UNMANNED AIR GAS PLANTS: DESIGN AND OPERATION

AIGA 028/22

Revision of AIGA 028/06

Asia Industrial Gases Association
N0 2 Venture Drive, #22-28 Vision Exchange, Singapore 608526
Tel: +65 67055642 Fax: +65 68633379
Internet: http://www.asiaiga.org | LinkedIn Profile: https://www.linkedin.com/company/asiaigaorg

UNMANNED AIR GAS PLANTS: DESIGN AND OPERATION

As part of a programme of harmonisation of industry standards, the Asia Industrial Gases Association (AIGA) has published AIGA 028, "*Unmanned Air Gas Plants: Design and Operation", jointly* produced by members of the International Harmonisation Council and originally published by European Industrial Gases Association (EIGA) as EIGA Doc 132, "*Unmanned Air Gas Plants: Design and Operation"*.

This publication is intended as an international harmonised publication for the worldwide use and application by all members of the International Harmonisation Council whose members include the Asia Industrial Gases Association (AIGA), Compressed Gas Association (CGA), European Industrial Gases Association (EIGA), and Japan Industrial and Medical Gases Association (JIMGA). Each association's technical content is identical, except for regional regulatory requirements and minor changes in formatting and spelling.

Disclaimer

All publications of AIGA or bearing AIGA's name contain information, including Codes of Practice, safety procedures and other technical information that were obtained from sources believed by AIGA to be reliable and/ or based on technical information and experience currently available from members of AIGA and others at the date of the publication. As such, we do not make any representation or warranty nor accept any liability as to the accuracy, completeness or correctness of the information contained in these publications.

While AIGA recommends that its members refer to or use its publications, such reference to or use thereof by its members or third parties is purely voluntary and not binding.

AIGA or its members make no guarantee of the results and assume no liability or responsibility in connection with the reference to or use of information or suggestions contained in AIGA's publications.

AIGA has no control whatsoever as regards, performance or non-performance, misinterpretation, proper or improper use of any information or suggestions contained in AIGA's publications by any person or entity (including AIGA members) and AIGA expressly disclaims any liability in connection thereto.

AIGA's publications are subject to periodic review and users are cautioned to obtain the latest edition.

ASIA INDUSTRIAL GASES ASSOCIATION
No-2 Venture Drive,# 22-28 Vision Exchange, Singapore 608526
Tel: +65 67055642 Fax: +65 68633307
Internet: http://www.asiaiga.org LinkedIn Profile: https://www.linkedin.com/company/asiaigaorg

Table of Contents

Amendments to 028/15

Section	Change
	Editorial to align with IHC associations
6.12	New section on process leaks into the cryogenic enclosure
8	Revision to bullets
Appendix A	Minor update

NOTE Technical changes from the previous edition are underlined

1 Introduction

This publication has been written to address issues relating to the increasing number of air gas production facilities that are run unmanned or remotely operated.

There are many similarities in the operation of manned, unmanned, and remotely operated plants; however, there are some differences. These differences are not only in how the plant is operated and maintained but also how the plant is designed. In particular, designing new unmanned plants or converting existing plants from manned to unmanned or remote operation requires specific design considerations to ensure an equivalent level of safety to that of a manned operated plant.

2 Scope and purpose

The purpose of this publication is to provide guidelines for the design, operation, and maintenance of a plant that has unmanned or remote operations.

Unmanned or remotely operated plant functionality can range from a plant with full remote functionality i.e., satellite plant controlled by a remote operating centre (ROC) to a plant with autonomous operation.

The installations that are included in this publication are:

- cryogenic air separation plants;
- cryogenic nitrogen generators;
- non-cryogenic plants (pressure swing absorption, vacuum pressure swing absorption, membrane, etc.,) for oxygen and nitrogen;
- pipeline compression stations;
- compressed dry air facilities; and
- back-up systems and site storage, if existing and integrated with the production unit.

Specifically excluded are product supply tanks installed at a customer's premises, home care units (for example, concentrators), and non-cryogenic plants with a capacity of 5 000 kg (5 ton) per day or less. For non-cryogenic plants from 5 000 to 20 000 kg (5 ton to 20 ton) per day, a risk assessment shall be carried out to identify which requirements of this publication apply.

3 Definitions

For the purpose of this publication, the following definitions apply.

3.1 Publication terminology

3.1.1 Shall

Indicates that the procedure is mandatory. It is used wherever the criterion for conformance to specific recommendations allows no deviation.

3.1.2 Should

Indicates that a procedure is recommended.

3.1.3 May

Indicates that the procedure is optional.

3.1.4 Will

Is used only to indicate the future, not a degree of requirement.

3.1.5 Can

Indicates a possibility or ability.

3.2 Technical definitions

3.2.1 Personnel roles

3.2.1.1 Local operator

Person who is on site and has control of the plant. Personnel who are working at the plant but are not in control of the plant are not considered to be local operators.

3.2.1.2 Remote operator

Person remotely located that has control of the plant.

3.2.2 Remote control / remote monitoring

Two-way communication from the plant to or from the ROC, (for example, receiving plant alarm / trip signals and the ability to remotely start / stop machinery, etc.).

Remote monitoring implies one way communication from the plant to the ROC, (for example, receive only plant alarm / trip signals, plant data, etc.).

3.2.3 Remote operating centre (ROC)

Any location that remotely monitors and/or controls a plant or multiple plants from outside of the plant boundary. It can be a dedicated centre, be located at a plant site, or any other remote location.

The ROC can also provide specialist operations support (maintenance, engineering, control systems, etc.).

3.2.4 Remote operation

Condition where a plant operates for period of time with operational control of a plant performed at a location other than the plant site.

Such a condition can exist whether or not there are personnel (for example, performing trailer filling or maintenance tasks) at the plant site.

