Safety System, Protective and Monitoring Devices

5 MW series

Document No.

Issue No.

Pages

Date of release

Author:

Checked by:

Approved by:

Revision history

Revision	Issue date	Summary	Affected pages
Draft	2014-01-05	First issue	
0	2014-03-20	Rotor lock description, CCTV, FPS	10, 14
1	2014-06-02	CCTV	10, 11

1. Scope

This document describes the design of the safety system, protective and monitoring devices of the wind turbine Hyosung HS13X according to the requirements of the Germanischer Lloyd guideline.

2. Normative references

The following standards and guidelines have been used for the design of the wind turbine Hyosung HS13X.

Germanischer Lloyd, “Guideline for the Certification of Wind Turbines”, edition 2012

IEC 60204-1:2005, Safety of machinery – Electrical equipment of machines – Part 1: General requirements

IEC 62061:2005, Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

ISO 13849-1:2006 + C1:2009, Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

ISO 13849-2:2012, Safety of machinery - Safety-related parts of control systems - Part 2: Validation

ISO 13850:2006, Safety of machinery - Emergency stop - Principles for design

3. Terms and definitions

If not indicated different the definitions given in the pre-mentioned standards apply.

Pitch system
System that turns (pitch) the rotor blades around their longitudinal axis

Yaw system
System that aligns the rotor axis to the wind direction

Safety system
System that in the event of a malfunction keeps the wind turbine in a safe condition

Protection function
Protection functions are functions of the control system and / or safety system ensuring that the wind turbine remains within the design limits

Safety function
The term “safety function” as used in ISO 13849-1covers the protection functions plus other possible functions providing safety for the maintenance personnel.

4. Symbols and abbreviated terms

WT	Wind turbine
CS	Control System, general monitoring tasks of defined parameter and recording functions of operation modes
SRP/CS	Safety-Related Part of a Control System
PL	Performance Level acc. to ISO 13849-1
CW	Clockwise
CCW	Counter clockwise
GL	Germanischer Lloyd

5. General description

The wind turbine is equipped with a control and safety system achieving a safe operation in the defined limits according to the specification of the load calculation.
The design of the control and safety system ensures minimal hazards to people and livestock as well as minimal potential damage to the wind turbine during operation and maintenance under normal and extreme external conditions defined in chapter 4.2 of the GL guideline 2012. The control and safety system itself is independent to the wind turbine (type) class but some parameters used in the control and safety system depend to the different wind turbine classes. The control and safety system ensures sure that the prerequisites for the load assumptions as per chapter 4 of the GL guideline 2012 are safely met with respect to the operating conditions of the wind turbine.
In the technical description basic information to the concept and structure of the wind turbine is given.
The wind turbine is designed for the production of electrical energy in automatic operation.
The design of the control and safety system is made with respect to chapter 2 of the GL guideline 2012.

6. Brake system

The wind turbine Hyosung HS13X is equipped with an aerodynamic brake system by turning the rotor blades into the feathered position stopping the wind turbine to the idling mode. The idling mode is reached even one of the three pitch systems is failing. The mechanical brake is able to full stop the rotor under all conditions up to the so called maintenance wind speed. In case of an emergency stop this brake is also activated.
Due to the high mass inertia of the rotor the stop time is limited not to harm structural integrity of the wind turbine.
This has to be considered in the risk analysis and the relating measures.

6.1. Power supply for braking systems

During normal operation of the wind turbine the pitch system is connected to the external power supply. If this power supply fails (grid loss, failure in power supply) the pitch system switches to the battery storage system which is independent for each pitch axis. The rotor blades are turned into the feathered position with a pitch rate of 3.5 °/s.
The rotor brakes 1 and 2 are operated with hydraulic pressure. Two separate identical hydraulic units control each brake. For each rotor brake an accumulator stores the energy including conservative safety margin needed for a brake procedure. If the rotor brake valve is engaged the rotor brake is released. A throttle between accumulator and rotor brake valve protects the valve against overflow.
The wind turbine is equipped with additional rotor park brakes on the rotor shaft to protect the gearbox from inappropriate operating conditions.

6.2. Energy storage for braking systems

The condition of the batteries of each pitch system is constantly monitored. At least a weekly back-up condition check is done. During the condition check the rotor blades are pitched to 70 ° blade angle from the feathered position and then the safety stop by using the batteries as power supply is activated. The voltage drop is measured. If this voltage falls below the defined limit the wind turbine will stay stopped / idling and

an error message is generated. If the pitch test cannot start from an idling status the rotor will be stopped first.
The function of the rotor brake is tested if the wind turbine is idling by applying the rotor brake and pitching the blades to e.g. 70 ° blade angle. No movement of the rotor is allowed. The accumulator for the rotor brake is monitored by a separate pressure sensor. If the pressure falls below a limit a warning message is generated. In this case it is not allowed to start any work like maintenance in the nacelle before the rotor lock is set or the fault has been corrected. In this case operation of the wind turbine with persons inside the wind turbine is strictly forbidden.

