quality and other requirements related to software, firmware, and interoperability

254. When the MCS is unavailable or a communication loss occurs, the QPLANT:CIS shall continue to operate as long as the systems safety as well as personnel safety are guaranteed.

255. All the control parameters relevant for User Integration and monitoring (e.g.: setpoints and thresholds), including calibration data shall be available to the remote-control interface with MCS.

256. Interlock thresholds shall not be writable through the remote-control interface.

257. The QPLANT:CIS should allow every actuator to be controlled manually in the event of a malfunction (for example a motor can have an auto, manual override to fixed values).

258. The QPLANT:CIS shall allow every sensor value to be set by the operator (mode maintenance) to be interpreted by the QPLANT:CIS as it is the real value coming from the sensor.

259. Records of all measured values, valve positions, operator actions, logbook and alarms shall be accessible in QPLANT:CIS.

1. Software development

260. As part Control System Dossier, the following controls related information shall be provided to SCK CEN:

- The detailed documentation of the software architecture, covering all modules, functional blocks, and components, along with their inputs and outputs.
- lists of alarms, protection functions, instruments, events, and parameters.
- In the offer, the Applicant shall provide sufficient detail deemed representative of the anticipated software development scope and fixed-price offer, including assumptions, planned methodologies, and architectural breakdown.

261. All PLCs shall be programmed in full compliance with the IEC 61131-3 standard.

The use of Instruction List (IL) is highly discouraged. Higher-level languages like Structured Text (ST) are highly recommended for better clarity, maintainability, and portability of PLC programs. Therefore, users and developers are strongly advised to avoid new implementations in IL and to migrate any existing IL-based code to ST or other recommended IEC 61131-3 languages whenever possible.

In the offer, the Applicant shall:

- Declare the programming languages to be used per functional block.
- Justify any deviation from ST, including retained IL-based implementations.
- Demonstrate software structuring practices that favour maintainability, reuse, and modular design.
- Proposals will be evaluated with preference given to Applicants demonstrating disciplined use of structured IEC 61131-3 languages and long-term maintainability strategies.

262. When the Software Component includes human readable information (for example, but not limited to: HMI, logging, source code), it shall be in English.

263. The Contractor shall develop a functional analysis and a detailed description of all control scenarios including interfaces. The detailed description shall also include program sequence plan (functions and procedures used in the program).

- In the offer, the applicant shall provide a detailed preliminary functional analysis and indicative control sequence plan, representative of the anticipated implementation. This shall include key functions, procedural steps, and interface interactions necessary to support evaluation of scope, architecture complexity, and design maturity.

- The submission shall reflect a fixed-price offer and anticipated development consistent with the proposed control strategy.
- For each software module, functional block, component, or data block, the Contractor shall provide a detailed description of the logical conditions and input states that govern the activation, value assignment, or change of each output parameter.

264. Versioning info through MCS interface: Each Software Component and Hardware Node shall include a unique version identifier that uniquely represents the build date and Git commit hash, automatically generated during the build process to ensure traceability; this identifier shall be retrievable in a consistent and read-only manner through the MCS control and monitoring interface.

    1. Software Change Management

Prior to deployment in the production environment, software updates shall be rigorously tested in a staging environment. This minimizes risks of integration issues with MCS, MIT, MIS, or any interfacing systems and downtime of the QPLANT.

265. The Contractor shall use a dedicated test environment that replicates the production system's configuration, functionality, and critical interfaces for software changes. This environment may be virtual, physical or a combination.
266. The test environment shall mirror the production system to a level that allows reliable validation of all changes under simulated real-world conditions, including performance, response time and stress scenarios.
267. All changes shall undergo rigorous functional, integration, and regression testing in the staging environment before deployment to the production system.
268. No changes shall be implemented on the production system without prior approval based on documented test results and validation in the test environment.
269. The Contractor shall provide a pre-tested rollback plan to ensure the system can be restored promptly to its previous state in case of issues.
270. All changes shall be tracked in a version control system with an audit trail, providing clear documentation of modifications and approvals.
271. Changes shall be designed and tested to ensure minimal impact on system availability during deployment, including options for hot-swapping or scheduled maintenance windows.
272. The Contractor shall guarantee that all testing activities in the staging environment remain completely isolated from production operations to prevent any unintended disruptions.