Remote operation does not necessarily imply continuous communication with the plant.

3.2.5 Unmanned operation

Condition where a plant operates without the physical presence of personnel qualified to respond to a plant process or safety emergency, either independently or with direction from a qualified operator.

3.2.6 Unmanned plant

Plant that operates for any period of time without the physical presence of personnel qualified to respond to a plant process or safety emergency, either independently or with direction from a qualified operator.

4 Safety aspects of plant design

4.1 General considerations

This section briefly introduces the complex subject of safety in plant design and the reader is referred to Section 9 for more detailed information.

The starting point for evaluation of safety systems is always a review that is focused on safety. This can typically be a hazard and operability (HAZOP) review for new plant designs or a “What If” analysis for retrofits. Either type of analysis will lead to a hazard identification and risk assessment. The objective of these assessments is to identify the safety features necessary to reduce the risk to the as low as reasonably practicable (ALARP) threshold–the necessary safety target set by each country / company.

Safety related features can prevent, contain, or mitigate the hazard and comprise the following categories:

- passive engineering systems (for example, selection of pipeline materials to eliminate the hazard, secondary leak containment system, etc.);
- active engineering systems (for example, a device, safety valve, non-return (check) valve, or instrumentation (alarms and trips); and
- procedural controls / human actions (for example, operating instructions, emergency response–plant shutdown, isolation, etc.).

Plants should be designed to incorporate controls in the first category (which eliminate or reduce the risk) as these are inherently more reliable than those in the other two categories.

Certain safety related features that rely on instrumentation are called safety instrumented systems (SIS) and the following design standards give a systematic approach that is internationally recognised as best practice:

- IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems –All Parts* [1].[1] This standard is focused towards manufacturers and suppliers of devices; and
- IEC 61511, *Functional safety–Safety instrumented systems for the process industry sector – All Parts* [2]. This standard is focused towards system designers, integrators, and users.

Both standards give guidance on how to achieve suitable reliability for these SIS (risk graph, layer of protection, etc.). This reliability is called the safety integrity level (SIL) (which is numbered 1 to 4) and such systems are usually considered to be safety critical.

A high SIL rating means a more demanding safety function requiring more sophistication in the equipment (for example, SIL 4 is usually used in the nuclear industry) and requires duplication / redundancy / diversity in the instrumentation so that no single component could cause the overall system to fail.

Typically, air separation plants have only a few SIS. Most are passive systems (material selection, location, etc.) or active engineering systems (safety valves, etc.). The instrumentation elements of the SIS may be specified with SILs. Where applied, these are usually specified to SIL 1 or SIL 2 (i.e., 1 dangerous failure every 100 000 to 1 million hours for SIL 1 and 1 dangerous failure every 1 million to 10 million hours for SIL 2).

See 5.8.4 for typical examples.

[1] References are shown by bracketed numbers and are listed in order of appearance in the reference section.

Having established the required design reliability, there is also guidance on how to establish suitable hardware reliability. The key message here is an overall life cycle requirement for SIS so that the control function operates with the correct reliability over the whole life of the plant.

See AIGA 056, *Guideline for Safe Practices for Cryogenic Air Separation Plants* for more information regarding plant design and operation [3].

4.2 Requirements and recommendations for unmanned and remotely operated air gas plants

A risk assessment paying particular attention to the consequences of unmanned and remote operation shall be made for all unmanned and remotely operated plants. For new projects, the authorities normally require a risk assessment as part of the operating licence.

If the general risk assessment has not been done before, it shall be done prior to implementing unmanned or remote operation.

For retrofits, the existing risk assessment shall be reviewed in detail and updated where necessary.

The risk assessment for an operating plant shall be reviewed whenever a significant change is made to the process, see 4.4. The objective of the review should be to ensure that changes in operating conditions, connected supplier and customer processes, and surrounding communities have not created an unacceptable risk or altered safety features that were originally built into the design.

Whenever an unmanned or remotely operated plant is acquired from a third party, the risk assessment documentation for that process shall be reviewed to confirm compliance with company and industry standards. If there is no existing risk assessment documentation or the existing documentation is incomplete, a new formal risk assessment shall be conducted.

4.3 Plant location risk

For unmanned or remotely operated plants, detection and mitigation of off-site risks becomes more important since human intervention cannot be assumed.

Typical questions that shall be considered are:

- How could the installation and the total stored volume of products affect the surrounding area;
- How could the surrounding area affect the safety of the plant;
- Can planned future developments in the surrounding area or within the plant area have a negative influence on safety; and
- Can the local firefighters handle a major release of products from the plant?

See EIGA Doc 75, *Methodology for Determination of Safety and Separation Distances* [4].

4.4 Management of change review

Management of change (MOC) is the procedure used to ensure that changes are implemented correctly and safely and are documented. These documents shall be maintained at the plant. Any proposed change to equipment, controls, software, procedures, and facilities shall require a documented review by technically competent personnel and approval by authorised personnel before implementation. This review and authorisation shall apply to all proposed modifications or changes whether they are permanent, temporary, or emergency in nature. All appropriate plant documentation such as a process and instrument diagram, equipment specifications and drawings, and operating and maintenance procedures shall be updated.

Replacement-in-kind is an exact replacement or design alternative that meets all design specifications of the item being replaced. Replacement-in-kind does not require MOC approval, see AIGA 010, *Management of Change* [5].

5 Plant design and retrofit considerations

5.1 Compliance with permits and regulations

All applicable regulations shall be followed and appropriate permits acquired.

Delegation of responsibility for compliance with permits and regulations shall be defined in the company management system for each unmanned or remotely operated plant.