6.3. Torque-limiting components

The torque limiter as part of the high speed coupling is placed between rotor brake and generator. Thus braking torque to the rotor is not affected. The torque limiter protects the drive train against excessive torque peaks in case of generator short circuit. The torque limit is documented in the specification and / or the drawing of the coupling as part of the machinery components.

6.4. Rotor lock

The rotor locking system is situated in front of the main gearbox of the turbine. It provides 12 locking positions. The two locking cylinders are powered by two separate hydraulic units. Each hydraulic cylinder has an integrated position measurement system and further each cylinder has two limit switches so that the positions “locked” and “unlocked” can be monitored redundantly.
Automatic rotor lock on request

Involved Systems
• Length measurement systems at the hydraulic cylinders
• Hydraulic units
• Rotor brake
• Parking brake

Boundary conditions
The rotor lock is operated only upon request, no automatic activation by the control system takes place. Before activating the rotor locking procedure the lock disc holes shall be in front of the lock bolts. The position of the lock bolt shall be monitored by the length measurement system.

Description
In Service mode of the controller the procedure "Turn to specific condition" shall be activated. If the controller indicates that the set locking position has been reached the cylinder starts to move the lock bolt into the lock disc. During this operation the parking brake and the rotor brake shall remain closed. If the parking brake is not available, it is important to monitor the position of the lock disc to avoid collision of the locking cylinder with the side face of the disc. During the operation of the hydraulic cylinders their axial position shall be monitored in order to detect the position. In order to drive the lock bolt completely into the lock disc, it may be necessary to open the brakes, allowing the rotation of the lock disc. The unlocking process may be activated only, if at least two rotor blades are at 90° pitch angle. During this operation the parking brake and the rotor brake shall remain closed.

6.5. Pitch lock

The rotor hub has two positions to mount the pitch drive. As the pitch system is designed for one pitch drive per rotor blade, the second position is used for the blade

lock. The blade lock is a mechanical system, which consists of a locking pin which is engaged in the teeth of the blade bearing. The blade lock has an electrical switch which is connected to the pitch system so that the pitch will only be operated when the bolt is not engaged.

6.6. Yaw lock

The turbine does not have a yaw locking mechanism, due to the fact that six drive brakes provide 50% of the total brake power and the 15 hydraulic brakes provide the other 50% of the brake power. In case of repair works at one of the system, the yaw system can either be blocked with the drive brakes or with the hydraulic brakes. In addition, half of the hydraulic brakes are separated into two independent hydraulic units.

7. Safety system

The integral part of the safety system is the safety device Pilz PNOZ m1p, called WTP in the following, which is certified to relevant standards (ISO 13849-1 up to PL e respectively, IEC 62061 up to SIL 3).
For further information on the Pilz safety devices refer to the document “Pilz safety devices” in the annex.

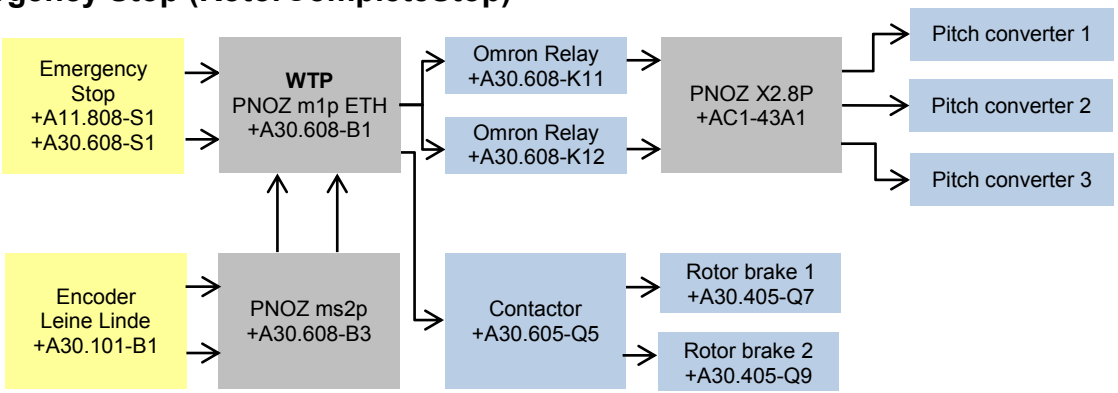
7.1. Protection functions

The protection functions of the safety system are:

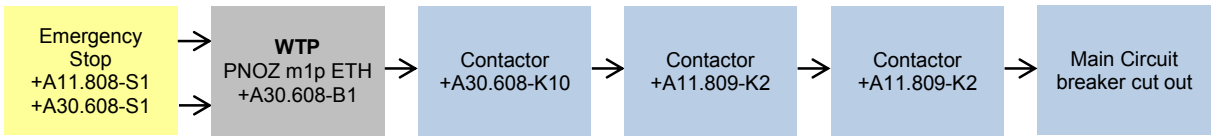
- Emergency stop
- Overspeed (activation speed n_A)
- Generator overload (activation power P_A)
- Short circuit in the electrical power system
- Excessive vibration (shock)
- Cable twisting
- Functioning of control system (Watchdog)

The safety functions according to ISO 13849-1 are part of a risk assessment.
Here just the ones relating to the above mentioned protection functions of the safety system are listed as block diagrams.
The reference designations (+A11 and +A30 kk-electronic, +AC1 SSB) can be followed up in the circuit diagrams listed in the annex.

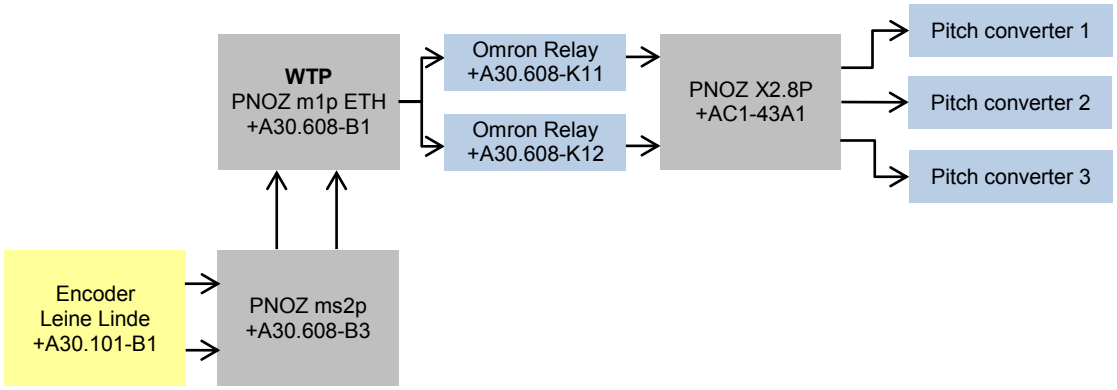
Emergency Stop (RotorCompleteStop)



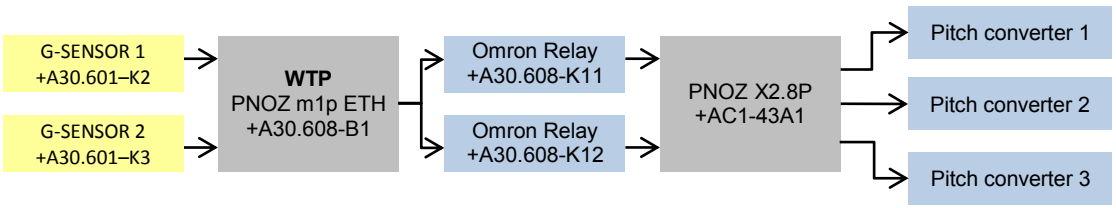
Emergency Stop (SafePowerOff)



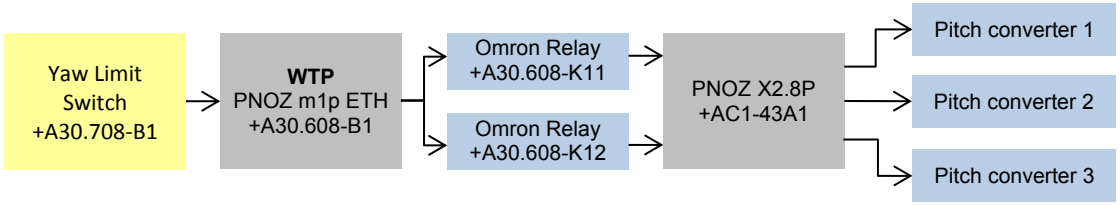
Excessive Rotor Speed



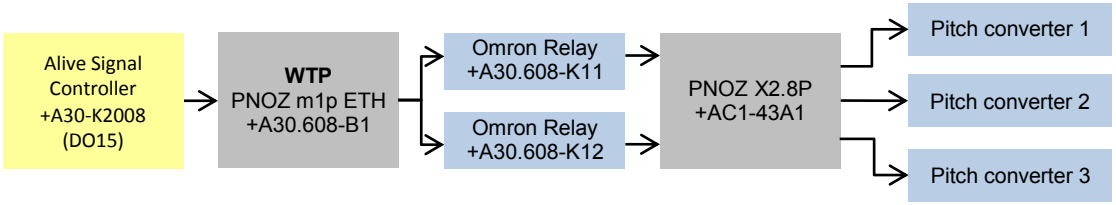
Excessive Shock



Excessive Cable Twist



Functioning of Control System



7.2. Performance level

The required performance level for the most critical safety functions overspeed and emergency stop have been determined by the risk assessment to “d”. Thus the architecture has to be a category 3 one. Category 3 SRP/CS must apply well-tried safety principles and be designed such that a single fault does not result in loss of the safety function.
For further safety functions the required performance level has been determined to “c”. For this performance level the category has to be minimum 1. Category 1 SRP/CS must be designed and constructed with the use of components and

principles which are well-tried for safety-related applications. The incidence of a fault may lead to loss of the safety function.

