

## Chapter 2: Access Management

### 2.1 OBJECTIVE

- To establish the Access Control Procedures, wherein the Users shall only be provided with access to the network and network services and OT services that they have been specifically authorized to use.
- To allow access, controlled by a secure log-on procedure and restricted in accordance with the access control policy.

### 2.2 PROCESS:

The process shall comprise of but not limited to the following:

- There shall be a user identity system for defining, authenticating, authorizing each of the user and their activities with role-based access.
- Each of the User Activities shall be logged and periodically audited.
- The Access Control Policy and Procedure shall ensure the following: -
  - ✓ Each of the User shall be created and defined for a Unique Login Credential. This ensures that nobody can log onto the system without uniquely identifiable credentials.
  - ✓ The authentication of user, shall be a Multi factor Authentication for a secure access. This makes Access Control more robust and enhances the effectiveness of uniquely identifying a User.
  - ✓ Stringent Password policy shall be defined and used, in order to ensure that the passwords created for Access Control by the user are not easily guessed and secure passwords are created.
  - ✓ Sharing of User Accounts and their passwords shall be restricted, by restricting concurrent access to resources with the same User Credential.
  - ✓ The Access Control Policy and Procedure shall define and authorize the users based on their Job-Roles. This ensures and enables the administrators to setup the granular access control for different employees.

- ✓ Periodic review shall be done for the Access of the Users and change the access rights based on the movement of individual users, group of users, to a different organizational unit.
- ✓ Automatically, users shall be logged off from the systems after a period of inactivity, for securing the systems from any unauthorized activity.
- ✓ A formal User registration and deregistration process shall be implemented, along with a defined process for user access provisioning. The same shall be authorized by the HOD.
- ✓ Physical entry to the restricted areas shall be controlled by access card and the biometric dual factor authentication.
- ✓ For Access control of OT systems that are not connected to any network, the following shall be ensured:
  - There shall be a separate user account for each user based on the role of the user and relevant privileges shall be given to the user account.
  - Users shall not share shared/public user accounts for common tasks.
  - Stringent Password policy shall be defined and used, in order to ensure that the passwords created for Access Control by the user are not easily guessed and secure passwords are created.
  - Sharing of User Accounts and their passwords shall be restricted.
  - Admin password of all the systems shall be defined and created and the password for the same shall be saved in a sealed envelope with the HOD. This shall only be used with HOD approval and only in case of emergencies. Post usage, the password of the same shall be changed and again placed back in the sealed envelope.

### 2.3 Physical Access Management

Access control is a method of controlling who and what resources can access premises and system and what type of access is permitted. Access control rule and rights should be clearly stated.



IndianOil

### 2.3.1 Physical Access Control

- Duties and Areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modifications or misuse of assets.
- Authorization according to zones and critical security levels to be maintained.
- Personnel to be identified on “who can do what” basis. Job roles to be clearly defined with authorization levels.
- Multiple authorized personnel security to be incorporated for high criticality/risk assets.

### 2.3.2 User Access Management

#### 2.3.2.1 User Registration

- 1 Individual unique user ID to enable users to be linked and held responsible to their actions. A group User ID can be formulated for group of users having same privilege level. e.g. Operation Group, maintenance group etc.
- 2 Facility for individual unique IDs with logging facility for higher privilege levels of accessing IACS assets is advised.
- 3 Supervisory Level should be provided with unique ID.
- 4 Administrator Levels should be provided with secret unique ID which may require multiple levels of authorization.

#### 2.3.2.2 Privilege Management

- 1 Privileges to the accounts formulated should be judicially reviewed.
- 2 The philosophy of least Privileges (only essential rights should be given at each level) shall be incorporated for all levels.
- 3 Minimum 3 rights level to be maintained, i.e. user, supervisor and administrator.
- 4 OEM or Vendor shall be consulted to implement least right philosophy.
- 5 Different user ID to be configured for Vendors and OEM.

#### 2.3.2.3 User Password Management

- 1 Password generation should be done through a formal procedure.



- 2 Users are required to keep personal and group passwords confidential.
- 3 Password lifecycle to be maintained and regeneration requirement is to be examined after each M&I.

#### **2.3.2.4 Review of User Access Rights**

- 1 Access Rights to be evaluated by managerial level periodically.
- 2 Reassignment of access level to be done if required.
- 3 Administrator rights to minimized and given only if necessary.

#### **2.3.2.5 Account Movement**

1. All unnecessary and Default accounts to be deleted to avoid any unauthorized access.
2. New installations to ensure that default users and password are not used for engineering.
3. Change in password to be incorporated on change of employee's role or location, in case of having individual supervisory or administrator rights.

### **2.3.3 User Responsibilities**

#### **2.3.3.1 Password Use**

1. User shall keep the password secret; groups shall not share their passwords outside group.
2. Password should be alphanumeric with minimum strength and incorporate CAPs and Special characters.
3. Group Passwords should not be shared in e-mails.
4. Passwords in general should not be documented however in case of documentation secrecy to be maintained (e.g. sealed envelope in HOD's custody).
5. Users shall logout from supervisory or administrator levels and ensures closing of all active sessions before leaving critical assets.

#### **2.3.3.2 Unattended User Equipment**

1. Auto Log-off facility for supervisor and administrator levels to be implemented.



IndianOil

### 2.3.3.3 Clear Desk and Clear Screen

- 2 All sensitive and critical documents like passwords, Licence keys, Hardware dongles etc. or storage media should be kept under lock and key with assigned custodian.
- 3 No password, user IDs, keys etc should be available at the desk.

### 2.3.4 Access Record

#### 2.3.4.1 Audit Logging

- 1 Audit logs/ record shall be maintained with date, time and details of key events e.g. log-on and log-off.
- 2 Audit log shall be maintained for all administrative & supervisory modifications.
- 3 Logs shall be maintained for minimum desired period of time for audit and evaluation purpose.
- 4 Records of failed password attempts to be maintained in audit log.
- 5 Facility to provide audit logs on assets as well as server to be explored.
- 6 Multiple level password requirements to clear audit trail to be explored.
- 7 Facility of storing access record at multiple locations for critical assets to be explored.

#### 2.3.4.2 Fault Login

- 1 Facility to block user on entry of maximum wrong attempts of user-ID and password combination to be explored.
- 2 Once a user is blocked, only an administrator shall have the authorization to release the blocked user.
- 3 Change in password to be enforced after maximum failed login attempts.

### 2.3.5 Visitor Control

- 1 Visitor access shall be controlled by physical access control to the IACS by authenticating visitors before authorising access to the facility where the IACS resides other than areas designated as publicly accessible.



- 2 Access records shall be maintained for all visitors.
- 3 Designated officials shall review the visitor access records clearly mentioning the purpose of visit.

## 2.4 Network Access Control

### 2.4.1 Use of Network Services

- Interconnection of networks should be through properly configured firewalls and routers.
- All unnecessary services should be barred. OEM to be consulted for essential services which are required for uninterrupted operation of IACS assets. Other services and applications should be disabled.
- All network sharing services e.g. printer, file sharing etc., if used, shall be properly justified.
- IP/ User IDs based read and write access by services to be clearly defined.
- All services which require third party software should be discouraged and only to be used if mandatory and certified by OEM.
- Network applications use of http protocol should not be used, if mandatory an encrypted https services (Secured encryption) should be used.
- OEM to be consulted for preparation of documentation on network services, users, data flow and rights to enhance awareness among users.

### 2.4.2 User Authentication for external connection

- 1 All external networks should have password security for connections and data transfers.
- 2 Possibility of creating Virtual Private networks between open networks and IACS network through Firewall or Router to be explored.
- 3 Applications requiring data flow between IACS network and external open networks should either be provided with different user IDs or should connect through a least privilege ID and password.

### 2.4.3 Equipment identification in Networks

- 1 Utility for network monitoring and stamping should be available and reproducible.
- 2 Unique names/ID to be provided to all assets and Nodes in Network.
- 3 Logging/stamping of all Equipments and assets using IACS network should be developed.
- 4 All failures in authentication should be logged in database.

### 2.4.4 Segregation in Networks

- 1 Different Zones shall be defined in an IACS sharing same criticality, application, proximity etc. E.g. SIS Zone, BPC Zone, External/enterprise Zone.
- 2 As far as possible a philosophy to be devised for complete network isolation of individual zones. (RTDBMS, DCS/PLC network to be isolated)
- 3 The communication between the zones should be through barrier mechanism restricting the unwanted data flow.
- 4 All barrier mechanism such as firewalls and routers should work on the philosophy of barring everything except what is necessary. (i.e. read write access should be clearly defined.)
- 5 Different Zones of IACS if sharing a common network component then network isolation by VPN or IP sub-netting or any other methodology suggested by OEM shall be followed.

### 2.4.5 Network Connection Control

- 1 All the connection to the network by assets or devices should pass authentication process. No direct connection of devices on to network without password security to be allowed.
- 2 Network optimisation in terms of network loading to be ensured in consultation to OEM.

### 2.4.6 Remote Access and Remote Diagnostic

- 1 Any remote connection to IACS if provided through internet are required to have multiple level password security, user identification and data encryption.

- 2 The remote access to be provided shall always be through a buffer machine which can be isolated from IACS network.
- 3 The buffer machine and IACS network should have different networks connected through firewall and routers.

#### **2.4.7 Permitted Actions without Identification and Authentication**

- 1 OEM/vendor to be consulted for the list of all mandatory process which requires connection without identification and authentication.
- 2 A document stating all such application and services along with justification to be maintained. As far as possible all such application and services should be minimised.

#### **2.4.8 Use of External information Systems**

1. IACS shall not be provided with an insecure internet connection for remote linking. If required, internet can be provided as per Corporate IS guidelines.
2. Whenever an internet connection is provided all software as well as hardware configuration to comply with IT standards/IEC 27001 series.

### **2.5 Operating System Access Control**

#### **2.5.1 Secure logon procedure**

- 1 Unique ID and Password based logging system should be used.
- 2 All Operating stations should have facility to log on directly to application window on system restart after successful OS login.
- 3 Operator Level login should not be allowed to minimize the application window.
- 4 Operator Level Login shall not have access to the control panels and accessories of OS.
- 5 Password strings should not be visible it should be encrypted type.
- 6 OS passwords should not be used for programming purpose.
- 7 Accounts without passwords and guest users shall be removed from Operating station (OS).



### 2.5.2 Password management system

- 1 All passwords from OEM, vendor post installation and commissioning to be provided in sealed envelope.
- 2 These passwords should be changed as specified in point no. 2.1.2 and 2.1.3.

### 2.5.3 Use of system utilities

- 1 Operating software utilities shall only be accessible in administrator mode.
- 2 Logging of all use of system utilities to be ensured.
- 3 Log should contain time stamping, user IDs, and utility accessed.

### 2.5.4 Session timeout

1. A timeout facility should clear the session screen and also possibly close both application and network session after defined period of inactivity.
2. This shall not be applicable for operator level users.
3. Administrator Logons on Operating stations shall have a maximum login time of 30 minutes and initiate auto logoff with appropriate warning.

## 2.6 Application and Information Access Control

### 2.6.1 Information Access Restriction

1. Programming and Application Configuration software should not be provide on operating station and shall have access only through engineering station with proper authentication.
2. User Level Rights like read, write, modify etc. for shared folder/files to be maintained for individual user IDs.
3. Logging of all events of modifications both successful and failed should be available.

### 2.6.2 Sensitive System Isolation

1. Application Software programming facility should not be available on Operating stations in Operator zones.
2. Programming and Application Configuration software to be installed only on higher secured stations like servers or engineering stations.

## Chapter 3: Architecture

### 3.1 Architecture for Central OS/AV Patch management

#### OBJECTIVE

Adversaries (such as malicious threat actors) always have an advantage over their IACS targets given the challenges product suppliers and asset owners face in keeping their systems up to date to minimize security risk caused by vulnerabilities.

#### PROCESS

Patch management fixes vulnerabilities on software and applications that are susceptible to cyber-attacks, helping the organization reduce its security risk. Regular patching of vulnerabilities helps to manage and reduce the risk that exists in the environment. This helps protect the organization from potential security breaches.

- There shall be a server-client system used in the environment for the purpose of delivery of OS patches and AV patches to OT assets, dedicated to the OT environment.
- All the assets in the environment shall communicate with the update server for downloading any patches.
- The update server shall be placed such that OT assets shall not directly communicate with the Corporate/IT environment or Internet.
  - ✓ The OT update server shall be placed in the DMZ zone of the OT environment.
- The OT update Server shall download the patches from corporate update server.
  - ✓ The OT update server shall not directly communicate with the Internet for new patch downloads.
  - ✓ Only corporate update servers should communicate with the internet for any new patch downloads.
- There shall be a secondary/ backup of the OT update server for availability during any failure in primary update server.
- The update servers shall send out all important logs to an external sys-log server.
- All OS patch updates shall be validated, tested and approved for compatibility and stability by the asset's OEM and the asset owner before installation is done on the assets. All the patches shall go

through the patch management lifecycle states as per the below table.

Patch State	Patch State Definition	Managed By
Available	The patch has been provided by a third party or an IACS supplier but has not been tested.	Asset owner Product supplier
In Test	The patch is being tested by an IACS supplier.	Product supplier
Not Approved	The patch has failed the testing of the IACS supplier and should not be used, unless and until the IACS supplier confirms that the patch has been Approved.	Product supplier
Not Applicable	The patch has been tested and is not considered relevant to IACS use.	Product supplier
Approved	The patch has passed the testing by the IACS supplier	Product supplier
Released	The patch is released for the use by the IACS supplier or third party, or the patch may be directly applicable by the asset owner for their internally developed systems.	Asset owner Product supplier
In Internal Test	The patch is being tested by the asset owner testing team.	Asset owner
Not Authorized	The patch has failed the internal testing or may not be applicable.	Asset owner
Authorized	The patch is released by the asset owner and meets the organization standards for updatable devices, or by inspection did not need testing.	Asset owner
Effective	The patch is posted by the asset owner for use.	Asset owner
Installed	The patch is installed on the system.	Asset owner

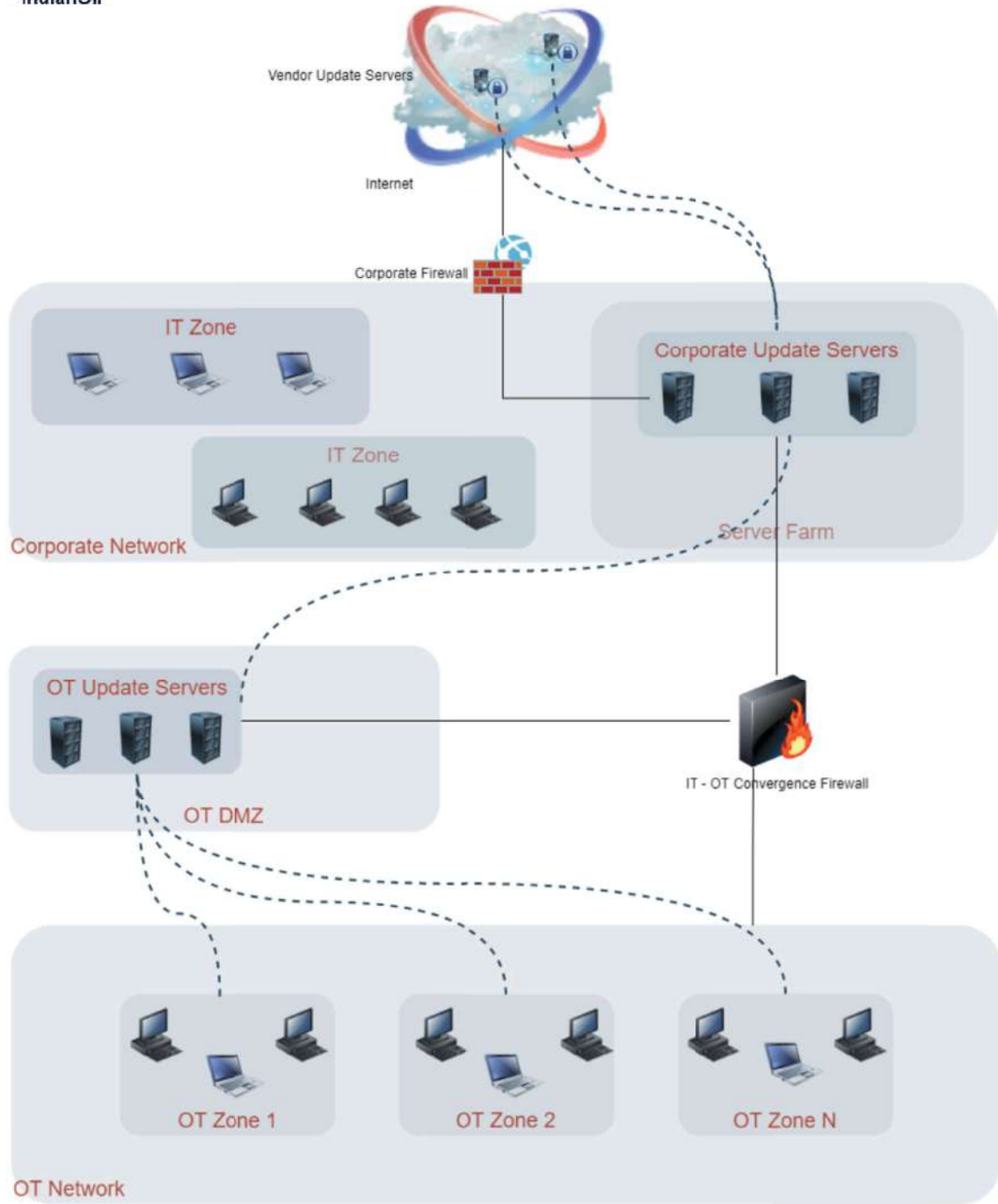


Fig. 1: Architecture for Central OS/AV Patch Management



IndianOil

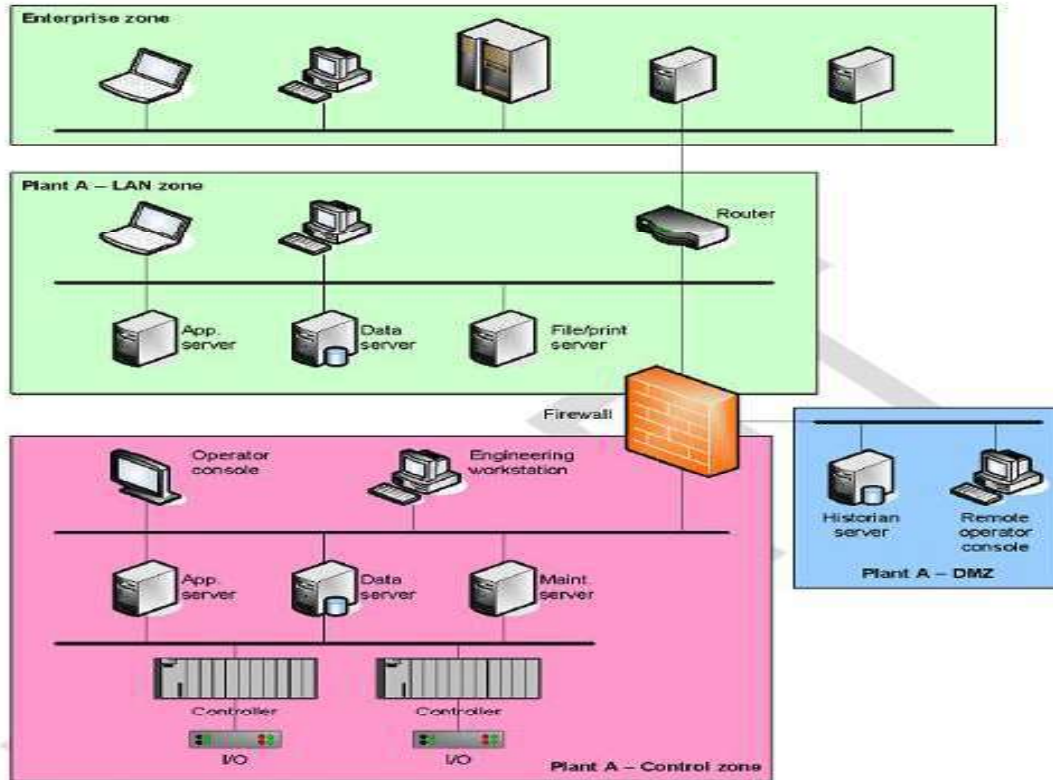
## 3.2 Recommended Network Designs

### 3.2.1 Network Management

- Network should be divided into Zones depending upon logical formation, criticality, application and physical proximity. E.g. PLC, DCS, Third Party Devices, Enterprise Network, RTDBMS, APC etc.
- These Zones shall be interconnected through conduits. Conduits are physical/ logical connections between zones in which the mode and protocols along with data traffic flow rules are defined.
- Security of individual Zones and Conduits shall be separately defined and documented.
- Data Flow rules are to be clearly defined between zones. E.g. PLC zone i.e. PLC controllers, engineering station and other peripherals in this zone should have only read access from DCS zone assets. Any assets in other like DCS, Plant Networks etc. should not be able to have write access on PLC Zone.
- Communication between zones shall be through firewall/ routers or any other methods which can incorporate the security in conduits and data flow.
- Assets being shared between the zones should be minimized.

### 3.2.2 Demilitarized Zones (DMZ)

- DMZ is a perimeter network segment that is logically between internal and external networks.
- A demilitarized zone aims to enforce the control network's policy for external information exchange and to provide external, un-trusted sources with restricted access to releasable information while shielding the control network from outside attacks.
- Antivirus Server, Patch Management Server, Buffer OPC servers etc. are part of DMZ.
- Figure shows a typical bifurcation into zones of IACS with connections through Firewall/Routers.



### 3.3 Network Controls

#### 3.3.1 Recommended DATA Traffic Flow

- PLC Zone shall have only read access from DCS zone.
- No asset in PLC Zone shall have WRITE access to PLC Controller other than PLC engineering station.
- PLC engineering station shall be made highly secure by applying physical and access management techniques as mentioned in chapter 1 and 2 of this document.
- PLC zone shall not have any direct access to Enterprise zone.
- All data from PLC zone to Enterprise Zone shall be through DCS Zone only. Wherever the facility of both PLC and DCS is not available simultaneously vendor/OEM to be consulted for buffer machine installation in between.
- Enterprise zone shall only have read access on to DCS Zone.
- No asset in DCS Zone shall have write accesses from enterprise level. This may be given to some dedicated asset after incorporating the rigorous security measures with authentication. E.g. APC.



- OEM /Vendor to be consulted for establishing DMZs for communication to enterprise zone.
- Third party Zone Rights to be clearly modulated as per requirement. A document for same shall be developed.

### 3.3.2 Recommended Firewall Configuration

- Data Flow restrictions to be maintained through Firewalls/ routers.
- All ports other than required shall be closed on Firewalls.
- IP based filtering and trust levels to be clearly documented.
- Wherever Read and Write both access are provided port configurations to be secured with authentication. Vendor/OEM of the Firewall shall be contacted to implement the same. Consultation of the same with IS Department also to be solicited.
- Firewall/ Router Passwords shall be high strength and must be in line with section 2.1 mentioned earlier.
- Any default password or access methods to firewall/ routers to be disabled.

### 3.3.3 User Authorization and Authentication

- A systematic user authorization and authentication facility to be maintained for all assets of IACS. Service authorization and authentication procedure to be developed in line with recommendations of section 2.1 earlier.

### 3.3.4 Interconnecting Different Networks

- Interconnection between all networks should be through firewall /routers.
- Data Flow, Rights and Authentication to be ensured.

## 3.4 System Hardening

### 3.4.1 Applications

- All third-party default applications which are not required in the system shall be uninstalled from all stations.
- OEM may be consulted to provide a list of required third party software's.



- This requirement shall be individual node based and shall not be applicable to all the nodes in the system.
- A documentation stating node-wise third-party software requirements for the IACS may be maintained.

### 3.4.2 Closing Software Ports

- All unnecessary software ports shall be closed.
- A node-based ports study for all assets in individual zone shall be made.

### 3.4.3 Disabling or Avoiding Unused or Dangerous Services

- All services like Mailer, SNMP, chat, media center etc. which are enabled by default in Operating Software should be disabled.
- Remote Desktop services should be disabled for all nodes.
- Only required services of third-party software which are mandatory as per IACS Asset OEM/Vendor requirement shall be enabled. All other services shall be kept as disabled.

### 3.4.4 Disabling the use of Removable Storage Devices

- Refer Chapter 4 for details on portable devices.

## 3.5 Domains and Trust Relationships

### 3.5.1 Information Exchange Policies and Procedures

- Possibility of multiple domains in single IACS depending upon zones to be explored.
- Data exchange policy between zones and different domains to be developed refer section 3.1.2 for details.
- IP sub netting to be explored for engineering and operation assets in IP based IACS system.
- Trust levels between zones in firewalls to be judiciously configured.

## 3.6 Electronic Messages

- Electronic messaging services for information should be encrypted.



- Under no circumstances incoming message flow from outside IACS should be possible to the involved asset.

### 3.7 Business information Systems

- Business information system for which internet access is possible should have encryption and multiple level of authentication with read only right management. This system shall be connected with highest level of security or minimal rights via routers/firewalls to IACS network.
- These systems should be connected to enterprise zones which may be further connected to IACS buffer zones. Firewall shall be incorporated between all zones.

### 3.8 Patch Management

- All application software's provided for DCS/PLC/Third party devices etc. shall be regularly patched in consultation with OEM.
- Frequency of patch update shall be decided with OEM/vendor to provide latest patch updates.
- All patches which required system restart shall be done on available opportunities or plant shutdown.
- Backup before patch update should always be ensured. The system shall be reverted back to original configuration if some discrepancy after patch update is found.
- Stability after patch update shall be ensured for a minimal time and support from OEM.
- OEM/vendor may be consulted to provide certified patch of operating system software.
- Migration plan for all the operating system for which OEM/vendor has stopped support shall be formulated.
- DCS/PLC/ third party OEM to be consulted for operating software upgrade.
- DCS/PLC/ third party OEM to be consulted for frequency of firmware up gradation for hardware.



IndianOil

## 3.9 Anti-virus Management

### 3.9.1 Anti-virus Availability

- DCS/PLC/third party OEM certified anti-virus shall be available on all work stations & server PCs.
- The Anti-virus updates shall be done at regular frequency.
- It is mandatory to have same anti-virus updates on all nodes.
- The possibility of using anti-virus capabilities of network connection monitoring /removable device monitoring shall be explored.
- The performance of the anti-virus if found not satisfactory the same shall be reported to OEM of DCS/PLC/ third party.
- Regular scan frequency with scanning strength to be decided with OEM.
- It is desirable to have higher frequency and highest scanning strength which is possible without affecting the performance of nodes.
- Higher critical nodes which are not in continuous operation may be set at higher scanning strength.
- Judicious exclusion list shall be made. OEM/vendor to be consulted to minimize the exclusion list.
- Possibility for anti-virus update through single server/node on all nodes shall be explored.
- If possible, this anti-virus update server may be provided an online access with all security measures as mentioned earlier in chapter 2 and chapter 3.
- The anti-virus server should be a part of DMZ.

### 3.9.2 Control against malicious code

- If a threat has been detected on single node than possibility to remove the same from the network shall be explored and forced anti-virus scanning shall be done.
- After removal of infected node from the network a manual anti-virus scan should be performed on all the nodes.
- A facility of forced auto anti-virus scan on all the nodes on detection of threat on any node of the network shall be incorporated in consultation with OEM/vendor.

- A forced anti-virus scan on detection of threat should be of highest possible strength with no exclusion. Same may be performed after taking the node out of the network.
- Disabling of anti-virus services shall not be allowed. If mandatory, anti-virus services may be disabled with password authentication available with administrator.

### 3.9.3 Security Alerts and Advisories

- Provision of critical alarms on threat detection may be explored and incorporated.
- Provision to be made for alarming threats on nodes in non-continuous operation or under no supervision to be provided on highly supervised node.

## 3.10 Access to External Networks (i.e. the internet)

### 3.10.1 Information Access Restriction

- Direct access to internet from IACS shall not be provided. If mandatory same can be provided from enterprise network zone fetching data from IACS through multiple zone level security and firewall/router configuration only.
- If connection through enterprise level is not possible and data has to be fetched from IACS network, the same shall be done using buffer service in DMZ with proper encryption, firewall/routers, right management, anti-virus services etc.

### 3.10.2 Network and Architectural Controls.

- The Refinery shall ensure that the OT Information systems implements the following minimum network and architectural controls

### 3.10.3 Application Partitioning

- Various user functionalities shall be separated either physically or logically. There shall be logical separation between privilege access and normal access as an example and there has to be access differences.



IndianOil

### 3.10.4 Boundary Protection

- Monitors and controls communications at the external boundary of the system and at key internal boundaries within the Refinery;
- Implements sub-networks for publicly accessible system components that are logically separated from internal organizational networks; and
- Connects to external networks of information systems only through managed interfaces consisting of boundary protections devices arranged in accordance with organizational security architecture.
- Implement DMZ.
- Limits inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;
- Limits inbound Internet traffic to IP addresses within the DMZ;
- Does not allow any direct connections inbound or outbound for traffic between the Internet and the Protected agency information system;
- Does not allow internal addresses to pass from the Internet into the DMZ;
- Does not allow unauthorized outbound traffic from the Protected agency information system to the Internet
- Implements state-full inspection, also known as dynamic packet filtering (i.e., only established connections are allowed into the network)
- Places system components that store Confidential data (such as a database) in an internal network zone, segregated from the DMZ and other un-trusted networks
- Does not disclose private IP addresses and routing information to unauthorized parties (Note: methods to obscure IP addressing may include: Network Address Translations (NAT))

### 3.10.5 Server Controls

- Information in Shared Resources: Refinery to ensure the agency information system prevents unauthorized and unintended information transfer using shared system resources
- Prevent Split Tunneling for Remote Devices: Refinery to ensure the agency information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote

connections with the system and communicating using some other connection to resources in external networks

- Minimum and Secure Services: Refinery to ensure information system component (e.g., server) enables only necessary and secure services, protocols, daemons, etc. as required for the function of the system
- Secure Configuration: configure the OT system component (e.g., server) security parameters to prevent misuse

### 3.10.6 External Telecommunications Services

- Implement a managed interface for each external telecommunication service;
- Establish a traffic flow policy for each managed interface;
- Protect the confidentiality and integrity of the information being transmitted across each interface;
- Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
- Review exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need

### 3.10.7 Protection of Information at Rest

- Refinery to ensure the OT system protects the integrity of audit log data at rest

### 3.10.8 Anomaly Monitoring

- Refinery to ensure it has sufficient systems to monitor any anomaly happening inside the OT network. There should be a way to baseline the normal traffic and the deviation of such traffic should be reported as anomaly. This will ensure early detection of attack

## Chapter4: Portable Devices

### 4.1 Management of Removable Media

Removable media/ Portable device is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. It is required that the removable media used for storage of any necessary data is adequately protected during its usage and destroyed after it has served its purpose.