5.2 Shutdown systems

Manned, unmanned, and remotely operated plants are subject to different needs for shutdown systems. A risk assessment shall be performed to determine the type and methodology of shutdown systems and should account for the staff available to respond to an emergency at an unmanned or remotely operated facility.

The requirements for manual and automated shutdown systems for unmanned and remotely operated plants are described below.

5.2.1 Plant emergency shutdown

All unmanned or remotely operated plants shall be provided with an emergency shutdown system that, when activated, will put the plant into a safe condition. Where multiple emergency shutdown systems are present, the systems should control logical segments of the site (i.e., the storage areas, trailer filling areas, production units, etc.).

Emergency shutdown systems are hardwired stop buttons strategically located around the plant and include:

- machine stop buttons;
- switch gear stop buttons; and
- plant stop button.

At least one of the stop buttons shall be safely accessible by the initial responder, see 8.1.

Manually operated hardwired stop buttons shall be strategically located around the plant. At least one of the stop buttons shall be safely accessible by the initial responder, see 8.1.

The plant emergency shutdown system can also be manually activated from the plant control system, the ROC, or other locations such as the customer control room.

The storage and trailer filling emergency shutdown system shall isolate all storage tank liquid valves and cease filling operations. If the main storage tank is used to directly feed the backup vaporisation system to a pipeline customer, a risk evaluation shall be made covering the case for isolating the liquid outlet valve.

Remote or automatic reset of the emergency shutdown system shall not be possible. It is potentially hazardous to remotely or automatically reset the emergency shutdown system because it may not be possible to determine the complete nature of the emergency.

5.2.2 Plant shutdown system

All unmanned or remotely operated plants shall be provided with an automated shutdown system that, when activated, will put the equipment or plant into a safe condition.

The plant shutdown system will normally be activated by various trip signals, for example:

- critical safety devices identified during the risk assessment phase (for example, liquid leak detectors, hydrocarbon detectors, etc.);
- process safety devices (for example, pressure switch);
- quality control devices (for example, analysers);
- machine protection devices (for example, vibration, low oil pressure); and
- local or remote manual inputs.

Provisions to allow for remote reset of the plant shutdown system shall be documented.

5.2.3 Remote shutdown

The ability to trip the plant from a remote location (for example, ROC) provides additional operational safety, but this ability might not be available for all facilities. Remote shutdown shall not be the primary means of emergency shutdown or plant shutdown, as communication with the remote location can be interrupted.

5.3 Fire and gas alarm system

Subject to a risk assessment, unmanned and remotely operated plants may be provided with an automatic fire / smoke detection system. Examples of areas that could require protection are the control room, the electrical switchgear room, and compressor areas.

It is recommended that the fire detection system be monitored and form part of the emergency response plan.

Gas detectors (for example, hydrocarbons, ammonia, hydrogen, oxygen deficiency, etc.) and alarm systems shall be located according to the risk assessment evaluation. Portable gas monitoring should be considered for personnel when they are working in areas that can expose them to a hazardous atmosphere.

5.4 Remote detection of liquid spillage

The spillage of cryogenic liquid due to leakage or malfunctioning valves is a risk to be controlled closely. Process related drain valves should be connected to the liquid disposal system.

A specific risk assessment shall be made to identify any additional protective measures that may be required, for example, ground temperature measurement and video camera surveillance.

5.5 Process equipment guidelines

See Appendix A for detailed list of considerations.

5.6 Trailer filling systems

All merchant liquid plants include a filling and analysis system for transferring liquid to trucks. Some production plants have a fully automated weighbridge filling and analysis system while other plants include varying degrees of manual operation.

A risk assessment shall be completed for filling systems at unmanned and remotely operated plants and the following items should be reviewed:

- personnel access to the site;
- site access control (for example, password access, ID card, key entry, etc.);
- leak detection devices for areas around cryogenic liquid pumps and storage tanks; and
- man-down or driver push-button timer alarm system.

For more information regarding tanker loading procedures, see AIGA 085, *Liquid Oxygen, Nitrogen, and Argon Cryogenic Tanker Loading Systems* [6].

5.7 Distribution pipeline and vaporiser system

5.7.1 Distribution pipeline systems

Consideration should be given to maximum pipeline flow regulation, shutdown on low pipeline pressure and customer emergency shutdown. See AIGA 021, *Oxygen Pipeline and Piping Systems* [7].

5.7.2 Backup vaporiser systems

Backup vaporiser systems should share the following features:

- To protect the system against low process temperatures and to ensure reliability of a critical supply, the control system should rely on secure sources of power and instrument gas. This can require the use of an uninterruptable power supply (UPS) to supply an electronic control system or a completely pneumatic control system (including pneumatic low temperature trip);
- Sizing of storage tanks and vaporisers should be reviewed for unmanned and remote operation and response time for service and product delivery. Special consideration should be given to the sizing of ambient air vaporisers in regard to severe ambient conditions; and
- Remote monitoring of tank levels should be considered.

Backup systems should be tested on a regular basis to ensure that they will operate properly when required.

See AIGA 027, *Cryogenic Vaporisation Systems–Prevention of Brittle Fracture of Equipment And Piping* [8].

5.7.3 Liquid disposal systems

Liquid disposal systems are needed to safely dispose of plant liquids. Ambient air, water-bath, steam heated, or other vaporisers can be used.

The disposal system shall be designed to prevent an uncontrolled liquid discharge. This can include sizing for all possible load conditions, low outlet temperature alarm, and loss of utility alarm.

When converting from manned to unmanned or remote operation, consideration should be given to safe disposal of liquid from automated drains that can fail in the open position.

5.7.4 Fogging hazards

The operation of some vaporisers can cause fogging within the plant area, adjacent roadways, buildings, neighbouring facilities, and other areas where it can cause a hazard. Equipment should be located to minimise this hazard.