7.3. Fault consideration

The faults and possible fault exclusions which are to be assumed for mechanical, hydraulic and electrical components during the validation of SRP/CS can be found in fault lists in EN ISO 13849-2:2012.
Without the assumption of fault exclusions, some safe control systems would not be achievable at reasonable expense. Reasons for fault exclusion include, in particular, the physical impossibility of a certain type of fault or the technical improbability of a fault, and also good engineering practice (see also Section 7.3 of EN ISO 13849-1). EN ISO 13849-2 describes possible fault exclusions for certain discrete components, where considered permissible.

Basic safety principles have been considered in the design of the wind turbine.

Applicable to all technologies these are:

- Use of suitable materials and manufacturing processes
  Materials and processes for manufacture and treatment are selected with consideration for the use and stresses.
- Proper dimensioning and geometry of all components
  All components are selected in consideration of their compatibility with the anticipated operating conditions. Further criteria include switching capacity, switching frequency, electric strength, pressure level, dynamic pressure behaviour, volumetric flow, temperature and viscosity of the hydraulic fluid, type and condition of the hydraulic fluid.
- All components are resistant to the environmental conditions and relevant external influences.
  The SRP/CS is designed such that it can perform its functions under the external influences which are usual for the application. Important criteria include mechanical influences, climatic influences, the degree of sealing of the enclosure, and the resistance to electromagnetic interference.
- Principle of de-energization (closed-circuit current principle)
  The safe state is attained by removal of the control signal (voltage, pressure), i.e. by de-energization. Important criteria include the safe state when the energy supply is interrupted, or effective spring resetting on valves in fluid power technology.
- Protection against unexpected start-up
  Unexpected start-up, caused for example by stored energy or upon restoration of the power supply, is avoided.

Applicable to fluid power technology these are:

- Pressure limitation
  The pressure within a system or in subsystems is generally prevented from rising beyond a specified level by one or more pressure-relief valve(s).
- Measures for the avoidance of impurities in the pressure medium
  The required purity grade of the pressure medium for the components used is attained by a suitable facility, generally a filter.

Applicable to electrical technology these are:

- Proper connection of the protective earth conductor

One side of the control circuit, one terminal of each electromagnetically actuated device or one terminal of other electrical devices is connected to a protective earth conductor. This side of the device is not therefore used for example for deactivation of a hazardous movement. A short-circuit to ground cannot therefore result in (undetected) failure of a de-energization path.

- Suppression of voltage spikes
  A facility for the suppression of voltage spikes (RC element, diode, varistor) is connected in parallel with the load (not in parallel with the contacts).

Well-tried safety principles are employed in order to minimize or exclude critical faults or failures and thus to reduce the probability of faults or failures which influence the safety function.

Applicable to all technologies these are:

- Over-dimensioning/safety factor
  All equipment is subjected to loading below its rated values. The objective is to reduce the probability of failure.
- Positive actuation
  Reliable actuation by rigid mechanical parts with positive rather than sprung connections. The objective is to attain reliable transmission of commands, for example by the direct opening of a contact when a position switch is actuated, even should the contact be welded.
- Limiting of electrical and/or mechanical parameters
  Force, distance, time, and rotational and linear speeds are reduced to permissible values by electrical, mechanical or fluid power equipment. The objective is to reduce the risk by means of an improved hazard control.

Applicable to fluid power technology these are:

- The use of well-tried springs
  EN ISO 13849-2, Table A.2 contains detailed requirements for well-tried springs.

Applicable to electrical technology these are:

- Limiting of electrical parameters
  Limiting of voltage, current, energy or frequency, for the avoidance of an unsafe state.
- Avoidance of undefined states
  Undefined states in the SRP/CS must be avoided. The SRP/CS must be designed such that its state can be predetermined during normal operation and under all anticipated operating conditions. This is to be achieved for example by the use of components with defined response behaviour (switching thresholds, hysteresis) and with a defined sequence of operations.
- Separation of non-safety and safety functions
  In order to prevent unanticipated influences upon safety functions, the functions concerned are implemented separately from non-safety functions.