The following procedure to be followed:

- The use of various removable media under different circumstances
- Protection of the removable media
- Disposition of the removable media after it has served its purpose
- The contents of any re-usable media that are to be removed from the organization should not be recoverable

#### 4.1.1 USB

- All Un-Used USB ports other than those required for the system like hardware dongle should be disabled.
- If enabled, then it should require user authentication and USB port should be hard locked.
- Provision for removing the USB cable from motherboard of CPU to be explored.

#### 4.1.2 CD/DVD Drives

- Only authorized personnel should use CD/DVD Drive.
- Re-writeable CD/DVD drives should not be used.
- Single writeable CD/DVD with complete (100%) burn-out to be used.
- Writing of CD/DVD should only be allowed through Windows OS in-built writing feature. Third party CD/DVD writing software should not be used.
- The CD should only be used for writing from IACS assets, externally written CD/DVDs should not be used on IACS assets.
- OEM supplied CD/DVD to be used for loading necessary software& patches/updates etc.



IndianOil

### 4.1.3 Laptops

- Vendor's personnel's laptops should not be used in IACS network.
- Dedicated laptop shall be provided for individual unit/zone only if required.
- Laptops shall be kept in lock and key with login security.
- As far as possible dedicated engineering station shall be provided for third party system.
- Anti-Virus software and OS patches to be done in similar philosophy of IACS assets.
- It's preferable to use same Anti-Virus as on IACS network and these Laptops are kept in surveillance.
- Laptops which are used for IACS should not be utilized for any other purpose and should not be allowed to be taken out of IACS premises.

### 4.1.4 Mobile Phones/PDA

- Carrying of mobile phones/PDA shall be prohibited in Control room.

### 4.1.5 Printers

- Printers shall be installed with individual workstations wherever required and network printers shall be discouraged.
- Printer sharing should be discouraged, and all prints should be taken from printers installed on workstations.
- Network printers if provided shall be installed outside the firewall.
- Wireless connectivity e.g. WI-FI, Bluetooth is not desirable for Printers.

## 4.2 Disposal of media

- Adequate measures shall be taken to prevent misuse of obsolete media and licenses. Whenever a PC or a server or a hard disk is replaced or reallocated, same shall be positively formatted.
- A record of such removals should be kept in order to maintain an audit trail.





IndianOil

### 4.3 Media labeling Storage and Transport

- Media containing information from IACS shall be clearly marked.
- All such media should be stored in secured location with proper access control.
- All media containing data which is old and not required should be suitably disposed as given in section 4.2.
- Only identified and authorised personals should be allowed to transport and use the media.
- While using the media which has returned from another location, facility of offline verification of the integrity before using the same with IACS should be developed.

### 4.4 The usage of the removable media should be followed as per the defined process:

- USB media shall not be allowed on any assets.
- Optical drive media may be allowed to be used on assets for the backup and restore purpose, only if the asset is not part of the network hence backups over the network is not possible.
- One-time writable optical drive should be used, re-writable optical drive should not be allowed.
- One media should not be used on more than one asset.
- The media shall be physically protected within controlled areas.
- It shall be ensured that only the authorized personnel have access to the removable media.
- The media shall be destroyed properly after it is no longer required as per the "Information and Document Management Policy".
- The destruction of the media shall be witnessed or carried out by authorized personnel.

## Chapter 5: Awareness and Personnel Management

### OBJECTIVE

It is required that all the necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed or are of no value are discarded at the proper time.

The document shall aim to aid employees in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

### PROCESS

Implementing an Information and document management policy begins by knowing what kinds of data the organization holds and then classifying that data. Information and document management policies are critical to ensuring all local and federal regulations and retention schedules are being met. This includes retaining data and records for the specified period, and also prompt deleting or destroying records once the retention policy is up.

#### 5.1 Management Commitment to Cyber Security

- Sustained management commitment & oversight to cyber security are vital for an organisation.
- Management intervention wherever necessary to develop new guidelines & for auditing of the existing policy is essential.
- Stringent action should be taken against those employees or external agencies that are found bypassing the organization's cyber security guidelines.
- Regular monitoring of training need identification for employees awareness towards cyber security & its technological advancement.
- Providing certified courses on cyber security to employees.
- Rewards to employees for new suggestions on implementing cyber security which in turn shall be a motivational tool for all.



IndianOil

## 5.2 Sub Contractor Policy

### 5.2.1 Identification of risk related to external party

- All jobs to be performed by Sub-Contractor or Vendors to be analysed with respect to security policies.
- The configuration assets required to be utilized shall be security checked for any malwares.
- To maximum extent, all configuration software and assets maintained by IACS user and shall be provided to Sub – Contractor and Vendors.
- Refer section 4.1.3 regarding security of Laptops.

### 5.2.2 Addressing Security in Third Party Agreements

- The subject policy Cyber security policy must be clearly spelt out in every contract lined up for any IACS related jobs.
- Any agency found to be bypassing the policy shall be liable to pay a certain bond amount to the organization which shall be clearly spelt out in the agreement.

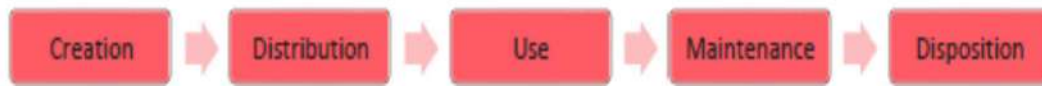
### 5.2.3 Exchange agreement

- Wherever any exchange of information/ physical media is necessary the same must be clearly spelt out in the contract which shall be agreed both by third party & IACS user.
- All asset transfers to adhere chapter 1 section no. 1.1.7 to 1.1.9

## 5.3 Information & document management and data retention

- A committee shall be established to define the different categories, in which organization's records and data can be classified.
- All the existing and new records and electronic data shall be classified into one of the defined categories based on its contents.
- The retention period shall be as follows: -
  - ✓ Application data of the OT systems shall be retained for a minimum period of 3 years.
  - ✓ Data historian logs shall be retained for a minimum period of 45 days.

- The destruction of the media shall be witnessed or carried out by authorized personnel.
- All the documents and records shall be backed up as per article 9.1 of chapter 9
- All the documents and records shall go through a lifecycle from creation through disposition as shown below:-



- ✓ Creation: Documents that will represent formal, compliant and trusted communications or records shall be well-designed from the point of creation, using relevant naming conventions and document templates when necessary.
- ✓ Distribution: Documents shall be transmitted or made available to authorised personnel only. Documents with sensitive information shall be password protected.
- ✓ Use: Use takes place after a document has been distributed internally, and can generate business decisions, further actions or serve any other purposes.
- ✓ Maintenance: While a document is in active use, it is vital that the content is maintained, accurate and available to those who require it, at all times. Document versions shall be clearly mentioned with date and version numbers.
- ✓ Disposition: The practice of handling information that has reached its assigned retention periods. This could mean destruction of the documents and records, or transfer to an archive until the assigned retention period is reached.

#### 5.4 Awareness and Training & Validation Training

To provide an organized security awareness and training program that will inform of relevant and recent security topics. Training provides the motivation, tools, and best practices needed to comply with policies, secure, and classify the information they will access, store, and transmit. Unit should work with Human Resources, departments, and relevant stakeholders to provide information security training: -

- Training shall be provided during orientation sessions for employees.
- Training may be classroom-based or web-based.



- Security training records shall be maintained in a central training system, or in relevant department of the respective refineries.
- Units shall develop general awareness training to re-enforce awareness of security best practices for all OT and associated network users.

#### 5.4.1 Training Development

- Basic training shall be provided to individuals prior to any protected information access.
- Targeted training and awareness sessions shall be developed and presented for users that will need more than the basic understanding of information security based on departments or regulatory updates.
- Role based training.
  - ✓ Those with access to protected information.
  - ✓ Those with assigned security roles and responsibilities.
  - ✓ When required by regulation.
- Specific Departments, IT team members with special information protection requirements.
- Training shall consist of, but not limited to, the following areas:
  - ✓ Information Security Policies, Standards, Controls, and Guidance.
  - ✓ Confidentiality, integrity, and availability of information.
  - ✓ Security practitioner responsibilities and practices for IT staff and system custodians.
  - ✓ Practical information security safeguards for the employees.
  - ✓ User response to suspected security incidents.
  - ✓ Common security threats and vulnerabilities.
  - ✓ Information Security best practices.
  - ✓ Secure use of IOCL networks and information systems.
  - ✓ Legal and department requirements.

#### 5.4.2 Information Security Awareness

- IOCL RHQ (M&I) portal should be the resource for the– policy, guidelines, how-to information, and training material.
- IOCL RHQ (M&I) should produce communication – articles, posts, newsletters, and digital images – covering changes in policy, compliance efforts, legal mandates, and best practices.

- Special notices should be issued addressing incidents, known threats, and methods to reduce their risk.

### 5.4.3 Related policies, standards, procedures and guidelines

Security Control	Relevance
Information security policy manual.	Describes the organization's Information Security Management System and a suite of information security controls based on the good security practices recommended by different security standards
Information governance, information risk management, information classification, incident reporting and various cyber security policies	Awareness and training are essential if employees are to know, understand, appreciate and fulfill their responsibilities towards information risk management, information security and cyber security, reporting incidents, resisting social engineering attacks, avoiding malware, patching systems etc.
Oversight and assurance policies	Awareness and training give employees the information and motivation to fulfill various expectations and obligations relating to information security
Business Continuity Management policy	Employees need to understand their roles following serious incidents and disasters
Information security standards, procedures and guidelines	These amplify and explain the information security policies, providing greater detail on particular topics and/or pragmatic advice for particular audiences
Information security awareness and training materials.	A broad range of information security awareness and training materials is available from the Security Zone or from Information Security, covering both general security matters and more specific security topics; the materials are proactively maintained to maintain relevant to the ever-changing information security risk and control landscape



IndianOil

#### 5.4.4 Training Validation

- Organization should define the Training Calendar, comprising of different sets of Training including the Security Awareness Training.
- Trainings should be conducted as per the defined schedule.
- The Security Awareness Training should also incorporate the different Techniques and Trends from the Industry.
- Each Training should be recorded with the Attendance sheet.
- Participants in the Training should be provided with the relevant material for self-study, either before or after the training.
- All Trainings should be followed by a Feedback or Review Document
- The Trainings should incorporate the different designs, process and policies that are being practiced by the refinery. The designs, process should be for specific for each unit.
- The Trainings should be reviewed or validated from the participants through a defined procedure. This should be done post every training, if not at least in every six (06) months.

#### 5.5 Personnel, Physical and Environmental Security

- All computer equipment, systems, PLC, Workstations, HMI, etc. that provides access to Refinery operations and information should be kept secure by physical means or by using good practice.
- Equipment that stores or process key information or high availability data shall be located in physically secured areas.
- Entry to secured areas shall be restricted to authorized users:
  - ✓ Employees of the Refinery shall have their Identity encoded with the access rights authorized by their line manager and the approving authority.
  - ✓ Employees shall not lend their Identity card to anyone or allow anyone to follow them through card-controlled doors (tail gating).
  - ✓ Access rights shall be revoked immediately for staff who leave the organisation.
  - ✓ Other visitors shall be granted access for specific and authorized purposes only and shall be supervised.

- ✓ A log shall be maintained of all access to restricted areas, via the signing out of access keys and the entry card system logs.

#### 5.5.1 Prerequisite for persons in information security roles: -

- ✓ The Refinery shall define and document roles and responsibilities and entitlements for employees and contractors performing information security work and/or duties in accordance with the Information Security Policy and all relevant policies of the Refinery.
- ✓ The Refinery shall assign a risk designation to all security roles and job functions regardless of job title such that access rights are accordingly assigned.
- ✓ The refinery shall review and revise risk designations annually.
- ✓ Refinery shall have screening criteria for security roles as defined above.
- ✓ An individual or dedicated team shall be assigned to manage the information security of the organization and its users.
- ✓ Background checks to be performed as per IOCL Organizational policies.
- ✓ All other personnel policies to follow IOCL Organizational personnel policies.

**5.5.2 Equipment Maintenance:** Equipment shall be maintained in accordance with manufacturers' recommendations, to ensure its availability and integrity. All faults (or suspected faults) shall be logged in the current Incident Management System and all changes shall be logged in the current Change Management System. All regular maintenance checks such as PAT testing shall also be recorded.

**5.6 Environmental Controls:** Server rooms shall be protected by appropriate air conditioning and very early smoke detection (VESDA) systems or other mechanism of similar nature. Temperatures in server rooms shall be monitored by Operations staff, and undue variances reported immediately to the Refinery. Equipment shall be protected from power failures or electrical anomalies. Server rooms shall be protected by suitable local stand-by power supplies (generator or uninterruptible power supply). Wiring cabinets, and the rooms in which





they are located, should be inspected annually to assess security risks and hazards arising from environmental conditions.

**5.6.1 Cables between buildings:** should be underground wherever possible. Ducts and entry points into buildings should be secure and inspected annually for signs of damage or interference. A log of these inspections shall be retained by plant manager.

**5.6.2 Internal cabling:** wherever possible, cabling within buildings should be installed in ceiling voids and secure ducts.

**5.6.3 Wireless access points:** wherever possible, wireless access points should be installed at a high level to make them less exposed and more secure from theft or tampering.

**5.6.4 Communications racks and wiring cabinets:** All communications equipment shall be kept secure, either in locked rooms or in racks and cabinets with locks. Keys to communications rooms, racks and cabinets shall be held securely by technical specialists so that they are not available to individuals who are unauthorized to access network devices.

## **Chapter 6: Cyber Security Incident Management**

### **6.1 Reporting Cyber Security Event and Weaknesses**

#### **6.1.1 Reporting Cyber Security Events**

- Cyber Security Event shall be reported through appropriate management channels as quick as possible.
- All threats which are recognised shall undergo Root Cause Analysis to locate the exact cause for penetration of threat.
- All Events even as small as Trojan or Malicious software deleted by Antivirus should be documented with date and Root Cause Analysis (RCA) of penetration.

#### **6.1.2 Reporting Weaknesses**

- A report should be made on evaluation of RCA done for reported cyber security event.
- If it is found that counter measures to stop penetration of the threat were not appropriate this should be defined as weakness and should be appropriately reported to the management and OEM.
- Documentation of all such reported weaknesses along with counter measures which are taken to stop such breaches should be made.
- All audit reports evaluating weaknesses of security mechanism should be incorporated with counter measures.

### **6.2 Management of Cyber Security Incidents and Improvements**

#### **6.2.1 Responsibilities and Procedures**

- A risk based contingency plan for all nodes in an IACS should be developed.
- The responsibilities and procedures during such an event should be categorically mentioned in this plan.
- A contingency plan should clearly indicate the location of physical inventories of assets and backups that should be utilised in case of threat detection.
- This plan should be based on what to do when basis. E.g. **“what to do If a threat/virus is detected on node”**

- ✓ Then the node should be removed from the network and a manual anti-virus scan should be performed on all the nodes.
- ✓ A forced anti-virus scan on detection of threat should be of highest possible strength with no exclusion. Same may be performed after taking the node out of the network.
- ✓ Responsible person doing such activity should be identified.
- Similarly, all possible events should be addressed, and contingency plan shall be made.
- All critical events like failure of DCS system, PLC system, engineering station due to a threat shall be planned in consultation with OEM.
- All hardware/software, backup requirement referred in contingency plan should be made readily available at site.
- If possible, a pre-configured critical asset should be maintained at site and it should be possible to use them in plug and play mode.
- All such asset which is maintained as contingency plan spares shall adhere to security policies given vide this document.
- All such asset which is maintained as contingency plan spares shall be treated as active part of IACS network and regularly checked and updated with other similar assets.
- Facility to do secure backup updates on these assets shall be devised in consultation with OEM/vendor.

### 6.2.2 Backup

- Schedule for regular backups should be made in consultation with OEM.
- After any change in application the backup of same shall be taken.
- All such application shall be recorded, indicating date and reason of change.
- After any major changes or several applications changes a complete backup should be taken.
- System backups installation on assets required to meet contingency plan should be done suitably. It should be ensured that these inventories can be used in plug and play format with minimum requirement of changes and backup installation.
- All minor application changes may be kept in soft with copies at three different assets.

- All major system backups should be taken and triplicated and burnt on to CD/DVDs. Refer section 4.1.2 for uses of CD/DVDs.
- Wherever system backups cannot be taken into CDs/DVDs and there is no alternative other than using USB drive, same shall be done by portable CD/DVDs writer.
- Wherever large data backup is required and there is no alternative other than dedicated USB removable media, these USB drives shall be kept under high security with authorised person only.
- USB port should only be enabled for taking the backup and mandatorily disabled after performing the task as per section 4.1.1.

### 6.2.3 Learning from Security Incidents

- All root-cause analysis finding should be shared among organisation.
- All counter measures used to plug the weaknesses shall be circulated with other IACS users.
- Findings in RCA shall be implemented in all similar type of architecture (horizontal implementation).

### 6.2.4 Incident Response Training

- A formal training for contingency plan and procedure shall be given to all responsible employees.
- A drill/demo to execute the plan with OEM/vendor presence shall be performed at suitable availability of site.
- Personnel from OEM/vendor to be involved for such a plan execution shall clearly be identified with their contact nos., e-mail IDs shall be a part of contingency plan.
- All identified and responsible person contact shall be clearly displayed at suitable locations.

### 6.2.5 IACS Monitoring tools and Techniques

- OEM/vendor to be contacted to develop monitoring tools and technique which can analyse network loading, processor loading etc. type critical features of the IACS.
- This can be utilised to analyse threat which have penetrated and are not recognisable by anti-virus or other counter measures.

### 6.3 Risk Assessment, Risk Management & Recovery Plan

The broad areas to look for in a Risk management plan are essentially the following: -

- People and policy security risks
- Operational security risks
- Insecure software development life cycle (SDLC) risks
- Physical security risks
- Third-party relationship risks
- Network security risks
- Platform security risks
- Application security risks

#### 6.3.1 Development of RISK Management plan

It is advised that the following is adopted by IOCL Refineries as part of the RISK Management procedure and plan for rolling out this plan.

The overall guiding factor in developing this plan will involve doing the following exercises by the Refinery team: -

Activity / Security Control	Rationale
Provide active executive sponsorship.	Active and visible support from executive management at each stage of planning, deploying, and monitoring security efforts is crucial to success.
Assign responsibility for security risk management to a senior manager.	Have security risk mitigation, resource-allocation decisions, and policy enforcement roll up to a clearly defined executive with the requisite authority.
Define the system.	Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cyber security.
Identify and classify critical cyber assets.	It is important to understand the assets that may need to be protected, along with their classification (e.g., confidential information, private information, etc.). That way an informed decision can be made as to the controls needed to protect these assets, commensurate with

Activity / Security Control	Rationale
	risk severity and impact to the business.
Identify and analyze the electronic security perimeter(s) (ESPs).	To build a threat model, it is important to understand the entry points that an adversary may use to go after the assets of an organization. The threat model then becomes an important component of the risk assessment.
Perform a vulnerability assessment quarterly.	Realistic assessments of (a) weaknesses in existing security controls and (b) threats and their capabilities create the basis for estimating the likelihood of successful attacks. They also help to prioritize remedial actions.
Assess risks to system information and assets.	The risk assessment combines the likelihood of a successful attack with its assessed potential impact on the organization's mission and goals. It helps ensure that mitigation efforts target the highest security risks and that the controls selected are appropriate and cost-effective for the organization.

All the above points have to draw up and taken up by the refinery as a separate task and procedure. However, certain broad procedural tasks are highlighted in this document.

### 6.3.2 Appointing leadership in Risk Management

It is the executive management's responsibility to establish risk management fundamentals within the organization. This includes a business framework for setting security objectives and aligning strategic risk management with business needs as well as external statutory and regulatory compliance drivers. Without active sponsorship by executive management and a specific role dedicated to ensuring the fulfilment of security goals, instituting security controls is next to impossible.

A senior manager must have clear responsibility and authority to drive planning, enforce compliance with defined policies, and approve all exceptions to the security policy.



IndianOil

### 6.3.3 Establishing a Risk Management Framework

- Define the system.
- Identify cyber assets and their classification.
- Identify the electronic security perimeter (ESP) protecting these assets.
- Conduct vulnerability assessment:
  - ✓ Identify threats.
  - ✓ Identify vulnerabilities.
- Identify security risks along with their impact and likelihood.
- Assess the effectiveness of existing security controls in mitigating the risks.
- Recommend new security controls or changes to existing security controls to mitigate the severity of the risks to a level acceptable to the organization.
- Continuously monitor the effectiveness of security controls.

Periodically repeat this process to account for system changes and changes in the threat landscape.

### 6.3.4 Defining the System

The following are a few major elements of a system definition: -

- The logical and physical boundaries of the system within its environment:
  - ✓ Which components and resources belong to the system?
  - ✓ Which are external to the system?
- The system's mission and primary functions.
- The system's architecture (physical, logical, and security) and data flows.
- Details for interfaces and protocols.
- Types of information the system stores, uses, or transmits, and the sensitivity of each.
  - ✓ Existing management, technical, operational, and physical security controls.

### 6.3.5 Identify Critical Cyber Assets

Identify critical assets: -

- Identify the asset types to be evaluated:

- ✓ Facilities such as generation resources, transmission substations, control centres.
- ✓ Special systems such as SCADA systems, real-time decision-support systems.
- Enumerate the assets within each type. This is the list of critical assets.
- List the essential functions of each critical asset.
- Identify cyber assets associated with a critical asset. Grouping cyber assets by application can simplify the process.
- Narrow the list of identified cyber assets from above step to those supporting the essential functions of critical assets.

### 6.3.6 Classification of Cyber Assets.

Classifying cyber assets as public, restricted, confidential, or private will help dictate the rigor with which they need to be protected by security controls. Consider classifying your cyber assets in the following categories: -

- **Public:** This information is in the public domain and does not require any special protection. For instance, the address and phone number of the headquarters of your electrical cooperative is likely to be public information.
- **Restricted:** This information is generally restricted to all or only some employees in your organization, and its release has the potential of having negative consequences on your organization's business mission or security posture. Examples of this information may include: -
  - ✓ Operational procedures
  - ✓ Network topology or similar diagrams
  - ✓ Equipment layouts of critical cyber assets
  - ✓ Floor plans of computing centres that contain critical cyber assets

**6.3.7 Confidential Information:** Disclosure of this information carries a strong possibility of undermining your organization's business mission or security posture. Examples of this information may include: -

- Security configuration information
- Authentication and authorization information
- Private encryption keys





- Disaster recovery plans
- Incident response plans

**6.3.8 Personally, Identifying Information (PII):** PII is a subset of confidential information that uniquely identifies the private information of a person. This information may include a combination of the person's name and social security number, person's name and credit card number, and so on. PII can identify or locate a living person. Such data has the potential to harm the person if it is lost or inappropriately disclosed. It is essential to safeguard PII against loss, unauthorized destruction, or unauthorized access.

### **6.3.9 Identifying the Electronic Security Perimeter (ESP) Protecting Cyber Assets**

All critical cyber assets should reside behind logical security protections. Each collection of logical security protections is an *electronic security perimeter (ESP)*

This logical border is the collection of OT IT Integration point that monitor and control communications at the external boundary of the system to prevent and detect malicious and other unauthorized communication. At a minimum, identify and document the following:

- The critical cyber assets requiring an ESP.
- The access points to each perimeter, for example:
  - Firewalls
  - Routers
  - Modems
  - SCADA server
  - OPC servers
  - Web servers

The analysis of ESPs, and whether critical cyber assets reside fully within a secure perimeter, requires care. Identifying all access points and the controls on them can be tricky, and it is possible to overlook an avenue of access that could be exploited.

### **6.3.10 Conducting periodic Vulnerability Assessments (VA)**

Perform a cyber vulnerability assessment of the access points to each ESP at least once a year. The vulnerability assessment should examine ways in which the security perimeter can be breached, and existing security controls bypassed to compromise confidentiality, integrity, or availability of critical cyber assets.

A cyber *threat* is any entity or circumstance that has the potential to harm an information system and, through that system, the organization's mission and goals. A cyber *vulnerability* is a gap or weakness in a system's security controls that a threat can exploit.

VA has to be done very carefully and proper downtime needs to be taken if there is any type of intrusive scanning. Otherwise, it's better to do offline analysis.

### 6.3.11 Mitigating Risk

Vulnerability assessments (VA) will identify certain risks. An important part of the risk management process is to determine the severity of each risk as a function of its impact and likelihood. It is also important to understand the extent to which existing security controls completely or partially mitigate each risk. It is then possible to enumerate the gaps in protection and make an informed risk-based decision on next steps. Although a risk management strategy strives for risk prevention where practical, it also must balance the costs and benefits of security controls. The goal is cost-effective controls that ensure acceptable risk levels for participating cooperatives and the smart grid as a whole.

### 6.3.12 Mitigating Risk with Security Control

Understanding an event's impact allows the organization to make informed decisions about mitigating the risk by some combination of the following: -

- Reducing the likelihood of its occurrence
- Detecting an occurrence
- Improving the ability to recover from an occurrence
- Transferring the risk to another entity (e.g., buying insurance)
- It is important to apply risk mitigation strategies at each stage in the life cycles of system components and protocols.
- Questions such as the following can help guide strategy choices:
  - ✓ Is the risk a compliance issue, a privacy issue, a technical issue, or some other issue?
  - ✓ Does the mitigation deal primarily with people, process, or technology?
  - ✓ Is the assessed risk acceptable to the organization?
  - ✓ Is the cost of fully remediating the risk reasonable?

### 6.3.13 Recovery planning or Contingency planning

A disaster recovery plan applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an

extended period. It includes the preparation (e.g., off-site storage of system backups), emergency facilities, and procedures for restoring critical cyber assets and infrastructure at an alternate site after an emergency.

Continuity and recovery plans define interim measures that increase the speed with which organizations resume service after disruptions.

### 6.3.14 Recovery or Mitigation Plan Matrix

Operational Risks	Potential Impact	Mitigation/Recovery
Inadequate patch management process.	Missing patches on firmware and software have the potential to present serious risk to the affected system.	Automate the mechanism of monitoring and receiving alerts when new security patches become available. Make sure that security patches are applied as per OEM recommendations.
Unnecessary system access.	System access that is not managed can result in personnel obtaining, changing, or deleting information they are no longer authorized to access. Related problems include: <ul style="list-style-type: none"> <li>▪ Administrators with false assumptions of what actions any one user may be capable.</li> <li>▪ One user (or many individual users) with sufficient access to cause complete failure or large portions of the electric grid.</li> <li>▪ Inability to prove responsibility for a given action or hold a party accountable.</li> <li>▪ Accidental disruption of service by untrained individuals.</li> <li>▪ Raised value for</li> </ul>	Periodically review the access lists for each critical resource or system to ensure that the right set of individuals has authorized access. Establish standards procedures and channels for granting and revoking employee access to resources or systems.

Operational Risks	Potential Impact	Mitigation/Recovery
	credentials of seemingly insignificant personnel.	
Inadequate change and configuration management.	Improperly configured software/systems/devices added to existing software/systems/devices can lead to insecure configurations and an increased risk of vulnerability.	Ensure that all hardware and software are configured securely. When unclear, seek further clarification from vendors as to secure settings and do not assume that shipped default settings are secure. Establish change management and approval processes for making changes to the configuration to ensure that the security posture is not jeopardized.
Inadequate periodic security audits.	The audit process is the only true measure by which it is possible to continuously evaluate the status of the implemented security program in terms of conformance to policy, to determine whether there is a need to enhance policies and procedures, and to evaluate the robustness of the implemented security technologies. Failure to perform periodic security audits may lead to unidentified security risks or process gaps.	Ensure periodic security audits that focus on assessing security controls at the various levels, such as people and policy, operational, network, platform, application, process, physical security, and third-party relationships.
Inadequate continuity of operations and disaster recovery	An inadequate continuity of operations or disaster recovery plan could result in longer than-necessary	It is essential to ensure within the various plant/system disaster recovery plans that

Operational Risks	Potential Impact	Mitigation/Recovery
plan.	recovery from a possible plant or operational outage.	are in place that an associated cyber contingency plan and cyber security incident response plan is developed. Each plant/system disaster recovery plan should highlight the need to determine if the disaster was created by or related to a cyber security incident. If such is the case, then part of the recovery process must be to ensure cyber incident recovery and contingency activities are implemented. This means taking added steps like validating backups, ensuring devices being recovered are clean before installing the backups, incident reporting, etc.
Inadequate risk assessment process.	Lack or misapplication of adequate risk assessment processes can lead to poor decisions based on inadequate understanding of actual risk.	A documented risk assessment process that includes consideration of business objectives, the impact to the organization if vulnerabilities are exploited, and the determination by senior management of risk acceptance is necessary to ensure proper evaluation of risk.
Inadequate risk management process.	Lack of an adequate risk management process may result in the	Ensure that the organization's risk management process

Operational Risks	Potential Impact	Mitigation/Recovery
	organization focusing its resources on mitigating risks of little impact or likelihood, while leaving more important risks unaddressed.	uses the results of the risk assessment process to initiate the timely and appropriate mitigation of risks in a fashion commensurate with their likelihood and impact. A systematic approach should be developed; an executive dashboard needs to show all risks where mitigations are past due.
Inadequate incident response process.	Without a sufficient incident response process, time-critical response actions may not be completed in a timely manner, leading to the increased duration of risk exposure.	An incident response process is required to ensure proper notification, response, and recovery in the event of an incident.

#### 6.4 Business Continuity plan & its Annual Review

Having a Business Continuity Plan in the event of a Disaster, gives not only the redundancy and continuity to business but also provides a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service shall be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

##### Process

*The business continuity plan for the IOCL refineries shall be followed as per the laid-out business continuity plan of IOCL LTD. There will be no separate business continuity plan for the refineries as an individual entity.*

## **Chapter 7: Asset Management**

### **7.1 Asset Management**

#### **7.1.1 Responsibilities & Ownership of Assets**

- Owners should be identified for assets and responsibility for the maintenance of appropriate controls should be assigned.
- A hierarchical ownership tree should be developed for protection of assets.
- All assets of IACS should be owned by a designated group.
- The group should be custodian of the same. Management of inventories, backups, maintenance jobs of these assets shall be responsibility of the group.
- No asset or equipment of IACS shall remain orphan.

#### **7.1.2 Inventory**

- Inventory of assets hardware and software shall be maintained to meet contingency planning as indicated in chapter 6.
- Locations of these inventories shall be clearly indicated and documented.
- Critical Inventories with latest backups should be readily available.

