ABB Safety

Safeguard 400 Series
Product Guide

August, 2000

Use of **DANGER**, **WARNING**, **CAUTION**, and **NOTE**

This publication includes, **DANGER**, **WARNING**, **CAUTION**, and **NOTE** information where appropriate to point out safety related or other important information.

DANGER Hazards which could result in severe personal injury or death

WARNING Hazards which could result in personal injury

CAUTION Hazards which could result in equipment or property damage

NOTE Alerts user to pertinent facts and conditions

Although **DANGER** and **WARNING** hazards are related to personal injury, and **CAUTION** hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, comply fully with all **DANGER**, **WARNING**, and **CAUTION** notices.

TRADEMARKS

Advant, AdvaCommand, AdvaInform, and AdvaBuild are registered trademarks of ABB Asea Brown Boveri Ltd. Switzerland.

Safeguard 400 Series is a trademark of ABB Industri AS, Norway.

NOTICE

The information in this document is subject to change without notice and should not be construed as a commitment by ABB Industri AS. ABB Industri AS assumes no responsibility for any errors that may appear in this document.

In no event shall ABB Industri AS be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB Industri AS be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without ABB Industri AS's written permission, and the contents thereof must not be imparted to a third party nor be used for any unauthorized purpose.

The software described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

CE MARKING

This product meets the requirements specified in EMC Directive 89/336/EEC and in Low Voltage Directive 72/23/EEC.

3BSE001264/D

Template: 3BSE001286/E

3BNP000431R301

TABLE OF CONTENTS

Chapter 1 - Introduction

Chapter 2 - Software Functions

Chapter 3 - Hardware Functions

Chapter 4 - Product Configuration and Documentation

ILLUSTRATIONS

TABLES

Chapter 1 Introduction

1.1 Overview

This Product Guide describes Safeguard 400 Series, controllers designed to monitor and control safety aspects of an industrial plant. Safeguard 400 Series is derived from standard ABB control products, which have been expanded, enhanced and configured to offer the necessary safety functions. Hardware and software have been added, and configurations have been changed.

This Product Guide describes the Safeguard system, what it consists of, how it works in general, and what software tools that are included in the portfolio.

1.2 General information

Many modern processing industries present hazards which pose major risks for workers, machinery and the environment. At the same time, ever increasing demands are being made on productivity and quality. These developments have led to more complex, more sophisticated production systems, which in turn generate more process-related critical situations than ever before.

Although the automation system in itself represents a high level of security, there is still a need for superior safety systems exclusively dedicated to further reducing risks, and minimizing the effects if something should go wrong. These safety systems have two major tasks:

- Preventing the process from entering an unsafe state
- Re-establishing a safe state of the plant, or reduce the consequences and protect personnel, if the process for any reason has reached an unsafe state (e.g. gas leaks caused by pipe rupture).

An additional task is to protect vital and expensive process equipment

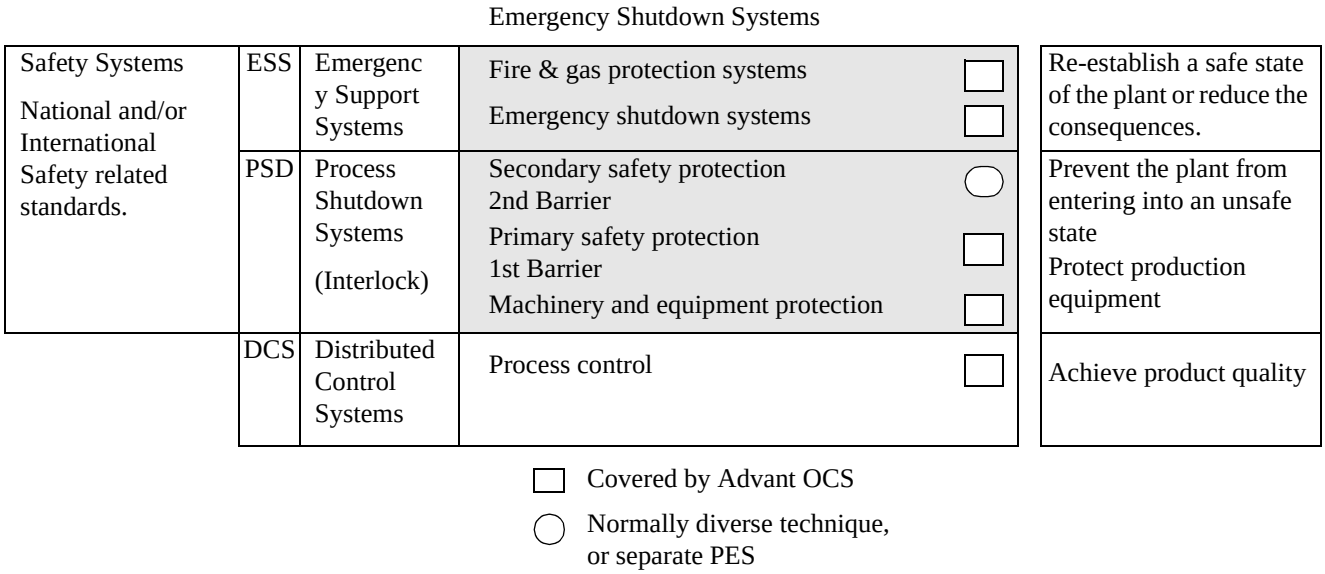

Figure 1-1. Structure and tasks of a safety system

Safeguard is a fault-tolerant safety system especially designed for the protection of industrial processes. Based on ABB's family of micro-computer based controllers and networks, it offers high reliability control and supervision in process applications such as Emergency Shutdown (ESD), Process Shutdown (PSD), Equipment Protection, Critical Control and Fire & Gas Protection (F&G) systems.

Important characteristics of this system are:

Safety and reliability

Safeguard 400 Series is based on Advant Controller 410 and is extended with software and hardware for handling safety signals, test, monitoring and advanced diagnostics. It adds an advanced output voting unit called Master Vote 3000. A single failure in the system will not prevent a pre-defined safety action from being executed.

Availability and fault tolerance

A combination of output voting, testing and monitoring detects and isolates faulty components in the system. Safeguard offers fault tolerance for critical single faults, and fail-to-safe action for multiple faults. This ensures high availability through error-free, uninterrupted process operation, while preserving a high reliability in safety operations.

Connectivity

The Safeguard system can be connected to virtually any control system on the market, and may use the same network to freely communicate with process, operator and engineering stations if so desired. This, in some cases, allows full integration of operator presentation, alarm handling, maintenance and information exchange between process control and safety applications.

Safeguard can easily be connected to:

- ABBs control systems w/ Master Software
- ABBs control systems w/ MOD Software
- ABB Bailey Products
- Former Alfa-Laval Automation Products
- Other DCS-vendors Products

Safeguard supports restricted access functions, offering password protection for safety application programs, key-lock restrictions for user-specified operator functions, and restricted access to database information.

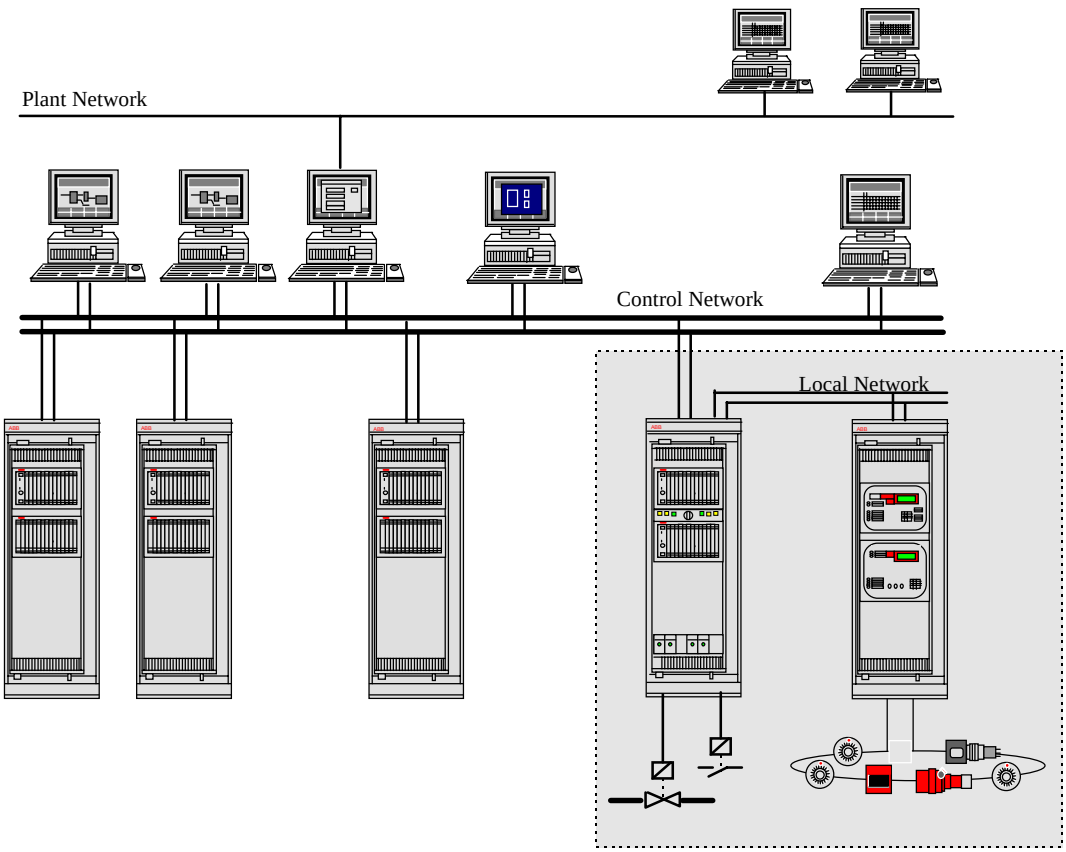

Figure 1-2. Integrated process control and safety system

Engineering efficiency

Reduced engineering time, increased efficiency and enhanced integrity of safety application programming are just three of the advantages of AdvaBuild, a series of engineering tools especially developed by ABB.

Safeguard 400 Series includes a highly versatile cause and effect schematic based configuration tool called Safety Builder. This configuration tool significantly reduces the time used and potential errors involved in converting the industry standard documentation to logic program representation and thereby increases the quality.

Safeguard 400 Series design criteria

Safeguard 400 Series is certified by TÜV Product Service (refer to Section 1.6, Certification) according to Requirement Class 1-6, and Safety Integrity Level (SIL) 1-3 as defined in DIN V VDE 0801, DIN V 19250 and IEC 61508. Safeguard 400 Series is also designed according to relevant chapters of DIN VDE 0116 and EN 298, which relates to burner management systems, and EN 54, which relates to Fire and Gas Protection.

1.3 Safeguard design concept

The Safeguard 400 Series is a system based on Refined Duplex Architecture (RDA). The architecture utilizes a refined version of the standard Advant Controller 410 from the Advant OCS product platform. The idea of offering a safety system with high safety integrity combined with a generic ability to be easily integrated into modern control systems, is a core strategy in ABB safety system product development.

Recognized architecture

The Safeguard 400 Series complies with the design standard 1oo2D (one out of two) and 1oo1D (one out of one), two of the designated architectures for safety systems defined by the IEC 61508, the international standard for functional safety. One main property of this architecture is to detect and localize potential failures by means of active self-testing.

For the 1oo2D it combines the safety factor of the 1oo2 architecture with the availability factor of the 2oo2 architecture. When comparing different generic control structures, the potential advantage of this architecture regarding safety/availability trade-off can be proved.