Well-tried components for mechanical and electrical systems are dealt with by Tables A.3 and D.4 of the informative annexes of EN ISO 13849-2. Well-tried components are used in order to minimize or exclude critical faults or failures and thus to reduce the probability of faults or failures which impact upon the safety function. In accordance with the provisions for Category 1, general criteria for a well-tried component are that it:

a. has been widely used in the past with success in similar applications; or
b. has been manufactured and verified with the application of principles which indicate its suitability and reliability for safety-related applications.

Applicable to fluid power technology these are:
EN ISO 13849-2 states no well-tried components for fluid power technology. Examples of well-tried components in a safety context are:

- Directional control valves, stop valves and pressure valves

Applicable to electrical technology these are:

- Fuse/miniature circuit-breaker
  Fuses and miniature circuit-breakers are facilities for overcurrent protection which interrupt an electrical circuit in the event of an excessively high current, caused for example by an insulation fault (principle of de-energization). Fuses and miniature circuit-breakers have for decades provided effective protection against overcurrents. Comprehensive provisions exist governing fuses and miniature circuit-breakers. Provided they are used as intended and are correctly rated, failure of fuses and miniature circuit-breakers can virtually be excluded.
- Emergency off device/emergency stop device
  Devices for emergency switching off and emergency stop in accordance with EN ISO 13850 are employed for the initiation of action in an emergency. Both types of device feature auxiliary switches with direct opening action for interruption of the energy supply in accordance with Annex K of IEC 60947-5-1.
- Switches with positive mode of actuation (direct-opening)
  This particular type of switch is available commercially as a pushbutton, position switch, and selector switch with cam actuation, for example for the selection of operating modes. These switches have proved effective over many decades. They are based upon the well-tried safety principle of the positive mode of actuation by direct opening contacts. As a well-tried component, the switch must satisfy the requirements of IEC 60947-5-1, Annex K.
- Further non-complex and non-programmable components, owing to their failure modes being predictable. Examples are passive components, resistors, diodes, transistors, thyristors, operational amplifiers and voltage regulators.

Details about fault consideration can be followed up in a list (see annex).

For further information on safety devices refer to the documents listed in the annex.

7.4. Clearance

In case of activation of a protection function the wind turbine needs clearance by human intervention. Clearance is only permitted to qualified and authorized personnel.
For onshore installation sites personnel performing the clearance need to be on site at the turbine. Personnel have to execute necessary repair or eliminate the cause of a malfunction before the wind turbine is released for operation.
For offshore sites clearance may performed from the remote control centre, if the following prerequisites are met:

- The outside of the turbine is inspected from a distance before performing the clearance, to make sure that the main components are in place and appear to be undamaged. This inspection may be conducted e.g. from a neighbouring turbine or by use of monitoring cameras.

- The inside of the nacelle is inspected after the clearance and during the start-up procedure, to make sure that the main components are in place and undamaged. This inspection may be conducted by using monitoring camera(s).
- The number of allowable remote clearances of the safety system is limited to 3 times within 24 hours and as a total for the same failure.

After the case of grid loss the wind turbine controller will engage the safety system automatically if no critical error is present in the error stack of the wind turbine controller.

8. Control system

8.1. WTC

The control system is based on programmable logic controller MPC 240 of the company Bachmann.

The basic control functions are:

- Power
- Rotor speed
- Wind direction
- Wind speed
- Operation mode
- Grid condition
- Cable twist
- Temperatures
- Ice sensor

The pitch control algorithm is described in the safety and control scheme (see annex) in chapter 4.3.
The modes of operation are described in the safety and control scheme (see annex) in chapter 2
The control logic flow charts are given in the following figures.

8.2. CCTV

Several cameras are installed in the wind turbine to have remote supervision of the wind turbine condition in case of remote clearance.
According to the GL guideline chapter 2.2.2.5 Clearance sufficiently qualified personnel (well trained and authorized by the wind turbine manufacturer) performing the clearance need not necessarily be on site at the turbine, but may perform the clearance from the remote control centre. For this purpose monitoring cameras are used inside and outside the wind turbine.

Outside wind turbine: three cameras with Pan/Tilt/Zoom function are installed outside of the nacelle cover to have an overview of the main components c.a. rotors with blades and towers, offshore foundations. The first camera is located on the rear top of the nacelle cover, the second one on the front bottom and the third one on the rear bottom. Alternatively if no outside cameras are available the outside of the turbine is to be inspected from a distance before performing the clearance, to make sure that the main components are in place and appear to be undamaged. This inspection may be conducted e.g. from a neighbouring turbine.