#### **7.1.3 Acceptable use**

- Acceptable use of all assets should be defined. They shall not be used in improper fashion regardless to capabilities of assets for multi-tasking.
- These rules shall be clearly defined, and misuse of assets should not be allowed in any case.
- Assets should not be moved out of IACS environment to other environments without judicial reasons.
- Personal Usage of IACS assets by employees should be checked by higher management levels.

### **7.2 CHANGE MANAGEMENT & CONFIGURATION MANAGEMENT**

Change management is paramount to maintaining the integrity of both IT and control systems. Unpatched software represents one of the

greatest vulnerabilities to a system. Software updates on ICS cannot always be implemented on a timely basis. These updates need to be thoroughly tested by both the vendor of the industrial control application and the end user of the application before being implemented. Additionally, the ICS owner must plan and schedule ICS outages days/weeks in advance. The ICS may also require revalidation as part of the update process. Change management is also applicable to hardware and firmware. The change management process, when applied to ICS, requires careful assessment by ICS experts (e.g., control engineers) working in conjunction with security and IT personnel.

The change management process also includes configuration level changes.

- Mitigate risk and impact
- Retention of current working state
- Communication and approval management
- Effective change planning using available resources
- Reduction in number of incidents due to change

### 7.2.1 Request for Change (RFC)/ Management of Change(ROC)

Any change is initiated from an RFC/MOC, which in turn can be a result of the following: -

- Incident causes a new change: Any incident which happens in the Refinery can lead to a change request and this need be captured and get reflected during HAZOP study also, in terms of the incident details and the impact which it has had. The type of change related to this is considered as an incident led change
- Change is created as a result of a known problem: Any change which is outcome of known problem and is related to a rectification request. This will have problem description and then the effected changes. This kind of change is planned change from observations of past known problems and is documented accordingly
- Request a new functionality/ Logic: This change is a new change request wherein functional upgradation or new functionality requires some augmentation or enhancement
- Refinery functions request for a configuration change/ new configuration: The change is a new change request wherein



new configuration or modification of existing configuration is required.

- Change manager creates a change as result of an ongoing maintenance: Maintenance related changes which can be temporary or permanent are part of these change requests.
- The change request has to have the following fields captured before passing to further stages of change approval: -



- The reason for change shall have category of change and the crisp need and justification of the changes.
- Impact of the risk and full assessment of the change shall be documented.
- The implementation of the changes with all POA, any downtime and all impacted systems shall be captured.
- The request for change to have complete documentation in templated formats.
- The MOC (Management of Change) shall have the following components which have to be captured and shall be ideally a system driven approach through ITIL based tools.
- An MOC procedure should be followed, which shall have approval of competent authority.

Field	Description
Reference Number	A unique identifier that can be used to distinguish the RFC.
Submission Date	The date the RFC is submitted. If an automated system is being used to track change requests, this may be a system-generated field.
Change Requester	The name of the person requesting the change.
Change Implementer	A description of who is responsible for implementing the change.
Service or System Being Changed	A simple description of the service(s) or system(s) being changed.
Change Description	A description of the change. It should provide both an overview of the change and its scope and enough detail to understand what the change will

Field	Description
	accomplish and how it will be implemented.
Business Justification	A simple description of why the change is needed.
Date and Time of Change	The proposed implementation period for the change. It should include a start date and time and the expected duration (or an end date and time).
Risk and Impact Analysis	An assessment of the risks and impact of the change. This should include the scope of the change's impact (e.g., how many people are affected) and state the expected availability of the service or system during the change (e.g., whether there will be an outage). HAZOP shall be done jointly by all disciplines linked and risks and impacts to be clearly highlighted.
Proven Procedure	The change has to be proven with prior experience of carrying out similar job in past.
Test/Validation Plans	A brief description of how the implemented change will be tested and validated to know if it was successful.
Remediation/Back-Out Plan	Details of what steps will be taken if the change implementation fails. The plan may take the form of a back-out plan for changes that can be reversed or may involve invoking the organization's continuity plan for changes that cannot be reversed. No request should be accepted or approved without a remediation plan. The plan details don't need to be included in the RFC, but there should be an acknowledgment that there is a documented plan, where to find it, and who would implement the plan if needed.
Communication Plan	Details of what is needed based on the nature and impact of the change to the organization. The plan should include known and possible impacts from change implementation, changes to how a user interacts with the service, and what process should be used to report issues after the change is completed. The plan details should include communication channels needed to inform all stakeholders and users affected by the change.

## 7.2.2 Change Evaluation and planning

IOCL MOC process shall evaluate the change request as a next step. The change evaluation committee shall evaluate and then loop back to the change initiator from the Refinery on parameters as below but not limited to the same:

- Prioritization of changes
- Schedule of changes – depending on priority and importance and also kind of changes and its impact.
- Roll out plan – The role out plan for the change has to be validated and evaluated
- Stakeholders – All stakeholders for the change will be identified and informed about this change

A strong part of the change evaluation will include the overall Risk and Impact Analysis. Below is a sample question which covers various aspects of Risk and impact analysis of a change which should be looked into.

What is the designed scope of impact for this change?

- ✓ Enterprise-wide/all
- ✓ Small work team/small department
- Is this a complex or high-risk activity? (Y or N)
- Can this change potentially affect the availability, integrity, and/or security of other OT systems? (Y or N)
- Has this change been tested? (Y or N)
- Is there history in other refineries involved in making this change? (Y or N)
- Are there any related changes involving different activities? (Y or N)
- In what state will the system/service be during implementation?
  - ✓ System/service outage
  - ✓ Limited/reduced functionality
  - ✓ Read only
  - ✓ Normal functionality or handled by redundancy/HA (high availability)
- When will this change occur?
  - ✓ During a scheduled maintenance window?
  - ✓ Nonpeak hours on nonpeak dates
  - ✓ Anytime on peak days
- What is the back-out effort?
  - ✓ Difficult, impossible, or undesirable

- ✓ Possible, though not easily executed; would extend beyond the maintenance window
- ✓ In place and easily executed within the maintenance window

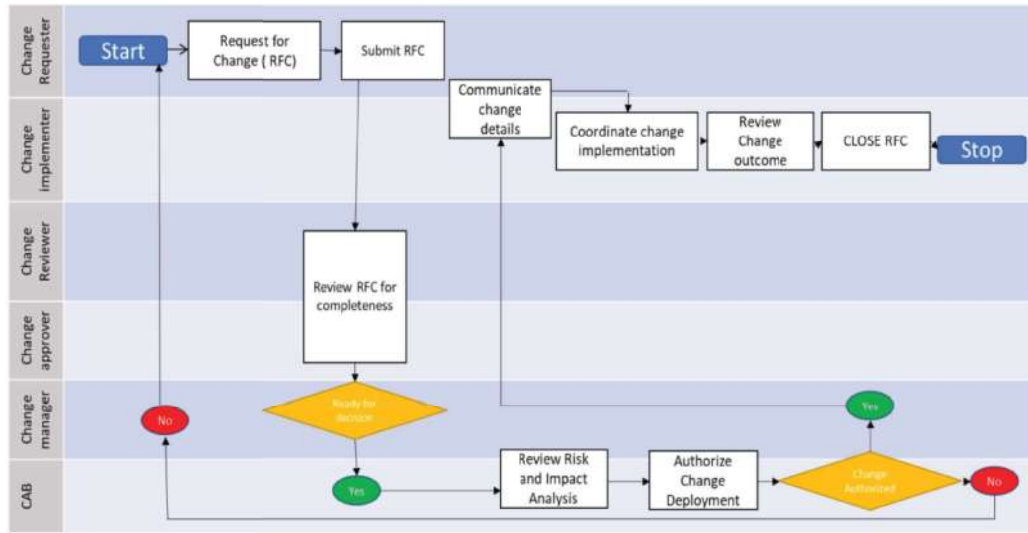
### 7.2.3 Change approvals

Change request is approved as per the approving authority defined in MOC. it. Upon rejection, reassessment review is done and submitted again for approval.

### 7.2.4 Change implementation & review

Once the change is approved, implementation is carried out with the help of the responsible team for carrying out such changes. This team shall follow their own processes that include planning and testing. Change review shall happen once implementation is completed to determine whether it's a success or failure. Review of completed changes help in revisiting and modifying existing change management process if necessary.

The overall Change management workflow can be shown to be summarized as below. The diagram is self-explanatory.



### 7.3 Secure Coding Practices

OT systems in general involve very limited coding practices and required by refineries only under exceptional circumstances.



IndianOil

### 7.3.1 Secure Coding Approval

- Each coding (scripts in DCS) shall be carried out by authorized engineers and vetted by HOD
- Any logic modification in OT systems using FBD, LD and STL etc. is to be endorsed by MOC and carried out after HAZOP study & JSA

## 7.4 Time Synchronization for network components

In modern computer networks, time synchronization is critical because every aspect of managing, securing, planning, and debugging a network, involves determining when events happen. Importance of time synchronization among the Operational Systems and Components of an OT network environment gets even more critical.

### 7.4.1 Time Synchronization

Keeping the time of all the devices synchronized among the OT devices with each other using a common Time Server is essential for carrying out accurate operations in OT environment. Time synchronization is also critical for the network devices as time provides the only frame of reference between all devices on the network. Without synchronized time, accurately correlating events of a production environment is difficult, even impossible.

- The OT Time Server shall synchronize its own clock with the Corporate Time Server
  - ✓ The OT Time Server shall not directly synchronize with the Internet time server.
- Inputs from asset's OEM should be considered for requirement of time transfer accuracy among the assets. Based on that the type of system should be finalized for use
- There shall be a secondary/ backup of the OT time server for availability during any failure in primary time server.
- The time servers shall send out all important logs to an external syslog server.
- The synchronization accuracy shall be periodically validated.

## 7.5 Maintenance for OT & IT hardware

**7.5.1 Maintenance of IT and OT environment:** Maintenance of IT and OT environment require a streamlined process in order to maintain the maintenance process efficiency during the lifecycle of the hardware.

The maintenance of the OT & IT hardware shall be followed as per the following defined process: -

- Equipment shall be maintained as per laid down procedure to ensure its continued availability and integrity.
- Any hardware moving in or out of the IOCL for maintenance/replacement purpose shall be recorded as per the IOCL standard practices.
- New / repaired equipment shall be properly diagnosed by authorized personnel before taking the same into network.
- Detailed records including dates and jobs performed during maintenance shall be maintained.
- Systems to be developed for periodic maintenance and checking of critical networking components that are being used for external connections by competent person /Expert/ OEM.
- Only authorized maintenance personnel shall carry out repair and maintenance jobs.
- Records shall be maintained for all re-useable equipment indicating their past installations & performance. Further, reason for disposal to be categorically indicated.
- All items of equipment containing storage media shall be checked to ensure sensitive data & license before disposal.
- Information should be physically destroyed or overwritten to make it non retrievable.
- All re-useable components shall be properly diagnosed and cleaned before using them.
- All operating stations being reuse should be mandatorily formatted & genuine original licensed software to be reloaded.
- Wherever formatting is not possible OEM/vendor to be contacted to authenticate the healthiness of the component.
- All re-useable type equipment shall be stored at secured locations therefore mandating no unauthorized access & misuse.

## **Chapter 8: Auditing and Updating**

### **8.1 Auditing**

#### **8.1.1 Review of Cyber Security Policy**

- Policy should be reviewed periodically.
- A dedicated team shall be made for updating and reviewing policy.
- Addendums to be made in security policy on the basis of incident and weakness reporting and technological updates.
- Cyber security policy should be reviewed at multiple levels of management.
- Any procedural bypass from policy should be done through management of change.

#### **8.1.2 Audit and Accountability Procedures**

- Formal procedures to auditing of policy indicating purpose, scope, rules and responsibilities should be made.
- All audit reports shall formally be documented and changes in policy should bear reference to the audit reports.

#### **8.1.3 Audit Record Retention**

- The audit reports records shall be retained for a defined period to provide support for after-the-incident investigations of security breach.
- The disposal and destruction of audit reports after the retention period shall be in consultation and approval of management.

### **8.2 Security Policy Updating**

- Policy shall be updated after regular intervals.
- All new technology adopted shall be in accordance to the security policy. In case of noncompliance policy may be suitably updated with justification.
- The compliance of the policy with international standards shall be reviewed with availability of new standards and draft.
- All statutory requirement changes given in rules and regulation of regulatory boards shall be suitably updated in security policy.

### 8.3 Network Switch Configuration File Audit

There should be a periodic internal and external audit of the network switch configuration in order to assess the compliance of the network switch configuration in accordance with this policy.

#### 8.3.1 Compliance of Network Switch configuration

Every audit shall assess the compliance of Network Switch configuration as per but not limited to the following configuration standards:

- There shall be a quarterly audit for verification of the existing configuration of the switch and its compliance with the policies defined in this document.
- Network switches shall be accessible only the authorized personnel of the refinery.
- User access authentication on the Network Switches shall be with a third-party authentication factor like TACACS+, Radius, etc. There shall not be any defined Local Accounts for regular User Authentication and Access.
- One emergency Local Account shall be defined and created and the password for the same shall be saved in a sealed envelope with the HOD. This shall only be used with HOD approval and only in case of emergencies. Post usage, the password of the same shall be changed and again placed back in the sealed envelope.
- The enable password on the switch must be kept in a secure encrypted form. The switch shall have the enable password set to the current production router/ switch password from the device's support organization.
- The following services or features shall be disabled: -
  - ✓ IP directed broadcasts
  - ✓ Incoming packets at the router/ switch sourced with invalid addresses such as RFC1918 addresses
  - ✓ TCP small services
  - ✓ UDP small services
  - ✓ All source routing and switching
  - ✓ All web services running on switch
  - ✓ IOCL discovery protocol on Internet connected interfaces
  - ✓ Telnet, FTP, and HTTP services



- ✓ Auto-configuration
- The following services shall be disabled unless a business justification is provided: -
  - ✓ IOCL discovery protocol and other discovery protocols
  - ✓ Dynamic trunking
  - ✓ Scripting environments if present, such as the TCL shell
- The following services shall be configured:
  - ✓ Password-encryption
  - ✓ NTP configured to a corporate standard source
- If participating in Dynamic Routing, then all routing updates shall be done using secure routing updates.
- Switch shall use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
- Access control lists shall be used to limit the source and type of traffic that can terminate on the device itself.
- The switches shall be included in the ICS asset management system with a designated asset owner and respective point of contact.
- Each switch shall have the defined Banner presented for all forms of login whether remote or local. An example of the same is defined below: -
- "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action
- Telnet shall never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 shall be the preferred management protocol.
- Dynamic routing protocols shall use authentication in routing updates sent to neighbors. Password hashing for the authentication string shall be enabled when supported.
- The switches shall not be configured in the default mode as unmanaged. Each switch shall be configured and secured with a defined configuration.

- All the ports in the switch which are not used shall be placed in Shut mode.
- The Console password for the switch shall be defined and kept in a secured sealed envelope with the HOD. This shall be only used in case of emergencies or on a defined console-based activity. Post the same, the password shall be changed and again saved in a sealed envelope.
- There shall be defined timeouts for the session login.
- All the switch activity shall be logged either locally or to a supported logging device like syslog.
- The VLANs shall be defined with the appropriate ports. Only the ports which are supposed to be part of the VLAN shall be added into the VLAN.
- The Trunks that are defined shall be with appropriate VLAN, which are supposed to be passed through the Trunk and shall not have a complete or default VLAN access.
- Required STP shall be enabled for prevention of loops.

#### 8.4 Monitoring and Review

For following and adhering to the Monitoring and Review of different systems, design and equipment's, we need to have in place the following:

- Any information stored on electronic and computing devices whether owned or leased by IOCL Refinery, the employee or a third party, remains the sole property of IOCL. It must be ensured through legal or technical means that proprietary information is protected in accordance with the defined Data Protection Standards of IOCL Refinery
- All individuals have the responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.
- For security and network maintenance purposes, authorized individuals within organization may monitor equipment, systems and network traffic at any time, as per the defined Infosec's Policy.
- IOCL Refinery reserves the right to audit networks and systems on a periodic basis to ensure compliance as per the standards followed in the Refinery.
- System level and user level passwords must comply with the Password/Access Control Policy. Providing access to another

individual, either deliberately or through failure to secure its access, is prohibited.

- Any change in the systems architecture, design, etc. should be followed with the properly defined process and methodology with complete documentation and review.
- All the Systems security Logs should be monitored for any kind of breach or security threats. Any such incident should be immediately reported and addressed.
- All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging informationsufficient to answer the following questions:
  - ✓ What activity was performed?
  - ✓ Who or what performed the activity, including where or on what system the activity was performed from (subject)?
  - ✓ What the activity was performed on (object)?
  - ✓ When was the activity performed?
  - ✓ What tool(s) was the activity was performed with?
  - ✓ What was the status (such as success vs. failure), outcome, or result of the activity?
- Activities to be Logged, logs shall be created whenever any of the following activities are requested to be performed by the system:
  - ✓ Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
  - ✓ Create, update, or delete information not covered in #1;
  - ✓ Initiate a network connection;
  - ✓ Accept a network connection;
  - ✓ User authentication and authorization for activities covered in #1 or #2 such as user login and logout;
  - ✓ Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
  - ✓ System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;

- ✓ Application process start-up, shutdown, or restart;
  - ✓ Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
  - ✓ Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.
  - ✓ End of Life of assets and Software's should be monitored
  - ✓ When Technology assets have reached the end of their useful life they should be sent to the disposal office for proper disposal.
  - ✓ The disposal office team will securely erase all storage mediums in accordance with current industry best practices.
- 
- The logs that had been captured should be stored as per the defined frequency by IOCL refinery, and should be reviewed for acceptance
  - Audit logs should be periodically reviewed as per the defined frequency by IOCL refinery, and should be reviewed for acceptance
  - Technology Changes, any change in the Technology and their equipment's should be monitored and reviewed as:
    - ✓ End of Life of assets and Software's should be monitored.
    - ✓ When Technology assets have reached the end of their useful life, they should be sent to the disposal office for proper disposal.
    - ✓ The disposal office team will securely erase all storage mediums in accordance with current industry best practices.

## **Chapter 9: Best Practices on Cyber Security and Risk Assessment**

### **9.1 Back-Up & Restoration**

The data of IOCL Ltd is a valuable asset which could be lost or destroyed by intentional/ unintentional actions or events. Therefore, a procedure for backing up and restoring assets and protecting backup copies shall be established, used, and verified by appropriate testing. This process shall not affect the normal plant operations. In addition, identifying and storing backup systems (hardware, software, and documentation) in a safe location should be provisioned.

- All assets shall be classified into categories based on their criticality. (e.g. critical and non-critical, or High/Med/Low).
- Recommendation from asset's OEM should be considered in defining the backup frequency.
- A frequency for periodic backup shall be defined for: -
  - ✓ Criticality of the assets falling into respective category (e.g. critical and non-critical, or High/Med/Low) shall be considered while deciding the backup frequency.
  - ✓ All assets shall be backed up either automatically or manually as per the defined frequency of the backup of their respective categories.
- Process shall be defined to perform manual backups apart from the scheduled periodic backups in case of special planned events. Backups shall be performed before and after these special events. These events may include but not limited to:
  - ✓ Power Shutdown
  - ✓ Software/OS upgrade of asset
  - ✓ Patch installation on asset
  - ✓ Any maintenance activity on asset etc.
- Defined process as per emergency /disaster and its recovery.
- Delete/dispose the old backups after their defined retention period is over.

#### **9.1.1 Data Confidentiality**

Once the information is placed into a backup, it most likely will not have the same controls in place to protect it.

Thus, the component backup ability needs to include the mechanisms to support the necessary protection of the information that is contained in the backup.

This may include:

- Encryption of the backup
- Encryption of the sensitive information as part of the backup procedure
- Or not including the sensitive information as part of the backup
- Access to the backups should be restricted to authorized personnel only

Below should be considered for backup encryption:

- If the backup is encrypted, it shall not include the cryptographic keys as part of the backup.
- Backup the cryptographic keys as part of a separate more secure backup procedure.

The availability of up-to-date backups is essential for recovery from a control system failure and/or misconfiguration. Automating this function ensures that all required files are captured, reducing operator overhead and chances of human errors.

- Recommendation from asset's OEM should be considered in defining the backup and restoration method.
- Automated periodic backups shall be as per OEM recommendations/ best industry practices
- For assets on which backup cannot be automated, asset owner shall ensure periodic backup process is carried out manually as per required frequency.
- Integrity of backed up data should be validated
- Retention of the backup data shall be as per best industry practices keeping following in view: -
  - ✓ How many iterations of backup should be stored before the old ones are deleted permanently, shall be defined for each category the assets are classified into.
  - ✓ Criticality of the assets falling into respective category shall be considered while defining the retention period.
  - ✓ Frequency of assets configuration changes shall be considered while defining the retention period.

### 9.1.2 Storage location

Backup at different location is required to ensure the availability of backups in case of full system crash.

- Onsite: The primary backup generated should be transferred from the local device to an external device/storage located on the same geographic area.
  - ✓ The backup data should be transferred and stored on the backup system over the network.
  - ✓ For storing backup of systems which do not have any network connectivity, a removable media may be used with the following considerations.
    - Any removable media used for backup purpose shall have a defined owner.
    - Only owner of the media shall have access to the media.
    - Media shall be placed in a secure location with a restricted access.
    - Media should be properly labelled.
- Offsite: Creating and locating secondary backup for critical systems in different geographic areas. If this is not feasible, storing backup data and/or equipment in an area that is not subject to the same physical disaster as the primary backup system, should be considered.

## 9.2 Validation of Hardening

Hardening is the process of securing a system by reducing its surface of vulnerability. By the nature of operation, the more functions a system performs, the larger the vulnerability surface. The systems perform a defined and a specific function, so it is possible to reduce the number of possible vectors of attack by the removal of any software, user accounts or services that are not related and required by the planned system functions. System hardening is a vendor specific process, as different system vendors install different elements in the default install process. The possibility of a successful attack can be further reduced by obfuscation. By making it difficult for a potential attacker to identify the system being attacked the attack cannot easily exploit known weaknesses. The hardening policy shall take into account of various surface vectors to reduce the attack surface area.

### 9.2.1 Procurement Hardening

- System Installation: The system should be installed as per the Instruction Manual and Best Practices of the Vendor
- Remove Unnecessary Software: The default installation of the systems come with a variety of software packages to provide

functionality to all users. Software that is not going to be used in a particular installation shall be removed or uninstalled from the system.

- Disable or Remove Unnecessary Usernames: The systems come with a set of predefined user accounts. These accounts are provided to enable a variety of functions. Accounts relating to services or functions which are not used shall be removed or disabled.
- Change Default Passwords: For all accounts which are used the default passwords shall be changed.
- Rename Default User Accounts: If the product permits, the default User shall be renamed, keeping in view that the same will not adversely affect the system.
- Define and Assign User Access Roles: Access to the systems shall be provided in compliance with the IOCL "Access Control Procedures" policy.
- Power Supply Redundancy: The system shall have dual power supply for redundancy.
  - ✓ Hot swappable components may be preferred for business-critical systems.
- Hard-disk Redundancy: The system shall have dual hard disk for redundancy.
  - ✓ Hot swappable components may be preferred for business-critical systems.
- Disable or Remove Unnecessary Services: All services which are not going to be used in production shall be disabled or removed.
- Patch System: The system shall be patched up to date. All relevant service packs and security patches shall be applied.
- Conduct VA Scan: The system shall be scanned with a suitable vulnerability scanner. The results of the scan shall be reviewed, and any issues identified shall be resolved.
- Install Anti-Virus and Anti-Malware: A suitable anti-virus and anti-malware package shall be installed on the system to prevent malicious software introducing weaknesses into the system. In case the application requires certain files or folders to be excluded, the same shall be documented and approved.
- Configure Firewall: If the system can run its own firewall then suitable rules shall be configured on the firewall to close all ports not required for production use.
- License:
  - ✓ All the software shall be licensed in the name of IOCL.





- ✓ All software shall come with necessary support to be made available to IOCL during the contract period.
- ✓ All software shall come with necessary patches to be made available to IOCL during the contract period.
- ✓ No solution shall be used with trial or evaluation licenses.

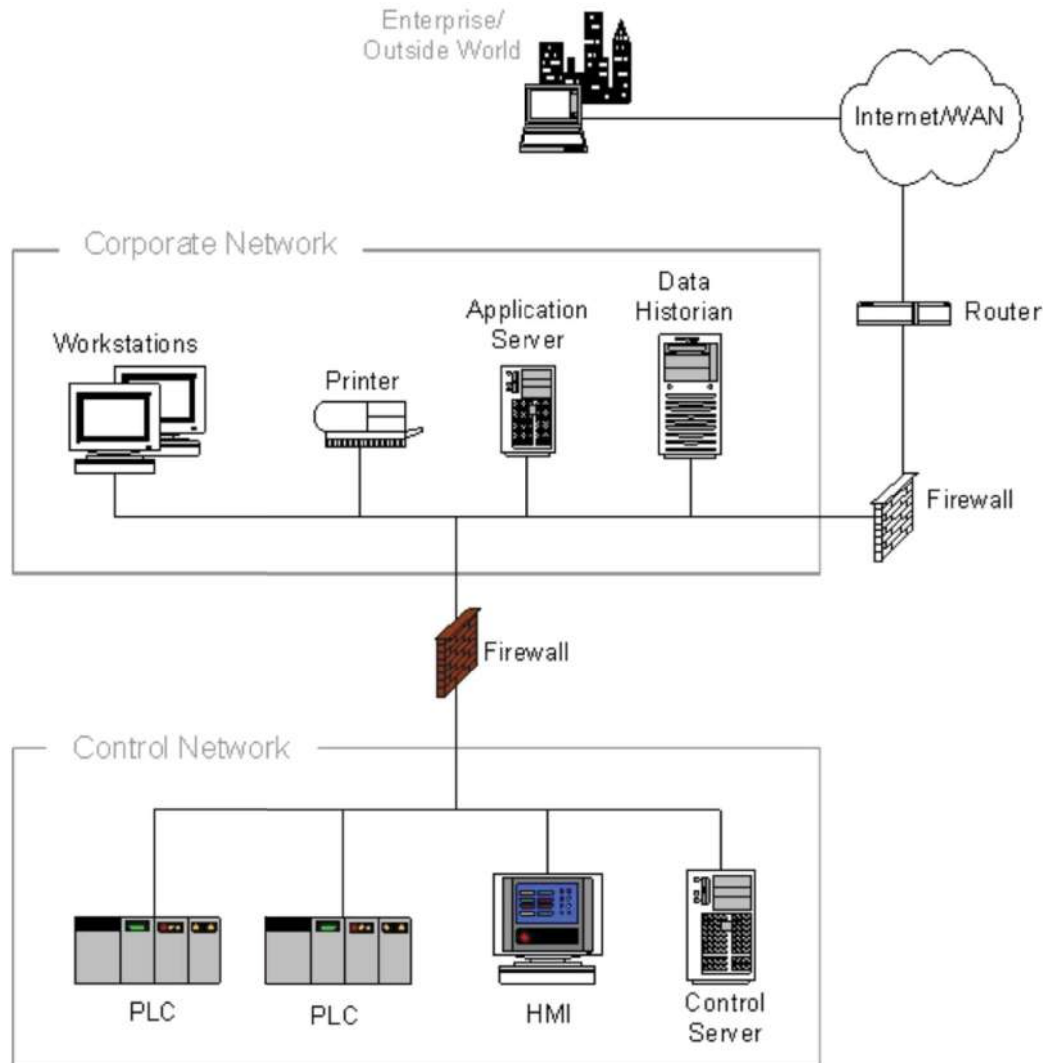
### 9.2.2 Hardening Validation

- A local firewall shall be installed on all PC's and laptops. The firewall shall be configured to only allow incoming traffic on approved ports and from approved sources.
- The use of removable media shall be disabled for all OT systems.
- The "Back-up & Restoration" Procedures shall comply with, for system backup purpose.
- All servers and other devices shall pass a vulnerability assessment prior to use. The systems shall be scanned using the organization's vulnerability scanning tools. All network and operating system vulnerabilities shall be rectified prior to use.
- All devices on the organization's network shall be scanned for vulnerabilities every three (03) months. Any issues identified shall be reviewed and rectified as appropriate.

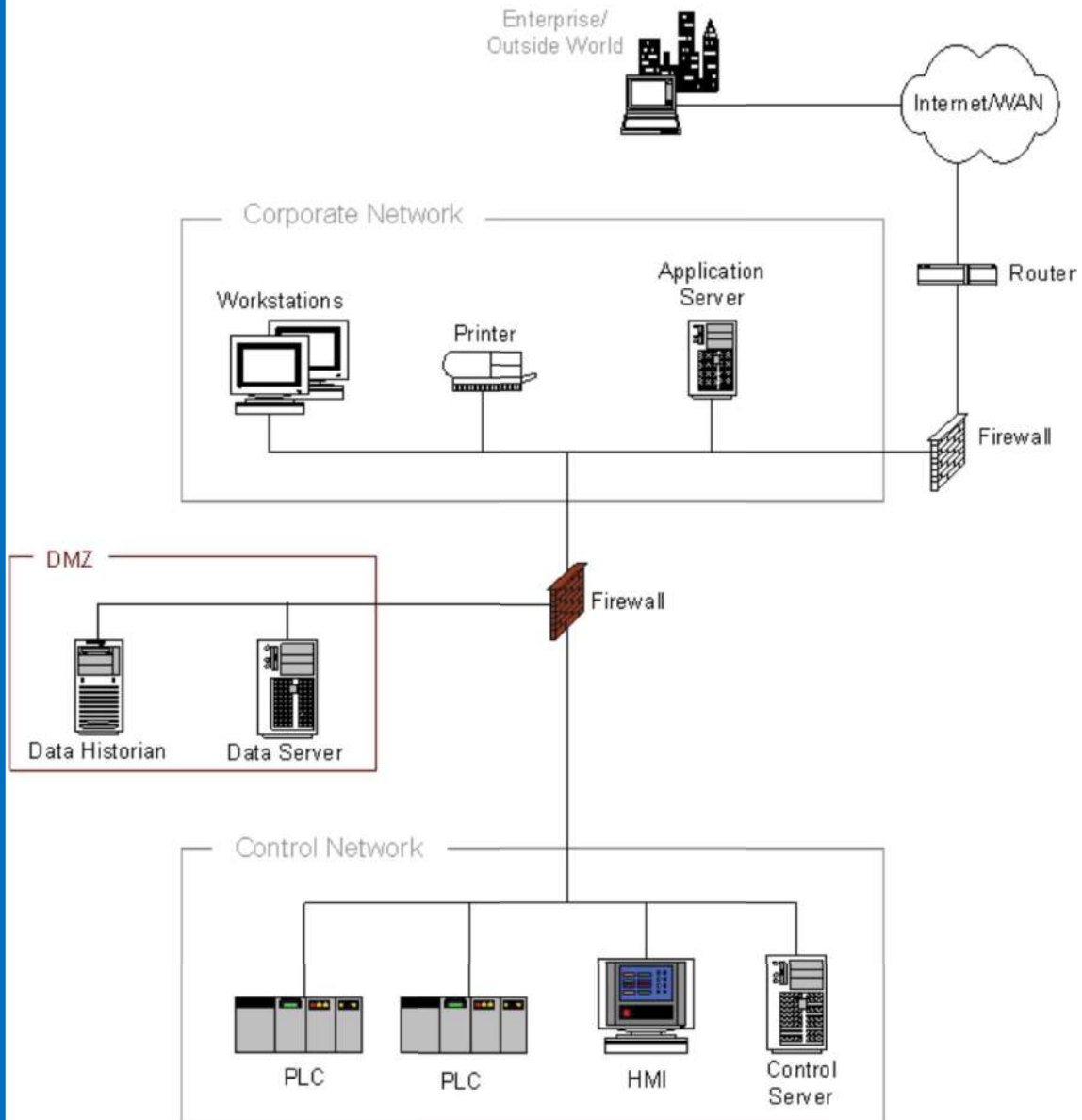
## Chapter 10: References

- This document is prepared in reference of following documents:
  1. ISA 99.0.1
  2. ISA 99.0.2
  3. ISA 99.0.3
  
- The equivalent IEC 62443 standard which has been adopted from ISA 99 has also been referred:
  1. ISA-62443-1-1-WD
  2. ISA-62443-1-3-WD
  3. ISA-62443-1-4-WD
  4. ISA-62443-2-1-WD
  5. ISA-62443-2-2-WD
  6. ISA-62443-3-2-WD
  7. ISA-62443-3-3-WD
  8. ISA-TR62443-2-3-WD
  
- Information system security standard ISO/IEC 27001
  
- Security policy for Information Systems by IndianOil Corporation Limited.