For the 1oo1D it combines the safety factor of the 1oo2 architecture for the safety outputs with the availability factor of the 1oo1 architecture for the system. This gives a system with a comparable safety to the 1oo2D system.

The main difference between a 1oo2D system and a 1oo1D system:

- 1oo2D has two independent controller branches for processing and diagnostics of the signals.
- 1oo1D has one controller branch for processing and diagnostics of the signals.

Safeguard 400 Series

The Safeguard 400 Series consist of the two product variants; Safeguard 410 and Safeguard 415. The difference between these two variants are described below. Description contained in all other parts of this manual are common for both variants unless otherwise specified.

The hardware for Safeguard 400 Series consists of processor module, sub-modules, sub-racks, and power supplies.

Common characteristics:

The processor module used is PM150V08 and has the following characteristics:

- The CPU board contains a Motorola MC68020 processor and dynamic read/write memory (RAM) with ECC (Error Correction Circuit). The memory houses the system software as well as the user application. The CPU board is delivered with PM150V08 which is a 8 MB dynamic read/write memory version.
- One slot for flash memory Program Card holding the safety system software.
- Two RS-232-C ports dedicated for printer and MasterView 320
- One port dedicated for connection of Advant Station 100 Series Engineering Stations
- Four slots for communication sub-modules, two slots are configured with MB300 interface.
- Direct access to Fireguard and Autronica addressable detector systems connected via the communication sub-module slots.

Safeguard 410

The safety system consists of one central S100 I/O rack where the CPU-module and the I/O boards are located.

- Direct access to up to 15 S100 I/O boards.

Safeguard 415

The safety system consists of one central S100 I/O rack where the CPU-module and I/O boards are located plus up to two additional S100 I/O sub-racks where I/O boards are located

- Direct access to up to 54 S100 boards.

Single Safeguard

This is the product variant with only one controller. These are called Safeguard 410 Single and Safeguard 415 Single. The hardware and functions described in this manual are valid for both variants with the exceptions described in Appendix A of the Safety Manual (3BNP000432R301).

Isolation of failures

If a critical failure is detected in one of the safety control branches, the process will continue, uninterrupted. The failure will be isolated upon detection, thus preventing spurious trips.

Safeguard 400 Series will then operate as a 1oo1D (single) system. Alarm messages and detailed diagnostic information will be presented to the operator so that the fault can be repaired quickly.

Fail-safe action

In the very rare case where critical failures are detected in both safety controller branches, a partial or complete fail-to-safe action is initiated. The fail-safe function in the RDA is to de-energize the field devices connected as critical outputs to the Master Vote 3000 termination units in the Safeguard 400 Series. In this way ABB Safety fully maintains the philosophy of fail-safe shut down control.

1.4 Applications

As indicated in Figure 1-1, there is no exact border between safety systems and process control systems regarding safety application functions (e.i. equipment protection can be performed in both PSD and DCS). The safety system is normally considered to be a shutdown system taking action when the process goes outside the safe operating range. This may be due to an event in the process equipment itself, such as a pipe rupture, a stuck valve, or detection of fire or gas in the plant. Equally critical are abnormal process conditions arising from loss of control (for example reaction runaway) or failure in the process control system itself.

Further, the safety and process control systems must interact during recovery from a trip (safety action) or at normal process start-up. As the process is outside the normal state for a long interval, the normal cause-effect actions should not be taken. However, to simply bypass these safety actions during start-up poses serious safety risks at a time when the process state is normally very unstable. Therefore, the process control and safety systems must communicate to ensure that safety mechanisms are being applied during the various phases of plant start-up. This is one main argument for an integrated system design.

The safety systems can be divided into two main application areas:

1. Process safeguarding:
    a. **PSD** (Process Shut Down) system
    b. Equipment Protection
    c. Critical Control.
2. Plant/Area safeguarding and personnel safety:
    a. **ESD (**Emergency Shut Down) system
    b. **F&G (**Fire and Gas) Detection and Protection system.

1.4.1 Process safeguarding

Safeguard 400 Series includes hardware and software constructed to assist in the design of safety system structures that meet industry regulations for such systems. A large number of pre-defined application solutions for commonly used process transmitters, detectors and actuators are defined as function block macros.

Process Shutdown

The purpose of a PSD (Process Shutdown) system is to prevent the development of an abnormal process condition into an undesirable event (emergency). The PSD safety system goes into action when the process control system, DCS, is no longer able to control the process in a safe manner. This may be a result of faults in the process equipment, instrumentation or computer hardware, or caused by unwanted control program actions (for example from an erroneous set-point) with process instability as a result. Generally the action is to section off the process, to prevent the situation from spreading, and for example cool/de-pressurize the process to achieve thermodynamic stability.

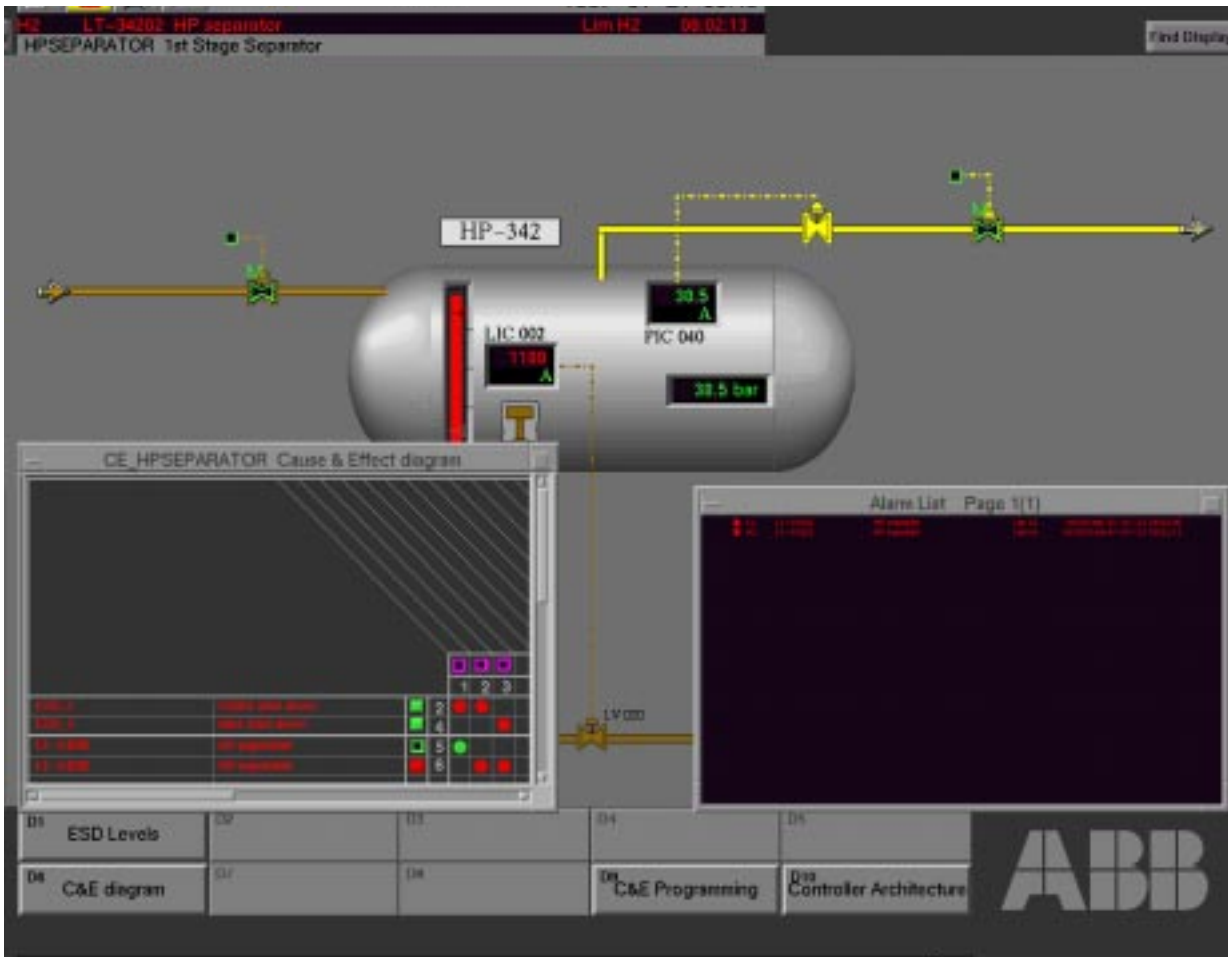

Figure 1-3. Operator Station presentation of an ESD application

Equipment Protection

This is related to single equipment protection and will in many cases be part of the process control system but with its own outputs for shutdown purposes. This could be monitoring of control equipment, as well as vulnerable, investment-intensive production equipment. For example, all types of rotating machinery - turbines, generators and compressors

Critical Control

Safeguard also supports safety applications with critical control functions, e.g.critical valve control on a pipe line. This enables application solution for implementing analog outputs and PIDCON (predefined function block for PID control in the ABB Masterpiece language, AMPL) in a dual system.

1.4.2 Plant/Area safeguarding and personnel safety

Emergency Shutdown

The **ESD** (Emergency Shutdown) system comes into action when the situation has developed into an emergency. The purpose of the system is to limit the consequences of the uncontrolled state, contribute to evacuation and emergency blow-down actions, and to re-establish safe operation.

Fire and gas detection and protection

The purpose of the F&G system is to detect a fire and/or gas situation at an early stage, fight the fire and limit the gas leakage by de-pressurization, process section shutdown and closing of ventilation (dampers). Personnel warnings such as beacons, horns and messages (PA system) may be activated to initiate evacuation of the area.

In addition to flammable compounds, detection includes other gases and fluids, for example toxic and corrosive substances that may cause personnel or environmental hazard.

Safeguard 400 Series include hardware and software solutions to support all commonly used detectors and fire fighting equipment. Some examples are heat, flame and smoke fire detectors, optical and electro-catalytic gas detection, and CO2, halon or water based extinguishing systems.

Safeguard 400 Series can be configured with both conventional or/and addressable fire and gas detectors.

1.4.3 Application implementation

There are two methods for realization of safety system logic within Safeguard.

- **AMPL** (ABB Master Programming Language)
- **Safety Builder** (Cause & Effect tool).

The two methods can be combined in a system for optimal solutions.

1.4.3.1 AMPL

AMPL is the standard function-block/Process Control (PC)-elements language with graphic representation used for application programs in both Safeguard and ABB OCS. See also Section 2.4, Engineering Software for AS 100 Series ES for enhanced use of AMPL as Type Circuits or/and Circuits in the Advant Station 100 Engineering Station.

User elements

User Defined PC elements is an optional function which when installed enables the user to create typical application solutions (based upon the AMPL) as user defined function blocks. These function blocks will be handled like a standard AMPL function block element in the safety controller. The UDPC function is a software module which enables you to simplify implementation and documentation of frequently used safety and control solutions and adapt them to your own requirements. It is possible to design and combine a number of user elements into libraries which can be downloaded into the controller. These libraries can be modified by adding new elements to existing libraries, or by creating new libraries when required.

1.4.3.2 Safety Builder

Safety Builder is a software package used to configure, verify and document Cause and Effect (C&E) matrices and is especially suitable for safety shutdown and -protection related applications.

The application interacts with the signal database where the inputs (causes) and outputs (effects) of the process in question are defined. The database includes signal specific information such as signal names and descriptions, input alarm levels, alarm delays etc. The inputs and outputs are entered into a C&E matrix. Corresponding interaction is plotted in relevant cells.

Safety Builder supports shut-down level (ESD level) definition. An ESD level is a defined action on a fixed set of outputs. Associating an input with a defined ESD level, ensures a structured shutdown philosophy and the predetermined action for the cause in question is performed.