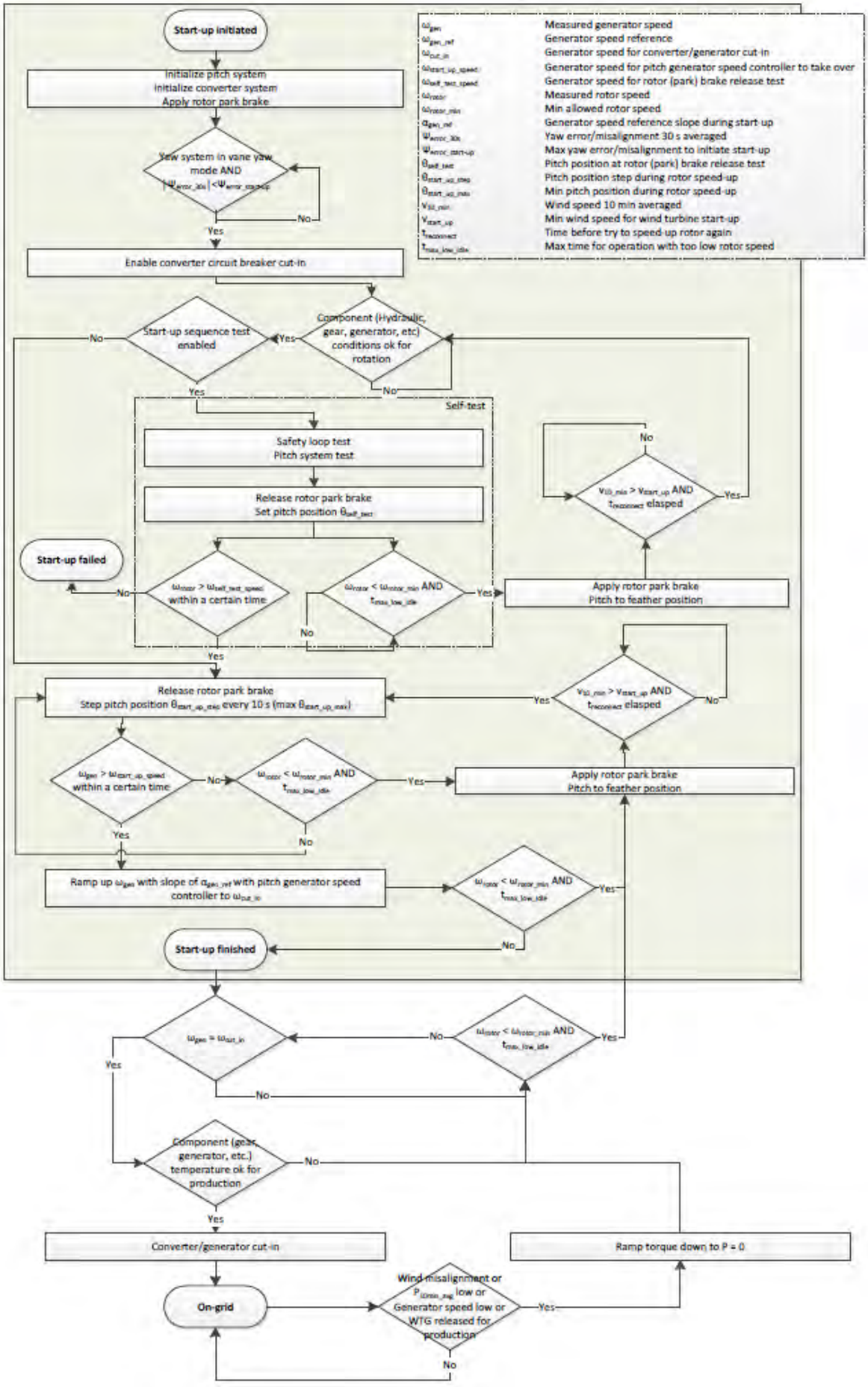
The inside of the nacelle is to be inspected after the clearance and during the start-up procedure, to make sure that the main components are in place and undamaged.

Inside nacelle: A camera with Pan/Tilt/ Zoom function is installed under the roof of nacelle to have an overview of the various zones in the nacelle which include mechanical brake, converter, transformer and control switch cabinet zone.