### Firewall between Corporate Network and Control Network



### Firewall with DMZ between Corporate Network and Control Network



**Controls Summary Table**

Sl. No.	Industrial Automation and Control system security control	Comments
1.	Implement Access Control	Implement processes for arbitrating requests for access to critical system information
2.	Conduct Risk Assessment	Identify risks to systems including potential impacts, probabilities, and mitigation options.
3.	Remove Default Accounts	Many automation system manufacturers have default accounts and passwords in place for maintenance or system access. These accounts should be deleted and any default passwords changed or eliminated.
4.	Develop Security Policies	Have policies in place that express management intent, address the security mission, define roles and responsibilities, and address the use of computational resources.
5.	Develop Security Plan	Generate a plan to define and implement security controls, conduct incident response and evaluate security throughout the system's life cycle.
6.	Develop Personnel Screening Policies and Procedures	Implement personnel-related policies and procedures, including screening, transfers, and termination.
7.	Manage Maintenance	Develop and implement policies and procedures to address all parts of system maintenance.
8.	Protect System Information Integrity	Implement policies and procedures to ensure the integrity of data.
9.	Develop Hiring Policies	Implement policies for employee background checks, employment terms, responsibilities, and so on.
10.	Develop Acquisition Policies	Apply risk-assessment-based acquisition policies throughout the system's life cycle.
11.	Provide for Strong Authentication	Employ strong authentication mechanisms at interfaces to the internet and any other public networks.
12.	Test and Evaluate Critical	Implement mechanisms to evaluate

Sl. No.	Industrial Automation and Control system security control	Comments
	Software	software elements for vulnerabilities.
13.	Implement Audit Procedures	Provide for independent evaluation of audit records to determine adequacy of security controls and compliance
14.	Implement and Effective Password Policy	Establish a strong password policy that specifies characteristics, such as length, types of characters, audit frequency, and change periods. The password policy should take into account the balance required between the types of password protected access mechanisms used and the need for an automation system operator to quickly access system components under stress in the event of an emergency.
15.	Identify Critical System Elements	Determine the critical system elements that have to be protected and included in disaster recovery planning.
16.	Apply Defense in Depth	Apply security in layers, beginning with perimeter defense and employing SCADA-aware firewalls and intrusion detection and prevention systems.
17.	Protect Critical Data and Media	Protect sensitive information in all stages of its life cycle, include its use, storage, transit, and disposal. Encryption should be applied according to good security principles.
18.	Provide for Physical Security	Implement physical security controls including back-up power, fire detection and prevention, physical access controls, cameras, badges, and tokens.
19.	Develop an Up-to-Date System Diagram	Prepare and maintain a diagram of the automation system, including topologies, devices (such as PLCs), software in use, protection mechanisms, locations of devices, transducers, and sensors.
20.	Protect Equipment	When possible, place equipment in locations that prevent unauthorized

Sl. No.	Industrial Automation and Control system security control	Comments
		access.
21.	Develop and Implement a Patching Policy	When compatible with real-time and production requirements, test and install patches to critical software that address vulnerabilities. Patches should not be installed on production systems without evaluation on test systems or off-line to ensure that no faults are introduced into production equipment.
22.	Conduct Vulnerability Assessments	When compatible with real-time and production requirements, perform vulnerability assessments in a manner that does not interfere with system operation.
23.	Implement System Logging	Log and review critical system parameters in a manner compatible with the production requirements of automation and control systems.
24.	Manage and Control Remote Access	It is important to control and manage remote access using strong authentication and encrypted links, such as VPNs. Give special security consideration to wireless devices and desktop modems.
25.	Protect communications	Implement methods to protect system transmission elements.
26.	Implement Filtering and Screening	Use devices such as firewalls to protect critical data and support access control.
27.	Provide Security Awareness Training	Provide personnel with security awareness training to alert them to issues such as social engineering, and phishing. They should also be informed on how to determine if an incident has occurred, whom to notify if an incident has occurred, and any actions to be taken in that event.
28.	Maintain Only Necessary Services	Disable any unnecessary systems services and unused open ports.
29.	Undergo Certification and Accreditation	Obtain certification and accreditation and accept residual risk.

Sl. No.	Industrial Automation and Control system security control	Comments
30.	Employ Configuration Management	Implement configuration management practices that document any system hardware and software changes.
31.	Implement Back-Ups	Arrange for backing up system hardware, software, and data in the event of a disaster or other failure of critical systems.
32.	Develop Business Continuity and Disaster Recovery Plans	Develop, test, and implement disaster recovery and business continuity plans.
33.	Secure Extranets	Minimize and secure partner networks or extranets if they are necessary
34.	Use Antivirus Software Intelligently	Implement antivirus software, taking into account the limitations and requirements of automation systems, including its effect on response time and memory capacity.
35.	Implement Program Management	The program management plan specifies the individuals within the organization responsible for the security program management controls and the appointment of a senior information security officer, ensures that all capital planning and investment requests including the resources needed to implement the information security program, develops an enterprise architecture with consideration for information security, and defines mission/ business processes with consideration for information security and the resulting risk to the organization, personnel, and the critical infrastructure.
36.	Predictable Failure Prevention	Control that protects the information system from harm by considering mean time to failure for critical components in specific environments of operation.



## SECTION-V ( SCOPE OF WORK)

---



---



---



---

0	04.11.24	ISSUED with MR	BO	KKP	SM
<b>Rev. No</b>	<b>Date</b>	<b>Purpose</b>	<b>Prepared by</b>	<b>Checked by</b>	<b>Approved by</b>

## 1.0 SCOPE OF WORK

1.1 The scope of work for DCS shall comprise of the following:

Sr No	DESCRIPTION	VENDOR	PURCHASER
1.	Design & system Engineering of specified system including coordination with various contractors/ package vendors during system engineering.	<input checked="" type="checkbox"/>	
2.	Manufacture/ supply of all hardware & software for hooked up new additional I/O as per I/O Summary and sizing consideration (Annexure-II) with existing system to meet specified functional requirements. The scope shall include system configuration, system integration, factory testing & acceptance of the system.	<input checked="" type="checkbox"/>	
3.	Manufacture & supply of auxiliary cabinets and consoles as per material requisition including marshalling cabinets, relay cabinets, MCC interface cabinets, power supply distribution cabinets for all DCS loads (DCS PDB) and NON DCS Loads, along with all accessories & instruments, barriers, alarm cards, terminals, relays, FO cables & converter, Fiber optic patch panel, Network switches , LAN cable power supply distribution cabinets with accessories duly mounted, wired & tested including consoles/ cabinets for other free issue items to meet specified MR requirements. The scope shall include their engineering, wiring, testing, integrated factory testing & acceptance.	<input checked="" type="checkbox"/>	
4.	Manufacture & supply of power supply distribution cabinets for all Non-DCS loads in DDCS-III control room (Non-DCS PDB) with accessories duly mounted, wired & tested as per MR requirements. The scope shall include their engineering, wiring, testing, integrated factory testing & acceptance.	<input checked="" type="checkbox"/>	
5.	Supply of MCT frame and MCT Blocks , Special tools and tackles, tables, chairs etc, asper Special Instruction to Vendor doc. no. B568-304-YE-SP- 1509.	<input checked="" type="checkbox"/>	
6.	Supply of all type of Interconnecting wiring & cabling including power cabling within control room for all vendors supplied equipment's as well as power cabling from vendor's PDB to 3 <sup>rd</sup> party equipment's within control room .	<input checked="" type="checkbox"/>	

7.	Supply of all trays and conduits for all cables within Control Room.	<input checked="" type="checkbox"/>	
8.	Supply of serial link cable between DCS and other foreign devices wherever required as per this requisition.	<input checked="" type="checkbox"/>	
9.	Supply of cable trays (with or without cover) as per MR specifications for DCS vendor supplied cables under false flooring within the existing DDCS-III control room	<input checked="" type="checkbox"/>	
10.	Supply of cable trays (with or without cover) as per MR specifications for all field/MCC cables, cables among 3 <sup>rd</sup> party equipment's and cables between 3 <sup>rd</sup> party equipments and DCS equipments under false flooring and trench within the existing O&MS control room	<input checked="" type="checkbox"/>	
11	Supply of all accessories for installation of cabinets including channel base frames, fasteners, glands for all cables at SRR & new Console area of existing O&MS control room.	<input checked="" type="checkbox"/>	
12	Supply of all accessories for installation of cabinets including channel base frames, fasteners, glands for all cables at SRR & new Console area of Existing DDCS-III control room Rack room area etc for 3 <sup>rd</sup> party's supplied cabinets/conssoles.	<input checked="" type="checkbox"/>	
13.	Packing, forwarding, transportation, custom clearance, insurance, storage at site including unloading of all equipments, keeping under safe custody and shifting of all cabinets/ consoles to Control room of complete system.	<input checked="" type="checkbox"/>	
14.	Installation of all vendor supplied instruments and equipment including cabinets, consoles, racks, equipments, free issued instruments/ cabinets as specified and any other item indicated specifically in the MR including the following:	<input checked="" type="checkbox"/>	
a)	Installation of cabinets including channel base frames, fasteners, glands for all cables at DDCS-III control room etc for DCS vendor's supplied cabinets/conssoles .	<input checked="" type="checkbox"/>	

b)	Installation of cabinets including channel base frames, fasteners, glands for all cables at Existing DDCS-III control room etc. for 3 <sup>rd</sup> party supplied cabinets/consolas /monitors/Equipment's and servers etc. as per MR.	<input checked="" type="checkbox"/>	
c)	Installation of MCT frame, blocks and all its accessories for all field/MCC cables at SRR & new Console area of Existing O&MS control room etc as per MR.	<input checked="" type="checkbox"/>	
d)	Laying and Installation of cable trays (with or without cover) as per MR specifications for DCS vendor supplied cables under false flooring area of Existing DDCS-III control room.	<input checked="" type="checkbox"/>	
e)	Interconnecting wiring & cabling including power cabling between vendor supplied items in Control room including those required for interface with free issue items.	<input checked="" type="checkbox"/>	
f)	Interconnecting wiring & cabling including power cabling within CR between 3rd party supplied items and between 3rd party supplied items and DCS vendor supplied items within CR.	<input checked="" type="checkbox"/>	
g)	Glanding, ferruling & termination of all field cables, interconnecting cables, power cables including those for Package/ Free issued items within DDCS-III Control room.	<input checked="" type="checkbox"/>	
h)	Glanding, ferruling & termination of all field cables, interconnecting cables, power cables for Package/ Free issued items other than DCS vendor supplied items, within Controls rooms.	<input checked="" type="checkbox"/>	
i)	Laying of vendor supplied system cables FO Cable & Prefabricated cable & wiring within DDCS-III Control room as well as between DDCS-III Control room and EPCC-11 Control room.	<input checked="" type="checkbox"/>	
j)	Laying and installation of all trays and conduits for all cables within Control Room.	<input checked="" type="checkbox"/>	
k)	installation of all accessories for installation of cabinets including channel base frames, fasteners, glands/ MCT blocks for all cables at Control Room.	<input checked="" type="checkbox"/>	
l)	Installation of MCT frame, blocks and all its accessories for all field/MCC cables in SRR.	<input checked="" type="checkbox"/>	
m)	Termination of all serial link cables from foreign devices at DCS end including implementation of serial interface of the foreign devices with the DCS.	<input checked="" type="checkbox"/>	

o)	Coordination with various contractors/ package vendors and Owner/ EIL during installation, cable core identification and termination.	<input checked="" type="checkbox"/>	
p)	Powering of all equipment's including free issue cabinets/ equipment's and interconnecting power cabling within control room including vendor supplied equipment's in Check-in change room.	<input checked="" type="checkbox"/>	
q)	Preparation of instrument earth pits near control room as required including supply, laying and connectivity of system earth cables from all cabinets including purchaser's free issue cabinets in control room to system earth pits and further connectivity of system earth pits to electrical earth system through surge protection and isolation devices including supply and installation of the same.	<input checked="" type="checkbox"/>	
r)	Connectivity of all cabinets in control room to electrical protective earthing system including supply and laying of earthing cables	<input checked="" type="checkbox"/>	
15.	Field-testing, loop checking which shall include interlock simulation, commissioning, post commissioning backup & final acceptance of complete system. This includes coordination with various contractors (through EIL/ Owner), EIL/ Owner/ Field Contractor/ other package vendor during above-mentioned activities.	<input checked="" type="checkbox"/>	
16.	Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) as per MR.	<input checked="" type="checkbox"/>	
17.	Supply of consumables and commissioning spares as per MR for DCS system.	<input checked="" type="checkbox"/>	
18.	Supply of two year operation and maintenance spares for DCS system in case ordered by Owner.	<input checked="" type="checkbox"/>	
19.	Documentation including as-built documentation of complete DCS system.	<input checked="" type="checkbox"/>	
20	Integration and interfacing of signals of tankage area to existing IAMS, AIMS, DON, RTDBMS etc		<input checked="" type="checkbox"/>

**1.2** As part of engineering, vendor shall develop documents required for the system engineering of the project, as detailed below:

- a) For all the units including packages, vendor shall develop functional schematics, dynamic graphic display drawings, shutdown logic diagram based on the Piping and Instrumentation Diagrams (P&IDs), Cause and Effect Tables and EIL guidelines for preparing graphic display, which will be provided to the vendor during detailed

engineering. Instrument details/ Point data base, cable schedule shall be provided by Purchaser.

- b) In addition to above Instrument details/ Point data base, shutdown logic diagram and loop / wiring diagram for package items such as compressors, pumps etc. shall be supplied by Purchaser, which will be generated by respective package vendor.
- c) All the above Documents shall be provided to successful vendor only during detailed engineering.
- d) Connectivity between DDCS -III control room IO system and existing EPCC-11 Control system shall be through Fiber Optic cable which shall be supplied and laid by vendor. Termination of FO cable with all required accessories including testing requirement shall also be in the scope of vendor.

**1.3** The detailed scope of work shall be as per this MR.

**1.4** Attachments to Section-V are as below:

- a) DCS/PLC data sheets (Doc. No. B568-304-YE-DS-1501)
- b) I/O Summary and sizing consideration - Annexure-VII
- c) System Configuration Diagram
  - i. System Configuration Diagram B568-304-16-51-2201 RevA.
- d) UPS Power Distribution (B568-304-16-51-31001)
- e) AC UPS Non DCS and 24 V DC Power Supply Distribution List
  - i. AC UPS Non DCS Power Supply Distribution List, Annexure-VIII
  - ii. 24V DC Non DCS Power Supply Distribution List, Annexure-IX
- f) Non UPS Power Distribution (B568-304-16-51-31002)
- g) Existing DDCS-III Control Room Layout showing the new rack room area
  - i. Layout , B568-304-81-46-12111 Rev-B
- h) Existing EPCC-11 Control room layout drawing: EPM24-6373-COO-BLG-DWG-RCBG-2508
- i) Overall Plot Plan B568\_000-81-45-00001 Rev1
- j) ATS Scheme (Annexure-X)
- k) SUPPLIER LIST (INSTRUMENTATION) (Annexure-XI)

## DCS / PLC DATA SHEETS

0	04.11.24	ISSUED with MR	BO	KKP	SM
---	----------	----------------	----	-----	----

Rev. No	Date	Purpose	Prepared By	Checked By	Approved By
---------	------	---------	-------------	------------	-------------

TABLE OF CONTENT

<u>S.No.</u>	<u>Description</u>	<u>Page</u>
I.	Notes	3
II.	Distributed Digital Control System	4
III.	Communication sub-system	8
IV.	Controller and Data acquisition sub-system	11
V.	Operator Interface system	19
VI.	Engineer Interface Sub-system	25
VII.	Network Printers	27
VIII.	Configuration and maintenance printers	28
IX.	Hard-wired consoles	29
X.	Programmable Logic Controller	31
XI.	Foreign Device Interfaces	37
XII.	Hardwired Instruments	39
XIII.	Intrinsic Safety Barriers	41
XIV.	Foundation Fieldbus (FF)Requirements	43
XV.	Consoles, cabinets& accessories	46
XVI.	Notes on wiring	49
XVII.	Training Kit	50
XVIII.	Sequence Of Event Recorder	52



**I - NOTES:**

1. Information already filled-in specifies the minimum system requirements.
2. DCS/PLC Vendor shall provide unambiguous information against all items marked as `\*' in the following data sheets.
3. DCS/PLC Vendor shall complete information against all items marked as `\*\*' in the following data sheets.
4. Note that information provided against all items marked as `\*\*\*' and `\*' must be such that system performance is not degraded.
5. DCS/PLC Vendor shall categorically confirm all items marked as `#' in the following data sheets.

**II - DISTRIBUTED DIGITAL CONTROL SYSTEM**

\* MODEL NO. \_\_\_\_\_

- 1# a) Type of system distribution      Geographical  Functional   
 b) Location      Control Room (O&MS) (Note-1)   
                         Satellite Rack Rooms (SRRs)      [ ]  
                         Others CRs      [ ]

**Note1: Control and Monitoring shall be done from existing console located in existing O&MS DDCS control room.**

- 2.\* System Size (No. of loops per controller):  
 a) Considering all inputs as closed loops \_\_\_\_\_  
 b) Considering all inputs as open loops \_\_\_\_\_
- 3.\*\* System availability for the specified configuration    99.995% [ ]      Offered \_\_\_\_\_
- 4.\* Max communication bus length  
 Standard: \_\_\_\_\_m      With bus Expander: \_\_\_\_\_m
- 5.\* Max number of sub systems on the communication sub system

	No. of Nodes	No. of Consoles	Computer Interface	Other Sub-Systems
STANDARD				
WITH BUS EXPANSION				

- 6.\*\* Type of sub system(s) :
- a) Controller & Data Acquisition sub system      [ ] Model No. \_\_\_\_\_
  - b) Communication sub system      [ ] Model No. \_\_\_\_\_
  - c) Operator Interface sub system      [ ] Model No. \_\_\_\_\_
  - d) Engineers Interface sub system      [ ] Model No. \_\_\_\_\_
  - e) Programmable Logic Controller (ESD)      [ ] Model No. \_\_\_\_\_
  - f) Programmable Logic Controller (Gas Detection)      [ ] Model No. \_\_\_\_\_
  - g) Supervisory computer      [ ] Model No. \_\_\_\_\_
  - h) OPC Server      [ ] Model No. \_\_\_\_\_
  - i) Foreign device interface      [ ] Model No. \_\_\_\_\_
  - j) Personal computer      [ ] Model No. \_\_\_\_\_
  - k) Hardwired instruments
  - l) Unit History Node (UHN)      [ ] Model No. \_\_\_\_\_

- m) Documentation node [ ] Model No. \_\_\_\_\_
- n) Giant Screen [ ] Model No. \_\_\_\_\_
- o) Instrument Asset Management System [ ] Model No. \_\_\_\_\_
- p) Alarm Information Management System [ ] Model No. \_\_\_\_\_
- q) Field Multiplexer [ ] Model No. \_\_\_\_\_

7.\* Foreign Device interfaces required for **(Note 2)**:

- Package Programmable Logic Controllers [X]
- Anti-surge controller [ ]
- Analyser System / Gas Chromatograph [ ]
- Vibration and Temperature monitoring system [ ]
- Machine Condition Monitoring and Analysis System thru OPC server [ ]
- IS Display unit [ ]
- Turbine Speed Control (Governor) [ ]
- Wireless Gateways [X]
- Tank Farm Management System & Blending system [ ]
- Supervisory PC [ ]
- APC thru OPC server [ ]
- Plant LAN thru OPC server [ ]
- RTDBMS thru OPC server (Note-3) [ ]
- Stepless control system for Recip. Comp. [ ]
- Comp. Air Control System (LCP) [ ]
- Alarm Information Management system (AIMS) [ ]
- Giant Screen thru TCP/ IP [ ]
- Others as per I/O list [X]

**Note 2: Refer I/O Summary and System Configuration for the actual type and quantity of the foreign devices**

- 8.# On line self-diagnostic message Required [ ] Module level [ ]  
Local Level [ ] Engg. Station [ ]

9.# Redundant Power supply required for

- a) Controller & Data acquisition sub system [ ]
- b) Communication sub system [ ]
- c) Operator interface sub system [ ]
- (Required for Common Redundant Electronics only)
- d) Engineers interface sub system (individual power supply) [ ]
- e) Programmable Logic Controller (PLC) [ ]

- f) Foreign device interface [X]
- g) Hardwired Inst. including IS Barriers [X] 24V DC Bulk PSU
- h) Racks requiring 24 V DC power supply [X]
- i) Fieldbus power supply [ ] Bulk PSU
- j) Miscellaneous Instruments [ ]

Note: Non redundant systems which doesn't have provision to accept redundant power shall be powered from ATS supplied by vendor.

10.\*\*Power supply availability

- a) AC Voltage for Control Systems:

Details	Supplied	Permissible
Voltage	110 V $\pm$ 10% UPS	
Frequency	50 Hz $\pm$ 3Hz	
Max. Static Transfer Time	5 mSec	

- b) DC Voltage for output devices (SOV): 24V DC [X]
- c) DC Voltage for other interrogation: 24 V DC [X]
- d) AC Voltage for lighting: 240V, 50HZ (Non-UPS) [X]

11.\*\*#UPS System Requirement

- a) \* UPS System : By purchaser

- b)# Type of UPS for DCS &

- Other vendor's supplied Systems

Isolated	[X]	
Grounded	[X]	Ungrounded [ ]

- c)# Type of UPS for Equipment

- Other than the system

Isolated	[X]	
(using isolation transformer)		
Grounded	[X]	Ungrounded [ ]

12.\*\*# Earthing Requirements

- a) Type of Earthing system

Type of Earthing System	Reqd.	Resistance upto Earth Pit	Remarks
Instrument System Earth	Yes	Less than 1 ohm	See Note
Electrical Earth	Yes	Less than 5 ohm	Plant Electrical Earthing System to be used

- b) No. of Earth pits

Common	[ ]	Separate for each earthing system [X]
--------	-----	---------------------------------------

Others \_\_\_\_\_

c) Instrument System Earth pits  
In redundant configuration

By Owner  By Vendor   
[X] (for DCS as well as owner's supplied systems/  
cabinets in CRs- Refer SIV for details)

d) Connectivity between electrical &  
Instrument earthing system

Required  By vendor   
(Note)

**Note – System Earth shall be connected by the vendor to the Plant electrical Earthing System through suitable Surge Protection Device at each building location.**

13.\* Installation details

a) Type of foundation required

Firm  (Console Room & Engg  
room, SRR and CRs)  
On false floor  (Control room)

b) Max. loading for foundation design \_\_\_\_\_ Kg/m<sup>2</sup>

14.# Operating Environment

Control Rooms  Safe area   
Satellite Rack Rooms  Safe area   
Local Operator Rooms  Safe area   
Temperature :- 24 ± 2°C  
Humidity :- 50 ± 5 %  
Others \_\_\_\_\_

**III - COMMUNICATION SUB-SYSTEM**

\* MODEL NO. \_\_\_\_\_

- 1\* Communication Topology      Bus Structure    [ ]  
    Closed ring    [ ]    Any other \_\_\_\_\_  
    STAR            [ ]
- 2# Redundancy in Communication      Required      [ ]
- 3.# Type of Bus redundancy      Active      [ ]    Others \_\_\_\_\_
- 4# Switch-over of communication Buses    Auto only    [ ] Auto & manual    [ ]
- 5\* Type of communication bus      Co-axial      [ ] (Note)  
    Fiber optics    [ ]  
    (Between Control Rooms/ Remote I/O locations)

Note : Vendor's standard Fiber Optic type of cables as communication bus within the control room is also acceptable.

Others \_\_\_\_\_

- 6\* Type of communication      Floating Master    [ ]  
    Fixed Master      [ ]  
    Periodic reporting    [ ]  
    Exception reporting    [ ]  
    Deterministic      [ ]  
    Non-Deterministic    [ ]

Others \_\_\_\_\_

7\* Type of protocol      \_\_\_\_\_

8\* Communication speed      \_\_\_\_\_

- 9\* Message error checking method      CRC      [ ]    DEM      [ ]  
    Others \_\_\_\_\_

- 10\*\*#a) Bus Controller      Required      [ ]    Not required    [ ]  
       b) Redundant bus controller      Required (if 'a' is required)      [ ]

- 11# a) Redundant Communication interface required for the following subsystems/  
 systems (only typical, actual shall be as per I/O summary):  
       Controller & Data-acquisition Subsystem      [ ]

Communication Subsystem	[ ]
Operator Interface Subsystem	[ ]
Engineer Interface Subsystem	[ ]
Programmable Logic Controller (PLC) (ESD)	[ ]
Programmable Logic Controller (PLC) (Gas Detection)	[ ]
Analyser systems / Gas Chromatograph	[ ]
Vibration and Temperature Monitoring System	[ ]
Machine Condition Monitoring and Analysis System thru OPC server	[ ]
Anti-Surge Controllers	[ ]
Turbine Speed Control (Governor)	[ ]
Wireless Gateways	[ ]
Fire Alarm (DGFAP) System	[X]
Tank Farm Management System & Blending Automation System	[X]
APC through OPC server	[ ]
RTDBMS through OPC server	[ ]
Unit History Node(UHN)	[ ]
Instrument Asset Management System (IAMS)	[ ]
Alarm Information Management system (AIMS) (Note-1)	[ ]
Package PLCs	[ ]
Giant Screen through TCP/ IP	[ ]
Stepless control system for Reciprocating Comp	[ ]
Others as per I/O list	[X]

Note-1: If connected through control network

b)# Single communication interface required for the following subsystems/ systems:

Supervisory Computer	[ ]
IS Display units	[ ]
Other	[ ]

12# Switch-over to redundant communication interface

Auto only	[ ]	Auto & Manual	[X]
-----------	-----	---------------	-----

13# Power supply for communication interface	Redundant	[X]
--	-----------	-----

14.# Communication Loading	50 %	[X] (Note-1, 2& 3)
----------------------------	------	--------------------

\*\*Maximum no. of nodes per DCS Network \_\_\_\_\_

\*\*Maximum no. of nodes connecting multiple DCS networks \_\_\_\_\_

Note-1: The communication network loading shall not exceed 50% for networks following deterministic protocols. Networks following non-deterministic protocols i.e. IEEE 802.3 shall be based on maximum allowable loads recommended by manufacturer. (Typically the loading shall be of the order of 15% at maximum throughput).

Note-2: The loading of all communication interface units or communication processors shall not exceed 50% for each DCS.

Note-3: The maximum number of nodes in the network shall not exceed 60% of maximum capacity for each DCS.

15.\* Communication Bus Model No. \_\_\_\_\_

16.# Type of Communication cable

Within Control rooms/SRRs Copper cable (Note) [X] Fiber Optic cable [ ]

Between Control rooms/SRRs Fiber Optic cable [X]

17\*# Communication Cable mechanical protection

Within control room Closed GI tray [ ] Flexible GI Conduit [X]  
in separate GI tray

Outside Control room GI Conduit [ ] Closed PVC conduit [X]

Armoured [X]



**IV - CONTROLLER & DATA-ACQUISITION SUBSYSTEM ( EXISTING)**

\* MODEL NO. \_\_\_\_\_

**A. OFFERED SYSTEM DETAILS**

1# Offered subsystem:

Combined Controller & Data-acquisition

2# Type of Controller Single loop  Multi-loop

**B. GENERAL**

1\* Number of controllers per 19" Rack / Carrier \_\_\_\_\_

2\* Number of 19" Racks / carriers per cabinet \_\_\_\_\_

3\* Number of Controller & Data acquisition cabinets \_\_\_\_\_

4\* Cabinet-wise MTBF \_\_\_\_\_ hours

5\* Cabinet-wise MTTR \_\_\_\_\_ hours

**C. SPECIFICATION**

1# Type   $\mu$ p based  Configurable

2# Enclosure General purpose

3# a)Type of controller Multi-loop

i)\*\*#Multi-loop controller Indicating  Blind   
 Facia size \_\_\_\_\_

Display Bar graph  Digital

Mounting Flush  Rack

Manufacturer's Standard

Number of close loops per controller Available \_\_\_\_\_

With 50 % loading Maximum 100  Actual Offered \_\_\_\_\_

No. of I/O cards per controller Maximum \_\_\_\_\_ Actual Offered \_\_\_\_\_

Back-up controller Required  **1:1 redundancy**

Provided  Not provided

One for Three  One for One

Other \_\_\_\_\_

Switch-over time (Bumpless) Max.1 s  Offered \_\_\_\_\_

Response Time / Scan Time/ Loop Response Time

Variable  Fixed

Flow, Pressure and Differential

Pressure close loops Maximum 500 mSec  Offered \_\_\_\_\_

Level, Temperature, Analysers

Close loops and all open loops Maximum 1 Sec  Offered \_\_\_\_\_

Configuration from Central level  Local level

Tuning from Central level  Local level

MTBF \_\_\_\_\_ hours

MTTR \_\_\_\_\_ hours

Model No. \_\_\_\_\_

b)# Control Modes	Manual	[ <input type="checkbox"/> ]	Auto	[ <input type="checkbox"/> ]
	Cascade	[ <input type="checkbox"/> ]	Computer	[ <input type="checkbox"/> ]

c)\*\*# Tuning constants

Tuning Constant	Required	Offered	Remarks
PROPORTIONAL BAND	1 - 800 %		
INTEGRAL RATE	0.05 - 100 repeats/ min.		
DERIVATIVE TIME	0.01 - 10 min.		
DEAD TIME	0.07 - 10 min.		
LEAD LAG TIME	0.005 - 10 min.		

d)# Reverse/ Direct selection	Required	[ <input type="checkbox"/> ]		
e)# Anti-Reset wind up feature	Required	[ <input type="checkbox"/> ]		
f)# Output status on controller failure	Flunk	[ <input type="checkbox"/> ]	Freeze	[ <input type="checkbox"/> ]
	Engineer Configurable	[ <input type="checkbox"/> ]		

4\*\*# INPUT-OUTPUT SUBSYSTEM

Mounting	Rack	[ <input checked="" type="checkbox"/> ]		
Number of Input /Output per module	Analog	[ <input checked="" type="checkbox"/> ]	Maximum 16	[ <input checked="" type="checkbox"/> ]
			Offered_____	
	Digital	[ <input checked="" type="checkbox"/> ]	Maximum 32	[ <input checked="" type="checkbox"/> ]
			Offered_____	

Redundancy for close loops  
 and interlocks Required [  ]  
 for open loops Required [  ]

(Note: AI card limited to maximum of 16 channels and DI card limited to maximum of 32 channels).