When fogging hazards cannot be mitigated by the location of buildings and equipment, consideration should be given to installing equipment to disperse fog away from the affected area for example, ground mounted fans, barriers, etc.

Warning signs shall be installed where fogging presents a hazard.

5.8 Control system guidelines

Different levels of automation and alarm monitoring are possible. In any case, automation systems contain both a monitoring control function and a safety function.

5.8.1 Monitoring control function

The monitoring control system automatically controls the unit to set values. This can include:

- start-up of the unit;
- process variables;
- product quality and / or adapting to customer requirements;
- transmission of alarms;
- process and machinery trip and interlock signals;
- management functions, for example, reports, alarm logs, etc.;
- access to information locally or remotely; and
- controlled shutdown.

5.8.2 Safety function

The control system performs safety functions based on control system internal logic functions and / or on external detectors.

The safety system performs several functions:

- shut down of the unit in a safe mode, if a process value reaches a critical limit;
- warn of rotating machinery imminent start – for example, horn, flashing light; and
- send high priority alarm information to the ROC or to any other designated point of contact.

These high priority alarms can include fire detection, hazardous atmosphere, man down, site intrusion, etc., see 5.8.4.

When the plant is installed on the customer’s site, these requirements should generally be coordinated with the customer, in accordance with local regulations, and be specified in the customer's safety and emergency response plan.

5.8.3 Plant network and communication system integrity and security

The emergency shutdown system shall always be independent of any external communication system.

The plant control system operates the plant safely and will, when needed, shut down the plant without any remote action.

Communication systems associated with unmanned or remotely operated plants should be designed in a reliable way. Consideration should be given to the installation of a redundant network or modem backup.

Remote access to the plant system shall be made by secure methods for example, password protection, firewalls, defined IP addresses, etc. Depending on the complexity of the plant, different access security levels may be identified for different classes of user (for example, operator access, controls engineer access, etc.).

An emergency plan should be prepared to cover the failure of the ROC. The plan could involve deploying operators to the plant sites, moving the network connections to another location, installing redundant network connections, etc.

5.8.4 Alarm prioritisation

Each alarm shall be reviewed against potential consequences if corrective action is not promptly initiated. The following shall be considered:

- safety – reacting to the alarm could prevent / mitigate a plant incident with potential injury or loss of life;
- environment – reacting to the alarm could prevent / mitigate potential breach of environmental permit limits or contamination; and
- equipment/production – reacting to the alarm could limit financial consequences for example, by preventing damage to equipment, lost production, loss in efficiency, output loss during plant outage.

A guide for prioritising alarms shall be developed. The system should be designed to minimise potential nuisance alarms that are communicated to the ROC in order to prevent alarm overload.

Detailed information on alarm prioritisation is available from several publications for example, EEMUA Publication 191, *Alarm systems - a guide to design, management and procurement* [9].

Typical alarm categorisation includes high, medium, and low priority.

5.8.4.1 High priority

Any abnormal condition that plant supervision shall immediately address so emergency response procedures or customer outages can be initiated. For reliability requirements, see Section 4.

Special consideration shall be given to the design of high priority alarm systems with respect to loss of the primary communication system.

Typical examples of high priority alarms / trips include:

- man-down alarm;
- fire alarm (building alarms, oxygen compressor fire, etc.);
- main condenser high / low level;
- high hydrocarbon concentration in reboiler / condensers;
- high storage tank level;
- uncontrolled cryogenic liquid spillage detection; and

- critical safety alarms defined with the customer (for example, low pipeline pressure, backup system failure, loss of safety nitrogen purity, etc.).

5.8.4.2 Medium priority

Any abnormal condition that plant supervision shall address to maintain or restore facility production.

Typical examples of medium priority alarms can include:

- loss of product purity;
- machine trip;
- loss of remote control capability (for example, switched to local control or communication failure);
- process alarms that indicate an imminent failure (for example, cycle timer failure on the molecular sieve adsorbers);
- machine alarm that indicates a possible problem (high oil temperature, vibration alarm etc.); and
- supervisory control system failure (for example, watchdog timer alarm, programmable logic controller (PLC) failure, etc.).

5.8.4.3 Low priority

An abnormal condition not classified as high or medium priority about which plant supervision wishes to be advised.

5.8.5 Management of plant alarms

A system shall be designed so that high priority safety alarms are processed without delay. For plants that are remotely operated, the local plant alarm system shall transmit at least all high priority alarms to the ROC or to any other designated point of contact. These can be transmitted as grouped common alarms if the system functionality is limited.

5.9 Design aspect of maintenance

In order to minimise safety issues associated with lone working, attempts should be made to reduce or facilitate as many routine maintenance tasks as possible at the design phase.

Examples of this include:

- work to be performed at elevated heights should be modified for ground or platform access; and
- work involving heavy lifting by one person should be automated (for example, by providing lifting beams, etc.).

6 Plant operation

6.1 Plant safety requirement

Special considerations shall be made for the operating procedures of unmanned or remotely operated plants.

These considerations shall include:

- Emergency response plan;

- Work permit systems;
- Work instructions;
- MOC requirements;
- Maintenance of machinery, process control equipment, and calibration of instruments and safety devices;
- Regular testing of high priority loops (alarms/trips) and critical safety systems; and
- Training of new personnel, contractors, and other persons visiting the plant.

These considerations may also include:

- access procedures;
- specific customer safety rules for example, sign in procedures, personal protective equipment; and
- safety procedures as agreed with the customer.

6.2 Plant responsibility

The individual or individuals responsible for key operations activities for unmanned or remotely operated plants such as safety, employee training, maintenance, etc., shall be clearly defined.

Local regulations and operating permits shall be followed for assignment and delegation of responsibility.