Larger installations often integrate several safety systems along with other ABB controllers. Safety Builder supports routines enabling a subscription to inputs and ESD levels defined in integrated, remote systems. The remote inputs can be assigned action in the controller in question.

1.5 Theory of operation

1.5.1 Dual controller structure

The 1oo2D system has an architecture that consists of two parallel control branches that act independently and with equal priority on the control decision. The common mode of operation and any common source of failure is reduced.

Active self-tests instead of voting mechanisms reduces the probability of accumulated hidden dangerous failures in the system.

The two parallel control branches read the field signals, execute the safety control logic, calculate the control outputs and set the field output signals individually and independent of each other. However, each control branch is able to set the field output signals only when its diagnostics control gives an active permissive signal.

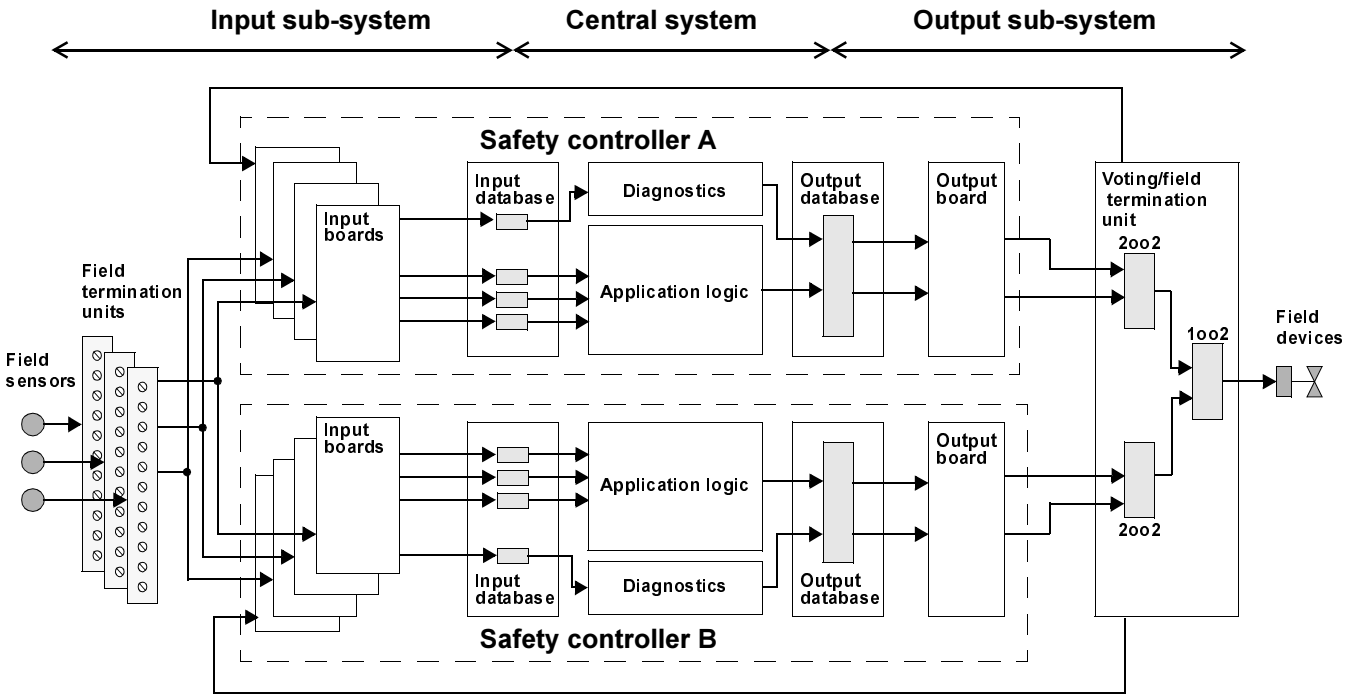

Figure 1-4. Dual controller principle

The combination of active self-testing with permissive control of any control action adds optimal failure tolerance capability to the superior attributes of the 1oo2 architecture regarding safety integrity.

Extensive and active self-tests with replication are implemented individually in both control branches. Detected failures are generally isolated from causing any spurious interruption of the process. In the event of correlated failure in both branches a fail-to-safe action takes place.

1.5.2 Single controller structure

The 1oo1D system has an architecture that consists of one control branch that performs the control decision. The safety output handling is duplicated as in the dual controller structure to maintain the test and availability of the safety function.

The controller reads the field signals, execute the safety control logic, calculate the control outputs and set the field output signals individually. However, each output branch is able to set the field output signals only when its diagnostics control gives an active permissive signal.

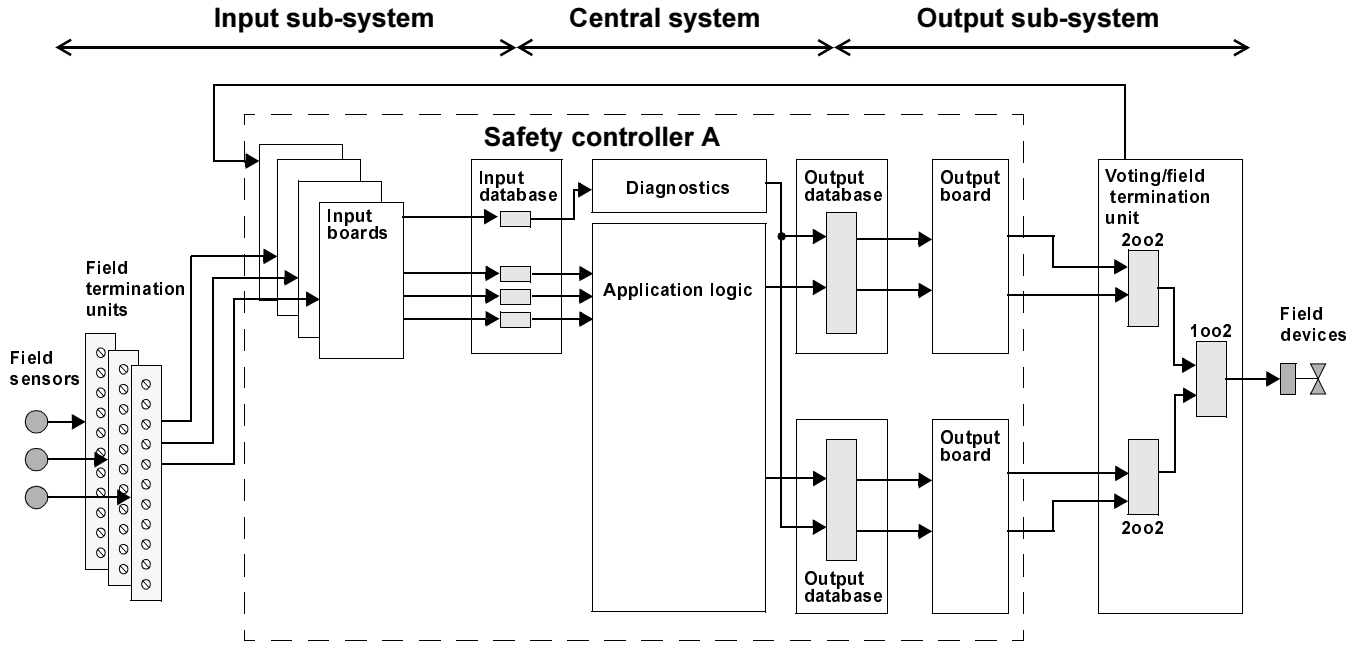

Figure 1-5. Single controller principle

1.6 Certification

ABB Safety has chosen TÜV Product Service GmbH as our external validation and certification partner. TÜV Product Service is a highly recognized certification authority.
All development of the Safeguard 400 Series product is performed in a close relationship with TÜV. The following major milestones are part of a development project:

- Concept approval
- Design approval
- Functional validation

For details regarding certification, please refer to the Safeguard 400 Series Safety Manual, 3BNP000432R301. The Safety Manual is a TÜV approved document and contains relevant information for implementation and maintenance of the safety system.

Single Safeguard and dual Safeguard have different levels of certification. Safeguard 410 and Safeguard 415 are designed to comply with the requirements of AK 6/SIL 3. A Single Safeguard system may be configured to comply with the requirements of AK 4/SIL 2

The different types of certification status for the various system components are defined as follows.

Certified:

Hardware and software functions certified for use in a safety system.

Safety critical:

Hardware and software functions certified to be used to control safety devices in a safety system.

Non-interference:

Hardware and software functions certified to be used in a safety system for non-safety related devices.

Non-certified:

Hardware and software functions not certified for use in a safety system.

Chapter 2 Software Functions

2.1 Safeguard 400 Series Software

2.1.1 General base system operation

Most of the operation of the Safeguard/AC410 base system is transparent to the end user, who only sees the system database and application program, unless explicitly accessing other functions by means of system commands.

Database

The **database** is distributed to each individual Safeguard 400 Series controller. Access is symbolic, which means that all information is available by specifying the signal name. All relevant information about an I/O point or a loop is available in one record, which is simultaneously updated to ensure that all data for a single point is consistent.

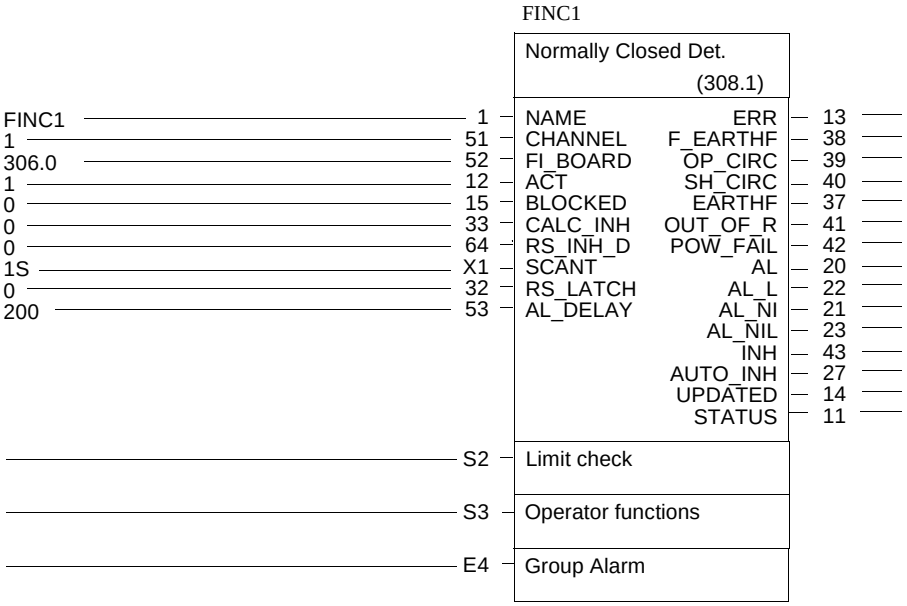

Figure 2-1. Database entry for a Normally Closed loop monitored digital input

The following data given in the database specifies how the underlying software will treat that point:

- Name, description, service status etc. for all objects.
- Range, hysteresis, scaling, filtering, addresses etc. provides data for the I/O handlers to access the hardware to obtain data, perform basic treatment and convert it to engineering units.

- Alarm limits and alarm handling parameters specify how event and alarm handling is to be carried out.
- Engineering unit, number of decimals, accessed, blocked, manual entry and others define basic parameters for the operator interface.

Application program

The **application program** works with the database to define additional treatment (for example input voting) and the cause & effect algorithm. This program can be designed in two formats:

- As a function block program, using the functional element library of basic algorithms.
- As a cause & effect chart, table files loaded in the system.