One for One	[ <input checked="" type="checkbox"/> ]	(If Redundant)
One for N	[ <input type="checkbox"/> ]	(Define 'N')
Others_____		

Switch-over time (Bumpless)	Max.1 s	[ <input checked="" type="checkbox"/> ]	Offered_____
-----------------------------	---------	---	--------------

5. CONTROL AND DATA ACQUISITION PROCESSOR( EXISTING)

- a)\*# Back up processor Required [ ]  
 Provided [ ] Not Provided [ ]  
 One for one [ ]  
 Any Other \_\_\_\_\_
- b)\*# Switch-over time (Bumpless) Max.1 s [ ] Offered\_\_\_\_\_
- c)\*# Processor Cycle Time  
 For close loops pertaining to Flow, Pressure & Diff. Pressure  
 Conventional 250 mSec [ ] Any Other\_\_\_\_\_  
 Foundation Fieldbus (FF) 250mSec [ ] Any Other\_\_\_\_\_  
 For close loops pertaining to Level, Temperature, Analysers and all open loops  
 Conventional 500 mSec [ ] Any Other\_\_\_\_\_  
 Foundation Fieldbus (FF) 500 mSec [ ] Any Other\_\_\_\_\_  
 (Above indicates maximum acceptable values. Lower Processor Cycle time to be selected if required to meet the Response Time/Scan Time/ Loop Response Time/ Control Response Period specified in clause 3.a (i) above.)
- d)\* No. of control Blocks \_\_\_\_\_
- e)\* Execution rate \_\_\_\_\_sec/control block
- f)\* Updation rate of back up processor Per Scan [ ] Any Other\_\_\_\_\_
- g)\*# Mounting Manufacturer's Standard [ ]
- h)\* MTBF Value \_\_\_\_\_
- i)\* MTTR Value \_\_\_\_\_
- j)\* Model No. \_\_\_\_\_
- 6# Input isolation Required [ ]
- 7# Output isolation Required [ ]
- 8\*\*# Type of Input Modules:

Type of module	Model No.	Isolation	No. of Inputs per module
4-20 mA DC [X] (Built in HART type)		Through external Isolator	
0-20 mA DC(2 wire) [ ]			
4-20 mA DC(non Hart) [ ]			
1-5 V DC [ ]			
0.25-1.25 V DC [ ]			
OTHER_____			

THERMOCOUPLES	[ ]			
RTD	[ ]			
CONTACT POTENTIAL FREE	[X]		Through external relays / IS barriers	
PULSE/FREQUENCY	[ ]			
RS 232 C/ RS 422/ RS485	[X]			
ETHERNET TCP/IP	[X]			

9\*\*# Type of Output Modules:

Type of module	Model No.	Isolation	No. of outputs per module
4-20 mA DC [X] (Built in HART type)		Through external Isolator	
4-20 mA DC(non Hart) [ ]			
POTENTIAL FREE CONTACT [X]		Through external relays/ IS barriers	
Other [ ]			

10\*\*# Type of Foundation Fieldbus (FF) Modules:

Type of module	Model No.	Isolation	No. of FF segments per module
Foundation Fieldbus H1 Interface module [ ]		Through FF Power Supplies	Maximum 4 nos.

11\*\*# Power supply for Transmitters & Positioners  
(Non Fieldbus)

24 V DC [X]  
Other \_\_\_\_\_

With Controller [ ]

Power supply for SOVs

24 V DC [X]

Redundant common power supply system

[ ]

\*\*# Intrinsically safe(Note) Yes  No   
 With External barrier   
 Without External barrier

Note : Intrinsically safe barrier shall be used for instruments wherever identified in the I/O summary. For non-intrinsically safe instruments/signals (including MCC), vendor shall provide external isolators for analog signals and interposing relays for digital I/Os.

12# Power supply for Fieldbus Field devices FF Power Supplies   
 (with built-in segment isolation as well as power conditioning)

Dedicated & Redundant FF power supply unit for each FF segment

\*\*# Intrinsically safe Yes  No   
 High powered trunk (Field barrier)

13\*Maximum number of alarm settings \_\_\_\_\_

14\*\*#A/D Converter resolution 16 bits  Actual \_\_\_\_\_

15\*\*#D/A Converter resolution 12 bits  Actual \_\_\_\_\_

16\*\*#Load Driving capability 750 Ω  Actual \_\_\_\_\_

17# Load Driving capability of transmitter (non Fieldbus) @ 24 V DC 600 Ω

18\*\*#Maximum allowable source resistance for:

Thermocouple input module  Ω

RTD input module  Ω

19# On-line Diagnostic message available at Local level

Centralised level

20\*\*#Memory type for Configuration Retentive  Volatile

If Retentive Erasive  Non-erasive

\*Erasing by \_\_\_\_\_

If Volatile Battery back-up

\*Battery type \_\_\_\_\_ \*Battery life \_\_\_\_\_

Chargeable

Continuous trickle charge

Configuration protection time 48Hrs

Battery drain indication

\*Retentive memory back up

21# CPU / MEMORY LOADING

- a) CPU loading 50% [ ]  
 b) Memory Utilisation 50% [ ]  
 c) Communication processor loading 50% [ ]

**22 # Auto boot-up on power On Required [X]**

**23\*\* ALGORITHMS**

ALGORITHMS	REQUIRED	OFFERED FOR		REMARKS
		SINGLE LOOP	MULTI-LOOP	
<b><u>BASIC FUNCTIONS</u></b>				
Manual loader	[ ]	[ ]	[ ]	
Cascade(with set point tracking)	[ ]	[ ]	[ ]	
High alarm limit	[ ]	[ ]	[ ]	
Extra High Alarm	[ ]	[ ]	[ ]	
Low Alarm	[ ]	[ ]	[ ]	
Extra Low Alarm	[ ]	[ ]	[ ]	
Rate of change alarm	[ ]	[ ]	[ ]	
Deviation Alarm	[ ]	[ ]	[ ]	
Output High	[ ]	[ ]	[ ]	
Output Low	[ ]	[ ]	[ ]	
High Dev. from set point	[ ]	[ ]	[ ]	
Low Dev. from set point	[ ]	[ ]	[ ]	
<b><u>CONTROL ALGORITHMS</u></b>				
Proportional Control	[ ]	[ ]	[ ]	
PI	[ ]	[ ]	[ ]	
Error Square PID	[ ]	[ ]	[ ]	
Adaptive Gain	[ ]	[ ]	[ ]	
Ratio Control	[ ]	[ ]	[ ]	
PID with Dead Band	[ ]	[ ]	[ ]	
<b><u>ARITHMATIC</u></b>				
Addition/ Subtraction	[ ]	[ ]	[ ]	
Multiplication	[ ]	[ ]	[ ]	
Division	[ ]	[ ]	[ ]	
Absolute value	[ ]	[ ]	[ ]	
Square Root	[ ]	[ ]	[ ]	
Average	[ ]	[ ]	[ ]	

Summation (Integration)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bias	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ramp Function	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<u>LINEARIZATION</u>			
Square Root Extraction	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Flow Computation(Pressure & Temp. compensation)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Thermocouple Linearisation & compensation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
RTD Linearisation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Polynomial	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<u>DYNAMIC</u>			
Lead/Lag	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dead time	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Timer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Feed Forward	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<u>LIMITER</u>			
Low Output Limiter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High Output Limiter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alarm Limiter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Set point Limiter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<u>COMPARISON</u>			
Greater than/ Less than	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Greater or Equal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lesser or Equal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Equal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not Equal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<u>SELECTOR</u>			
Low Selector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High Selector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mean value Selector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auto Ranging for Dual transmitters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Over-ride	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<u>LOGIC</u>			
And	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Or	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Nor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b><u>MISCELLANEOUS FUNCTIONS</u></b>			
Bump-less transfers between all control nodes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Direct or Reverse outputs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>





S.No.	ITEM MODEL No.	FUNCTION	REDUNDANCY (Refer Note)	REMARKS
1.			REQUIRED [ ]	
2.			REQUIRED [ ]	
3.			REQUIRED [ ]	
4.			REQUIRED [ ]	

(Note: Full Redundancy is required if dedicated Centralised database is provided for each Operator group as per System Configuration)

STORAGE DEVICES ARE APPLICABLE IN EACH OPERATOR STATION

3\*\*# Number of Devices (per console)

S. No	TYPE OF DEVICE	NO. OF DEVICES REQUIRED	NO. OF DEVICES POSSIBLE	REMARKS
1.	MONITOR	AS per System Configuration Drawings		
2.	KEYBOARD & MOUSE SETS	ONE/ Monitor		Common keyboard & mouse for dual stack monitor
3.	MULTIPURPOSE PRINTER	AS per System Configuration Drawings.		
4.	HARD COPY UNIT	AS per System Configuration Drawings.		
5.	DVD DRIVE	ONE/ Monitor		Common DVD drive for dual stack monitor

Note: All Network Printers shall be provided as shown in the System Configuration drawing.

4# Inter-changeability between Monitors within a network Required [ ]

5\*\*# Data base update rate 1 second [ ] Actual \_\_\_\_\_s

6\*\*# Spare memory requirement Min. 40% [ ]

System capacity \_\_\_\_\_GB

7. Keyboard Set

a)# Type of keyboard Membrane type [ ] Other \_\_\_\_\_

b)# Number of Operators' keyboards One per Monitor [ ] Other \_\_\_\_\_



- j) Surface Treatment Hard Coating anti Glare [ ]
- k) Length of tag number (characters) 16 alphanumeric [ ] Other \_\_\_\_\_
- l) Length of description (characters) 24 alphanumeric [ ] Other \_\_\_\_\_
- m)#Display update rate 2s [ ] Other \_\_\_\_\_
- n)#Dynamic graphics Required [ ]
- Multi Window Capability Required [ ]
- o)#Control through dynamic graphics Required [ ]
- p)\*\* Screen displays and Call-up time

S.No.	TYPE OF DISPLAY	REQUIRED	CALL-UP TIME(S)*	REMARKS
1.	OVERVIEW	YES		
2.	GROUP DISPLAY	YES		
3.	LOOP DISPLAY	YES		
4.	DYNAMIC GRAPHICS	YES		
5.	REAL-TIME TREND	YES		
6.	HISTORIC TREND	YES		
7.	ALARM SUMMARY	YES		
8.	ALARM HISTORY	YES		
9.	CONFIGURATION	YES		
10.	DIAGNOSTIC	YES		

q)\* Additional vendor standard displays

S.No.	TYPE OF DISPLAY	AVAILABLE	OFFERED	REMARKS

r)\*\*# Display Hierarchy

S. No.	DESCRIPTION	REQUIRE-MENT	SYSTEM CAPABILITY	REMARKS
1.	NO. OF OVERVIEW PAGES	AS REQD.		
2.	NO. OF GROUPS/OVERVIEW	AS REQD.		
3.	NO. OF LOOPS / GROUP	8		
4.	NO. OF GRAPHIC PAGES	AS REQD.		
5.	NO. OF POINTS IN ALARM SUMMARY	AS REQD.		
6.	NO. OF POINTS IN ALARM HISTORY	AS REQD.		

7.	NO. OF TRENDS PER DISPLAYS	AS REQD.		
8.	NO. OF MULTI-TREND DISPLAYS	AS REQD.		
9.	OTHERS	AS REQD.		

Note: Loop display shall also display trends for process variable, set point and output with a sample interval time scale of 1 second and full scale time base of 60 second for tuning the process control loops.

- s)\* Zooming facility Available [ ]  
 t)\*\* Multi Windowing facility Required [ ]

Note: Opening of more than four windows on the same Monitor shall be restricted by the system

u)\*\*#Trending functions: **(Each Operator Console shall be capable of trending all analog points)**

i) Real-time trend

Number of parameters Required ALL TAGS System capacity\_\_\_\_\_

Time base Minimum 0.25 s [ ] Other 1s [ ]

Maximum 5 s [ ] Other User selectable

Time period

10 Min. [ ] Other\_\_\_\_\_ ii)

Historical trend

Number of parameters Required ALL TAGS System capacity\_\_\_\_\_

Time base Minimum 1 minute [ ] Other\_\_\_\_\_

Maximum 10 Minute. [ ] Other\_\_\_\_\_

Time period

31 Days [ ] Other-----

v)\* Dynamic graphic generation:

Number of standard symbols available \_\_\_\_\_

Number of user defined symbols \_\_\_\_\_

10)\*\* Logging Function

a) Number of tags to be logged Required ALL TAGS System capacity\_\_\_\_\_

b) #Number of log reports

Alarm History per shift [ ]

Event logging [ ]

Hourly logs [ ]

Shiftly logs [ ]

Daily logs [ ]

Weekly logs [ ]

Shutdown report [ ]

Trip initiated log [ ]

Others (Note) [ ]

Note: Other log reports as required shall be furnished during execution stage.

c) # Log formats User definable [ ]

11\*\*# Memory type for Configuration Retentive [ ] Volatile [ ]  
 If Retentive Erasive [ ] Non-erasive [ ]  
 \*Erasing by \_\_\_\_\_  
 If Volatile Battery back-up [ ]  
 \*Battery type \_\_\_\_\_ \*Battery life \_\_\_\_\_  
 Chargeable [ ]  
 Continuous trickle charge [ ]  
 Configuration protection time 48 hours [ ]  
 Battery drain indication [ ]  
 \*Retentive memory back up [ ]

12\* System boot-up from Operator console [ ] Engineer console [ ]  
 Other \_\_\_\_\_

13.# Auto boot-up on power On Required [ ]

15\*# Storage disks

a)\* Type of storage disk HDD [ ]  
 Optical (DVD) [ ]

b)\*\* Number of disks and capacity

Sr. No.	TYPE OF DISC	NUMBER (MINIMUM)	MEMORY CAPACITY PER DISK	REMARKS
1.	HDD	One Per Monitor	As per latest configuration as well as OEM's recommendation	Common for dual stack monitor
2.	OPTICAL (DVD) DRIVE (Note)	One Per Monitor	As per latest configuration	
3.	USB Port (Note)	Two Per Monitor		
4.	OTHER			

Note: It shall be possible to activate/ deactivate the external drives only through authorized password.

16\* Any other feature available as a standard:

a) \_\_\_\_\_

b) \_\_\_\_\_

c) \_\_\_\_\_

17#	CPU Loading	50 %	[ ]
18#	Memory Utilization	50 %	[ ]

**VI - ENGINEER INTERFACE SUB-SYSTEM (EXISTING)**

\* MODEL NO. \_\_\_\_\_

- 1# Number of Engineering Station One [ ]  
Other **As per System Configuration**
- 2# Number of Monitors per Engg. Station Two [ ] One [ ]
- 3\* Type of electronics Individual per Monitor [ ] Common [ ]  
Number of Monitors per electronics One [ ] Two [ ]  
µP type 32 bit [ ] 64 bit [ ]  
Memory size \_\_\_\_\_  
Model No. \_\_\_\_\_
- 4# Number of engineering keyboards with Mouse One per Monitor [ ] Other \_\_\_\_\_
- 5# Number of Operation keyboards with Mouse One per Monitor [ ] Other \_\_\_\_\_
- 6\* Maintenance keyboard Required [ ]
- 7# Functional Capability Same as operator interface subsystem [ ]
- 8# Basic functions of Engineering Console  
a) System configuration and reconfiguration [ ]  
b) Group & multi-groups alarm inhibiting [ ]  
c) Plant views with/ without plant operation [ ]  
d) Graphic page compilation [ ]  
e) Setting/ resetting real-time clock [ ]  
f) Loop tuning on selectable basis [ ]  
g) System maintenance and diagnostics [ ]
- 9# Monitor specification As per operator interface subsystem [ ]
- 10# Keyboard specification As per operator interface subsystem [ ]

11\*\* Data storage Devices and capacity

Sr. No.	TYPE OF DISC	NUMBER (MINIMUM)	MEMORY CAPACITY PER DISK	REMARKS
1.	HDD	One		RAID-5/RAID-10 Configuration



2.	OPTICAL (DVD) DRIVE (Note)	One		
3.	USB Port (Note)	Two		
4.	OTHER			

Note: It shall be possible to activate/ deactivate the external drives only through multi-level authorized password.

12# Peripheral requirements:

- i) Printer (C&M) Required [ ]  
(As per System Configuration)
- ii) Hard copy unit Required [ ]
- iii) Other \_\_\_\_\_

**VII - NETWORK PRINTERS( NOT APPLICABLE)**

\* MODEL NO. \_\_\_\_\_

1#\*\* Type of Printer Dot Matrix [ ]  
 Laser Printer with Scanner [ ] Colour [ ](Note)

(Note: As per System Configuration)

Serial Printer [ ]

2# Function Multipurpose with scan function(As per System Configuration) for

Alarm & Event Report [ ] Log Report [ ]

SOE [ ] C&M [ ](Note)

Hard Copier Unit for

Graphic report [ ]

3\*\* Network Connectivity TCP/IP Ethernet [ ] Others \_\_\_\_\_

4# Print Command from Each Operator console [ ] Engg. Station [ ]

PLC Engg. Station [ ] Others [ ]

SOE Station [ ]

(As per System Configuration)

5\*\* Distance from Various Consoles/stations As per ,SRR & Existing CR Layout

Limitation (if any) \_\_\_\_\_

6\*\* Printing Speed 6 Pages/Min or more [ ] Actual \_\_\_\_\_

7 a) Dot Matrix:

i)\* Paper type Continuous [ ] Cut Sheet [ ]

ii)\*\* Paper size A4 [ ] Offered \_\_\_\_\_

iii)\* High voltage protection type Optical barriers [ ] Other \_\_\_\_\_

b)\* Laser:

i)\*\* Resolution 640 dpi or better [ ] Actual \_\_\_\_\_

ii)\*\* Paper Size 'A4' & 'A3' [ ] Actual \_\_\_\_\_

iii) Paper Type Continuous [ ] Cut Sheet [ ]

iv)\*\* Paper Feed Friction [ ] Pin Feed [ ]

iv)\* Acoustic Cover Required [ ]

v)\*\* Noise level (in dBA) while printing at a distance of 1 m:

Required < 65 dBA

Offered \_\_\_\_\_

8# Power Supply 110 V, 50 Hz [ ] 240V, 50 z [ ]

(Note: Printers shall be suitable for operation from 110 V to 240 V AC with 110 V AC UPS distribution)

9# Mounting Self contained with Integral stand [ ]

10# Quantity As per System Configuration.



**IX - HARDWIRED CONSOLES**

\*Model No. \_\_\_\_\_

1. Number of Hardwired console per operator console:

S.No.	OPERATOR CONSOLE	NUMBER OF HARDWIRED CONSOLES	REMARKS
1.	Offsite Tankages and associated facilities	AS REQUIRED	In existing console of O&MS Control room.( Note)

**Note: Additional Push Button , Annunciation, Lamp, Selector switch , Emergency shutdown Push button shall be accommodated in the existing hardware console.**

2. Instrument Located on Hardwired consoles:(AS REQUIRED)

INSTRUMENT TYPE	NUMBER REQUIRED ON HARDWIRED CONSOLE WITH	
	REQUIREMENT	CONSIDERED BY VENDOR ##
INDICATORS (Electronic Water Level- Free issue item)	AS PER MR	
HARDWIRED ANNUNCIATORS	AS PER MR	
INDICATING LAMPS	AS PER MR	
SWITCHES	AS PER MR	
PUSHBUTTONS	AS PER MR	
TELEPHONE SETS ( Free issue)	AS PER MR	
HAND SETS FOR COMMUNICATION SYSTEM (free issue items)	AS PER MR	
OTHERS	AS PER MR	

3# Power supply for Alarm Annunciator 110 V AC, 50 Hz. [X]

4# Power supply for switches, lamps, pushbuttons etc. 24 V DC [X]

**X - PROGRAMMABLE LOGIC CONTROLLER**

\* MODEL NO. \_\_\_\_\_

- 1# Functional requirement Plant ESD including all Process  
 Safety & Operational Interlocks  [X]  
 Fire & Gas Detection  [X]

**Note: ESD PLC shall be separate from Fire & Gas Detection PLC and existing ESD PLC and Fire & Gas Detection PLC shall be used.**

2# System Configuration Type

- 2.1# Single PLC  [ ]  
 a) Redundant dual processor with dual tested I/O  [ ] I/O auto-testing  [ ]  
 b) Triple Modular Redundant (TMR)  [ ] 2oo3vote output  [ ]  
 c) Quad  [ ]

(Note: Both configuration b & c are acceptable. Vendor to specify the type of PLC configuration being offered)

- d) Safety Certification (as per IEC 61511) SIL 2  [ ] SIL 3  [ ]  
 (for both point b & c above)

3. PROCESSOR SYSTEM

- 3.1\*\*# Functional capability Logic Functions  [ ] Timing Functions  [ ]  
 Range: 0-99,999 s  
 Least count: 0.01 s

\*Other available as standard \_\_\_\_\_

- 3.2\*\*# Interfacing capability I/O Racks  [ ] DCS Bus  [ ]  
 PLC Consoles  [ ] Printer  [ ]  
 Other \_\_\_\_\_

3.3\* Memory capacity \_\_\_\_\_

3.4\* Memory used \_\_\_\_\_

3.5\* Spare memory available \_\_\_\_\_

- 3.6\*\*# Memory type Retentive  [ ] Volatile  [ ]  
 If Retentive Erasive  [ ] Non-erasive  [ ]

\*Erasing by \_\_\_\_\_

If Volatile Battery back-up  [ ]

\*Battery type \_\_\_\_\_ \*Battery life \_\_\_\_\_

Chargeable  [ ]

Continuous trickle charge  [ ]

Configuration protection time 48hours  [ ]

Battery drain indication  [ ]

Retentive memory back up  [ ]

3.7\*# Scan Time 250 mSec [ ] Actual \_\_\_\_\_ ms

3.8\* Power supply Redundancy / Processor Individual [ ]  
Redundant [ ]

3.9.# Outputs on processor system failure Freeze [ ] Open [ ]  
Close [ ] Configurable [ ]

(Outputs shall be configured to open on processor failure, unless otherwise specified)

3.10\* Maximum distance between PLC & Console - As per SRR , & CR Layouts  
Allowable \_\_\_\_\_ m

4# INPUT/ OUTPUT SYSTEM

4.1# Type Discrete [ ] Analog [ ]

4.2# Mounting 19" Rack [ ] Other \_\_\_\_\_

4.3 Input / Output Type

a)#Intrinsic safe [ ] With external barriers [ ]

b)#Non-Intrinsic Safe [ ]

With external isolator [ ] (for Analog inputs and outputs)

With interposing relays [ ] (for Non-IS for Digital I/Os)

4.4\*\*#Remote I/O capability Required [ ] Available [ ] Not Available [ ]

Note : Only for signals shown in System Configuration

a)#Redundant [ ]

b)#I/O rack to processor link

Redundant [ ] SIL 3 [ ]

4.5##Online replacement of I/O modules Required [ ]

\*\*#With installed cards in the hot slots only in case of TMR [X](See Note)

**(Note: One installed spare I/O card of each type for each TMR PLC sub-system**

4.6# I/O status Indication Required [ ] Local level [ ]  
PLC Console [ ]

4.7\*\*#Input Isolation Required [ ] Optical [ ]  
Other \_\_\_\_\_

Output Isolation Required [ ] Optical [ ]  
Other \_\_\_\_\_

4.8\*I/O Capability

TYPE OF MODULE	MODEL No.	CAPACITY	I/O's USED
ANALOG INPUT WITH HART			
ANALOG OUTPUT			

DIGITAL INPUT			
DIGITAL OUTPUT			
REMOTE ANALOG INPUT			
REMOTE DIGITAL INPUT			
REMOTE DIGITAL OUTPUT			

4.9 Maximum distance between I/O rack & Processor - As per Overall & CR Layouts

Allowable \_\_\_\_\_ m

4.10# I/O redundancy Required  Not Required [ ]

Redundancy level As per PLC system configuration (TMR/ Quad)

Auto testing of I/O's Required

4.11#Power Supply per I/O rack Individual [ ] Dual Redundant

4.12#\*\*I/O Rack to processor link SIL 3

Individual [ ]

Dual Redundant [ ]

Triplicate  (for TMR)

Redundant for each set of dual I/O  (for Quad)

4.13# I/O Conditioning for / TMR/ Quad configuration Required

4.14 Input module:

a)# Input Type 4-20 mA with HART

Volt free contact

contact rating 0.5 A @ 110 V DC [ ] 2 A @ 24 V DC

(through interposing relay)

Other \_\_\_\_\_

b)\*\* Maximum number of Inputs per module Single Eight [ ]

Dual Sixteen [ ]

TMR Thirty two [ ]

Quad Sixteen [ ]

Other - As Per Safety Certification

Note : The no. of channels per card shall be as per Safety Certification subject to limitation of 32 channels per card.

c)# Input Interrogation voltage 24 V DC

Other \_\_\_\_\_

d)# Transmitter power supply 24 V DC  With I/O module [ ]

2-wire  [X]

3-wire  [X] (Only for Gas detectors)

e)**	TYPE OF MODULE	MODEL No.	INPUTS / MODULE	INPUT IMPEDENCE ( $\Omega$ )	INRUSH CURRENT (A)
	4-20mA DC With HART				
	1-5V DC				
	Contact				
	Any Other				

4.15 Output module

a)# Output Type

Volt free contact  [X]

4-20 mA  [X]

Contact rating

0.5 A @ 110 V DC  [ ] 2 A @ 24 V DC  [X]

5 A @ 240 V AC  [X] 0.2 A @ 110 V DC  [X]

Other: \_\_\_\_\_

b)\*\*Maximum number of Outputs per module

Single Eight [ ]

Dual Sixteen [ ]

TMR Thirty two [ ]

Quad Sixteen [ ]

Other - **As Per Safety Certification**

Note : The no. of channels per card shall be as per Safety Certification subject to limitation of 32 channels per card.

c)*	O/P CONTACT RATING	MODEL No.	NUMBER OF OUTPUTS/MODULE
	24 V, 2 A dc (Inductive)		
	240V, 5.0A AC		
	110V, 0.2A DC		
	Any Other		

d)# Output Load Capability

600  $\Omega$   [X]

e)# Line monitoring

[X] (Note)

(Note:- Refer cl.6.1.5 of 6-52-0055. Suitable End-of Line resistance / accessories shall be provided by vendor for Line monitoring upto field device.)

5. PLC CONSOLE( NOT APLICABLE)

\*Model No. \_\_\_\_\_

5.1# Function

Engineering

[ ] Operation  [X] (Note-1)



Number of Monitor per console      One      [ ]      Other  
 Type      Colour – LED      [ ]      Monochromatic [ ]  
 Size      21" Diagonal      [ ]      Other\_\_\_\_\_

**Note-1:** PLC Engineering cum Operator Console shall be provided separate from PLC SOE stations. Refer System Configuration.

**Note-2:** Other specifications same as Operation console monitor. The number of engineering stations and SOE stations shall be as per System Architecture)

5.2# Redundant Link between processor system & console      Required      [ ]

5.3\* Number of Keyboards      One per monitor [ ]  
 Type      Spill Proof      [ ]      Offered\_\_\_\_\_

5.4\*\* Printer      Required      [ ]      Model\_\_\_\_\_

(Specification same as given for the network printers)

5.5\*\* Programme storage      Required      [ ]      On CD      [ ]  
 Capacity\_\_\_\_\_GB      Access time\_\_\_\_\_ms  
 Other\_\_\_\_\_

5.6# System Boot-up on power-on      Auto      [ ]

5.7\*\*#Software features:

- a) Online Programming      Required      [ ] **Note-1**
- b) Online Programme modification      Required      [ ] **Note-1**
- c) Disable/Force facility      Required      [ ] **Note-1**
- d) Power flow on Ladder/ logic      Required      [ ] **Note-1,2**
- e) First out alarm Capability      Required      [ ] **Note-2**
- f) Self diagnostics      Required      [ ] **Note-1**
- g) I/O mapping      Required      [ ] **Note-1**
- h) Plant operation      Required      [ ] **Note-2**
- i) Alarm Printing      Required      [ ] **Note-1,2**
- j) Documentation      Required      [ ] **Note-1,2**
- k) Ladder Logic Monitoring      Required      [ ] **Note-1,2**
- l) Graphic capability      Required      [ ] **Note-2**
- m) Shutdown Report Generation & printing Required      [ ] **Note-1,2**

Note-1:Required in PLC Engineering station.

Note-2:Required in F&G PLC Operator station.

5.8\* Additional special software:

- a)\_\_\_\_\_
- b)\_\_\_\_\_
- c)\_\_\_\_\_

5.9# Interface with DCS      \*Model No.\_\_\_\_\_

a)\*\* Type of Interface  
 Serial      [ ]      Bi-directional      [ ]

OPC  RS-232   
Common Redundant Communication sub-system for DCS and PLC   
Other \_\_\_\_\_

b)\* Protocol Type MODBUS  TCP/IP   
Other \_\_\_\_\_

c)\* Module details:

CONFIGURATION	INTERFACE MODEL No.	NUMBER OF MODULES	NUMBER OF ADAPTERS PER MODULE
DUAL PROCESSOR			
TRIPLE MODULAR REDUNDANT			
QUAD			

d)\* Total time taken to Display alarms generated by PLC on DCS operator console through the communication link \_\_s

#### 5.10#Power Supply

- a) System 110 V AC, 50 Hz UPS
- b) Input Interrogation contact voltage& rating 24 V DC, 2A   
(See Note)
- c) Output Contact Voltage& rating 24V DC, 2A   
(See Note) (For solenoid valves)  
240 V AC, 5A   
(For contactor fed LT motors)  
110 V DC, 0.2A   
(For breaker fed LT motors & HT motors)
- d) AC Voltage Distribution Vendor's Scope
- e) Dual redundant 24 V DC Vendor's Scope

Note: Interposing relays to meet the ratings specified above to be provided.