273. All regulatory requirements applicable to the delivery of the plant shall also be adhered to for any changes made after delivery, ensuring compliance with safety, environmental, and industry standards.

274. The contracting authority reserves the right to audit the testing process, staging environment, and changes at any time to ensure adherence to requirements.

275. The Contractor shall collaborate with stakeholders to evaluate and improve the testing and change management process based on operational feedback and lessons learned.

276. The Change management should be in place after Factory Acceptance Test and used for changes needed to integrate the consumers.

    1. Human Machine Interface (HMI)

277. The Contractor shall deliver local operator stations to provide local data collection and reporting for the QPLANT system to support maintenance activities. As a minimum one is expected in the Compressor Room and one in the Cold Box Room.

278. The Contractor shall not deliver or implement an enterprise level QPLANT SCADA system (multi-user or multi-server architecture) as part of the scope.

279. The Contractor shall deliver and implement a temporary QPLANT SCADA system exclusively for use during the standalone commissioning phase. This solution is intended solely to support initial testing, commissioning, and operator training, and should be decommissioned and replaced by the MCS solution once integration is realized. This temporary system shall also be used as reference design for the development of the MCS Navigator therefor sufficient documentation is required.

280. The Contractor shall provide support for integration of the QPLANT:CIS with the MCS Navigator. This includes, but is not limited to:

281. Providing support in designing the Operator Screen for the Plant.

282. Supplying necessary communication protocols (e.g., OPC UA, TCP/IP)

283. Coordinating with the project SCADA team to ensure data consistency (e.g., tags, alarms)

284. Sharing relevant technical documentation and engineering details to enable seamless integration

285. The Contractor shall ensure that the operator stations (whether HMI panels or dedicated Industrial touch PCs) are based on industrial-grade hardware specifically designed for continuous operation in a production environment. This includes robust construction, compatibility with the

QPLANT’s environmental conditions (temperature, dust, vibrations, ...), and adherence to relevant industrial standards.

286. The platform shall be supported with software updates, firmware updates, and security patches for a minimum of 20 years from the date of commissioning. The Contractor shall provide documentation or official manufacturer statements guaranteeing availability of updates throughout this period.

- In the offer, the Applicant shall explicitly address the obsolescence management strategy for the proposed PLC or control system platform, considering the anticipated forty (40) year operational lifetime of QPLANT. This shall include:
- Manufacturer support lifecycle documentation
- Spare part availability forecasts and migration plans
- Platform evolution roadmap (e.g., upgrade compatibility or virtualization strategy)
- Technical or commercial approach to sustaining software and hardware support beyond the guaranteed 20-year update period (e.g., stockpiling, long-term service contracts, emulation layers).

   1. Migration to Newer Hardware

287. The visualization (HMI) project shall be designed in such a way that it can be migrated to newer hardware of the same manufacturer if the originally delivered hardware becomes obsolete or requires upgrade. This includes ensuring future compatibility of project files and software licenses and providing guidelines for seamless transfer of project data and configurations.

288. The touchscreen display shall have a minimum diagonal size of 24 inches to ensure sufficient screen space for detailed process graphics and user interaction.

289. The display shall support a resolution suitable for clear viewing of process graphics, text, and trends. A minimum resolution of 1920×1080 (Full HD) is recommended for a 24-inch display.

290. Where the system includes a local Human Machine Interface (HMI) that supports local control, it shall implement a control selection mechanism based on a 3-state principle: Local - Free - Remote.

- Local or remote control can only be granted when the system is in the ‘free’ state. If the system is not free, the requester will be denied the requested control, and any write commands from that side will be ignored. However, reading the system state shall always be permitted in any state, allowing either side to retrieve information about the system's status and confirming whether a request was successful. Writing (changing) is only allowed when the request is accepted.