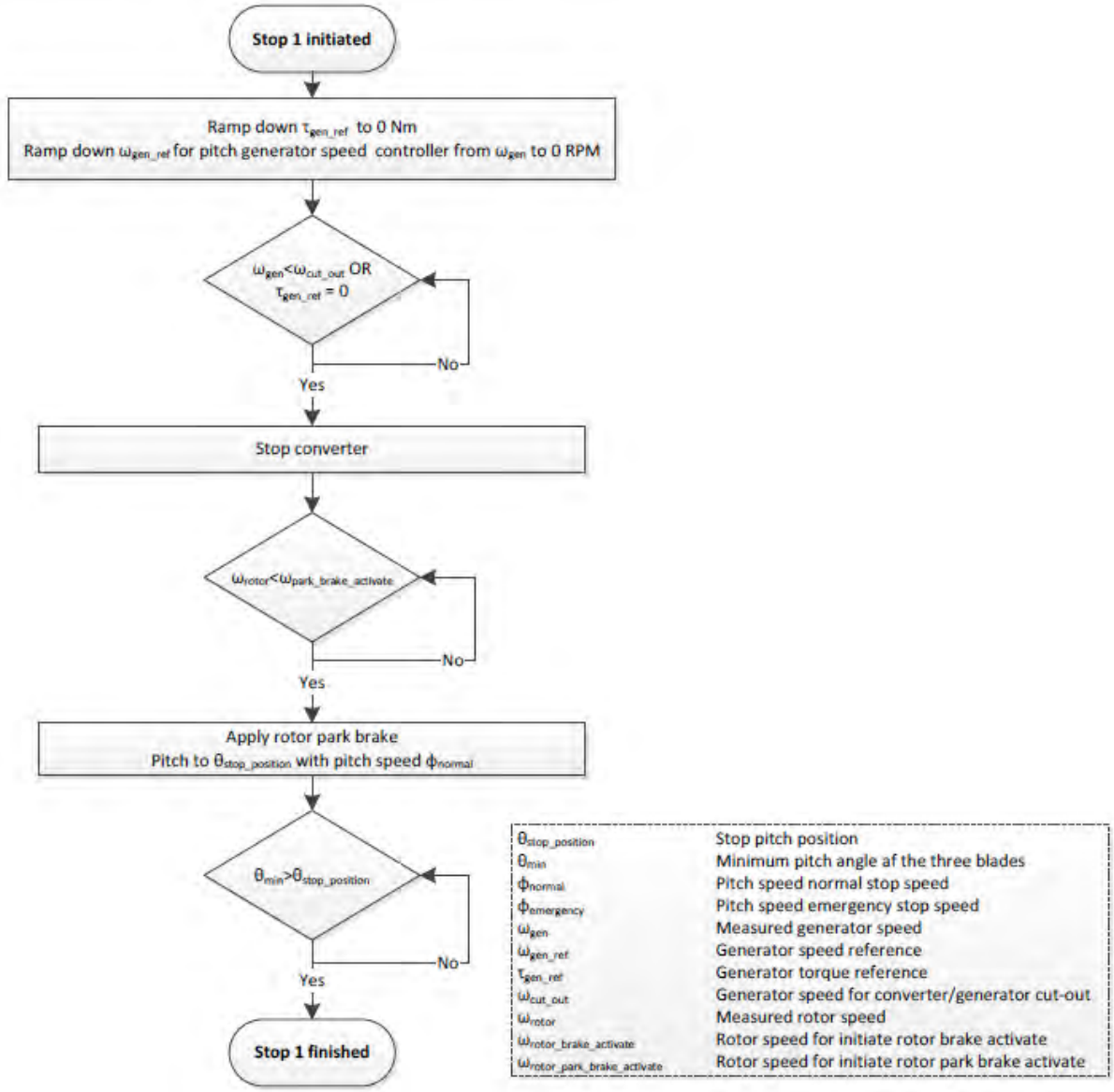
Inside tower: The CCTV design includes the tower area. The first of the three cameras is placed to confirm to the entry of service personnel in bottom tower. The second and third camera are also installed in order to confirm that the service personnel enters into and come out of the service lift in both bottom and top tower.
Please refer for details to the documentation noted under chapter 10.