2.1.2 AMPL Safeguard features

AMPL is a function block language with graphical representation. The function blocks offer a high level of configuration from simple to complex. The language is common for all ABB controller products with Master software. However, as the products are optimized to different application areas the functional extent and the execution environments differ between the products. For the Safeguard 400 Series the following AMPL elements are supplied additionally, either as an option or as a part of the base product.

NOTE

For the range of standard elements also included (AC410) refer to PC Elements Advant Controller 400 Series Reference Manual.

Table 2-1. Safety PC elements.

Type	Function	PC Element
Safety address	**Reads the node number.**	**S-ADDR**
Fire and gas input voting	**Combines inputs from loop monitored digital inputs or gas detector inputs for coincidence signals and for area presentations.**	**FI-VOTE, GI-VOTE**
Integer word handling	**Performs AND, OR, bit reversal and bit extractions on integer values.**	**IOR, IAND, I-NOT, BTST**
Data base network transfer	**Copies values in the data base from one node on the network to another node.**	**DB-COP**

Table 2-1. Safety PC elements.

Type	Function	PC Element
C&E matrix control (optional)	**Controls the execution and supervises the C&E matrixes.**	**CE-MATR**
C&E matrix output control (optional)	**Enables access to outputs in a C&E matrix from other AMPL logic.**	**CE-OPC**

2.1.3 Cause & Effect programming

The AdvaBuild Safety Builder is an advanced Microsoft Windows based programming tool especially designed for safety engineering applications. The tool offers a straight forward WYSIWYG cause & effect application design. The application programming is simply performed by graphically creating shutdown levels, inserting inputs and outputs and plotting in the correlation between them, just as it appears in the cause & effect engineering documentation. The Safety Builder increases the efficiency and reduces the possibility of faults in the application programs caused by “translation” of C&E diagrams to AMPL function block logic. The AdvaBuild Safety Builder cause & effect tool can be ordered as an option.

The Safety Builder supports a number of functions such as:

- Hierarchical shutdown level definition.
- Possibility of remote shutdown level interaction on installations with several safety systems.
- Flexibility in changes of each individual C&E diagram and number of diagrams and shutdown levels.
- Standard function for defining time delays.
- Standard reset function.
- Direct access to the I/O database.
- Cause & effect diagram format documentation of the application.
- Revision handling on the individual C&E documentation diagram.

2.1.4 Safeguard 400 Series Central Processing Unit

The Safeguard 400 Series controllers are configured with Advant Controller 410 central processing units. The main tasks handled by the central processor unit are:

- Execute the operating system and communications system functions
- Hardware and firmware basic fault detection
- Field I/O handling and database updates

- Application program execution
- Application dependent test routines

In addition to the standard AC410 basic system function (QC01-BAS11, QC01-OPF11 and QC01-LIB11), the following safety system software modules are provided as a part of the Safeguard 400 Series standard product:

- QC05-BAS11 which includes:
  - Routines for safety input sets, including alarm treatment and input inhibit
  - Handling of Master Vote 3000 including application dependent test routines
  - Dual system start-up and maintenance functions, including status synchronization between branches at system restart (in 1oo2D dual system only)
  - Loop monitored digital inputs
  - Gas inputs
  - Improved system diagnostics
  - Bypass management

Most of the functions included in the safety software are transparent to the user. Application programming, database fill-in and cause and effect logic are done as if working with a single system. In the 1oo2D Safeguard system, identical applications are loaded into the two system branches, and the only difference between the two branches is their data highway bus addresses (set in hardware).

- As options the following system functions can be selected:
- QC05-CEM11, Handling of the cause and effect files from the Safety Builder
- QC05-FIE11, High functional level communication with Fireguard addressable fire detector system
- QC05-FIA11, Communication with Autronica BS-100 addressable fire detector system
- QC05-SIO11, Safety analog and digital inputs
- QC01-UDP11, Program module for User Defined PC elements (UDPC)
- QC01-LIB12, Element library for advanced process control
- QC01-LOS11, Local operator station support, MasterView 300

2.1.5 Basic system testing

This section describes the basic system testing performed by the main CPU.

Most test and diagnostics information is available as safety messages and in system status displays on the operator station. If a serious fault does occur, and the system is not considered reliable, the CPU will be halted, and diagnostic information is presented on the CPU board front.

Indicators on the CPU board front include power status, halt (system stopped), stall (watchdog time-out), and a two-digit system status display. With these indicators, and indications on the

I/O boards, most errors are diagnosed simply by locating the red error indicators. The same status, including more detailed diagnostic messages are also available on operator station displays.

Further information in this state can be obtained with the Advant Station 100 or 500 Series Engineering Station.

Basic system tests include:

- CPU Instruction set test
- CPU Illegal instruction trap
- CPU watchdog, high and low level (Fail, Infinite loop, overload)
- Bus backplane supervision, address error, bus time-out (no response)
- Dynamic RWM error detection and correction
- System clock supervision
- CRC sign calculation on system software modules
- CRC sign calculation on application database and AMPL program
- Task execution supervision
- Operating system call error detection
- Communication handlers (ISO OSI 7-layer model)
- Peripheral driver diagnostics.
- Power supply fail
- Cabinet fan fail, over-temperature.

For dangerous errors, such as program system illegal execution, appropriate actions and reporting are taken directly by the operating system. In less serious situations, the status is also available to the application program, which can decide on the correct action to take. Some safety applications may for example allow execution to continue when communication to other systems is lost, while others would regard this as a shutdown condition.

The result of a serious system fault is to shut down operation and halt the CPU. This action will cause the CPU Run status line to fall (i.e. go to zero) and de-energize all outputs.

It is important to note that the main function of the basic tests is to ensure that all hardware components are operable, that the firmware and application software is executing and is not corrupted by spurious changes. It is therefore **not** necessary to design additional test programs, (for example pattern tests with output vector comparison of the logic) to ensure that the safety system has not changed.

2.1.6 Master Vote 3000 safety outputs

There are two types of Master Vote 3000 connection units. DSTD N020 is for normally energized outputs and DSTD N021 is for normally de-energized outputs. They have a fail-to-safe design and support a 1 out of 2 voting system. The functions on the units are continuously supervised and tested by the Safeguard 400 Series system software.

2.1.6.1 Signal processing

The control of the field outputs from Master Vote 3000 relies on the correct operation of the Isolate-Not and Shutdown/Activate signals.
(-Not is logically negated signal):

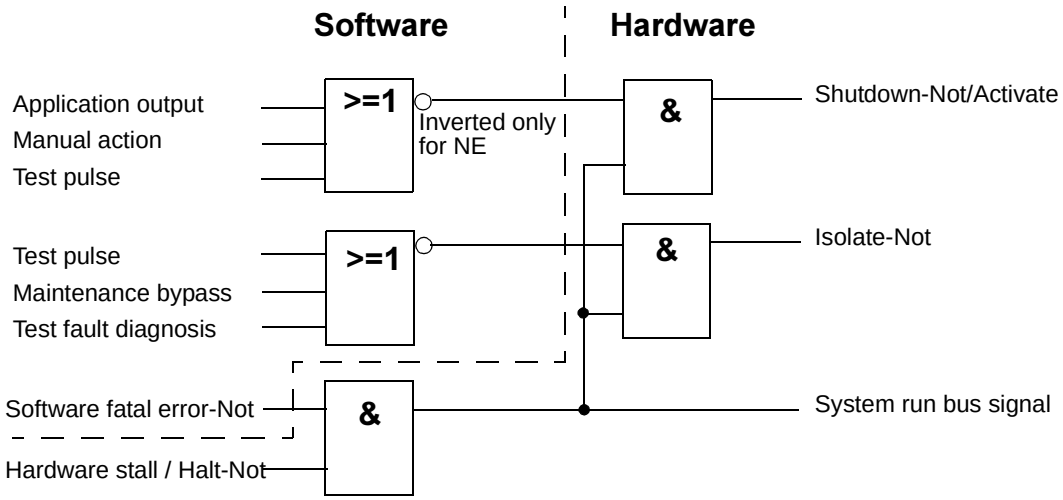

Figure 2-2. Isolate and shutdown/activate signal operation

Isolate-Not

The Isolate-Not is a composite signal that represents a number of control unit states in the control unit that should result in branch isolation. Isolate is negated (goes low) as a result of system malfunction (see previous chapters on system diagnostics), a manual request for maintenance purpose, or when a test reveals a fault that must be handled by disabling the failing branch. This is particularly applicable to NE outputs.

The Isolate signal is timed so the loss of a control unit or an output board will always cause a low Isolate signal to be recognized first. The shutdown output is timed to go low after isolate to prevent it from requesting a shutdown when the isolate is still high.

In a similar fashion, the isolate is designed to return high after a valid signal is presented on the shutdown output to prevent spurious action on system restart or isolate removal. This function allows fault tolerant action to be taken on failure or during maintenance.

Shutdown-Not or Activate

The Shutdown-Not (Normally Energized) or Activate (Normally De-Energized) signal is a combination of an application generated action, manual action and signals from the test program. It is also affected by system errors, and is forced low (NE) or will stay low (ND) on a control unit malfunction.

2.1.6.2 Output testing

Master Vote 3000 automatic output tests are performed as a part of the Safeguard 400 Series base software and consists of:

The output tests consist of:

- Channel test
- Isolate test
- Option for monitoring of read-back of the output status.
- Option for feedback of the output loop supervision signal.

The basic test uses the Isolate-Not and Shutdown-Not (NE) / Activate (ND) signals to control the test, and receives information back on two inputs (Isolate Status and Test Status). These are common to all seven outputs on one Master Vote 3000 unit. The standard tests cover all functions of the Master Vote 3000. The normal action for a NE output on detection of a fault is to isolate the branch by deactivating Isolate-Not, and report this as a safety message and on the diagnostics displays. ND stays low.

2.1.7 Bypass Management

The functions of Bypass management are:

- Operator station access control
- On-Line Builder (engineering tool) access control
- Override control and reset

Override is generally used as a collective term for inhibit, input block, output block and manual mode for the relevant signal types.

The use of override functions in safety related equipment introduces a potential hazard to the installation and to the people it is designed to protect. Any inhibit of a safety critical input or override on a safety critical output represents a degradation of the safety level and a possibility for failure on demand.

Nevertheless, such functions are necessary to achieve a reasonable availability of the process. All field equipment needs maintenance or replacement at regular intervals, and this is included in the design of the safety system regarding e.g. number/wiring and placement of instruments. In these cases the safety level may be maintained by other measures while necessary maintenance operations are carried out.

There are also requirements for use of inhibits during start-up in certain applications.

The Bypass management function enables project/application specific configuration of the appropriate level of restrictions regarding operation of the Safeguard 400 Series.

2.1.7.1 Operator station access control

Operator stations which shall be accepted for write access must be configured in the Safeguard 400 Series and a key switch shall be hard wired to the Safeguard 400 Series for control of permission to operate the system.

2.1.7.2 On-Line Builder (engineering tool) access control

Communication with engineering tools can be controlled by the isolation key switch on the local panel and/or by a successful isolation of the safety controller.

2.1.7.3 Override control and reset

The number of simultaneously occurring overrides are controlled by a configuration parameter.

The reset of the overridden signals can be done in several ways:

- The primary reset of overrides is via normal communicated dialog operations (manual entry).
- A hard wired input to the Safeguard 400 Series is the secondary possibility for reset of all overrides in the safety system, independent of communication with any operator stations.
- Automatic reset of all overrides in case of loss of communication with all access granted operator stations.
- Automatic reset of all overrides in case of maximum allowed time exceeded timed from the first occurring override.

The number of configured and active overrides are presented on the operator station and it is also possible to configure any active override in the system as an activation of a dedicated digital output.

All activation and de-activation of overrides is recorded on the operator station event list.