This control mechanism only pertains to local versus remote control states. Any other state machines within the system shall remain active, ensuring that, for example, regulation loops continue to function in either state.

291. Once a system is reserved in a specific control mode, it shall automatically transition to the "Free" state if a configurable timeout period (maximum of 5 minutes) of non-activity expires. "Releasing" means transitioning from a specific control state to the "Free" state. Non-activity refers to the absence of local or remote actions.

292. The Operator Station shall be designed as a non-critical component of the control system. No real-time or safety-critical control functions shall reside in the Operator Station; it is purely for monitoring, visualization, and local interaction.

293. The Operator Station shall store operational data (e.g., trends, alarms) only for a limited amount of time, sufficient for short-term analysis and troubleshooting. The data stored locally shall not be formally backed up; once data ages out of the configured retention period, it may be overwritten or discarded.

294. The Operator Station shall provide capabilities for plotting curves and trends, enabling real-time and short-term historical visualization of key process variables.

295. The Operator Station shall include graphical process views, providing an intuitive interface for monitoring equipment states and process flows.

296. The Operator Station shall show and log alarms and events for immediate operator awareness without functionality to acknowledge alarm occurrences

297. Graphical process views shall be agreed with SCK CEN.

298. All the sensors and actuators shall be integrated in different graphical views.

299. The Operator Station (PLC with IO mirroring QPLANT:CIS (PLC in WCS and PLC in QRB) software shall support a default data acquisition period of maximum two seconds. For critical turbine data an acquisition rate of 100 ms is required.

300. The HMI software shall allow at least two permission levels with distinct functions available.

301. The QPLANT:CIS shall allow to automatically call or e-mail “on call” staff through MIT

302. The graphical views shall be in accordance with the Process & Instrumentation Diagrams to easily understand and operate the system.

303. The HMI software package shall be installed on two workstations with large screens (at least height 24 inches monitors) to visualize the useful

information during QPLANT operation

1. Network

   1. Reference Architecture

From Figure 11 above the hierarchy and levels are shown:

Enterprise Network: Represents the high-level IT network connecting various business operations, services, and systems. It serves as the foundation for communication across the organization.

Industrial Network: Focuses on the network responsible for managing industrial operations and controls, connecting systems such as SCADA, PLCs, and field devices. It ensures reliable data transmission for production and automation processes.

Plant: This is the central infrastructure that interconnects different network segments, providing high-speed data transfer and ensuring scalability and reliability.

Zone: Acts as an intermediary between the cell and the industrial network, handling traffic distribution and optimizing data flow.

2. General

304. The Contractor shall supply a detailed list of the network ports and protocols necessary for the correct functionality of their system and application.)

305. The Contractor shall be responsible for configuring the necessary network elements based on the inventory of network ports, protocols, internal and external applications.

306. The Contractor shall use IP address ranges for the QPLANT:CIS as provided by the customer. This includes equipment in Level 0 of the Perdue model. These ranges will be pre-assigned by MIT to ensure consistency with the overall network architecture and addressing schemes. The Contractor is responsible for implementing the provided IP ranges without deviation, and any additional IP requirements shall be communicated to and approved by MIT prior to implementation. Additionally, the Contractor shall document the use of the assigned IP ranges for each device and submit this documentation to MIT upon completing the configuration. MIT reserves the right to audit the Contractor's implementation to ensure adherence to the assigned IP ranges and network configuration standards.

307. Where a Software Component can be upgraded, the QPLANT:CIS shall support an upgrade procedure which can be automated as script(s), without the need for an Internet connection. A list of required tools must be provided.