6.3 Training and skills

6.3.1 Plant operator training

All plant operators (local and remote) shall be trained in safety, emergency procedures, and plant operation. They shall also be trained in the operation of the type of plants they are controlling. Periodic retraining is recommended to ensure the operator's skill level remains current. Satisfactory completion of training / retraining shall be documented.

For other information, see AIGA 009, *Safety Training for Employees* [10].

6.3.2 Cooperation between local and remote operators

Local and remote operators shall work in close cooperation. Clear responsibility and communication procedures shall be established.

Communication regarding plant activities shall be documented in the log book (may be electronic or logbooks at both sites).

6.4 Documentation

Documentation that shall be available to the remote operator includes:

- Emergency plan (including contact names and phone numbers);
- Process and instrumentation diagrams;
- Plant operating procedures used for remote operations;

- Log book;
- MOC documents when applicable; and
- Internal ROC procedures.

Additional examples of documentation that can be provided to the remote operator include:

- mechanical and electrical drawings; and
- alarm / trip list.

NOTE Standardised documents or site-specific documents can be used and may be provided electronically. The documentation provided shall be the same as that used by the local operator.

6.5 Transfer of plant control

Clear procedures shall be established to transfer operational control from:

- remote operation to local operation;
- local operation to remote operation; and
- remote operation to another remote operation (for example, ROC to control system engineering).

These procedures shall comply with all applicable rules and local permits.

The transfer shall be recorded in a traceable way (for example, log book entries, work permits, historical record in the control system, etc.).

It is technically possible for multiple locations to operate the plant at the same time. However, it is recommended that only one operator have overall operating responsibility.

NOTE These procedures do not replace the need for on-site technicians to protect themselves from accidental equipment starts caused by the control system or through possible remote operation of a plant. Always use lockout / tagout (LOTO) and other safety measures (circle of safety, work permit, etc.) when working on equipment.

The non-observance of these procedures can endanger personnel working on site and affect the plant operation.

6.6 Alarm handling procedures

Procedures for calling out on duty personnel shall be available.

In case of automated call out systems (local installations), escalation steps shall be defined in case the called out support does not respond.

In case of a major incident, a large number of alarms of the same priority can occur simultaneously. In such cases, it is very important to support the operator with a plant prioritisation and an alarm prioritisation system, which helps to determine the most important plant/alarm and deal with it first.

It is preferred that a first-out system be implemented that allows the operator to identify the initial alarm.

Whenever it is possible (for example, when notified by the ROC), the person called out shall be informed of any hazards to be expected on arrival.

6.7 Remote restart considerations

Procedures for remote restart shall be documented. A warning should be provided when the remote start of rotating machinery is imminent (for example, horn, flashing light).

There are certain circumstances where remote restart is not recommended unless a local investigation and analysis has been carried out. Typical examples include:

- oxygen compressor safety related trip;
- any machinery vibration trip; and
- any high priority alarm that caused a plant trip.

6.8 Activity communication follow up

Activities on an unmanned or remotely operated plant shall be recorded in a log book.

Procedures shall be established in order to inform people entering the unmanned or remotely operated plant about the current operating situation.

Activities on the unmanned or remotely operated plant shall not be started without permission from the operator in control of the plant.

Notification of technical changes shall be available at both locations.

6.9 Work permits

Work permit systems shall be established and followed regardless of the manning condition, see AIGA 011, *Work Permit Systems* [11].

6.10 Truck driver safety and security

Security systems and procedures should be in place to limit free access to plant controls other than those strictly related to the trailer filling operation. Drivers performing trailer filling activities should follow documented security access procedures.

Truck drivers are often the most frequent personnel at the site. Measures should be taken so that they are aware of situations that can endanger their health and safety. Systems should be in place so that they can escalate problems that they encounter at the site. Communication between the ROC and the trailer filling area should be considered.

They shall be trained on filling trailers at unmanned and remotely operated plants and in emergency procedures.

The training shall be refreshed periodically and after technical changes on the filling station.

The training and authorisation shall be documented.

6.11 Atmospheric monitoring / man-down systems

Areas with the potential for oxygen deficiency or enrichment shall be reviewed to determine which areas require atmospheric monitoring systems. Atmospheric monitoring systems (fixed or portable) shall be used for these areas and appropriate warning, labelling, and marking installed at points of ingress to the hazard area.

A man-down procedure shall be considered to minimise the risk for a single worker performing duties at an unmanned or remotely operated plant. Factors affecting the design and complexity of the man-

down system include the frequency and duration of the visit, the process risk, the tasks to be performed, and any environmental factors.

6.12 Process leaks into the cryogenic enclosure

Responding to available instrumentation outputs that indicate a potential process leak in the cryogenic enclosure such as the insulation space high pressure alarm, requires the remote operations to request an immediate investigation by the local operations. Based on the local operations site findings, a risk assessment in accordance with the owner's procedures shall be completed by subject matter experts. The results of the risk assessment may determine that the plant can continue to run for an extended period of time, that additional testing and monitoring is necessary, or require immediate shutdown and repair of the unit. For more information, see AIGA 079, *Safe Design and Operation of Cryogenic Enclosures* [12].

6.13 Plant / site security

All unmanned or remotely operated plants shall be provided with security systems to prevent intrusion by unauthorised persons. The level of security installed at the site depends on the process risk and on the local environment. Unmanned or remotely operated plants located inside a customer's property may not need additional security systems.

Typical security systems used inside the plant can include:

- fencing;
- security cameras;
- self-locking doors;
- security alarms; and
- signage / labelling.