**XI - FOREIGN DEVICE INTERFACES**

- A) INTERFACE WITH PACKAGE PLCs \*Model No. \_\_\_\_\_
- (Third Party Package PLCs / Control system as identified in the System Configuration and I/O Summary)
- 1#\*\* Type of Interface Serial  Bi-directional   
RS-422/485/TCP-IP  Other \_\_\_\_\_
- (Note: Package wise type of interface i.e. RS 485 or TCP/IP shall be intimated during detail engineering)
- 2 Type of Redundancy:
- # For Dual redundant processor / Quad / TMR Dual Redundant   
Active   
\*\* Switchover time \_\_\_\_\_ s
- (Note: Each link shall be connected to separate serial interface cards)
- 3\* Interface Throughput: Number of Digital I/Os \_\_\_\_\_  
Number of Analog I/Os \_\_\_\_\_
- 4#\*\* Standard interface software available for MODBUS RTU   
Other \_\_\_\_\_
- 5\* Proven interface software available for following Package PLC's:
- a) Make \_\_\_\_\_ Model No. \_\_\_\_\_  
b) Make \_\_\_\_\_ Model No. \_\_\_\_\_  
c) Make \_\_\_\_\_ Model No. \_\_\_\_\_  
d) Make \_\_\_\_\_ Model No. \_\_\_\_\_
- 6# Functional Requirements:
- Type of communication Simplex  Full Duplex  (Note)
- (Note: Each link shall be connected to separate serial interface cards)
- Automatic Time synchronization Required   
Transfer of PLC diagnostics Required   
Interface diagnostics available at Central level  Local level   
Other \_\_\_\_\_
- 7# Interfacing of Package PLC with DCS
- Gateway
- Gateway for package PLCs/ control systems interface to DCS shall be as per the details shown in the System Configuration.**
- 8.\* Time taken to transfer data  
from Package PLC to operator console \_\_\_\_\_
- 9.\* Model No. \_\_\_\_\_

B) INTERFACE WITH OTHER FOREIGN DEVICES ( TFMS SYSTEM)

(Third Party Systems as identified in the System Configuration and I/O Summary)

- 1.\*\*# Type of Interface Serial  [X]  
 RS 422/485/TCP-IP  [X]  
 Any other \_\_\_\_\_
- 2.# Communication Protocol Vendor Standard [ ] MODBUS RTU  [X]
- 3.# Type of Redundancy Dual  [X] Triple [ ]
- 3.# No. of Foreign Device \_\_\_\_\_ [ ] As per I/O Summary  
 Interfaces Maximum
- 4.\* Input capability Number of Digital I/Os \_\_\_\_\_  
 Number of Analog I/Os \_\_\_\_\_
- 5.\*\* Proven interface software available for  
 Wireless Gateways (HART) Makes \_\_\_\_\_  
 Wireless Gateways (ISA) Makes \_\_\_\_\_  
 Anti-Surge control system Makes \_\_\_\_\_  
 Turbine Speed Controller (Governor) Makes \_\_\_\_\_  
 Machine Monitoring System Makes \_\_\_\_\_  
 Analyser Systems Makes \_\_\_\_\_  
 IS Display units Makes \_\_\_\_\_  
 Others Makes \_\_\_\_\_
- 6.# Functional Requirement  
 Type of communication Simplex [ ] Duplex  [X] Note)  
 (Note: Each link shall be connected to separate serial interface cards)  
 Automatic Time Synchronisation Req'd.  [X]  
 Transfer of Foreign Device System Diagnostics Req'd.  [X]  
 Interface diagnostics available at Central level  [X] Local level  [X]  
 Any other \_\_\_\_\_
- 7#\*\* Interfacing of Foreign Device with DCS (Note-2)  
 Serial Interface Card of CDAS  [X]  
 Gateway  [X](Note-1)  
 (Note-1:- Separate Gateway is also acceptable subject to meeting the provenness requirement of the system as per MR).  
 Note-2: No. of serial link ports per serial interface card / gateway shall not be more than 4 nos. subject to meeting loading criteria and considering separate card/ gateway for redundant interfaces)
- 8.\* Time taken to transfer data  
 from Foreign Device to operator console \_\_\_\_\_
- 9.\* Model No. \_\_\_\_\_

**XII - HARDWIRED INSTRUMENTS( EXISTING)**

- A) HARDWIRED ANNUNCIATOR \*Model No. \_\_\_\_\_
- a)# Type Audio  Visual   
Microprocessor based
- b)# Sequence As per ANSI/ISA-18.1 F3A / A2
- c)# Mounting Flush
- d)# Power supply location with logic
- e)# Logic Unit Integral  Separate
- f)# Display type Back lighted  Two lamp/alarm   
Clustered LED type/alarm
- g)# \*window size \_\_\_\_\_
- h)# Hooters External to DCS  Solid Sate
- i)# Alarm Acknowledgement Integral  Separate

**Note: Signals shall be accommodated in the existing HARDWIRED ANNUNCIATOR.**

- B) HARDWIRED SWITCHES/ PUSHBUTTONS/LAMPS \*Make \_\_\_\_\_  
\*Model No. \_\_\_\_\_
- a)# Contact type Silver Alloy Plated  Make Before Break
- b)# Sealed Contact housing Required
- c)# Contact rating 5 A @ 240 V AC  2 A @ 24 V DC
- d)# Lamps type Clustered LED type/alarm
- e)#Emergency shutdown switch Pull type red coloured with Mushroom head and protective cover with 3 independent contacts. All three contacts shall be wired to ESD in 2oo3 configuration   
Push type with Mushroom head and protective cover

(Note-1: Pushbuttons and bypass switches mounted on Hardwired consoles shall be back-lighted self-glow type without need for any return path for feedback

Note-2: Hardwired switches, pushbuttons, lamps in HWC in console room which are to be connected to PLC in SRRs shall be connected through hardwire cabling shown in system configuration)

- C) SIGNAL ISOLATOR FOR NON-IS ANALOG SIGNALS \*Make \_\_\_\_\_  
\*Model No. \_\_\_\_\_
- a)# Input 4-20 mA DC (2 wire)
- b)# Output 4-20 mA DC
- c)# Isolation (Galvanic 3 port) Required
- d)# Number of outputs One   
Two  (Note 1)

Note 1: Number of inputs and outputs shall be same as that specified for intrinsic safety barriers in Section XIII of this document)

e)# Power Supply 240 V AC, 50 Hz [ ] 24 V DC [X] (Note)  
Other \_\_\_\_\_

(Note: Through redundant BPS by vendor)

f)#SIL 3 / SIL 2 certified [X] (Note)

(Note: For DCS I/Os -SIL2 certified and for PLC I/Os SIL 3 certified)

f)\* Mounting Rack [ ] DIN Rail [ ] Others \_\_\_\_\_

D) INTERPOSING RELAYS

a)# SIL 3 certified [X](Note)

(Note: For PLC I/Os only)

Contact Ratings

i)#\*\* 24V DC, 2A [X] Make & Model No. \_\_\_\_\_

ii)#\*\* 240V AC, 5A [X] Make & Model No. \_\_\_\_\_

iii)#\*\* 110V DC, 0.2A [X] Make & Model No. \_\_\_\_\_

b)# non SIL certified [X] (Note)

(Note: For 'DCS I/Os)

Contact Ratings

i)#\*\* 24V DC, 2A [X] Make & Model No. \_\_\_\_\_

c)\* Mounting Rack [ ] DIN Rail [ ] Others \_\_\_\_\_

**XIII - INTRINSIC SAFETY BARRIERS**

- 1 Function : To limit the transfer of energy to hazardous area.  
2 Hazardous area Classification:

Unit/ Area	Electrical Area Classification	Remarks
BitiroX Unit (466)	IEC Zone __, Gas Group __, T3	In SRR

- 3 Location CR/SRR[X] Safe Area [X]  
4 Specifications  
4.1# Type Non Isolating [ ] Active Isolating [X]  
Three Port [X]

SIL 3 / SIL 2 certified [X] (Note)

(Note: For DCS I/Os -SIL2 certified and for PLC I/Os SIL 3 certified)

a)#\*\*For Analog inputs Single input, single output with HART [X]  
(Note-1)  
Make & Model No. \_\_\_\_\_

Single input, dual output [X]  
(Note-2)  
Make & Model No. \_\_\_\_\_

(Note-1: Analog input barriers with two field inputs shall not be considered.)

(Note-2: For 5% of the analog inputs (WB) barriers shown under PLC I/O summary, dual output barriers shall be provided with at least one of the outputs having HART alongwith 4-20 mA)

b)#\*\* For Digital inputs  
Contacts [X] Make & Model No. \_\_\_\_\_  
Proximity type Switches [X] Make & Model No. \_\_\_\_\_

c)#\*\* For Digital outputs  
Contacts [X] Make & Model No. \_\_\_\_\_

- 4.2\* External Power Supply Required [X] Not Required [ ]  
110 V, 50 Hz [ ] 24 V dc [X] (Note)  
Others \_\_\_\_\_

(Note: Through redundant BPS by vendor)

- 4.3\* Barrier specification  
4.3.1 Transfer accuracy Temperature 0.05%[X] Analog 0.075% [X]  
4.3.2 Response time Analog 250 µsec [X] Digital 20 msec [X]  
4.3.3 Status indication Required [X]  
4.3.4 Cold Junction Error 1°C [X]  
4.3.5 Cable Parameters As per Cable Specification  
4.4# Maximum fault voltage 250 V rms. [X]  
4.5\* Grounding Individual through bus bar [ ]

4.6\* Mounting Rack [ ] DIN Rail [ ] Others \_\_\_\_\_

5# Statutory Certification Required(From recognized statutory body)

6\* Safety Parameters : To suit Instrument and cables supplied. Ensure that the Barriers are suitable for the cable parameters of the cables supplied by the vendor

SIGNAL TYPE	CABLE TYPE	R( $\Omega$ /km) (max DC resistance at 20°C)	L/R( $\mu$ H/ $\Omega$ )	C(pF/m) at 1 KHz (core & screen) (max)	C(pF/m) at 1KHz (mutual) (max)
4-20 mA & CONTACTS	12P X 1.5 mm <sup>2</sup> Shielded (7 strand each of 0.53 mm dia.)	12.3	40	400	100 (All cables are with XLPE primary insulation)
4-20 mA & CONTACTS	12P X 2.5 mm <sup>2</sup> Shielded (7 strand each of 0.67 mm dia.)	7.5	70	400	
4-20 mA (for Gas detectors only)	8T X 2.5 mm <sup>2</sup> Shielded (7 strand each of 0.67 mm dia.)	7.41	60	400	

**XIV – FOUNDATION FIELDBUS (FF) REQUIREMENTS( NOT APPLICABLE)**

- 1# Control Methodology Control in Host (DCS) [ ]  
Control in Field [ ]
- 2# Close loop implementation through FF  
Simple Close Loops [ ] Cascade [ ]  
Split range [ ] Complex loops [ ]
- 3# FF Segment Philosophy: High Powered Trunk Field [ ]  
FISCO [ ] FNICO [ ]  
Maximum No. of close loops per segment One [ ]  
Maximum No. of Segments per FFJunction Box Two [X](refer SIV for details)
- 4# Topology Tree [ ] Chicken Foot [ ]  
Daisy Chain [ ]



5#	LAS Functionality	H1Card	[ ]		
		Transmitter	[ ]	Positioner	[ ]
	Back-up LAS	Redundant H1Card	[ ]		
		Transmitter	[ ]	Positioner	[ ]
6#	Loop Response Time				
	For Close loops pertaining to Flow, pressure, Diff. pressure	500 msec.	[ ]		
	For Close loops pertaining to Level, temperature, Analyser and all open loops	1 sec.	[ ]		
7#**	Macrocycle	500 msec.	[ ]		
		1 sec.	[ ]		
		Any Other	_____		
8#**	Scheduled Communication	Max. 50% of Macrocycle time	[ ]		
		Any Other	_____		
9#	FF Power Supply (FFPS)				
	a) Function: Segment Isolation and Power Conditioning		[ ]		
	b) Redundant for each segment		[ ]		
	c) External Power Supply	Required	[ ]		(Note)
		(Note: Through redundant BPS)			
	d)* Mounting	Rack [ ]	DIN Rail [ ]	Others _____	
	e) Output from FFPS	Required 28V DC, 500 mA	[ ]		
		Available _____			
	f) Min. voltage availability at last device of segment	9.5 V	[ ]		
	g) Short Circuit protection limit per segment	45 mA	[ ]		
	h)* Make & Model No.	_____			
10#**	Surge Protector	Required	[ ]		
		At Marshalling Racks	[ ]		
		At FieldJB	[ ]		
		At Spur devices	[ ]		
		Make & Model No.	_____		
11#**	Terminator	Required	[ ]		
		At Marshalling Racks	[ ]		
		At FieldJB	[ ]		
		Make & Model No.	_____		
12#	FF Segment Grounding	As per AG-181	[ ]		
	Individual for each Segment	[ ]			
	(Note: For each Segment, Grounding shall be at only one point and in CR/SRR)				
13#	FF Junction Box and Accessories				
	Construction	JB	SS316		[ ]

	Cable Glands	Nickel Plated brass	[ ]
Hazardous Area Certification	JB	Ex'e'	[ ]
	Cable Gland for Trunks	Ex'd'	[ ]
	Cable Gland for Spurs	Ex'd'	[ ]
No. of FF IS Barriers per JB	Maximum Three	[ ]	(Each JB shall have 12 spur devices)
**No. of Spurs per IS Barrier	Four	[ ]	Six [ ]
Installed Spare spurs per segment	25%	[ ]	
Isolation for Each Spur	Required	[ ]	
Statutory Certification			
from recognized statutory body	Required	[ ]	
**IS Barrier	Make & Model No.		_____
**Segment Terminator	Required	[ ]	
	Make & Model No.		_____
**Surge Protector	Required	[ ]	(as per SIV for spur devices)
	Make & Model No.		_____
14# Cable Parameters	As per Cable Specification (Note)		
	(Note: Fieldbus Cable shall be shielded 1Pair x 18 AWG (0.82 mm <sup>2</sup> ) [for each Spur] / 2Pair x 16 AWG (1.31 mm <sup>2</sup> ) [for Trunk of each segment] Type A defined in IEC-61158-2)		
	To suit Instrument and cables supplied. Ensure that the Barriers are suitable for the electrical parameters of the cables and instruments.		
15# Hazardous Area Classification	Refer 'Section XIII' on Intrinsic Safety		
16# Advanced Diagnostic Module	Required	[ ]	
Mounting	FFPS Motherboard		
Quantity			
**Model No.			_____
17# HIST for DCS	Required	[ ]	
18# FFTick Mark for all FF Components	Required	[ ]	

**XV - CONSOLES, CABINETS AND ACCESSORIES**

\*Model No. \_\_\_\_\_

1\* Installation Location

a) Location Indoor  [X]

b) Flooring False  [X] (CR)  
Concrete  [X]  
Console Room & Engg room and SRR Rack Room

c) Floor Loading Limits No  [ ] 1200 kg/m<sup>2</sup>  [ ]  
d) Vibration No  [ ] Yes  [X]  
e) Air Conditioning Yes  [X] No  [ ]

2 General Details

a)# Type Self Supported  [X] Free Standing  [X]  
b)# Panel/Cabinet Enclosed Cubicle  [X] (Note)

Note: Components other than utility sockets shall not be mounted on the cabinet side walls.

c) Graphic requirements Non-Graphic  [X] Semi-Graphic  [ ]  
d)# Lighting No  [ ] Yes  [X]  
For Inside Cabinet  [X] Door Switch  [X]

Power supply 240 V AC, 50 HZ  [X] Other \_\_\_\_\_

e)\* Ventilation Yes  [X] No  [ ]  
With louvers  [ ] With Fan  [X]

f)# Fan Failure Alarm Required  [X] (For both cabinets and consoles)

On Operator Console  [X]

g)# Doors Yes  [X] No  [ ]  
Rear  [X] Front  [X]

h)\* Door Width \_\_\_\_\_

i)# Special Features Vibration-proof  [X] Explosion-proof  [ ]  
Drip proof  [ ] Pressurized  [ ]

j)# Cable entry Bottom  [X] Top  [ ]  
Glands/MCT blocks  [X]

k)# Receptacles For 240 V AC  [X] For Telephone Set  [X]

**Note: Applicable except console as the existing console shall be used.**

3 a) Size and Quantity:

Note: Height for all panels/ cabinets shall be 2200 mm Max., including channel base.

DESCRIPTION	MAKE	DIMENSIONS IN mm			QTY.	WEIGHT WHEN FULLY LOADED
		WIDTH	HEIGHT	DEPTH		
DCS SYSTEM CABINET						
PLC SYSTEM CABINET						
AC POWER DISTRIBUTION CABINET						
BARRIER CABINET						
RELAY CABINET						
FF MARSHALLING CABINET						
OPERATOR CONSOLE						
ENGINEER CONSOLE						
HARDWIRED CONSOLE						

b) Channel Base 100 X 50 X 6 mm [X] MS [X]

4\*\* Painting Colour:

a) External RAL 7035 [X]  
 b) Internal RAL 7035 [X]  
 Beige (IS 388) [ ]  
 c) Channel Base Black [X]  
 d) Panel Finish Non Glossy High Satin [X]

5 Constructional details:

a)# System ,Marshalling cabinets

Front, Sides & Top CRCA 1.5 mm Thick steel [X]

Welded to frame [X]

b)# Door Panel CRCA 2 mm Thick steel [X] Single Side hinge [ ]

Both Side hinge [ ] Concealed Hinges [X]

Flush Pull Handle [X] Lever type Handle [ ]

c)\* Anchor Bolt Size \_\_\_\_\_

- |  |                            |      |           |
|--|----------------------------|------|-----------|
| d)# Frame angle size                           | 50 X 50 X 4mm              | [X]  |           |
| e)** Lifting Eye Bolt                          | Required                   | [X]  | Size_____ |
| f)# Card Rack Size                             | 19" Rack / Carrier         | [X]  |           |
| g)* Card Rack Type                             | Swing out pivoted          | [ ]  | Fixed [ ] |
| h)# Rack / Rail mounting plates inside cabinet |                            | 3 mm | [X]       |
| i)#Cabinet Frame                               | 9 fold profiled CRCA sheet | [X]  |           |
6. Wiring:
- |                                    |  |     |  |
|------------------------------------|--|-----|--|
| a)# Type                           | General Purpose  | [X] |  |
|                                    | Intrinsic Safe   | [X] | For Barrier Racks & other<br>Intrinsically safe equipment. |
| b) Wiring details                  | As per notes attached  | [X] |  |
| c)# 110 V AC, 50 Hz UPS Wiring     |  |     |  |
| External to Cabinet/Panel          | min. 3 x 2.5 mm <sup>2</sup> Copper conductor PVC insulated and armoured.  |     |  |
| Inside the Cabinet/Panel           | min. 19 strands, 16 AWG Copper conductor PVC insulated.  |     |  |
| d)# 240 V AC Wiring                | 1.5 mm <sup>2</sup> Copper Conductor PVC Insulated Armoured. (Internal)  |     |  |
| e)# Signal Wiring / 24 V DC Wiring |  |     |  |
| External to cabinet/ panel         | 1.5 mm <sup>2</sup> /2.5mm <sup>2</sup> copper twin twisted, individual shielded, overall shielded with overall drain, PVC insulated and armoured. |     |  |
| Inside the Cabinet Panel           | Stranded min. 7 x 20 AWG Copper conductor PVC insulated, twin twisted and shielded.  |     |  |
| f)# Terminal Type                  | Screwless clamp on type shall be used with front entry   |     |  |
| g)# Terminal size for Signal       | Suitable for min. 2.5 mm <sup>2</sup> size Conductor   |     |  |
| h) For Power Distribution          | Suitable for min. 4 mm <sup>2</sup> size Conductor or one size higher than power cable conductor sizes   |     |  |
| i)# Terminal Block                 | Clip-on Channel Mounted type (Note)  |     |  |
- (Note – All terminals shall be fused type except those used for MCC interface. For analog signals, terminal block is not required if the selected barriers have suitable terminating facility for directly terminating the field cables.)
- |   |          |            |     |
|---|----------|------------|-----|
| j) Wiring Colour Code                   |          |            |     |
| i)# Power supply                        | Live     | Red        | [X] |
| (110 V AC / 240 V AC)                   | Neutral  | Black      | [X] |
|   | Earth    | Green      | [X] |
| ii)# DC Wiring                          | Positive | Red        | [X] |
|   | Negative | Black      | [X] |
| iii)# Alarm System                      |          | White      | [X] |
| iv)# Control & Shutdown                 |          | Yellow     | [X] |
| v)# Analog Signals (Intrinsically safe) |          | Light Blue | [X] |

vi)# Analog Signals (Non-intrinsically safe)	Grey	[X]
vii)# FF Signals (non IS)	Orange	[ ]
6**# Power Distribution Box		
a) Location	Inside console/ panel/ cabinet	[X]
b) Power supply Isolation	Required for each loads and for all incoming feeders MCB/MCCB shall be used. All MCB/MCCBs shall be with plastic shrouds.	
c) Fuse Type/Rating	HRC	[X]
d) Switch Type/Rating	DPST / 5 A @ 240 V AC	[X]
e) Busbar Terminal Block	Required	[X]

### XVI - NOTES ON WIRING

- 1# All wiring shall conform to API RP 550 Part-I, Sections 7 and 12. Different signal level cables shall be routed under false flooring with separation distances as recommended by API RP 550 Section 7.
  - 2# All Wiring inside racks, cabinets, and back of the panels shall be housed in covered, non-flammable plastic raceways arranged to permit easy accessibility to various instruments for maintenance, adjustments, repair and removal.  
  
All wiring in the raceways shall be properly clamped. All incoming cable shall be terminated by vendor at marshalling rack with cable glanding including supply of cable glands. Total wiring cross-sectional area shall not exceed 50 % of the raceway cross sectional area.
  - 3# Separate wiring raceways shall be used for power supply wiring, DC and low level signal wiring, and intrinsically safe wiring. Parallel runs of AC and DC wiring closer than 300 mm shall be avoided.
  - 4# Vendor can alternately offer pre-fabricated cables for interconnection between different cabinets and panels.
  - 5# Wire termination shall be done using self insulating crimping lugs. Manual hand crimping shall be avoided and machine crimping shall be used.
  - 6# More than two wires shall not be terminated on one side of single terminal. The use of shorting links for looping shall be avoided.
  - 7# Terminal housing shall be strictly sized with considerations for accessibility and maintenance. Following points should be considered:
    - a) Distance between terminal strip and side of the cabinet parallel to the strip, up to 50 terminals, shall be minimum 50 mm.
    - b) Distance between terminal strip and, top and bottom of the cabinet shall be minimum 75 mm.
    - c) Distance between two adjacent terminal strips shall be minimum 100 mm.
    - d) Additional distance for each additional 25 terminals shall be minimum 25 mm.
    - e) Distance between cable gland plate and the bottom of the strip shall be minimum 300 mm.
  - 8# All terminal strips shall be mounted on suitable anodised metallic or plastic stand-off.
  - 9# No splicing is allowed in between wire/ cable straight run.
  - 10# Terminal strips shall be arranged group-wise for incoming and outgoing cables separately. 20% spare terminals shall be provided as a minimum.
  - 11# Cabinet and rack layout shall be made considering proper accessibility and maintenance. 20% spare accessories like relays, switches, lamps, fuses etc., shall be provided as a minimum. 10% spare space shall also be provided as a minimum within each cabinet.
  - 12# Terminal blocks for intrinsically safe wiring shall be separate and shall be blue coloured.
- NOTE: The distances given in point no. 7 are excluding the width of the race-way.

**XVII - TRAINING KIT( NOT APPLICABLE)**

Model No. \_\_\_\_\_

- |   |                              |            |     |       |       |
|---|------------------------------|------------|-----|-------|-------|
| 1 | Number of Training Consoles  | One        | [ ] |       |       |
| 2 | Number of Monitors           | One        | [ ] | Other | _____ |
| 3 | Type of Consoles electronics | Individual | [ ] | Other | _____ |
| 4 | Type of keyboards            |            |     |       |       |
|   | Engineering Keyboard         | Required   | [ ] | One   | [ ]   |
|   | Operator Keyboard            | Required   | [ ] | One   | [ ]   |
|   | Maintenance Keyboard         | Required   | [ ] | One   | [ ]   |
| 5 | Number of printers           | One        | [ ] |       |       |

**Note: One no. training kit console for DCS and one no. for PLC.**

6 System requirements:

a) System modules:

SYSTEM	MODEL No.	MODULE TYPE INSTALLED (list out all installed cards in sub-system)	MODULES OFFERED
CONTROLLER & DATA – ACQUISITION SUB-SYSTEM			
OPERATOR INTERFACE			
OPERATOR INTERFACE			
ANY OTHER (please specify)			

b) Signal simulator/ generator Required [ ]

c) Application software to meet all functional requirements of system. Required [ ]

7 Facilities and capabilities

Stand alone system for the following functions:

Training of plant operators [ ]

Training of maintenance staff [ ]

Checking of system hardware and electronics modules [ ]

8 Software Packages Furnace [ ]

Steam Drum [ ]

Reactor [ ]

Any other \_\_\_\_\_



9	Minimum I/O requirement (DCS)		
	Analog Input for control:	08	[ ]
	Analog Input for DAS:	16	[ ]
	Analog Output:	08	[ ]
	Fieldbus I/O(closed loop) No. of Segment	03	[ ]
	Fieldbus input (monitoring loop)- No. of segments	08	[ ]
	Digital Inputs:	12	[ ]
	Digital Output:	12	[ ]
	Minimum I/O requirement (PLC)		
	Analog Input for DAS:	16	[ ]
	Analog Output:	08	[ ]
	Fieldbus I/O(control loop)	X	[ ]
	Fieldbus input (monitoring loop)	X	[ ]
	Digital Inputs:	12	[ ]
	Digital Output:	12	[ ]

**XVIII - SEQUENCE OF EVENT (SOE)( NOT APPLICABLE)**

\*Model No. \_\_\_\_\_

A. Offered System Details

- 1# a) Dedicated Sequence of Event Recorder [ ]  
 b) Combined with PLC [X]
- 2 Total no. of cabinets offered \_\_\_\_\_  
 a) SCR Cabinets \_\_\_\_\_  
 b) Alarm Card Cabinets \_\_\_\_\_
- 3 MTBF \_\_\_\_\_ hours
4. MTTR \_\_\_\_\_ hours

B. SPECIFICATIONS

- 1 Type μP Based [ ] Configurable [ ]  
 CPU Type \_\_\_\_\_
- 2 Type of Enclosure General Purpose [ ]
- 3 Configuration Single [ ] Duplex [ ]  
 Switch Over Time (if Duplex) \_\_\_\_\_ sec
- 4 Scan time \_\_\_\_\_ msec
- 5 Processor cycle time \_\_\_\_\_ msec
- 6 Resolution Required  
 Digital 1 msec [ ] 10 msec [ ]  
 Analog 50 msec [ ] 100 msec [ ]  
 Any Other \_\_\_\_\_
- 7 INPUT DETAILS
- a) Input Isolation Required [ ]
- b) Type of Input Modules

Type of Module	Model No.	No. of Inputs per module
4-20 mA DC 2 wire (HART) [ ]		
0-20 mA DC (2 wire) [ ]		
1-5 V DC [ ]		
0.25-1.25 V DC [ ]		
Potential Free Contact [ ]		
RS 232 C [ ]		

- c) Max. No. of Input / Module
- Analog 8 [ ] 16 [ ]  
32 [ ]

	Contacts	16	[ ]	32	[ ]
d)	A/D Converter Resolution	1500 steps	[ ]	Actual	_____
e)	Load riving Capability	750 Ω	[ ]	Actual	_____
8*	SOE Capability				
	Analog Resolution	<b>same as PLC scan time</b> msec			
	Contact Input /output Resolution	<b>same as PLC scan time</b> msec (Refer SIV)			
9*	SOE PC	Required	[ ]	(As per System Configuration)	
		Not Required	[ ]		
	Function of PC:				
		SOE Configuration	[ ]		
		Alarm Display	[ ]		
		Diagnostics	[ ]		
		Any Other		_____	
	SOE Printer	Required	[ ]	(Note)	
	(Note: Multipurpose printer shown in System Configuration shall be utilized for SOE printing.)				
	Type	Dot Matrix	[ ]		
	Alarm Data Storage	Required	[ ]		
	Storage Time	96 hours	[ ]		
10*	Interfacing with:				
	PLC	Yes	[ ]	No	[ ]
	DCS	Yes	[ ]	No	[ ]
	AIMS	Yes	[ ]	No	[ ]
11*#	No. of Input Points	256 Nos.	[ ]		
		512 Nos.	[ ]		
		1024 Nos.	[ ]		
12*	Power Supply	110 V 50 Hz	[ ]		

**SECTION-V**


**ANNEXURE-VII**

**(I/O SUMMARY AND SIZING CONSIDERATION)**

**Job No. 568**


**BITUMEN MAXIMIZATION PROJECT**

**IOCL, BARAUNI**

						PROJECT :	 <p><b>इंजीनियर्स इंडिया लिमिटेड</b> (भारत सरकार का उपक्रम)</p> <p><b>ENGINEERS INDIA LIMITED</b> (A Govt. of India Undertaking)</p>		
						BITUMEN MAXIMIZATION PROJECT			
						CLIENT : <b>IOCL, BARUNI</b>			
						DOCUMENT TITLE :		<b>Section: V</b>	
						<b>I/O SUMMARY</b>			
						<b>AND SIZING CONSIDERATION</b>	Job No.	<b>Annexure VII to</b>	REV.
						<b>COVER SHEET</b>	<b>B568</b>	<b>B568-304-16-51-SP-1505</b>	<b>0</b>
0	07.11.24	Issued with MR	BO	KKP	SM				
Rev.	Date	Purpose	BY	CHK	APPD				

**GENERAL NOTES:**

1. Bidder shall be responsible for the correct sizing of DCS, PLC, its related sub-systems and nodes as indicated in system configuration drawing attached with the MR.
2. Bidder shall consider the following while sizing and loading the system:
  - a. DCS Controller and PLC processor sizing shall be done subsystem wise with loading of each DCS controller / PLC processor not exceeding 50%. For sizing purpose, consider as follows :  
 DCS Controller : Processor cycle time 250 msec. for P&F close loops, 500 msec for L&T close loops and for all open loops.  
 PLC Processor : Scan time 250 msec.
  - a. Serial link connectivity with the system shall be as per details given in this document. The sub-systems shown connected directly to system communication sub-system through separate serial interface must have dedicated individual gateway interface units as shown in configuration diagram.
  - b. Consider typically 1000 points as analog and 1000 points as digital per package PLC for sizing of serial interface modules and gateways.
  - c. For other serial interfaces following criteria shall be followed:-  
 Loading due to data transfer via serial link for Vibration and temperature monitoring systems, analyser system, wireless gateway systems (ISA HART and ISA 100), ASC system, governor system, etc. shall be considered. Consider typically 200 points as analog and 100 points as digital per such links for sizing I/Os. List of such interfaces is given as Table-V.
  - d. Input/ Output Summary table is enclosed as Table I to Table V.
  - e. The I/O summary does not include installed spares, future spare space requirements and system spares. As such, Bidder shall consider the following while sizing the systems:
    - i. All spares including 20% installed spares and 10% future space requirement and system spares as defined in SIV and Section 3.0 of Standard Specification for DCS – 6-52-0055 attached elsewhere in this MR.
    - ii. Installed Spare windows in Alarm Annunciators – 30%.
    - iii. Free Space for hardware with installed DIN Rail, Base plate, back plane - Min. 20%.
    - iv. Bidder shall consider additional I/Os for Input and outputs related to items (various system related alarms like UPS feeder failure, PDB voltage/current, BPS failure, Mosfet fault, Cabinet / consoles temperature/ fan failure, etc.) provided by Vendor and other signals like UPS failure, as specified in SIV.
    - v. 20% installed engineering spares shall be considered module wise. i.e 20% spare channel shall be provided in each module as a minimum.
  - f. For Gas detectors as indicated in Table-III, Bidder to note that Gas detectors shall be three wire types in general. These Gas detectors shall be powered from Marshalling cabinet only, suitable components power supply Cards/ Field Terminal Assembly as well as wiring shall be considered by vendor.