2.2 Operator Interface Software

2.2.1 General

The basic operator interface software, named AdvaCommand, is available for the HP-UX-based Advant Station 500 Operator Station and for a Windows NT-based PC. AdvaCommand is a family of operator control and interaction functions.

It provides functions for presentation of safety and process information, command entry, event and alarm handling, system status, window handling, process sectioning and status lists.
The AdvaCommand Safeguard Handler is an option which is required for handling of the Safeguard 400 Series products. All Advant Station 500 Operator Station series can also be delivered with the AdvaCommand Safeguard Handler option.

Table 2-2. Overview of functions and product series

Function	Safeguard 400 Series	AdvaCommand for Unix	AdvaCommand for Windows NT
AdvaCommand User Interface and Manual Control	- (1)	yes	yes
AdvaCommand Event&Alarm	yes	yes	yes
AdvaCommand Group Alarm	-	yes	yes

Table 2-2. Overview of functions and product series (Continued)

Function	Safeguard 400 Series	AdvaCommand for Unix	AdvaCommand for Windows NT
AdvaCommand Process Sectioning	-	option	option
AdvaCommand Status List	-	option	option
AdvaCommand System Status	yes (2)	yes	yes
AdvaCommand Safeguard Handler	-	option(3)	option

(1) Data to present in the displays are available in for example the Safeguard 400 Series, and subscribed to by the AdvaCommand User Interface at presentation.
(2) The System status function has software running in Safeguard 400 Series. The distributed software reports current status on request from the AdvaCommand System Status function at presentation.
(3) If the operator station is used in a plant network, the node number for the safety and process controllers must be unique for all nodes in all the connected control networks.

2.2.2 Safety functions

All Advant Operator Workplace functions are retained when used with the Safeguard 400 Series. This means that the product can be used as a common operator station for safety and process control.

With AdvaCommand Safeguard Handler the following functions are added to the basic Operator station:

- A dual system handler that allows both branches of the Safeguard 400 Series to appear as one object to the operator. This gives:
  - Single presentation of alarms in lists and on printer.
  - Single presentation of objects.
  - Dialogue handler with commands sent to both safety controllers.

NOTE

If the operator workplace is used in a plant network, the node number must be unique in all the connected control networks. This is due to limitations in the dual handling function in the operator station.

- Presentation and interaction for safety object types, e.g. detection and protection systems, required by Safeguard 400 Series is added to the standard operator station functionality. This consists of Object (Faceplate) displays, group displays and display elements as well as dialogs. The following safety object types are available in the Safeguard Handler:
  - FI (Fire Input), Loop monitored digital inputs
  - FD, for addressable Fire Detector signals
  - GI, for Gas input signals
  - Safety System Status, diagnostic status display for Safeguard 400 Series
  - FG, diagnostic status display for Fireguard

  - C&E shutdown level group display.
- Presentations and dialogs for these safety objects include:
  - **Presentations:**
  - Signal (On/Off or Value)
  - Alarm limits and alarms
  - Object status (inhibit, bypass, latched alarm, selected for operation etc.)
  - Loop and I/O diagnostics.
  - Maintenance.
  - **Dialogs:**
  - Activation and manual entry.
  - Control of status (for example inhibit, reset).
- Diagnostic and status functions.
  - Alarm/Event list.
  - Group alarm (option).
  - Status list (report special status and conditions).
  - System fault list and diagnostic displays.
- Process Parameter Backup, which includes functions for backup/restore of a process station's process parameters to/from an operator station. The process parameters stored in the backup are available for restore at a later time. The process parameters involved are those that are changeable by dialog commands from the operator station(s) such as alarm limits, initial values etc. Process Parameter Backup is not included in AdvaCommand for Windows NT.
- Signal Filtering function for filtering the events, alarms, system alarms and system status in the Operator Station to reduce system load in the controllers in the network.

Object display

The object display shows a message buffer where dedicated safety system messages are presented. The available dialogs enable a limited control of the safety system:

- Presentation of messages from the safety message buffer with scrolling facilities.
- Isolate control of the Master Vote 3000 outputs.
- Alarm and print blocking.
- C&E matrix communication blocking.

Regarding Figure 2-3: in Single Safeguard systems, only SIDE A is presented.

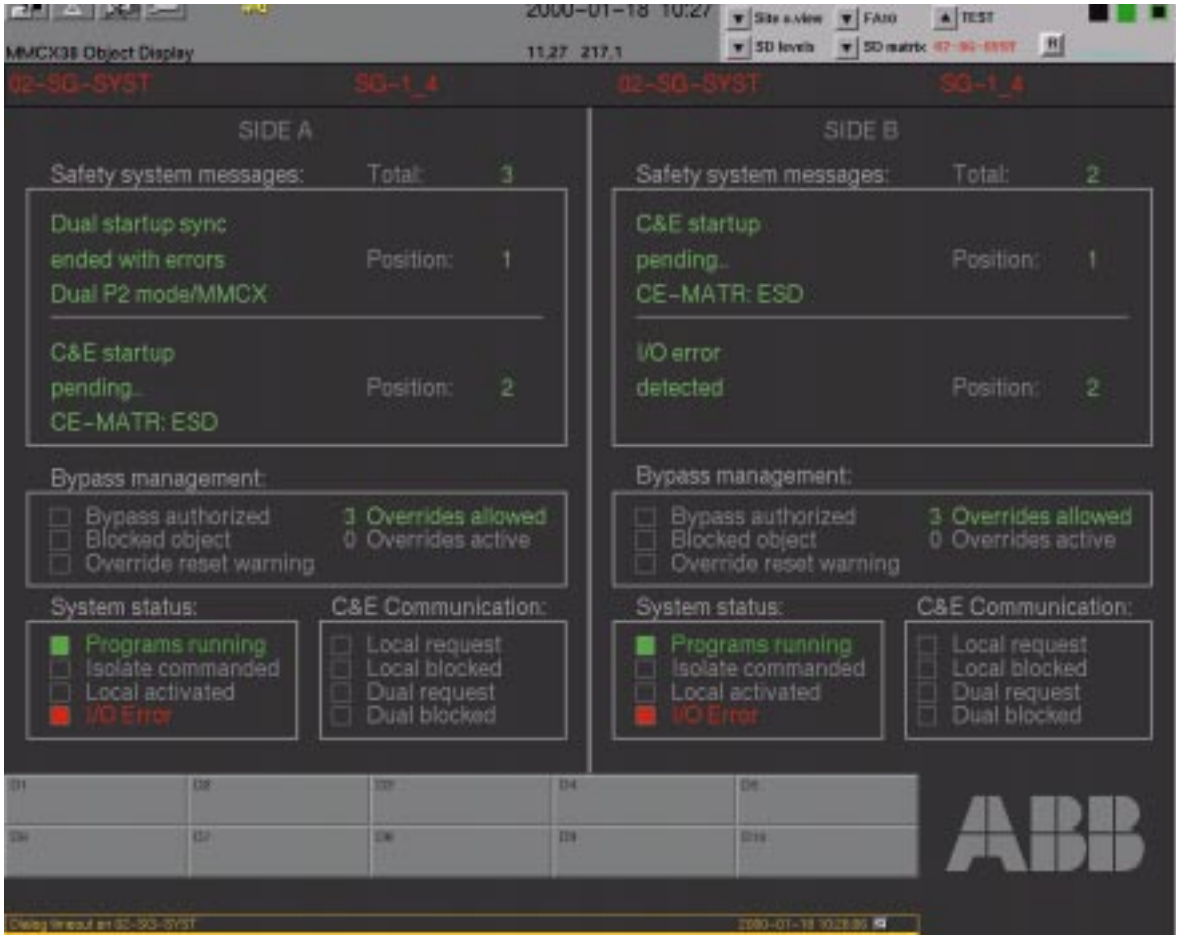

Figure 2-3. Safety system status object display

2.2.3 System security

For system security, access to objects and specific functions can be placed under key lock protection. Refer to Section 2.1.7, Bypass Management

- Process Sectioning and authorization allows the safety systems to be placed in separate process sections. Individual objects (for example an input or output) are assigned a section number. Access to systems are defined on a workstation basis as None, Inspect or Control towards each section. The function is key lock or password protected. This function is included in the optional AdvaCommand Process Sectioning
- When displays are designed each point is given a dialog. 'Dialogs are built in three forms. None, operator and maintenance. An operator dialog allows access for normal operation only, while a maintenance dialog allows full control. The maintenance dialog is key lock or password protected. A pre-defined set is included in the product, but as the dialog editor (option) allows design of custom dialogs, they can be adapted to individual requirements.

The AdvaBuild Display Builder will present these functions along with the basic functions (that is in the presentation element list), the difference lies in **which** displays that are defined for a fire & gas or shutdown system, rather than **how** they are built and operated.

2.2.4 AdvaCommand user interface

The operator interacts with the automation system using either the mouse/track-ball, the operator keyboard or a combination of both. The moment a process object has been selected for control, exclusive access is guaranteed and no other operator can interact.

The AdvaCommand User Interface supports different user categories by offering several dialog styles, which are adapted to the different users and their needs, for example menus for configuration and dynamic function keys for process control.

The screen is divided into areas, each reserved for a specific purpose. The basic screen layout is shown below:

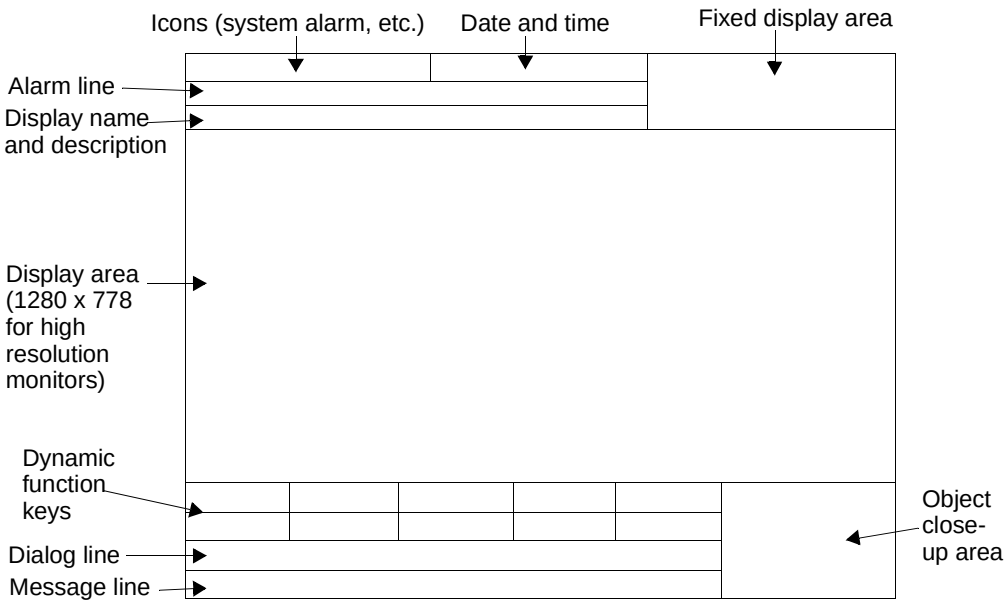

Figure 2-4. Screen layout

The different screen areas are as follows:

- The icon area contains various icons for indication and selection. The icons include for example system alarm, maximum authority, as well as external alarm and dedicated screen buttons.
- The date-and-time field shows the current date and time as measured by the internal system clock
- The fixed display area is for continuous presentation of a user-created display, for example a process overview, a production summary, or an alarm summary
- The alarm line shows the latest unacknowledged process alarm. There is also a list of current process alarms for trouble-shooting in the plant.
- The display-name and description field contains the name and description of the current display. Displays are searched for and accessed by name and the descriptions make it easy to find the right display on menus etc. at all times.
- The display area is where the displays called up appear.
- The dynamic function key field is the main means for operator input of commands both to the system and to the process. Commands are issued by pointing at the desired key with

the cursor and clicking a button or by pressing the desired function key on the keyboard.