8.3. FPS

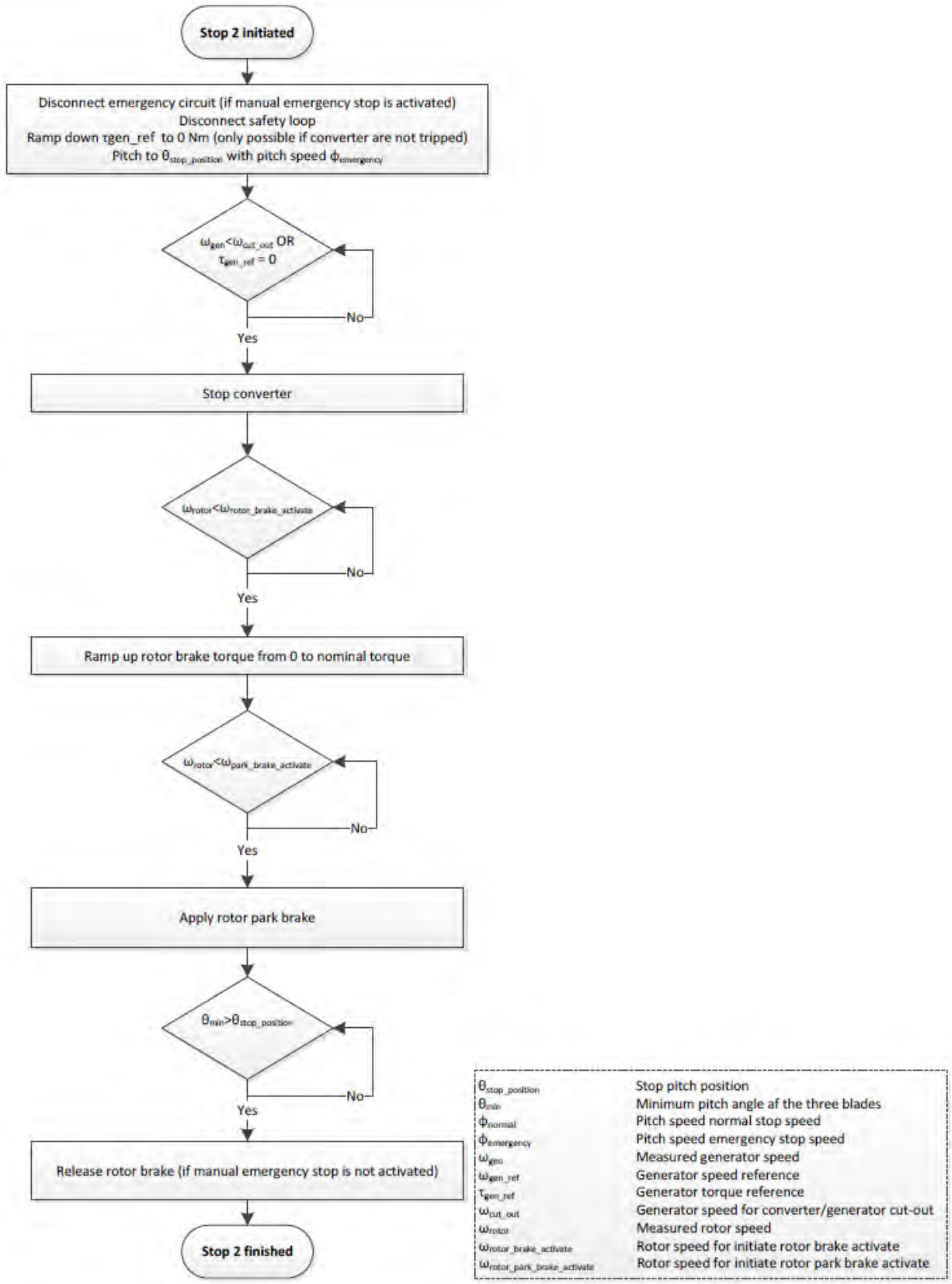
A fire protection system is installed in the wind turbine to prevent damage by fire.
Please refer for details to the documentation of the manufacturer FUNA and the assembly drawing noted under chapter 10.



Start-up sequence flow chart



Stop sequence 1 flow chart



Stop sequence 2 flow chart

Limits and set points are defined in the data sheet (see annex).
Turbine data relevant to load assessment are documented in “TDrLA_Hyousung_HS13X” (see annex).

9. Monitoring

Where the control system is acting directly in relation to parameters the monitoring is supervising processes by sophisticated procedures for plausibility and failures. Only the important ones are described here. Further ones are implemented using similar systematic procedures.

- **Rotational speed**
  The different rotational speed signals on the high speed and low speed shaft are checked against each other considering the gear box ratio. In case of a deviation the wind turbine is stopped.
- **Wind speed**
  The sensors for wind speed are checked against each other. The figures are compared to calculated values out of rotor speed, power and blade angle. In case of mismatch an alarm is generated. Even both wind speed sensors show faulty signals it is not necessary to the stop the wind turbine because the wind speed is taken from the calculated result generated by rotor speed, power and blade angle. An automatic restart is not possible in this case.
- **Wind direction**
  The wind vanes are checked for plausibility against each other by the control system. If both sensors are recognized as defect the wind turbine is stopped. Wind vanes are giving a dynamic signal for wind speeds above appr. 5 m/s. In case of static signals the wind vane is defect. If one sensor is defect the signal of the remaining one is used.

Additional information is given in the document safety and control scheme (see annex) in chapter 4.

10. Reference documents

a) Safety and control scheme V-18.33-BF.00.00.00-A, aerodyn Energiesysteme GmbH

b) Data Sheet D-18.33-00.00.00.01-A, aerodyn Energiesysteme GmbH

c) Load assessment relevant data “TDrLA_Hyosung_HS13X, Hyosung Corporation

d) Control and safety devices; CS-Devices; Hyosung Corporation

e) Electric circuit diagram HYO0500A11001, kk-electronic

f) Electric circuit diagram HYO0500A30001, kk-electronic

g) Hydraulic circuit diagram 3671862, Hydac

h) Documentation Pilz safety devices

i) Documentation data sheets control and safety devices

j) Operational manual M050041, Hyosung Corporation

k) Commissioning procedure M050042, Hyosung Corporation

l) Maintenance manual A-18.33-00.45.00.00-A, aerodyn

m) HYOSUNG Camera principle drawing

n) C3005151_01_Assembly Fire Protection System