For more information, see EIGA Doc 922, *Site Security* [13]

6.13.1 Entry and exit procedures

Entry and exit procedures shall be clear and detailed. A person working in a remotely controlled plant shall log in on arrival and shall log out on departure with the operator who has current plant control (usually the ROC), for example, by phone, electronic device, etc. This is necessary to maintain good communications and coordination between the ROC and local persons. Drivers performing routine duties and personnel located close to the plant for example, sales office etc., may be excluded from this requirement (see 6.10).

This requirement may not apply to plants that are only remotely monitored.

7 Plant maintenance

To ensure safe operation of unmanned or remotely controlled plants, maintenance activities should be performed in a controlled manner. The additional operational issues presented by unmanned or remotely controlled operation require a more detailed approach to communication, planning, and failure analysis, etc.

7.1 Planned maintenance and record keeping

Maintenance of unmanned or remotely operated plants is typically performed by different groups of contractors and / or technicians. This carries the danger that personnel are unaware of each other's actions. Therefore, it is essential that the record keeping and communication systems be documented and rigorously followed.

Maintenance activities require detailed instructions, work permits, and documentation of work performed. Maintenance procedures should be available for each major item of equipment.

The site should be inspected at defined intervals to ensure it is maintained in a safe condition.

7.2 Lone worker tasks

Activities should be reviewed to ensure that a single person can safely perform the task. Tasks prohibited for lone workers shall be documented. Examples include tasks that involve:

- confined space entry;
- high and medium voltage electrical work; and
- elevated work.

Procedures should address surveillance during lone worker operations based on the type and duration of the activity. Systems used to assist with surveillance of lone workers can include entry / exit procedures, routine telephone calls, operator presence control timer, man-down monitor, etc.

7.3 Training and skills

All personnel performing maintenance tasks shall be trained in safety, emergency procedures, and tasks for the specific unmanned or remotely operated plant. Periodic retraining is recommended to ensure the skill level remains current. Completion of training / retraining shall be documented.

This also applies to remote personnel (for example, control engineers, ROC operators) responsible for operations or maintenance and contractors.

7.4 Interface between operations and maintenance

The interface between operations and maintenance is important in remotely operated plants. There should be a documented procedure that coordinates the following areas:

- Control of personnel presence at site;
- Control of maintenance jobs at site (for example, LOTO procedure);
- Recording of any safety system taken out of service in the log book; and
- Continuity of supply to the customer (for example, scheduling the maintenance task when adequate product inventories are available).

7.5 Lockout / tagout

Most equipment in ASU plants is designed to remotely start or stop. It is important that these systems be locked out prior to the commencement of maintenance. This will prevent any unintentional restart during maintenance. Signs that warn of the potential of automatic start of the unit should be clearly posted around the equipment.

Before working on machinery or electrical systems, the effectiveness of the lockout shall be locally checked.

8 Emergency plans and external notification

Procedures shall be developed to cover the response to emergency conditions that personnel can encounter.

Typical examples of emergency conditions that should be considered include:

- fire;
- major product release, pipeline rupture, or energy release;
- major perlite release;
- significant process leak within the cryogenic enclosure;
- severe weather conditions such as hurricane, tornado, flood, or extreme cold;
- adjacent industry incidents (for example, explosions, hydrocarbon releases, toxic chemical releases);
- personnel injury (for example, man-down alarm);
- site intrusion / security breach. See EIGA Doc 922 [13];
- fog cloud from a cryogenic release; and
- air quality changes due to environmental events such as haze and smoke from forest fires, burning farmland, or other biomass combustion.

Maximum anticipated response times for emergency services and plant personnel should be considered as part of the emergency planning process. If the plant is located inside a customer facility (for example, chemical plant or refinery), close liaison with the customers emergency services organisation will be necessary. The emergency plan shall include procedures for warning and evacuation of on-site personnel or contractors (for example, assembly point, audible warning, etc.).

Emergency procedures and related fail-safe shutdown systems are an integral part of the plant design and shall consider the unique hazards of unmanned and remotely operated plants.

Emergency services shall be updated with the latest site emergency plan.

8.1 Initial responder function

As defined in the emergency plan, the functions of the initial responder are to secure the site and to organise the response.

8.2 Remote operator functions during an emergency

The emergency plan shall give instructions regarding the roles and responsibilities that the ROC could have during a major incident, including interaction with emergency services, initiation of the emergency plan, and participation in the emergency plan (for example, as a mobilisation coordinator).

8.3 External emergency services

External emergency services are often the initial responder to an incident at an unmanned or remotely operated plant. In some instances, they require additional training so they can take appropriate action without company personnel being present.

External emergency services can be provided by the customer, firefighters, police, or security service as defined in the emergency plan.

Emergency services shall be updated with the latest site emergency plan when changes are made. Communication of the site emergency plan and offers to provide training to emergency services personnel should occur at defined intervals.

8.4 Emergency drills

Emergency drills and training requirements shall be defined in the emergency plan and shall be based on the complexity of the installation.

Wherever possible, all the services that are named in the emergency plan should participate in the drills (firefighters, ambulance, police, security service, customer, ROC, authorised personnel, etc.).

9 References

Unless otherwise specified, the latest edition shall apply.

[1] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems–All Parts,* www.iec.ch.

[2] IEC 61511, Functional safety – Safety instrumented systems for the process industry sector – All Parts, www.iec.ch.

[3] AIGA 056, *Guideline for Safe Practices for Cryogenic Air Separation Plants*, www.asiaiga.org

NOTE This publication is part of an international harmonisation programme for industry standards. The technical content of each regional document is identical, except for regional regulatory requirements. See the referenced document preface for a list of harmonised regional references.

[4] EIGA Doc 75, *Methodology for Determination of Safety and Separation Distances*, www.eiga.eu.