- The dialog line guides the operator through command sequences by displaying intelligent, situation-sensitive prompting messages.
- The message line supplements the dialog line in guiding the operator by providing additional information, for example error messages.
- The object close-up area presents detailed information on the process or system object selected for control, thus providing the information the operator needs for the actions ahead without having to call up other displays with more details.

The status of the process is shown on different types of displays:

- Process displays are application-specific displays entirely defined by the user. Values and states of objects, such as regulators, sequences, measurement points, motors, etc., are presented dynamically.
- Overview and group displays offer a cursory view of the different parts of the process. Objects are arranged in groups, corresponding to process areas. The format of these displays is standardized; all that needs to be defined is which objects to show where.
- Object displays present all the information available about single objects. These displays require no configuration but are automatically made available for all the objects in the control system.
- Alarm and event lists providing records of the latest alarms and events in the process, in the system.
- AdvaCommand User Interface allows access to a vast amount of historical data stored throughout the automation system. For presentation on curves, histograms, and tables. In separate curve displays, overlapping windows or as part of basic process displays.

  Data for curve displays can be obtained from any log or log group containing the variable of interest, regardless of time interval. This means that the same data logs and log groups can be used for both short-range/high-resolution and long-range/low-resolution diagrams. Process objects can be selected for control directly from curve displays.

  Historical data can be presented on predefined curve displays or as elements of normal user-defined process displays. A number of curve displays are available for the purpose of presenting historical data and process trends. Curves can be panned smoothly or in jumps, in the latter case by specifying the desired time period. Values can be fetched from any log containing the variable concerned, regardless of time interval. This amounts to seamless retrieval” and convenient panning far back in time if need be. The value scale can easily be adjusted by the user and the latest value is presented numerically for best possible reading accuracy. There is also a ruler which can be slid across the graph for accurate numeric reading at any point.
- Status lists, extracting the process objects matching specified search keys.
- Display printouts.

2.2.4.1 User defined displays

The layout oriented user defined displays for a safety system are normally organized in a hierarchy by the dynamic function keys and display select buttons built in the free graphic display. For fire & gas, the hierarchy could normally be organized as follows:

1. Level 1: Plant overview
2. Level 2: Section floorplan
3. Level 3: Fire room/area detail.

Examples of these displays for an offshore oil production platform are given in the following displays

Plant overview

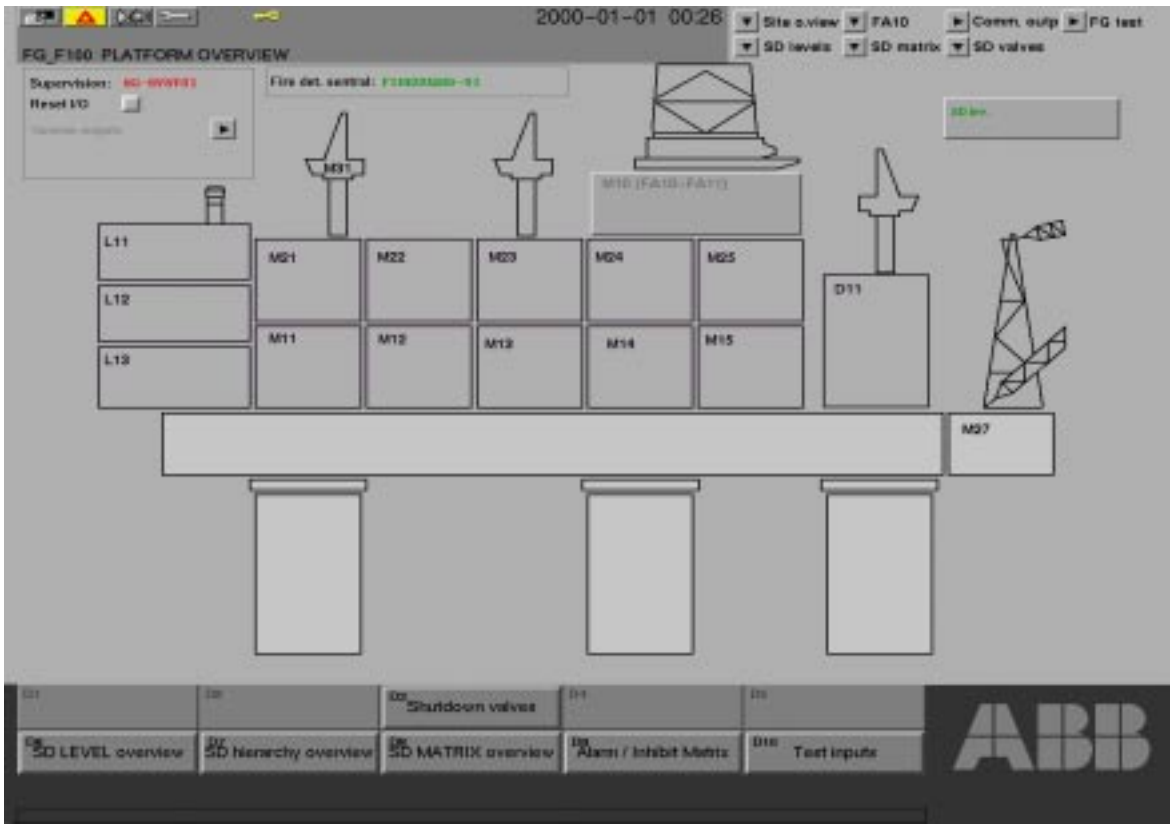

Figure 2-5. F&G overview display with gas alarm

The dynamic presentations are “hidden” when the Fire and Gas system are in a normal state (no alarms, inhibits, errors or releases anywhere on the platform) and visual when an abnormal situation, such as a detector alarm, occurs.

All information in the overview display are collected from the various module displays. The status from each module is represented with dynamic group indication for gas detection, fire detection, protection systems and a common error for the detection/protection systems. The grouping is performed in application logic and can be defined by the user.

Section floorplan

Figure 2-6. F&G level 2 section floorplan display

All information in the section displays are collected from the various fire area detail display (shown next). The status from each fire room/area is represented with dynamic group indication for gas detection, fire detection, protection systems. The grouping is performed in application logic and can be defined by the user.

Fire room/area detail

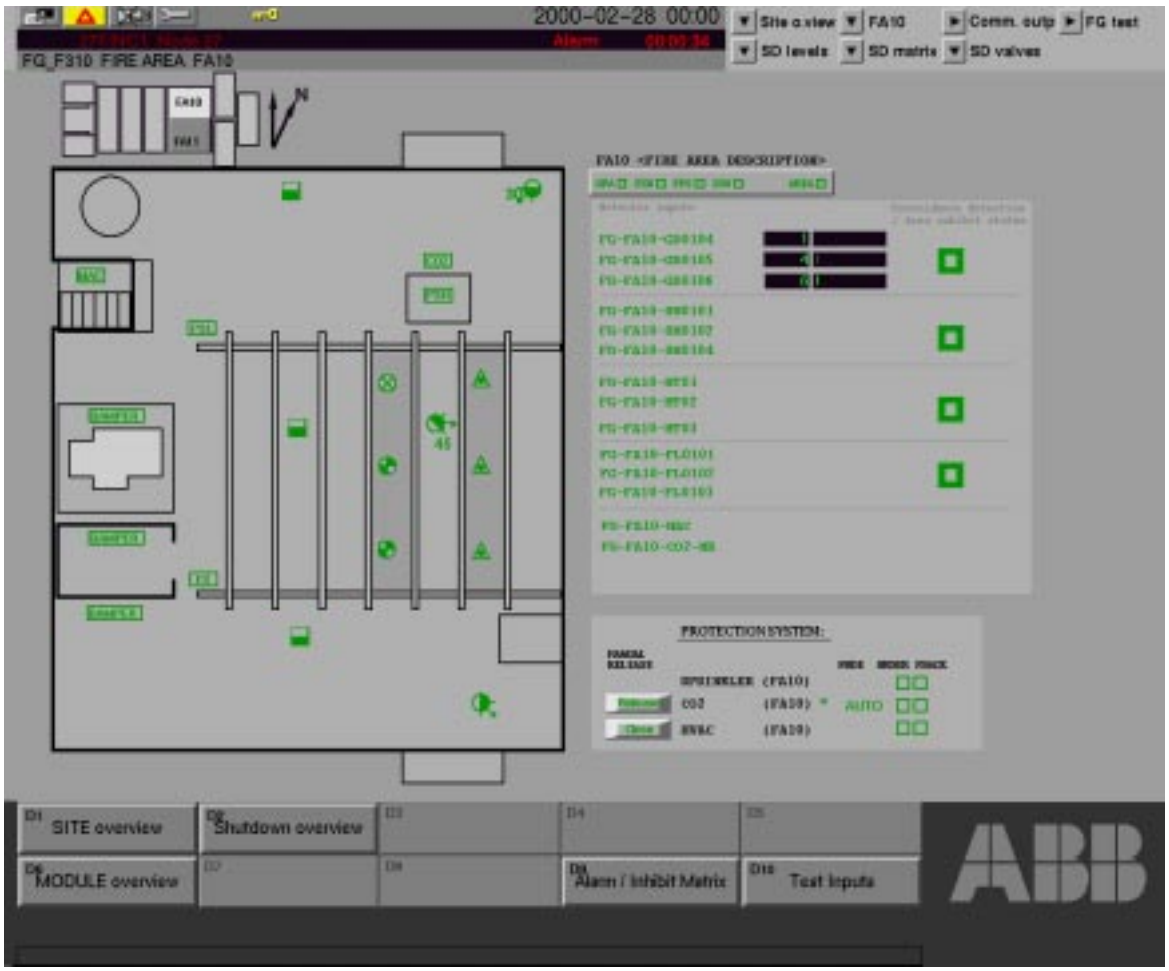

Figure 2-7. F&G level 3 fire room/area detail display

The fire room/area detail display contains information on all detectors and protection systems present in the fire area. The displays are normally divided in two parts. One part is layout oriented and includes dynamic symbols for all fire and gas detectors. The other part contains a listing of the detectors together with the protection systems

For shutdown systems, the displays are often a part of the process display hierarchy, with protection interlocks and shutdown actions indicated along with process equipment. Supporting displays (for example behind the help button) would detail the status of shutdown equipment and permit operator actions. Refer to Figure 1-3.

2.2.5 Predefined reports (Status lists)

The predefined reports/status lists are created with the AdvaCommand status list function.

An important aspect of system functionality is to avoid degradation of the system and protection mechanisms due to manual interactions.

The status list function aids in this process, and is used to search the control system for specific conditions. Any value or status in the real time object database may be searched. Wild card names, process section, object class etc. are used to select a range of objects to search, such as a module, building or fire area. This function is used to produce a variety of predefined reports such as (but not limited to):

- **Input Override List:** A list of all inputs that have the inhibited condition (override) set.
- **Output Override/Bypass List:** For all outputs, list special status of this type
- **Fault list:** A list of all detectors that have a fault condition detected
- **Special status:** Lists all systems in manual or blocked mode
- **Blocked alarms**
- **Gas detection LEL readings.**

The lists can be produced on demand, or are timed, e.g. per shift or per day. The output can be sent to a display or to a printer. For indication, the periodic timed lists can set or reset indication flags, that are used as alarms or for summary displays.