   1. Services

308. Where backup of a system is required, for each system following shall be defined DD5 ():
    - a clear list of all folders, files, databases, ... that are to be included in a backup
    - a document describing the backup and restore process
    - any script(s) required to perform these backups and restore actions
309. Where the system has an operating system, the System shall support monitoring by at least one of the protocols mentioned in the MIT interface catalogue chapter "Monitoring".
310. Where the system has no operating system and requires authorization, the System shall support authorization by at least one of the protocols mentioned in the MIT interface catalogue chapter "Authorization and security".
311. Where the System has an operating system, the System shall support authorization by at least one of the protocols mentioned in the MIT interface catalogue chapter "Authorization and security".
312. Where the system has no operating system and requires authentication, the System shall support authentication by at least one of the protocols mentioned in the MIT interface catalogue chapter "Authentication".
313. Where the System has an operating system which requires authentication, the System shall support authentication by at least one of the protocols mentioned in the MIT interface catalogue chapter "Authentication". Ref. SCK\55564083
314. The System shall support network addressing service by at least one of the protocols mentioned in the MIT interface catalogue chapter "Network addressing service".
315. The System shall support network naming service by at least one of the protocols mentioned in the MIT interface catalogue chapter "Network naming service".
316. The Contractor shall implement a mechanism for automatic IP address assignment based on MAC addresses whenever possible, utilizing DHCP services to ensure efficient and consistent configuration. In scenarios where DHCP is not feasible, the Contractor shall configure static IP addresses in accordance with MIT's assigned IP ranges. All configurations shall align with MIT's network architecture standards to ensure seamless integration and avoid IP conflicts.
317. The Contractor shall provide a comprehensive list of all devices, including their respective MAC addresses, prior to configuring the network. This list is crucial for tracking and managing devices, especially when configuring static IP addresses or ensuring proper DHCP assignment.

318. If a device is DHCP-capable but not configured for DHCP, the Contractor shall provide a detailed procedure for enabling and configuring DHCP on the device. The procedure shall include all necessary steps for ensuring proper DHCP functionality, such as network settings, IP lease time configuration, and alignment with MIT's DHCP service and network standards.

1. Infrastructure

An aggregation network ensures high reliability and performance by implementing redundancy to minimize downtime and enable fast recovery during faults. Redundant connections ensure continuous backbone network availability by enabling quick failover during link failures, minimizing disruptions, and maintaining system stability.

319. The aggregation network shall use a redundant ring topology, with a dedicated redundancy manager and client switches. The network shall automatically reconfigure within 300 ms in case of interruptions. Redundant connections to the backbone shall be established using a master/slave configuration, ensuring failover times under 300 ms. All links within the aggregation network, including connections to the backbone and cell networks, shall support 1 Gbit/s bandwidth. The network design shall incorporate fault recovery mechanisms to reroute traffic in the event of failures, ensuring uninterrupted data flow.

320. The QPLANT:CIS shall establish redundant connections to the backbone network using standby redundancy. Each connection shall include a master and backup device, with failover mechanisms ensuring that if one de[2]vice or connection fails, the other takes over seamlessly. The failover time shall be deterministic, with a maximum duration of 300 ms to minimize downtime.

1. Security

321. The Contractor shall comply with the SCK CEN cybersecurity policy, ensuring alignment with the IAEA NSS17 (Nuclear Security Series), ISO 27001 (Information Security Management), and IEC 62443 (Industrial Communication Networks – Network and System Security) standards. This includes implementing required security controls, risk management processes, and incident response protocols as outlined by these frameworks.

322. Documentation of the system's security features and their alignment with the client's standards must be provided for review and approval before deployment.

323. The Contractor shall work with the client to verify that the system integrates seamlessly with the client's existing security infrastructure, including firewalls, VPNs, and any other relevant security tools.

324. The Contractor shall identify all products and digital elements used in the production plant, including Commercial Off-The-Shelf (COTS) materials and custom-built systems, that fall under the scope of the Cyber Resilience

Act. These products must be evaluated for compliance with the CRA's cybersecurity requirements.

325. If the Contractor requires remote access to the plant, he shall utilize the standard solution provided by the customer. Access will be granted with restricted permissions to ensure that only necessary functions are available, safeguarding the integrity and security of the plant's systems. The Contractor is responsible for adhering to the defined access protocols and ensuring compliance with the customer's security policies.