[5] AIGA 010, *Management of Change*, www.asiaiga.org

[6] AIGA 085, *Liquid Oxygen, Nitrogen, and Argon Cryogenic Tanker Loading Systems*, www.asiaiga.org

NOTE This publication is part of an international harmonisation programme for industry standards. The technical content of each regional document is identical, except for regional regulatory requirements. See the referenced document preface for a list of harmonised regional references.

[7] AIGA 021, *Oxygen Pipeline and Piping Systems*, www.asiaiga.org

NOTE This publication is part of an international harmonisation programme for industry standards. The technical content of each regional document is identical, except for regional regulatory requirements. See the referenced document preface for a list of harmonised regional references.

[8] AIGA 027, *Cryogenic Vaporisation Systems–Prevention of Brittle Fracture of Equipment and Piping*, www.asiaiga.org

NOTE This publication is part of an international harmonisation programme for industry standards. The technical content of each regional document is identical, except for regional regulatory requirements. See the referenced document preface for a list of harmonised regional references.

[9] EEMUA Publication 191, *Alarm systems - a guide to design, management and procurement*, www.eemua.org.

[10] AIGA 009, *Safety Training for Employees*, www.asiaiga.org

[11] AIGA 011, *Work Permit Systems*, www.asiaiga.org

[12] AIGA 079, *Safe Design and Operation of Cryogenic Enclosures*, www.asiaiga.org

NOTE This publication is part of an international harmonisation programme for industry standards. The technical content of each regional document is identical, except for regional regulatory requirements. See the referenced document preface for a list of harmonised regional references.

[13] EIGA Doc 922, *Site Security*, www.eiga.eu.

[14] AIGA 048, *Reciprocating Compressors for Oxygen Service*, www.asiaiga.org

NOTE This publication is part of an international harmonisation programme for industry standards. The technical content of each regional document is identical, except for regional regulatory requirements. See the referenced document preface for a list of harmonised regional references.

[15] AIGA 071, *Centrifugal Compressors for Oxygen Service*, www.asiaiga.org

NOTE This publication is part of an international harmonisation programme for industry standards. The technical content of each regional document is identical, except for regional regulatory requirements. See the referenced document preface for a list of harmonised regional references.

Appendix A – Process equipment guidelines

The purpose of the check list is to assist in determining the automation level required for operating an unmanned or remotely operated plant. The list is not exhaustive and should be used as an aid for a detailed risk assessment.

The normal questions to be answered on each point include what manual interaction should be automated:

- during normal operation;
- following a trip;
- at start-up and shutdown; and
- during a process upset.

The automation level needed should be adapted to each plant depending on local circumstances.

CHECK LIST

No	Item	Considerations	Comments/Recommendations
1	Ambient	1. Air temp 2. Humidity 3. Wind direction and speed 4. Vents or emissions from nearby sources	1. Alert ROC on extreme weather conditions 2. Where risk of fog is an issue 3. For fan ejector, running when certain direction is restricted 4. Perimeter or feed air hydrocarbon detection
2	Air filter	1. Differential pressure (dP) filter monitoring (alarm) 2. Heaters 3. Roll filter 4. Filter room	1. In dusty areas, consider self-cleaning designs 2. For locations where snow and ice can plug the filter inlet 3. Automate, restrict roll advance 4. Restricted entry to filter room – confined space
3	Centrifugal compressor and turbine (air, nitrogen, oxygen)	1. Add surge information to the control system 2. Local trips/start-up interlock and alarms to be connected to the control system 3. Vibration signals connected to the control system 4. Remote start/stop 5. “First out” alarm 6. Implement auto load/auto start 7. Imminent start warning (local flashing light or horn) 8. Major oil spill 9. Oil demister running indication 10. Automated cooler drain valves 11. TV camera surveillance 12. Mixing of cooling water and oil 13. Mixing of water and gas (for oxygen and nitrogen) 14. Fire or smoke detection system	1. Improved visibility at the ROC 2. Improved visibility at the ROC 3. Improved visibility at the ROC 4. Consider the aspects when not being able to remote stop 5. Easier troubleshooting 6. Easier handling 7. Personnel safety, see **Error! Reference source not found.** and **Error! Reference source not found.** 8. Environmental – oil level switch, oil trap switch, locked wells, etc. 9. Environmental – oil leakage in the machine hall 10. Reduced energy consumption 11. Improved visibility at the ROC 12. Control environmental impact 13. Process protection 14. See 5.3
4	Oxygen compressor - additional considerations	Minimum instrument level for oxygen compressors, see AIGA 048, *Reciprocating Compressors for Oxygen Service* and AIGA 071, *Centrifugal Compressors for Oxygen Service* [14, 15]	-