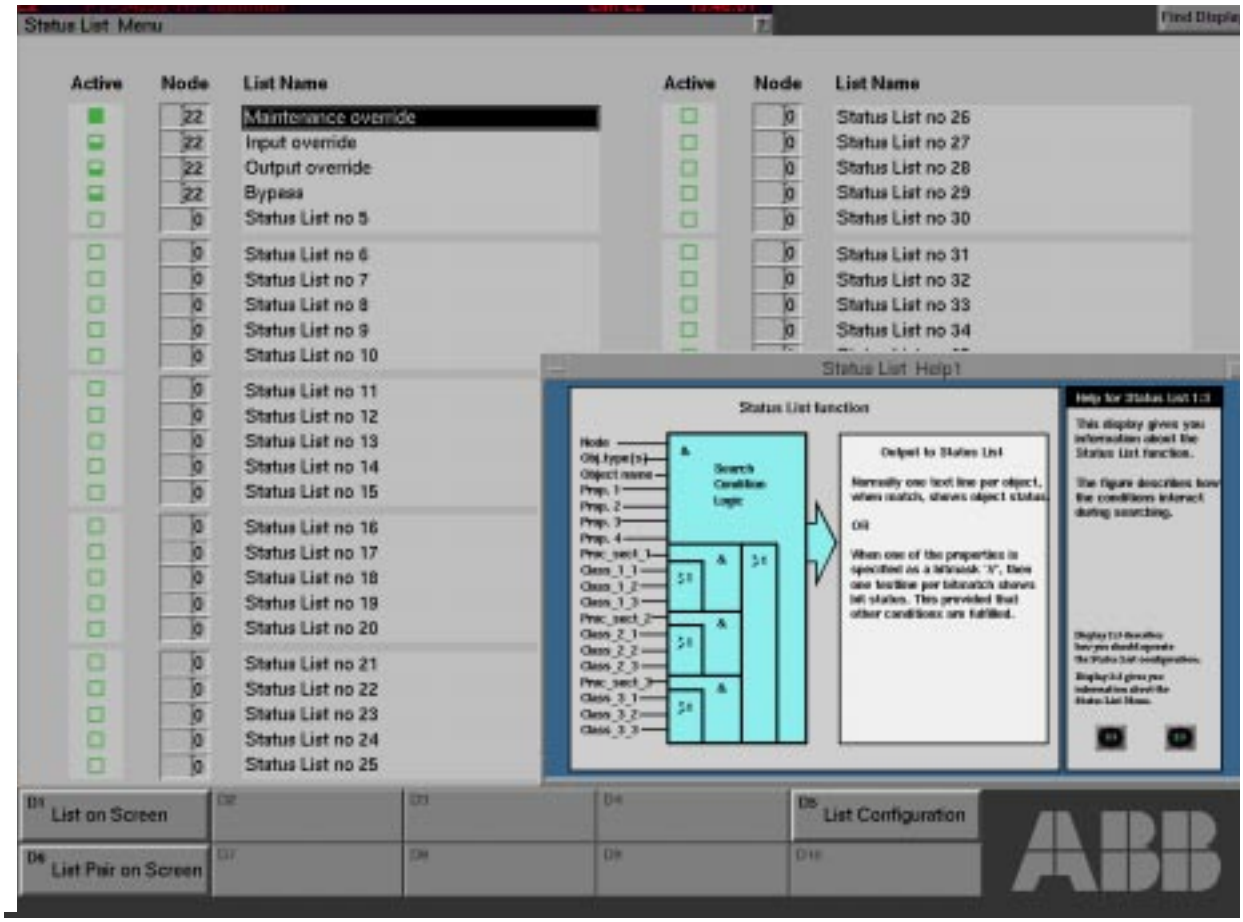

Figure 2-8. Status list menu

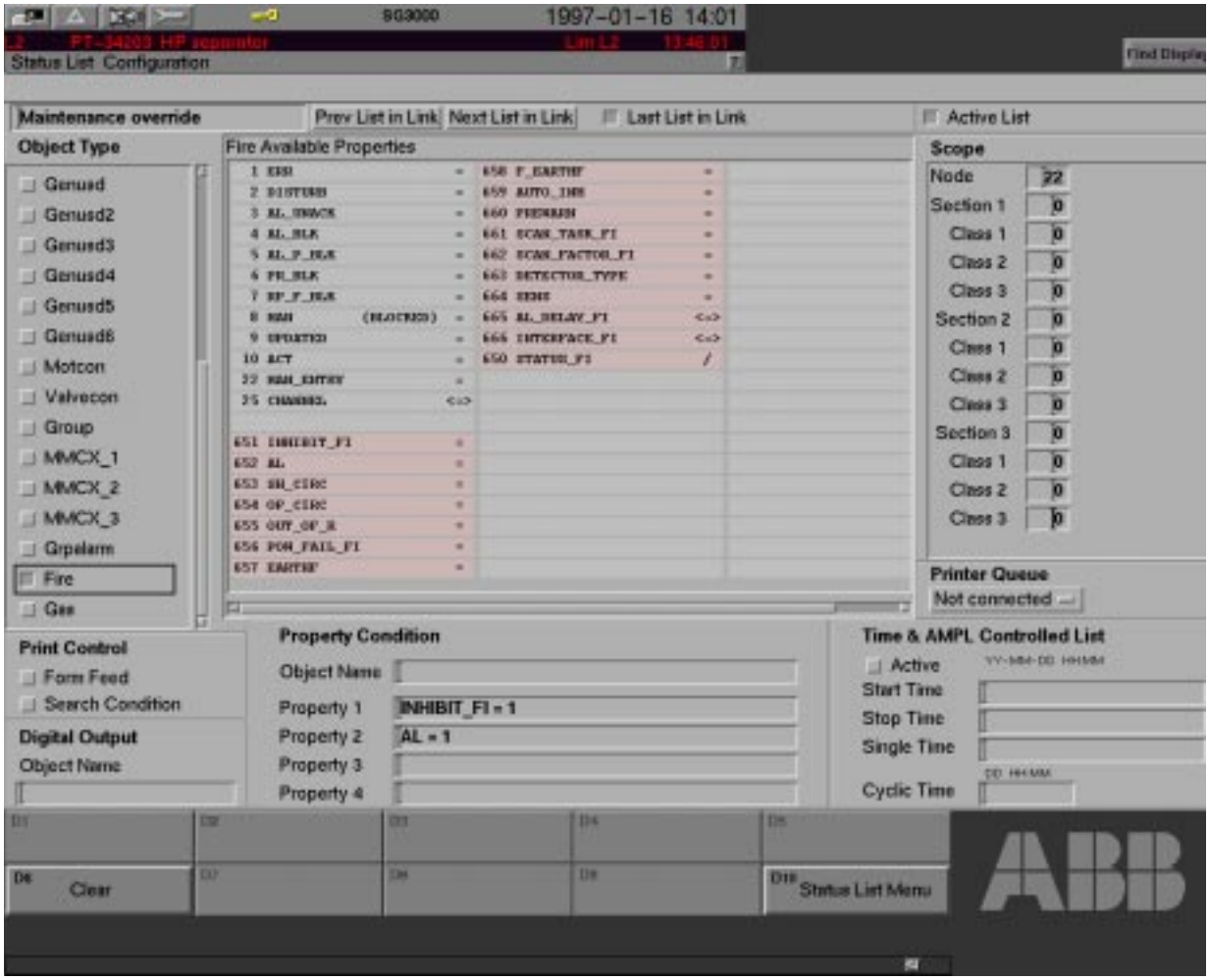

Figure 2-9. Status list configuration

2.2.6 Alarm management

Alarm management is a standard AdvaCommand Event & Alarm function

Alarm and Event messages are stored and presented in chronological lists. The list of events is circular and when the list is full, the next event will overwrite the oldest. An alarm is a special type of event, requiring your attention and acknowledgment. While events are generated whenever predefined conditions are met, for example, binary variables change state or analog values exceed limits, alarms are generated when abnormal events occur. By default, an alarm is not removed from the list until you have acknowledged the alarm and the error has disappeared. However, it is possible to configure the function in such a way that the message disappears after acknowledgment, even if the alarm condition still exists.

Alarms are also indicated on all displays as a latest unacknowledged alarm line, and as red status indications in displays with dynamic data from the objects concerned, flashing until the alarm is acknowledged, and then steady as long as the alarm condition persists.

You can also configure objects for repetition control of alarms, which means that repetitive reporting of the same alarm is suppressed if the object toggles between the normal and faulty states. On your request, the alarm and event messages can be presented in different types of lists. The lists can be presented as base displays or as overlap displays. When presented as base displays the lists can be directed to another screen by using the dedicated screen function. The following types of lists are available:

• Process event lists

• Process alarm lists

• System alarm lists

The system alarm lists contains messages of control system errors, indicating faults or other changes of state in the control system. All three types of lists can be printed on request, when the events and alarms occur. The length of the lists, for example, the number of alarms in the process alarm list can be configured.

NOTE

All Advant Operator Workplaces within one control network should have the same length of the lists since the automatic acknowledge facility starts when the alarm list is full.

The contents and the layout of the three types of lists and the alarm line showing the latest unacknowledged process alarm can all be configured from the System Configuration Dialog. Filter parameters can be set up in order to filter out not relevant alarms. Several alarm lists with different filter parameters can be specified.

Dual handling

Events and alarms are generated individually by each Safety controller, and sent onto the MasterBus 300 data highway. To avoid duplicate entries from the dual system in lists and on printers, the alarms are received in a temporary buffer in the Operator Station. The first alarm is immediately presented, but is also retained in the buffer. If a corresponding alarm is received from the other controller within 12 seconds, it is discarded.

The alarms are passed on into the operator station alarm and event list and sorted according to their time stamp which is set by the safety controller. The system time in the two safety controllers will be synchronized within 10 milliseconds of each other.

2.2.7 Safety management

The focus on environmental issues and safety aspects is increasing in modern industrial plant operation. Lifecycle safety management is the scope of coming standards that will affect all parties involved in industrial activities.

In day-to-day operations, the safety level of a plant depends mainly on the quality of the equipment, the quality of the execution of the different activities and on the quality of work management.

Analyses of major accidents and catastrophes generally document that a series of unfortunate coincidental events have taken place prior to such incidents, and also that adequate actions where not taken in the first critical phase of fighting them.

Knowledge, information availability and awareness are key factors and important safety criteria in the daily achievement of plant safety.

2.2.8 Matrix and mimic panels

All indications and actions are accessible from the operator station. The operator station can be complemented with panels. A subset of actions and indications can be present on the matrix and mimic panels, ranging from simple group indications and actions to a full matrix with status indication, inhibit, bypass and manual action for each individual input and output. The matrices and mimics can be hardwired or driven by a serial bus for lower cost and reduced wiring, and essentially is normal status Input/Outputs defined in function block macros.

2.3 Safeguard Handler for Advant Enterprise Historian

Safeguard Handler for Advant Enterprise Historian is a software option to be installed in an AEH or in an Advant Station 500 IMS.

Safeguard Handler software has been designed to present Safeguard 400 Series as a single controller in the AEH or in the IMS, even though every signal from the safety controller is duplicated.

2.4 Engineering Software for AS 100 Series ES

2.4.1 General

AdvaBuild Engineering Software is designed for use under Windows NT and is structured into three major product groups:

- Advant Engineering Workplace

  For establishing the engineering environment, navigation and administration functions.

- AMPL Control Configuration

  For configuration and commissioning functions for Advant controllers.

- Computer Aided Electrical Engineering

  For handling of electrical diagrams.

Each product group consists of a basic unit and some options. Tools which perform a dedicated engineering task are called Builders. A product may contain several Builders like Application Builder and Function Chart Builder, as well as utilities like a text editor or an example project.