							PROJECT :			
							BITUMEN MAXIMIZATION PROJECT			
							CLIENT :	IOCL, BARUNI		
							DOCUMENT TITLE :		Section: V	
							I/O SUMMARY			
							AND SIZING CONSIDERATION	Job No.	Annexure VII to	REV.
							NOTES	B568	B568-304-16-51-SP-1505	0
0	26.07.24	Issued with MR	BO	KKP	SM					
Rev.	Date	Purpose	BY	CHK	APPD					

g. The following are the sub-system of the DCS/PLC System in Refinery:

6. Refer Special Instructions to Vendor for other details.

7. Subsystem as specified in cl 3.1.1 of 6-52-0055 shall be subsystem under each unit / group in I/O list table and shall be used subsystem wise accordingly for spare calculation.

Further to this for each subsystem, the spare shall be calculated location wise (i.e. separate for each SRR/CR) including for Cl 3.1.1.5 (a), (b) and (c) for predefined mandatory spare.

8. All “ %” value shall round up to next higher whole number and accordingly the spare shall be supplied.

**ABBREVIATIONS**

P&F	PRESSURE & FLOW
L&T	LEVEL & TEMPERATURE
WB	WITH BARRIER
WOB	WITHOUT BARRIER
DCS	DISTRIBUTED CONTROL SYSTEM
ESD	EMERGENCY SHUTDOWN SYSTEM
PLC	PROGRAMMABLE LOGIC CONTROLLER
SRR	SATELLITE RACK ROOM
CR	CONTROL ROOM
I/O	INPUT OUTPUT

0	26.07.24	Issued with MR	PAGE 3 OF 10		

PROJECT :  
**BITUMEN MAXIMIZATION PROJECT**  
 CLIENT : **IOCL, BARUNI**  
 DOCUMENT TITLE :  
**I/O SUMMARY  
 AND SIZING CONSIDERATION**



**इंजीनियर्स  
इंडिया लिमिटेड**  
(सार्वजनिक उपकरणों का उद्यम)

**ENGINEERS  
INDIA LIMITED**  
(A Govt. of India Undertaking)


**Section: V**

**Annexure VIII**

Job No. \_\_\_\_\_

REV \_\_\_\_\_

Rev.	Date	Purpose	BY	CHK	APPD	NOTES	B568	B568-304-16-51-SP-1505	0
------	------	---------	----	-----	------	-------	------	------------------------	---

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
 <b>ENGINEERS INDIA LIMITED</b> <small>(A Govt. of India Undertaking)</small>				<b>DISTRIBUTED CONTROL SYSTEM</b>												<b>Section: V</b>						
				<b>BITUMEN MAXIMIZATION PROJECT</b>												<b>Annexure VII to B568-304-16-51-SP-1505</b>						
				<b>IOCL, BARUNI</b>																		
<b>TABLE - I: I/O SUMMARY (DCS- NON FIELDBUS)</b>																						
<b>SUBSYSTEM</b>		<b>CLOSED LOOPS</b>										<b>OPEN LOOPS</b>										
		<b>INPUT</b>					<b>OUTPUT</b>					<b>INPUT</b>					<b>OUTPUT</b>					
		4-20mA		4-20mA			4-20mA		4-20mA			4-20mA		RTD/TC	<b>Contacts</b>				4-20mA (PST)	4-20mA	Contact	Contact
		WB		WOB			WB		WOB			WB		WB	Switches	Switches	Proximity Switches	MCC	WB	WOB	WB	WOB
		P&F	L&T	P&F	L&T		P&F	L&T		P&F	L&T		WB	WOB	WB	WB	WOB	WB	WOB	WB	WOB	
BITUROX SYSTEMS FOR OFFSITES		20	10			15	13				2	2	84	15		10	25			20		



**TABLE - II: I/O SUMMARY (PLC for Plant ESD and Process Interlocks)**

SUBSYSTEM	INPUT							OUTPUT				PBs, HS AND SELECT. SW (NOTE-1)	EMER. SW (NOTE -1,5)	STATUS LAMP (NOTE -1)	ANN. WIN (NOTE -1)
	4-20mA (Note-2)	CONTACTS						CONTACTS							
		SWITCHES (Note-2)	SWITCHES (Note-8)	SWITCHES IN LCP	PROXIMITY SWITCHES	MCC	SOV (24 VDC) (Note-2,3,5,6)	Lamp in LCP	MCC	OTHER					
		WB	WOB	WB	WB	WOB	WB	WB	WOB	WOB					
BITUROX SYSTEMS FOR OFFSITES	20 (6)		80 (53)	0	0 (0)	10	0 0	10	20	15	25	1	10	10	

**NOTES:**

- This column is for counting hardware in Hardwired Console in EPCC-11 control room. Each EPB shall be considered with 3 contacts in 2oo3 configuration. Installed spares (30% for annunciator windows and 20% for all type of switches and Lamps) shall be considered for these items also.
- Quantity shown within brackets indicates the IO's in 2oo3 mode out of the total quantity.
- Vendor shall consider line monitoring status DI for SOV barriers in DCS in addition to the I/O counts provided in table.
- Hardwired Console (HWC) shall be common for mounting the items pertaining to the Sub-systems within each group.
- Quantity shown within brackets '{ }' indicates the outputs in 2 out of 2 mode out of the total quantity. Vendor to ensure line fault detection for each SOV from each barrier shall be provided in DCS. These additional digital inputs to DCS shall be considered over and above the
- Quantity shown within brackets '( )' indicates the outputs in 2 out of 3 mode out of the total quantity. Vendor to ensure line fault detection for each SOV from each barrier shall be provided in DCS. These additional digital inputs to DCS shall be considered over and above the digital inputs mentioned in DCS I/O count.
- I/O's mentioned with 'WOB' are for flameproof I/O's. However irrespective of the type of circuits (IS/ flameproof) all I/O's of DCS/PLC to and from field shall be through intrinsically safe barrier only. However contacts for MCC I/O's & F&G hooter / bacons shall be through suitable relays.
- These I/Os (DCS Digital Output and PLC Digital Input) are for facilitating the manual actuation of any open /close command for valves and start / stop command for motor through soft switches from the DCS operator console for actuating the desired action in the PLC interlocks.

**TABLE - III: I/O SUMMARY (PLC-FIRE & GAS DETECTION)**

UNIT	ANALOG INPUT		INPUT		OUTPUT		MCC	
	4-20mA (3-wire)	4-20mA (2-wire)	CONTACT		CONTACT		DIGITAL INPUT	DIGITAL OUTPUT
	(Note-6)		WB	WOB	WB	WOB	WOB	WOB
	WB	WB						
BITUROX SYSTEMS FOR OFFSITES	30 (6)	0	0	0	10	10	0	0

**NOTES:**

6: Quantity shown within brackets indicates the inputs in 2 out of 3 mode out of the total quantity for inputs.

7: Vendor shall consider line monitoring relay to be provided.

**TABLE- IV: SERIAL LINK TO DCS / PLC**

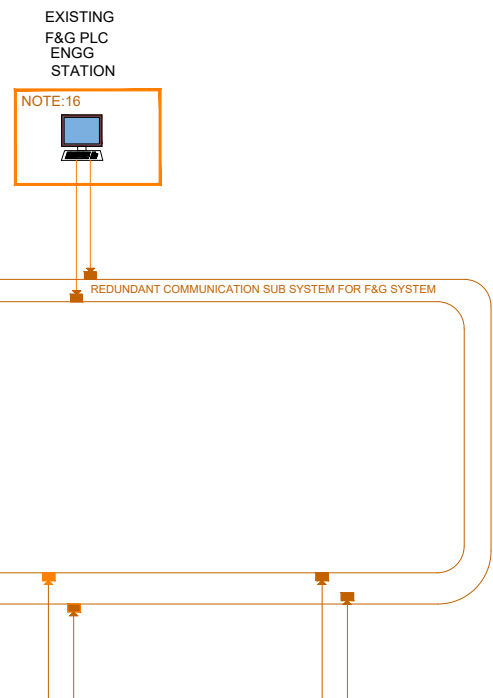
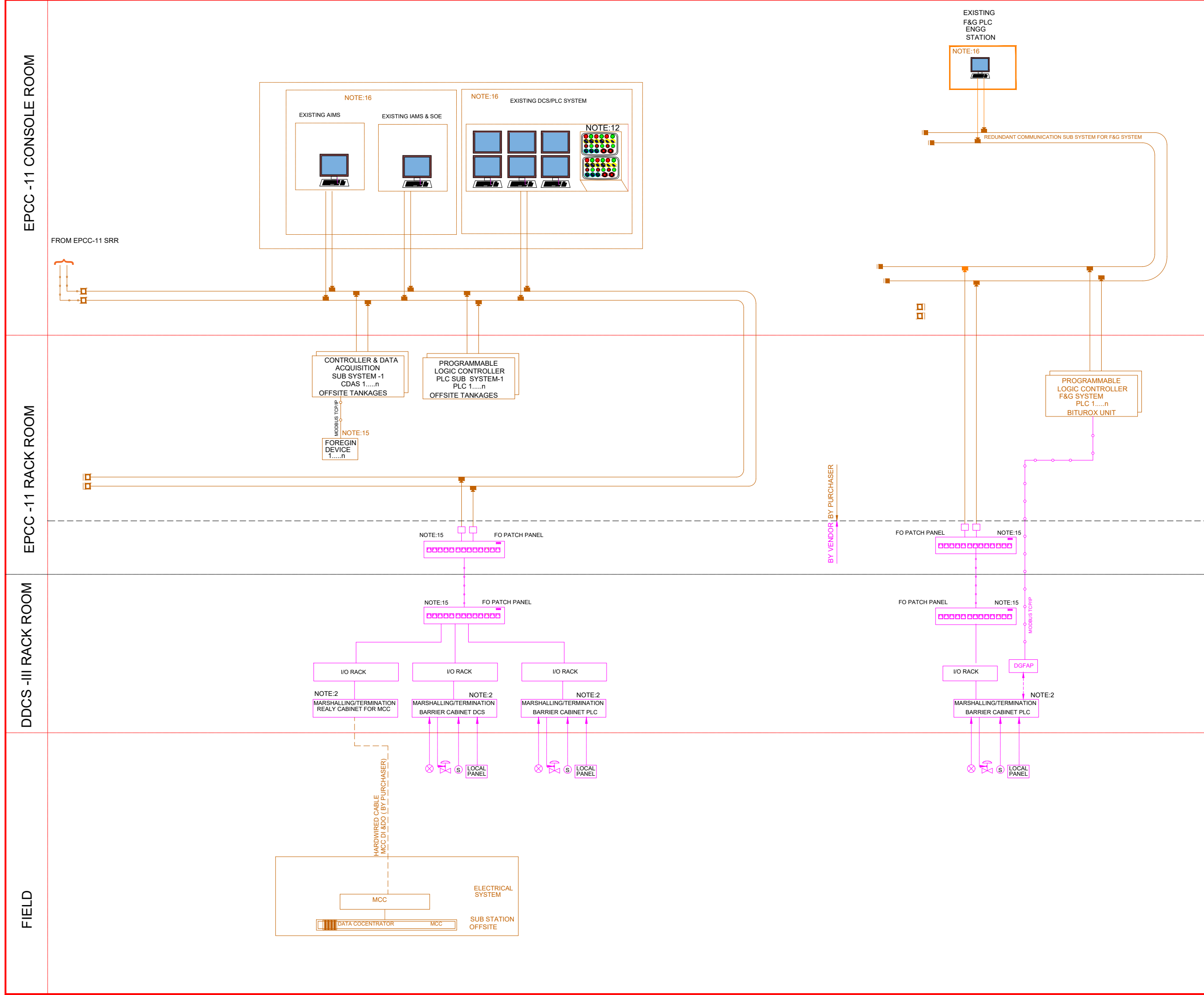
Sr. No.	From System	Location	Supply of Serial link cables & connectors at both ends	No. of Serial links	Single / Dual	Remarks
A.	<b>Foreign Device Interfaces through DCS CDAS Serial Interface Card</b>					
1	TFMS	Rack Room in New SRR of BITUROX -II Unit	By Vendor	1	DUAL	
2	Conductivity & PH Analyser	UPS Room OF New SRR of BITUROX -II Unit	By Vendor	2	SIMPLEX	
3	Automatic Transfer Switch in Vendor supplied Non DCS PDB	Rack Room in New SRR of BITUROX -II Unit	By Vendor	1	DUAL	
4	DGFAP-Fire Alarm System (for F&G PLC)	Rack Room in New SRR of BITUROX -II Unit	By Vendor	1	DUAL	
5	Spare-01	Rack Room in New SRR of BITUROX -II Unit	By Vendor	1	DUAL	
B.	<b>Foreign Device Interfaces through dedicated Serial Communication Interface Gateway (Note-1)</b>					

Note-1 Number of Dedicated Serial communication interface gateways shall be as shown in System Configuration Diagrams. Serial interface cards shall be separate for each link.

**TABLE- V: PACKAGE PLC/ CONTROL SYSTEM LINK TO IAMS**

Sr. No.	From System	From Location	To Location	Remarks
1				
2				

izLrqr vkjs[k ,oa blesa fufr IMI+kbu bathru;LkZ bafM;k fyfeVSM dh LkafIRr gSA ;s ek= m/kkj fn, x, gSa vkSj m/kkjdrkZ us ;g LTV Lke-kSrk fd;k gS fd u rks mUgSa igu% eqfmZr fd;k tk,akk] u udy dh tk,ak] u m/kkj fn, tk,aks] u iznfr;kZr fd, tk,aks vkSj] u gh Lkhfer vkSj] futh iz;ksx ds vykok budk dksbZ vu; iz;ksx vkSj] g iZ;ksx m/kkjdrkZ dks fyf[kr ; i esa nh abZ Lkgefr Lks gksak A



- NOTES :-**
- THE CONFIGURATION SHOWN HERE IS GENERIC IN NATURE VENDOR SHALL PREPARE THE CONFIGURATION DIAGRAM SHOWING ACTUAL HARDWARE USED WITH MODEL NO HOWEVER BASIC REQUIREMENT MUST BE MAINTAINED AS SHOWN IN THIS DRAWING.
  - SIGNALS FROM OFFSITE TANKAGE AREA AND PUMP AREA SHALL BE INTERFACED THROUGH NEW IO CARD AND MARSHALLING PANEL TO PURCHASER'S EXISTING DCS/PLC & F&G SYSTEM IN EXISTING OM&S CONTROL ROOM.
  - INTERFACING WITH OTHER SYSTEMS(OTHER THAN THOSE THROUGH DEDICATED SERIAL GATEWAY) REQUIRING SERIAL CONNECTIVITY SHALL BE THROUGH SERIAL I/O CARDS IN CONTROLLER/ DAS SUBSYSTEM, ALL SERIAL LINK INTERFACES SHALL BE THROUGH DEDICATED REDUNDANT SERIAL INTERFACE CARDS. NO MULTI-DROPPING SHALL BE CARRIED OUT BY DCS VENDOR.
  - THE NUMBER OF SERIAL LINKS FOR EACH SYSTEM SHALL BE AS PER I/O SUMMARY . TABLE .
  - ALL NECESSARY HARDWARE/SOFTWARE REQUIRED FOR SOE FUNCTION SHALL BE PROVIDED BY VENDOR TO MEET THE FUNCTIONAL REQUIREMENTS AS PER REQUISITION.
  - NO. OF LINKS SHALL BE AS PER RESPECTIVE . SUB-SYSTEMS SEGREGATION.
  - THE OPERATIONAL, HISTORICAL AND ENGINEERING DATA BASE SHALL BE FOR OFFSITE TANKAGE AREAN AND PUMP AREA SIGNALS SHALL BE KEPT IN THE EXISTING UHN .
  - ALL I/Os OF DCS & PLC INCLUDING F&G PLC AND I/O'S RELATED TO ALL PACKAGES SHALL BE CONNECTED TO PURCHASER'S EXISTING IAMS SYSTEM .
  - ALL ALARM SIGNALS OF OFFSITE TANKAGE AREA AND PUMP AREA SHALL BE CONNECTED TO PURCHASER'S EXISTING AIMS SYSTEM .
  - ALL THE SERIAL LINKS SHALL BE INDEPENDENT LINKS CABLING AND SHALL NOT BE MULTIDROPPED
  - NO OF SERIAL INTERFACE GATE WAY SHALL BE AS PER I/O SUMMARY AND MR REQUIREMENTS.
  - SIGNALS OF OFFSITE TANKAGE AREA AND PUMP AREA SHALL BE ACCOMADATED IN EXISTING HARDWARE CONSOLE THROUGH ADDITIONAL PUSH BUTTON/LAMPS. SELECTOR SWITCH ETC AS PER I/O SUMMARY.
  - TIME SYNCHRONIZATION SHALL BE DONE THROUGH EXISTING GPS SYSTEM.
  - PURCHASER'S EXISTING SYSTEM.
  - FO PATCH PANEL/LIU AND NETWORK SWITCH WITH ALL ACCESSORIES SHALL BE PROVIDED BY VENDOR.
  - EXISTING OPERATING CONSOLE, ENGINEERING CONSOLE , F&G SYSTEM , IAMS , AIMS, UHN , SHALL BE USED FOR MONITORING , CONTROL, ENGINEERING , ALARM MANAGEMENT ASSET MANAGEMENT, UNIT DATA HISTORIAN ETC.

- LEGENDS:-**
- BY PURCHASER
  - BY VENDOR
  - FO : FIBER OPTIC
  - MCR : MAIN CONTROL ROOM.
  - TCP : TRANSMISSION CONTROL PROTOCOL
  - IP : INTERNET PROTOCOL
  - RSL : REDUNDANT SERIAL LINK.
  - LAN : LOCAL AREA NETWORK.
  - REDUNDANT FIBER OPTIC LINK SERIAL LINK( MODBUS TCP/IP)
  - HARDWIRED LINK.
  - FO CONVERTER.
  - TERMINATOR.
  - REDUNDANT.

REV	DATE	PURPOSE	BY	CHKD	APPD	APPD
A	04.11.2024	ISSUED FOR CLIENT'S COMMENTS	BO	KWP	SM	

**INDIAN OIL CORPORATION LIMITED**  
 (A Govt. of India Undertaking)

bafM;u vkW;y dkWkZsjs'ku fyfeVSM  
 INDIAN OIL CORPORATION LTD.  
 (A Govt. of India Undertaking)

**CONTROL SYSTEM ARCHITECTURE**

SHEET 1 OF 1

SCALE	JOB NO.	UNIT	DEPT.	SECT.	DWG. NO.	REV.
NTS	8 5 6 8	3 0 4	1 8	5 1	2 2 0 1	A

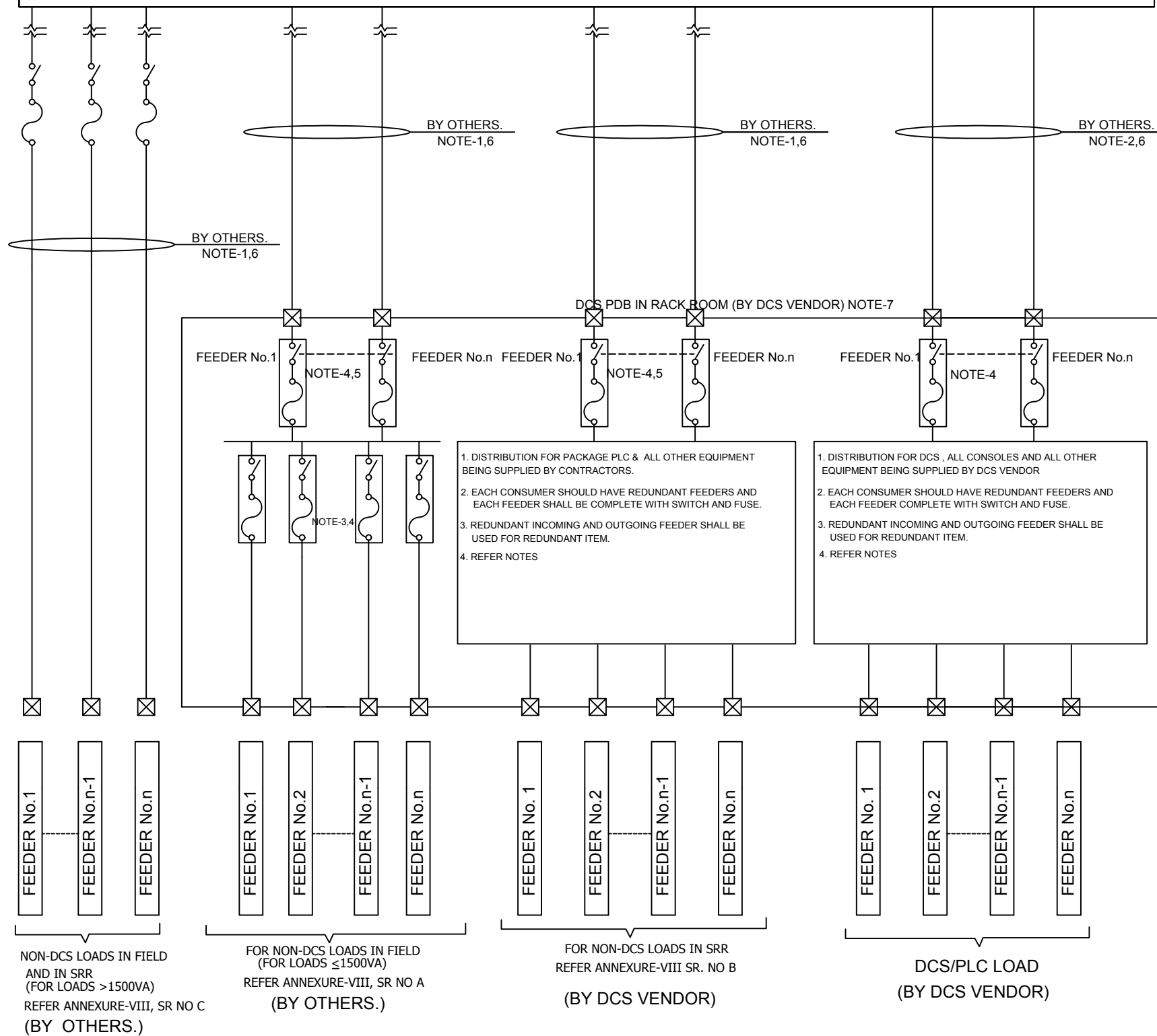
14 15 1-1641/503 REV.0 A2-594X20

The drawing, design and details given on this format are the property of ENGINEERS INDIA LIMITED. They are merely loaned on the borrower's express agreement that they will not be reproduced, copied, exhibited or used, except in the limited way permitted by a written consent given by the lender to the borrower for the intended use.

## CONTROL ROOM

### 110 V AC UPS DISTRIBUTION BOARD (UPS ROOM)

BY ELECTRICAL-UPS VENDOR



**NOTES:**

- 1) COMPLETELY GROUNDED AND ISOLATED FEEDERS SHALL BE PROVIDED FOR
  - a) NON-DCS UPS LOADS IN FIELD.
  - b) NON-DCS UPS LOADS IN SATELLITE RACK ROOM.
- 2) GROUNDED AND ISOLATED FEEDER SHALL BE PROVIDED FOR DCS LOADS.
- 3) MAIN ISOLATOR SHALL BE DPST TYPE TO ISOLATE BOTH PHASE AND NEUTRAL. LIKEWISE, INDIVIDUAL DISTRIBUTION FEEDERS TO HAVE ISOLATORS OF DPST TYPE TO ISOLATE LINE AND NEUTRAL.
- 4) IN ORDER TO OBTAIN PROPER FUSE CO-ORDINATION , FOLLOWING MUST BE TAKEN INTO CONSIDERATION:-
  - a) ALL REDUNDANT FEEDERS FOR DCS SHALL FEED TO SEPARATE SETS OF BUS BARS(LINE & NEUTRAL).
  - b) ALL SETS OF FEEDERS SHALL BE FULLY INDEPENDENT AND SHALL NOT BE JOINED TOGETHER AT ANY POINT.
- 5) AUTOMATIC TRANSFER SWITCH (ATS) SHALL BE PROVIDED BY DCS VENDOR FOR THE REDUNDANT UPS FEEDER.
- 6) NUMBER OF FEEDERS AND SIZE PROVIDED FROM UPS ACDB FOR CATERING EACH TYPE OF LOAD SHALL BE FINALIZED DURING DETAILED ENGINEERING. DEPENDING UPON THE FINAL SIZE AND RATING OF UPS SELECTED . ACCORDINGLY ,DCS PDB SHALL BE SUITABLE FOR TERMINATING MULTIPLE INCOMING FEEDERS
- 7) FOR UPS AC REDUNDANT POWER SUPPLY INCOMER IN THE RACK ROOM PDBS, AUTOMATIC TRANSFER SWITCH (ATS) SHALL BE CONSIDERED FOR NON REDUNDANT DCS AND NON DCS LOADS. POWER SUPPLY FOR ALL SUBSYSTEMS, WHERE FACILITY IS AVAILABLE FOR ACCEPTING REDUNDANT SUPPLIES, SHALL BE FROM REDUNDANT POWER SOURCE AND NOT FROM ATS.
- 8) FOR INDIVIDUAL INSTRUMENT DISTRIBUTION VENDOR MAY EITHER USE SWITCH FUSE OR CIRCUIT BREAKER. FOR DISTRIBUTION OF POWER TO VARIOUS SUBSYSTEMS SUPPLIED BY THEM, VENDOR MUST EVALUATE THE PROTECTION REQUIREMENTS BEFORE DECIDING UPON THE SWITCH/FUSE OR CIRCUIT BREAKER.
- 9) CABLE GLANDS IN VENDOR'S PANEL SHALL BE PROVIDED BY VENDOR.
- 10) PROVIDE VOLTMETER AND AMMETER IN EACH MAIN POWER FEEDER ENTRY POINT INSIDE THE POWER DISTRIBUTION BOARD
- 11) TYPICAL POWER DISTRIBUTION DIAGRAM OF AUTOMATIC TRANSFER SWITCH (ATS) SHALL BE FOLLOWED.
- 12) 20% (MINIMUM ONE NUMBER) SPARE POWER DISTRIBUTION OUTLETS SHALL BE PROVIDED COMPLETE WITH ISOLATOR AND FUSE FOR EACH TYPE RATING. SPARE FEEDER LOAD SHALL BE PROVIDED BY VENDOR.