No	Item	Considerations	Comments/Recommendations
5	Precooling (direct cooler, evaporative cooler, chiller)	1. Level indication and alarm / trip on water separator pots and dP over the direct contact aftercooler (DCAC) demister 2. Ability to open separator pot drains 3. Ability to remote start secondary pumps 4. Combining any chiller PLC control to the overall plant control system	1. Improved reliability, visibility at the ROC 2. Improved, reliability controllability at the ROC 3. Improved controllability at the ROC 4. Improved controllability at the ROC
6	Pre purification (reversing heat exchangers [REVEX], pre-purification unit [PPU]/ molecular sieve adsorber [MSA], adsorbers, regen system)	1. Air inlet temperature to purification unit to control system 2. Ability for remote step advance 3. Regeneration flow, temperature, and humidity (steam heater) 4. Regeneration gas outlet temperature to the control system 5. Air temperature, moisture, and carbon dioxide to control system 6. Automate midpoint temp control on REVEX	1. To avoid excess moisture 2. Improved capability at the ROC 3. Guarantee regeneration of the PPUs. 4. Guarantee regeneration of the PPUs. 5. To avoid contamination of the plant 6. To avoid contamination of the plant and improve efficiency
7	Coldbox/main column	1. Leaks into coldbox enclosure 2. Process indications 3. Automate any manual valves needed for liquid drainage 4. Need for automating process liquid pumps (including seal gas system) 5. Areas with potential for liquid oxygen boiling to dryness 6. Warm-end piping embrittlement protection	1. Coldbox enclosure pressure indicators and alarms output in the control system 2. Used for startup and major process upset 3. At plant trip and major process upset when liquid levels are too high or product quality excursions 4. To avoid long production outages 5. To avoid hydrocarbon build up in reboiler, liquid oxygen vaporiser, etc. Examples include hydrocarbon analysers, dP indicators, automatic reboiler low level trips, etc. 6. To automate trip to avoid piping failure
8	Storage and backup vaporisers (liquid pumps, high pressure buffer storage, pipelines)	1. Double block and bleed systems for all liquid flows to storage 2. Detection of liquid leaks. - Low temperature detection in the ground surrounding tanks and fill areas connected to control system - Low temperature detection on any liquid drain to atmosphere with alarm 3. Automation level required of the back-up pump and vaporiser system 4. Assess dependency on electricity, steam, and instrument air with specific reference to common modes of failure (for example, same source of power for back-up system and plant) 5. Risk of fog during atmospheric vaporisation 6. Adequacy of low temperature protection after vaporiser 7. Adequacy of pipeline purity protection (double block and bleed)	1. To ensure product quality in the storage tanks; bleed shall be safely disposed 2. See 5.4 3. Depending on the response time required by the customer 4. Depending on the required availability by customer 5. See 5.7.4 6. To avoid cold embrittlement. See AIGA 027 [8] 7. To guarantee the customer supply
9	Argon purification (cryogenic and hydrogen-based)	1. Need of automating process liquid pumps (including seal gas system) 2. Double block and bleed for hydrogen to the warm argon system 3. Ammonia and hydrogen leak detection 4. Automation level of the argon compressor(s)	1. To avoid long production outages 2. The block and bleed is for shut-down situations 3. See 5.3 4. To avoid long production outages or process upsets

No	Item	Considerations	Comments/Recommendations
10	Electrical system (high voltage [HV], medium voltage [MV], low voltage [LV] and motors)	1. How voltage disturbances or other power supply issues can be eliminated or minimised for auxiliary equipment shutdowns 2. Switch gear alarms needed to the control system 3. Fire alarm system 4. Redundant power supply for critical equipment for example, backup system, control system ups, oil pumps, lights etc.	1. To avoid long production outages and the need for local reset 2. Improved visibility at the ROC 3. See **Error! Reference source not found.** 4. Improved reliability
11	Auxiliary equipment (boilers, diesel generators)	1. Automation level required	1. Improved visibility and controllability at the ROC
12	Cooling system (including water treatment)	1. Cooling water temp and flow to control system 2. Automation level required for example, - fan control - cooling water pump(s) auto start - water treatment including blowdown and chemicals - tower bypass valve - side stream filter(s) 3. TV camera surveillance to monitor ice build-up on tower	1. Improved visibility at the ROC 2. Improved reliability, visibility at the ROC 3. Improved reliability, visibility at the ROC
13	Control system (including instruments/ analysers)	1. Back-up redundancy plan for loss of communications (dial in over telephone, local operators, backup network, etc.) 2. Alarm prioritisation 3. Need of full or limited remote control functionality at the ROC 4. Need for remote reboot of control system 5. Integration of local control into control system 6. A first-out feature for the plant tripping system 7. Assessment of UPS capacity 8. Back-up instrument air/gas. Ensure that any additional hazards are covered when using instrument nitrogen 9. Analysis system for example, replacement of manual analysis, auto-calibration, calibration switch status, auto-range, range feedback, procedures for when and how often to calibrate etc.	1. See 5.8.3 2. See 5.8.4 3. Improved reliability, visibility at the ROC 4. Improved reliability at the ROC 5. Improved controllability at the ROC 6. Improved troubleshooting 7. Improved reliability at the ROC. Ensure event logging after power failure 8. Improved plant reliability 9. Improved reliability, visibility at the ROC. Also see 6.11
14	Liquid disposal system	1. Automation level of the waste disposal system 2. Detection of liquid leaks/overflow 3. TV camera surveillance to monitor operation 4. Risk of fog	1. See **Error! Reference source not found.** 2. See **Error! Reference source not found.** 3. Improved visibility at the ROC 4. See **Error! Reference source not found.**
15	Trailer filling system	1. Automation level on fill system 2. Detection of liquid leaks 3. Risk of storage tank filling by road tanker	1. See **Error! Reference source not found.** 2. See **Error! Reference source not found.** 3. See **Error! Reference source not found.**

No	Item	Considerations	Comments/<u>Recommendations</u>
16	Site security, fire protection, signage	1. Ensure fire monitoring systems are integrated to control system and third-party monitoring company 2. Buildings have adequate ventilation and/or ambient air analysis for oxygen enrichment/deficiency 3. TV camera surveillance to monitor site perimeter 4. Control of entrance gates 5. Lone worker system in place (man-down alarm and procedures) 6. Signs indicating machinery can be started remotely/automatically 7. Greater restriction on access to the site 8. Intrusion alarm system / service 9. Define and segregate unmanned or remotely operated plant area from other activities for example, - Parking and maintenance of vehicles - Cylinder filling station by for example, locked door, fencing, etc. 10. Plant network and communication system integrity and security	1. See **Error! Reference source not found.** 2. See **Error! Reference source not found.** 3. Improved visibility at the ROC 4. Improved controllability at the ROC 5. See **Error! Reference source not found.** 6. Personal safety, see 6.7 and 7.5 7. See 6.13 8. See 6.13 9. See 6.10 10. See 5.8.3