**LEGEND:**

- MCB/MCCB
- FEEDER OUTLET WITH CABLE GLAND
- ISOLATION TRANSFORMER



PLANT- BITUROX -II OFFSITE  
 UNIT- 304  
 CLIENT- IOCL BARAUNI

0	04.11.2024	ISSUED WITH MR	BO	KKP	SM		
REV.	DATE	REVISION	BY	CHK	APPROVED	APPROVED	

**TYPICAL SCHEMATIC FOR  
 UPS POWER SUPPLY  
 DISTRIBUTION SCHEME**

<b>DRAWING NO.</b>	<b>REV.</b>
<b>B568-304-16-51-31001</b>	<b>0</b>
SHEET 1 OF 1	

**SECTION-V  
 ANNEXURE VIII  
 (110 V AC UPS NON DCS POWER DISTRIBUTION LIST)**

0	04.11.2024	ISSUED with MR	BO	KKP	SM
Rev. No	Date	Purpose	Prepared by	Checked by	Approved by

Legend

**Table 1`  
110V AC (UPS) non DCS Feeders Distribution List**

(R)- Redundant Feeder  
\* - By Vendor

**O&MS Control Room**

Sr. No	FEEDER DECSRIPTION	FEEDER RATING (VA)	FEEDER REQD (No's)	DISTANCE (meter)	CABLE SIZE (mm2)	CABLE OD (mm)
<b>A</b>	<b>110V AC non DCS load in field from DCS PDB in Rack Room</b>					
1.	304-LT-1201 (NON CONTACT RADAR)	100	1			
2.	304-LT-1202 (NON CONTACT RADAR)	100	1			
3.	304-LT-1203 (NON CONTACT RADAR)	100	1			
4.	304-LT-1301 (NON CONTACT RADAR)	100	1			
5.	304-LT-1302 (NON CONTACT RADAR)	100	1			
6.	304-LT-1303 (NON CONTACT RADAR)	100	1			
7.	304-LT-1401 (NON CONTACT RADAR)	100	1			
8.	304-LT-1402 (NON CONTACT RADAR)	100	1			
9.	304-LT-1403 (NON CONTACT RADAR)	100	1			
10.	304-LT-1501 (NON CONTACT RADAR)	100	1			
11.	304-LT-1502 (NON CONTACT RADAR)	100	1			
12.	304-LT-1503 (NON CONTACT RADAR)	100	1			



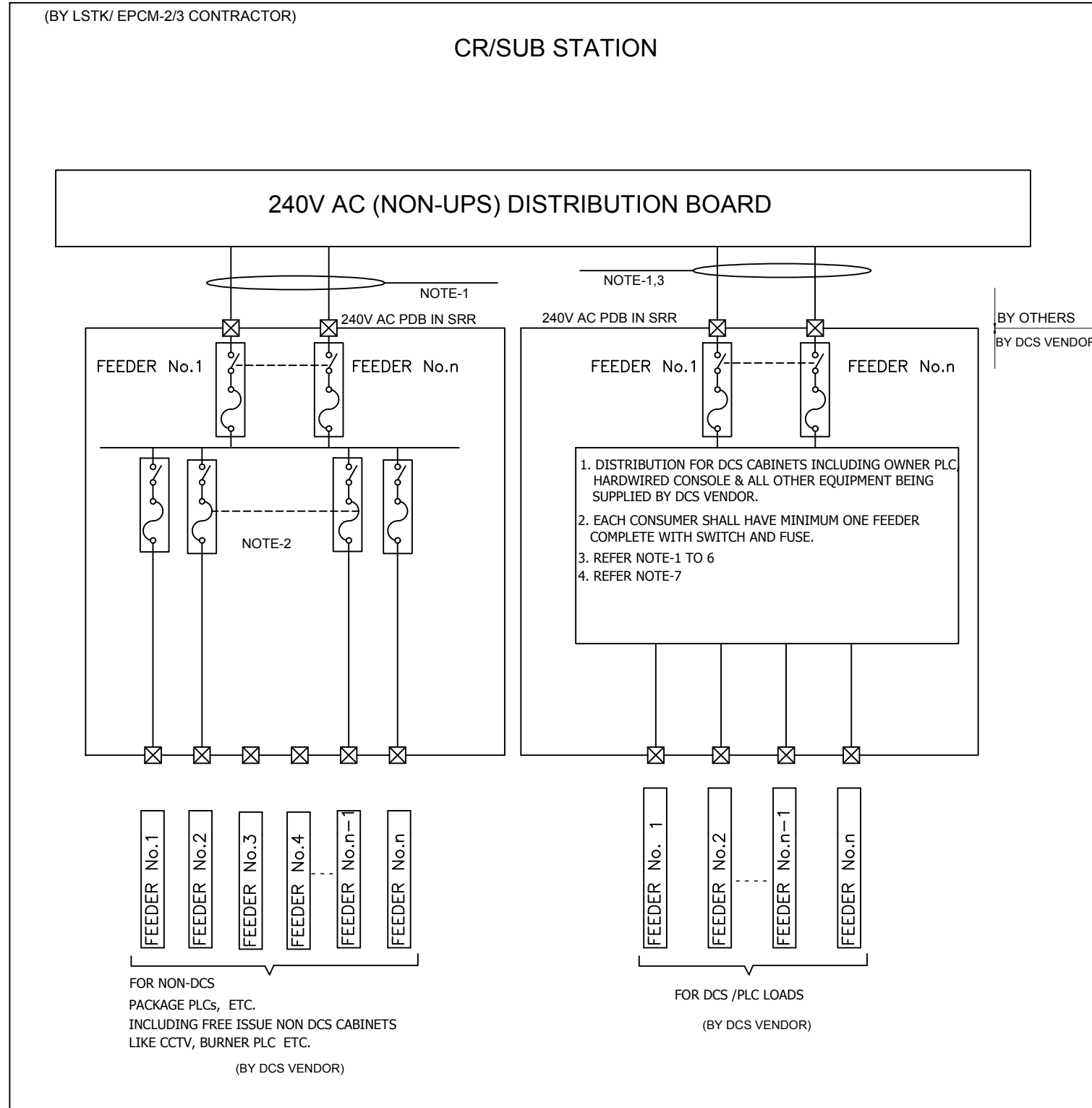
13.	304-LT-1601(NON CONTACT RADAR)	100	1			
14.	304-LT-1602 (NON CONTACT RADAR)	100	1			
15.	304-LT-1603 (NON CONTACT RADAR)	100	1			
16	304-LT-1701 (NON CONTACT RADAR)	100	1			
17	304-LT-1702 (NON CONTACT RADAR)	100	1			
18	304-LT-1703 (NON CONTACT RADAR)	100	1			
19	Hooters	50	1			
20	Beacons	50	1			
21	Misc Feeder -1	1000	1			
22	Misc Feeder -2	500	2			
23	Misc Feeder -3	200	2			
24	Misc Feeder -4	300	1			
25	Misc Feeder -5	100	2			
26	Misc Feeder -6	100	1			
<b>B</b>	<b>110V AC non DCS load within Control room from DCS PDB in Rack Room</b>					
1	TFMS SYATEM CABINET	1500	1(R)			
6	Misc Feeder -7	1000	1(R)			

<b>C</b>	<b>110V AC non DCS load from SRR DCS PDB in Rack Room to field</b>				
1	CCTV Cabinet/Camera.	1200	1(R)		
2	Misc Feeder -7	1000	1(R)		

The drawing, design and details given on this format are the property of ENGINEERS INDIA LIMITED. They are merely loaned on the borrower's express agreement that they will not be reproduced, copied, exhibited or used, except in the limited way permitted by a written consent given by the lender to the borrower for the intended use.

(BY LSTK/ EPCM-2/3 CONTRACTOR)

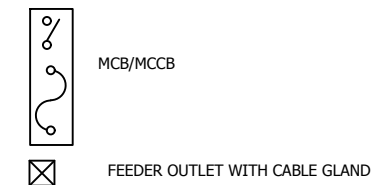
### CR/SUB STATION



**NOTES:**

- 1) MULTIPLE FEEDERS SHALL BE PROVIDED WITH EACH FEEDER OF RATING 240 V, 16A CATERING TO ILLUMINATION OF TEN NOS. CABINETS IN EACH ROW.
- 2) 20% (MINIMUM ONE NUMBER) SPARE POWER DISTRIBUTION OUTLETS SHALL BE PROVIDED COMPLETE WITH ISOLATOR AND FUSE FOR EACH TYPE AND RATING SHALL BE PROVIDED BY VENDOR.
- 3) NUMBER OF FEEDERS SHALL BE DECIDED DURING DETAILED ENGINEERING.
- 4) MAIN ISOLATOR SHALL BE DPST TYPE TO ISOLATE BOTH PHASE AND NEUTRAL. LIKEWISE, INDIVIDUAL DISTRIBUTION FEEDERS TO HAVE ISOLATORS OF DPST TYPE TO ISOLATE LINE AND NEUTRAL.
- 5) CABLE GLANDS IN VENDOR'S PANEL SHALL BE PROVIDED BY VENDOR.
- 6) PROVIDE VOLTMETER AND AMMETER IN EACH MAIN POWER FEEDER ENTRY POINT INSIDE THE POWER DISTRIBUTION CABINET.
- 7) ONE NO OF FEEDER SHALL BE PROVIDED IN SRR PDB CABINET FOR NEW CONSOLE AREA OF EXISTING AVU-III CONTROL ROOM. CABLING INCLUDING SUPPLY LAYING AND TERMINATION INCLUDING SUPPLY OF CABLE GLANDS AT BOTH END SHALL BE IN THE SCOPE OF VENDOR.

**LEGEND:**



PLANT- BITUROX-II OFFSITE  
UNIT- 304  
CLIENT- IOCL BARAUNI

0	04.11.2024	ISSUED WITH MR	BO	KKP	SM		
REV.	DATE	REVISION	BY	CHK	APPROVED	APPROVED	

**TYPICAL SCHEMATIC FOR  
NON UPS POWER SUPPLY  
DISTRIBUTION (BITUROX-II)**

<b>DRAWING NO.</b>	<b>REV.</b>
<b>B568-304-16-51-31002</b>	<b>0</b>

SHEET 1 OF 1

## SECTION-V (24 V DC NON DCS POWER DISTRIBUTION LIST)

0	04.11.2024	ISSUED with MR	BO	KKP	SM
<b>Rev. No</b>	<b>Date</b>	<b>Purpose</b>	<b>Prepared by</b>	<b>Checked by</b>	<b>Approved by</b>

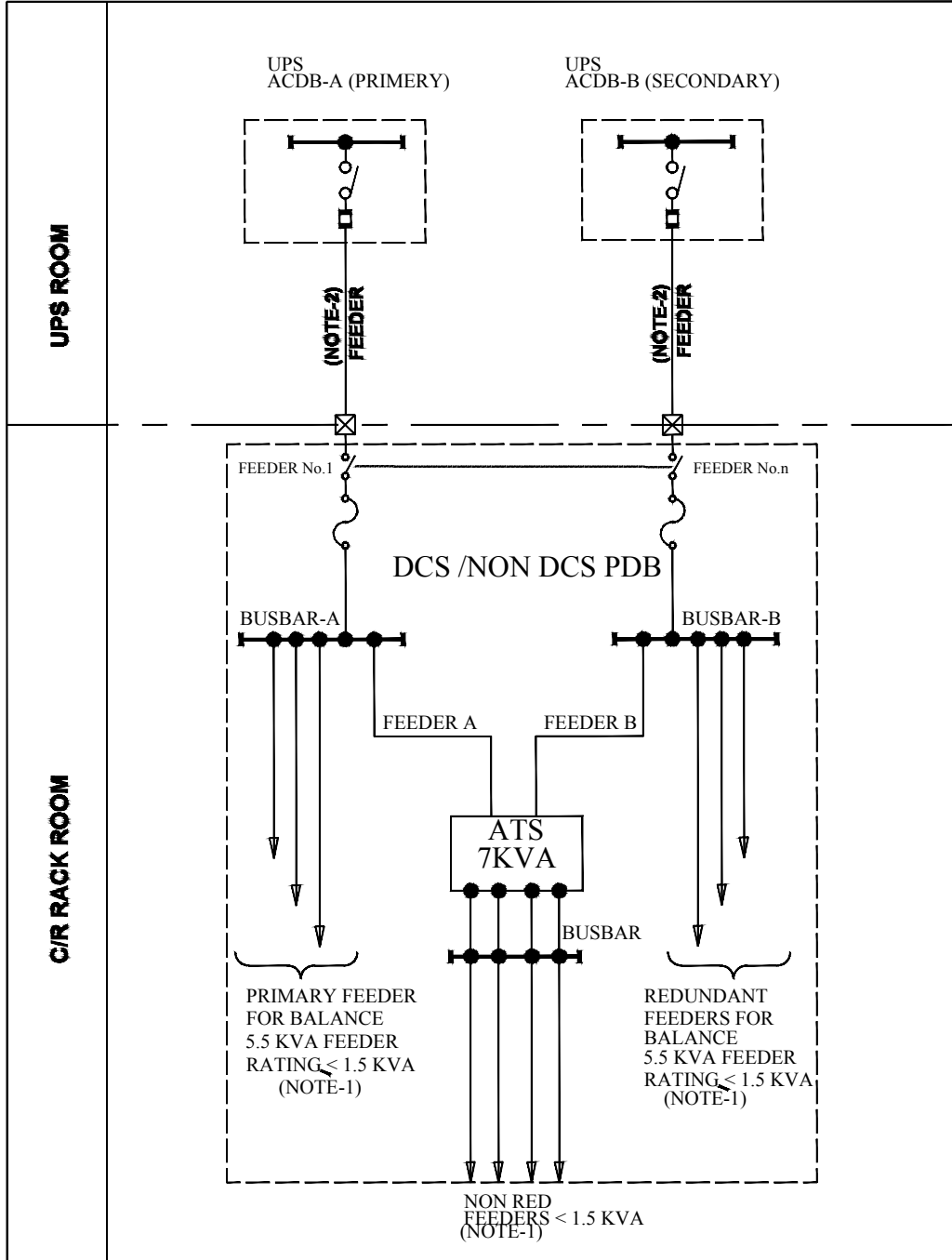
**Table – 1**  
**24 V DC non DCS Feeders Distribution List**

**DDCS-III Control Room**

Sr. No	FEEDER DECSRIPTION	FEEDER RATING (VA)	FEEDER REQD (No's)	DISTANCE (meter)	CABLE SIZE (mm <sup>2</sup> )	CABLE OD (mm)
<b>A</b>	<b>24V DC non-DCS feeder for load in field from DCS PDB in DDCS-III-Control Room</b>					
1.	Misc 1 to 10	20	4			

REV.	DATE	REVISION	BY	CHECKED	APPD.	APPD.
0	04/11/2024	ISSUED WITH MR/TENDER	BO	KKP	SM	

**ANNEXURE-X**  
**TYPICAL POWER DISTRIBUTION DIAGRAM**  
**OF AUTOMATIC TRANSFER**  
**SWITCH (ATS)**



- NOTE-1 : EACH FEEDER FROM THE BUSBAR WILL BE WITH SWITCH FUSE UNIT/MCB.  
NOTE-2 : FOR NON DCS PDB THE MAXIMUM REDUNDANT INCOMER FEEDER SHALL NOT EXCEED 12.5KVA.HOWEVER THE SAME SHALL BE FINALIZED DURING DETAILED ENGINEERING AS PER TOTAL FEEDING UPS CAPACITY.  
NOTE-3 : AUTOMATIC TRANSFER SWITCH (ATS) SHALL BE CONSIDERED FOR NON REDUNDANT DCS AND NON DCS LOADS.

The drawing, design and details given on this format are the property of ENGINEERS INDIA LIMITED. They are merely loaned on the borrower's express agreement that they will not be reproduced, copied, exhibited or used, except in the limited way permitted by a written consent given by the lender for the intended use.



ENGINEERS INDIA LIMITED  
NEW DELHI

TYPICAL POWER DISTRIBUTION DIAGRAM  
OF AUTOMATIC TRANSFER  
SWITCH (ATS)

DRAWING NO.

**ANNEXURE-X**

REV.

0

Sr No	Supplier Code	Supplier Name	Country	Holiday Description
<b>Item Code : 15CB</b>		<b>Description : SIGNAL CABLES</b>		
<b>Approved Suppliers</b>				
1	3722	POLYCAB INDIA LIMITED	INDIA	
2	3773	TEMPESENS INSTRUMENTS (I) PVT. LTD.	INDIA	
3	4001	RAVI INDUSTRIES	INDIA	
4	R203	LKB ENGINEERING PRIVATE LIMITED	INDIA	
5	3662	ELEGAR KERPEN KABEL INDIA PRIVATE LIMITED	INDIA	
6	3669	KEI INDUSTRIES LIMITED	INDIA	
7	K082	KEI INDUSTRIES LIMITED	INDIA	
8	L612	LEONI KERPEN GMBH	GERMANY	
9	D012	DELTON CABLES LIMITED	INDIA	
10	C145	CORDS CABLE INDUSTRIES LTD	INDIA	
11	U015	UDEY PYROCABLES PVT. LTD.	INDIA	
12	T243	T C COMMUNICATION PVT. LTD.	INDIA	
13	A034	ASSOCIATED CABLES PVT LTD	INDIA	
14	4135	PAGODA CABLES PRIVATE LIMITED	INDIA	
15	K190B	KEC INETRATIONAL - MYSORE	INDIA	
16	A132	ASSOCIATED FLEXIBLES & WIRES [P] LTD	INDIA	
17	3796	PARAMOUNT COMMUNICATIONS LTD	INDIA	
18	S304	SUYOG ELECTRICALS LTD	INDIA	
19	T212	THERMO CABLES LTD (FORM. T-150)	INDIA	
20	E063	ELKAY TELELINKS LTD.-	INDIA	
21	3765	THERMO CABLES LTD.	INDIA	
22	H060	HAVELLS INDIA LTD	INDIA	
23	3663	LAPP INDIA PVT LTD	INDIA	
24	3782	POLYCAB INDIA LIMITED	INDIA	
25	3724	CORDS CABLE INDUSTRIESLTD.	INDIA	

Sr No	Supplier Code	Supplier Name	Country	Holiday Description
<b>Item Code : 15CC</b>		<b>Description : OPTICAL FIBRE CABLE &amp; ASSOC.ITEM</b>		
<b>Approved Suppliers</b>				
1	B155	BIRLA CABLE LIMITED	INDIA	
2	S387	WEST COAST PAPER MILLS LIMITED (DIVISION: WEST COAST OPTILINKS)	INDIA	
3	3752	APAR INDUSTRIES LTD	INDIA	
4	U099	U M CABLES LTD	INDIA	
5	V092	VINDHYA TELELINKS LIMITED	INDIA	
6	H138	HFCL LIMITED	INDIA	
7	A400	AKSH OPTIFIBRE LIMITED	INDIA	
8	K190B	KEC INETRATIONAL - MYSORE	INDIA	
9	4140	HTL LIMITED	INDIA	
10	P610	PIRELLI CAVI SPA	ITALY	
11	K615	KABEL RHEYDT	GERMANY	

067052049057

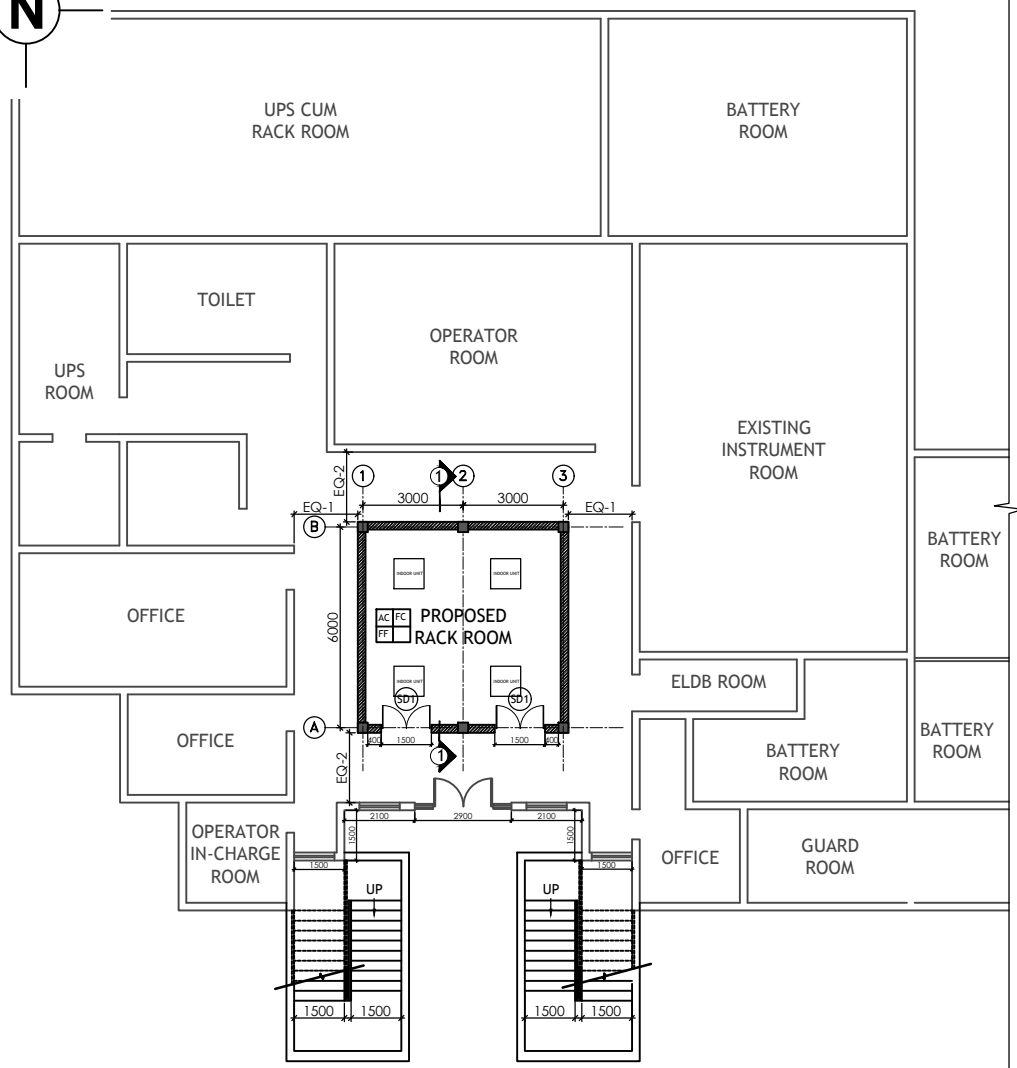


Sr No	Supplier Code	Supplier Name	Country	Holiday Description
<b>Item Code : 16ZA</b>		<b>Description : INTERFACE DEVICES</b>		
<b>Approved Suppliers</b>				
1	M154	MTL INSTRUMENTS PVT LTD	INDIA	
2	O031	OSNA ELECTRONICS PVT LTD	INDIA	
3	R506	R STAHL SCHALTGERATE GMBH	GERMANY	
4	C517	CAMILLE BAUER MESSINSTRUMENTE AG	SWITZERLAND	
5	P649	PEPPERL + FUCHS GMBH	GERMANY	
6	27506	PEPPERL + FUCHS ASIA PTE. LTD.	SINGAPORE	
7	27507	PEPPERL + FUCHS, INC.	UNITED STATES	
8	G634	GM INTERNATIONAL SRL	ITALY	
9	I599	IFM ELECTRONIC GMBH	GERMANY	
10	H620	HANS TURCK GMBH & CO. KG	GERMANY	

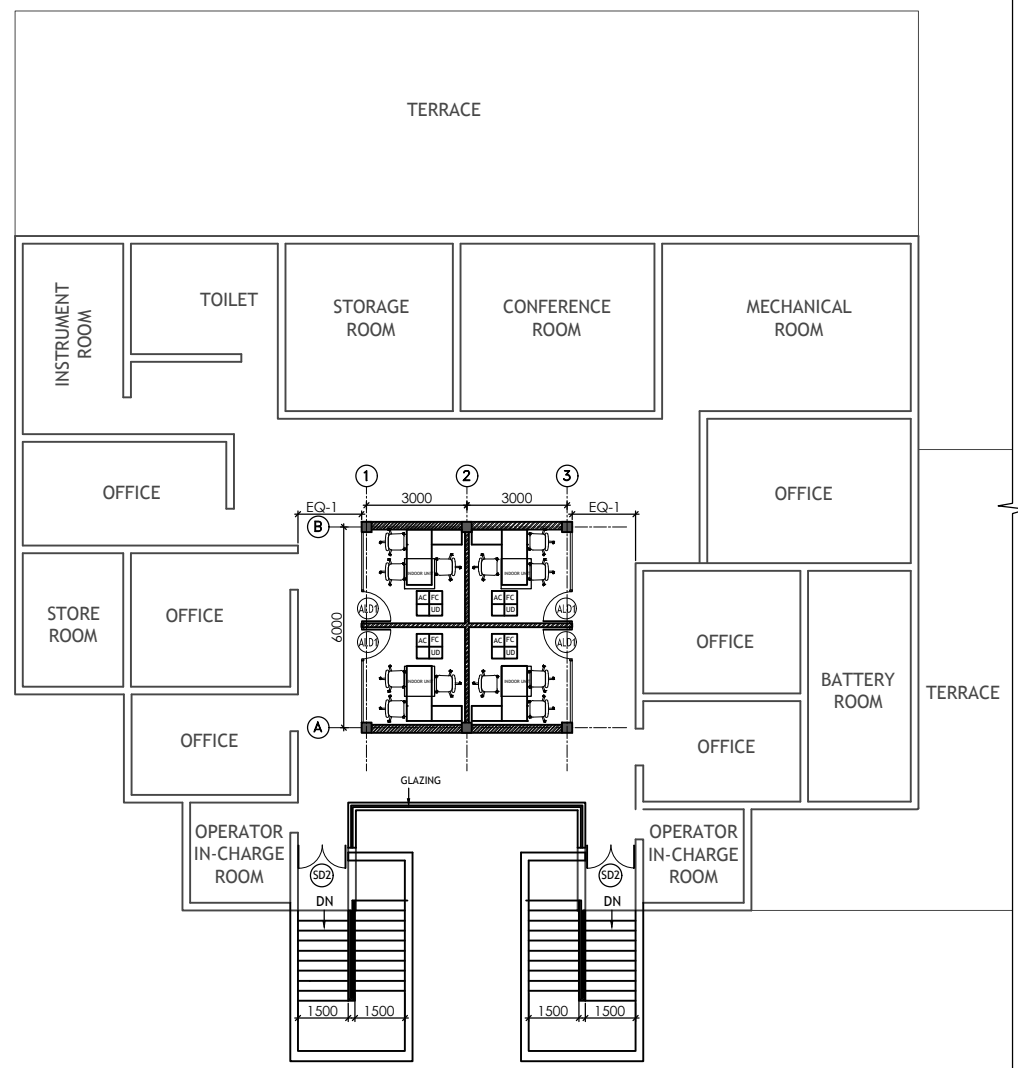


067052049057

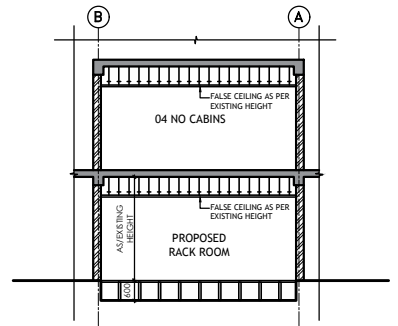
B568-304-81-46-12111



GROUND FLOOR PLAN



FIRST FLOOR PLAN



SECTION-1

REF. DWG. NO.	REFERENCE DRAWING TITLE

- NOTES:**
- DIMENSIONS, COORDINATES, LEVELS**
    - ALL DIMENSIONS ARE IN MILLIMETRES.
    - DRAWING IS NOT TO BE SCALED FOR ANY MISSING DIMENSION.
    - ALL COORDINATES ARE IN METRES.
    - LEVEL 100.000 CORRESPONDS TO TOP OF APPROACH/ACCESS ROAD NEAR THE BUILDING ENTRY CROSS REFERENCE TO STRUCTURAL DRAWINGS SHALL BE MADE.
    - FLOOR LEVEL OF THE BUILDING SHALL BE SAME THROUGHOUT UNLESS SPECIFICALLY INDICATED.
    - LOCATION ORIENTATION COORDINATES OF THE BUILDING SHALL BE CROSS-CHECKED WITH STRUCTURAL AND GENERAL CIVIL DRAWINGS. IN CASE OF ANY MISMATCH THE SAME SHALL BE GOT RESOLVED BEFORE CONSTRUCTION.
  - FLOOR**
    - FINISHED FLOOR LEVEL OF WC, DRINKING WATER SHALL BE 12MM LESS THAN ADJOINING AREAS AND SHALL HAVE PROPER SLOPE FOR FLOOR DRAINAGE.
    - FLOOR OF CABLE CELLAR, AC PLANT/ROOM SHALL HAVE PROPER SLOPE FOR FLOOR DRAINAGE.
    - REFERENCE SHALL BE MADE TO RELEVANT DRAWINGS BEFORE STARTING FLOORING WORKS. TRENCHES/CUTS IN FLOOR SHALL BE PROVIDED IN ACCORDANCE WITH RELEVANT ELECTRICAL INSTRUMENTATION/STRUCTURAL/EQUIPMENT DRAWINGS.
    - SKIRTING DETAIL SHALL BE AS I.E. STANDARD NO. 7.75-0002 & 7.75-0003.
  - WALL**
    - THICKNESS OF ALL BLOCK WALLS (EXCEPT WC) SHALL BE 230MM THK BRICK WALL IF NOT SPECIFICALLY INDICATED.
    - INTERNAL PARTITION WALLS OF WCBATH CUBICLE SHALL BE 200MM HIGH FROM FLOOR LEVEL.
    - ALL OTHER WALLS SHALL BE UP TO ROOF/ROOF BEAM IF NOT SPECIFICALLY INDICATED.
    - CUT-OUTS/OPENINGS FOR CABLES/DUCTS ETC. SHALL BE PROVIDED IN MASONRY WALLS AS PER RELEVANT ELECTRICAL INSTRUMENTATION/STRUCTURAL/EQUIPMENT, CABLE, DUCTING DRAWINGS.
  - CABLES/CONDUITS**
    - ALL CONDUITS SHALL BE CONCEALED TYPE EXCEPT IN AREAS CONCEALED BY FALSE CEILING AND SHALL BE LAID AS PER RELEVANT DRAWINGS.
    - IN CASE OF CONDUITS CONCEALED IN ROOF BEAM/LOOK, THEY SHALL BE LAID BEFORE CASTING.
  - FINISHING**
    - IN CASE OF ANY CONFLICT WITH TENDER PACKAGE, THE SAME SHALL BE GOT RESOLVED BEFORE PROCUREMENT AND EXECUTION.
  - PLINTH PROTECTION**
    - 1000 WIDE PLINTH PROTECTION WITH BUILDING DRAIN SHALL BE PROVIDED ALL AROUND THE BUILDING PERIMETER.
  - AIR CONDITIONING**
    - CASSETTE TYPE AIR CONDITIONERS SHALL BE INSTALLED FOR NEW RACK ROOM AND OFFICES. REFER TENDER FOR DETAILS ON SAME.
    - LOCATIONS OF CASSETTE AC, DDU & DDU ARE TENTATIVE AND SAME SHALL BE FINALIZED DURING DETAILED ENGINEERING BY BUILDING CONTRACTOR IN CONSULTATION WITH HVAC CONTRACTOR.

- LEGEND :-**
- A.S.L. - TOP OF APPROACH ROAD LEVEL
  - F.F.L. - FINISHED FLOOR LEVEL
  - AC FC - AIR CONDITIONED
  - FF - FALSE FLOORING
  - LD - UNDERFLOOR INSULATION
  - FF - FALSE FLOORING
  - 345 THK BRICK WALL AROUND TRANSFORMER AREA
  - 230 THK BRICK WALL
  - 115 THK BRICK WALL

REV.	DATE	REVISIONS	BY	CHKD	APPRD	TEMP
B	02.02.24	REVISED & ISSUED FOR COMMENTS	PS	AM	AV	
A	24.01.24	ISSUED FOR COMMENTS	PS	AM	AV	



INDIAN OIL CORPORATION LIMITED (IOCL)

ARCHITECTURAL FINISHES SCHEDULE			
ROOM	FLOOR FINISH	WALL FINISH	CEILING FINISH
RACK ROOM	FALSE FLOORING	CEMENT PLASTER, POP PUNNING & PLASTIC EMULSION PAINT	COMBINATION OF GYPSUM BOARD PANEL AND METAL TILE FALSE CEILING
04 NO WORKSTATIONS	VITRIFIED TILE FLOORING	CEMENT PLASTER, POP PUNNING & PLASTIC EMULSION PAINT	COMBINATION OF GYPSUM BOARD PANEL AND METAL TILE FALSE CEILING

NEW BITUROX PLANT AND ALLIED FACILITIES  
IOCL-BARAUNI REFINERY  
PROPOSED MODIFICATIONS FOR DDCS CONTROL ROOM  
FLOOR PLANS & SECTION

SCALE	JOB NO.	UNIT	DWN	DEPT	DWG NO.	REV
1:100	81568	8	3014	811	46	1/2/1/1/B

3-1041-0500 REV.2 AD-1189 x 841