2.4.2 Advant Engineering Workplace

The Advant Engineering Workplace is necessary to work in the cooperating mode. The components included are described in the following sections.

Structure Builder

Structure Builder is the tool to handle the Advant Objects and to visualize the structure of a plant. The plant is represented as a set of structures, containing Advant Objects in hierachical relations. Structure Builder enables the user to navigate between Advant Objects in a convenient way and to perform activities on a selected Advant Object, such as opening certain views, copying or moving Advant Objects, structures or even a whole project.

Advant Engineering Server

The Advant Engineering Server prepares the environment for the engineering data storage.

Parameter Builder

Parameter Builder is the tool for efficient bulk data handling. It allows to enter and modify engineering data which are used as parameters for other aspects. For example, Type Circuit instances in a Circuit aspect can refer to parameter aspects and can be updated by the actual values of the parameter aspects at the users request. Parameter Builder is based on Microsoft Access.

Document Builder

Document Builder is the tool to efficiently create, administer and integrate documents like functional descriptions, specifications, and memos. Various editing tools like Microsoft Word or Microsoft Excel can be used, depending on the dedicated purpose or existing installation. These tools mentioned are not part of Document Builder, but are assumed to be installed, and are supported by Document Builder.

2.4.3 AMPL Control Configuration

AMPL Control Configuration is a suite of builders necessary to configure Safeguard 400 Series, as well as other ABB controllers. The products run on Windows NT.

AMPL Control Configuration includes the following components:

- Application Builder
- Function Chart Builder
- Bus Configuration Builder

Two options which extend the functionality of AMPL Control Configuration are available,

- On-line Builder for on-line configuration and download of the Safeguard 400 Series applications.
- Optional AMPL PC (Process Control) and DB (Database) Element Libraries including the PC and DB element libraries and reference manuals for Advant Controller 400 Series

(Advant Controller 410 and Advant Controller 450) and Advant Controller 100 Series (Advant Controller 110, Advant Controller 70 and Advant Controller 55).

Product Benefits and Features

AMPL Control Configuration provides, together with the options, the following features:

- Administration of nodes, Circuits and Type Circuits simplifying project start-up and reuse
- Off-line editing with powerful cut/copy/paste
- On-line editing for rapid program modifications
- Target system control for easy testing of installed system
- Module diagnosis

In cooperating mode it supports much more features like:

- Support for the Advant Object concept including parameterized data in Circuits and Type Circuits

Type Circuits

Recurring process control tasks can be solved once by using type circuits.Type circuits are user-defined, configurable process control solutions which are pretested and stored in libraries on different levels (e.g. project level, organization level etc.). They can be reused whenever a similar task occurs again. Using well-tested and standardized type circuits increases the quality and the project efficiency and reduces maintenance efforts. The main difference between the Type Circuit and the UDPC function block (described in Section 1.4.3, Application implementation) is that a UDPC function block resides as a function block when loaded in a Safeguard 400 Series controller while a Type Circuit is expanded when loaded in a Safeguard 400 Series controller.

Type circuits consist of standard PC and DB elements. Symbols and terminals are formal parameters of type circuits. They allow to adapt each instance of the type circuit to the specific function needed.

2.4.3.1 Application Builder

Application Builder is the navigation tool for working in the independent mode. It handles the Safeguard configuration data. For detailed information about the independent mode,

Creating Advant Objects is not possible in this mode. Nevertheless, aspect type data for configuration, such as projects, nodes, Circuits, and Type Circuits are handled by Application Builder.

From within Application Builder the tools Function Chart Builder, On-line Builder, Bus Configuration Builder, and a text editor (for example AS100-EDIT) can be started. Application Builder can store default values to be used throughout a whole project. Application Builder assures that you always work on the application data with the correct Builder version. It supports exchange of configuration data between different nodes and across different projects.

2.4.3.2 Function Chart Builder

General

Function Chart Builder provides an easy-to-use environment for application programming of ABB controllers. It supports Advant OCS controllers as well as Safeguard 400 Series. It offers efficient methods of object oriented project engineering by supporting Type Circuits and Circuits. In the cooperating mode these entities are mapped to control aspects of Advant Objects, for example, the Type Circuit and the Circuit aspect. This ensures a high software quality and low maintenance efforts. It can be used in both cooperating and independent mode.

User Interface

With Function Chart Builder it is possible to have several windows open at the same time. For example, the user can create a DB element while working in the function chart representation. In addition, the tree representation can be open to keep control over the whole control logic. Multiple PC section windows can be opened, which is especially useful when working with large AMPL programs. Scrolling within each section window to inspect and connect different parts of that AMPL program at the same time is possible. To adjust the view to the interesting part of the control logic, zooming is supported.

2.4.3.3 Bus Configuration Builder

Function Chart Builder supports the possibility to store bus configuration data of Advant Fieldbus 100 objects.

2.4.3.4 On-line Builder

On-line Builder is the tool for configurating, commissioning and testing applications for Advant Controller 400 Series, Safeguard 400 Series, MasterPiece 200/1, MasterPiece 51, MasterGate 230/1 and Advant Operator Workplace.

Basic Functions

- Selection of target system
- Command file handling
- Symbol handling
- Performance analysis
- Backup and restore of application data
- Post-Mortem Analysis
- AMPL source code editing and handling
- Trend Recording
- Direct connection to Advant Controller 400 Series and direct connection to Master Bus 300 with possibilities of remote communication to other controllers is supported

- On-line Builder is split into a client and server part. Only the server part needs to be connected to an Advant Controller 400 via Advant Station 100 Series Engineering Board. Any On-line Builder - one at a time - running on a networked PC connected via TCP/IP with the On-line Builder server can use this server to access Advant Controller 400 Series.

Configuration and Programming

The following functions are included:

- Dimensioning of database and AMPL program areas
- Database population
- Application program entry, editing, and on-line modification of AMPL programs during program execution
- Application program and process database documentation, in graphic or list form
- Source code loading and dumping of application programs and database contents
- Testing and fault tracing
- Dynamic display and trend recording of variables; display and modification of parameters
- Forcing of inputs and outputs
- Reading/setting of date and time.

For information on Optional AMPL PC and DB Element Libraries and Computer Aided Electrical Engineering etc, refer to Advant Engineering Products Product Guide 3BSE 014 966R601.

2.4.4 Computer Aided Electrical Engineering

The products of Computer Aided Electrical Engineering (CAEE) efficiently supports the tasks of electrical engineering.

The user can decide on a project by project basis to work either in cooperating or independent mode. The project data of the independent mode can be reused in cooperating mode, if the Advant Objects with their Electrical Aspects are created later on.

2.4.4.1 Electrical Diagram Builder - Wiring Builder

Electrical Diagram Builder - Wiring Builder supports the electrical plant engineering process. The main functions of the Electrical Diagram Builder are:

ï editing of different electrical diagrams with a bi-directional database connection, making the diagrams live engineering documents,

- handling of documents such as electrical diagrams and reports,
- handling of product data for electrical equipment.

Diagram editing is supported using the power and performance of AutoCAD Release 14, enhanced by additional, comfortable drawing functions for electrical diagrams, such as circuit

diagrams, connection diagrams, layout diagrams, and overview diagrams. Different symbol libraries are available for different types of diagrams.

The title block and symbols in a diagram can be updated from attribute values in the database and vice versa.

2.4.5 AdvaBuild Safety Builder

The AdvaBuild Safety Builder is an engineering tool for designing and documenting Cause & Effect matrices. A Cause & Effect matrix is a presentation of the relation between a set of process inputs and the actions they trigger (outputs). The AdvaBuild Safety Builder is only available for Advant Station 100 series Engineering Station.

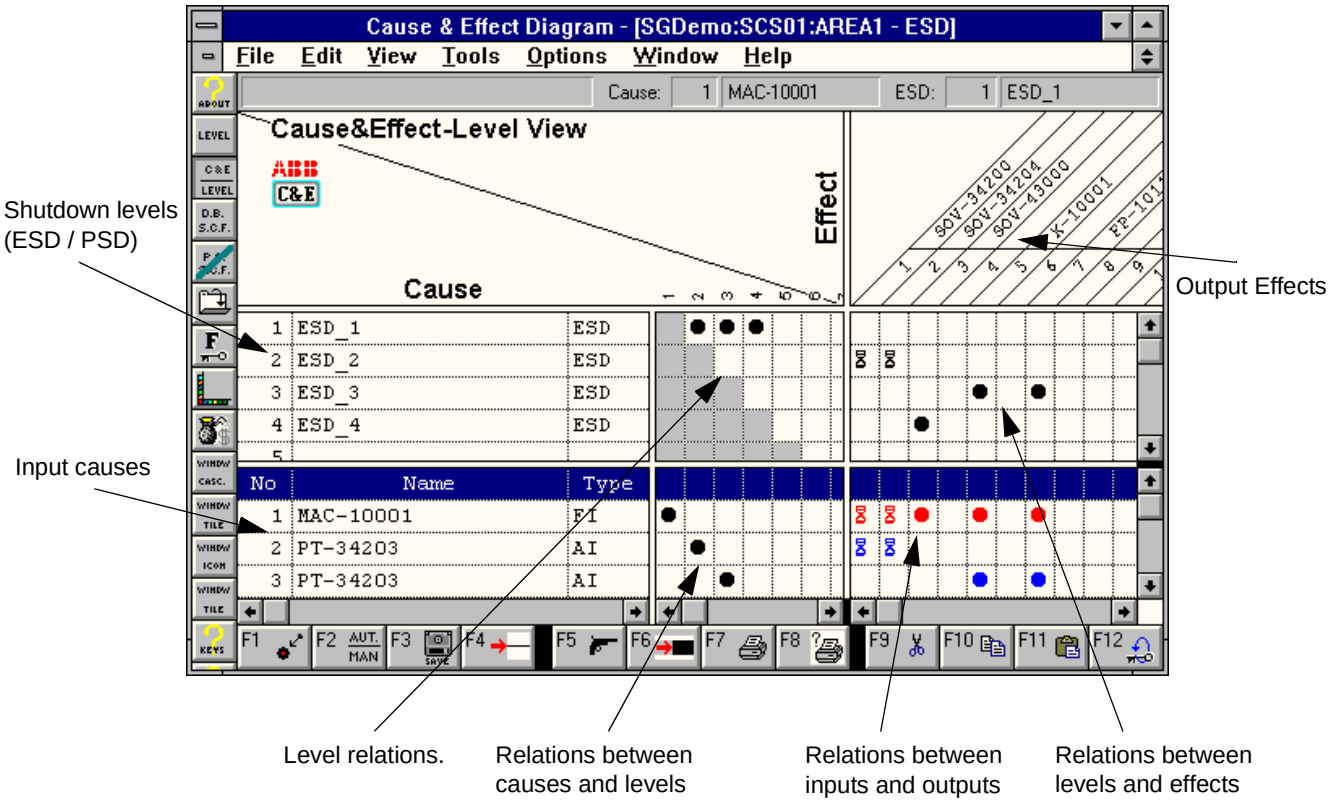

Figure 2-10. Safety Builder default display

This configuration method saves manual work and reduces possible errors in translating the C&E chart to logic element representation, and provides additional functions such as automatic definition of shutdown levels and automatic transfer of remote shutdown level and input status between control units in a network.

The Safety Builder allows database entry and configures connections between inputs, function blocks and causes as well as effects, function blocks and outputs. A function block is not needed between the C&E matrix and the input/output. The connection can be

direct if additional processing above the basic mechanisms provided in the database is not needed.

The following figure shows the definition dialogue for outputs to C&E effects:

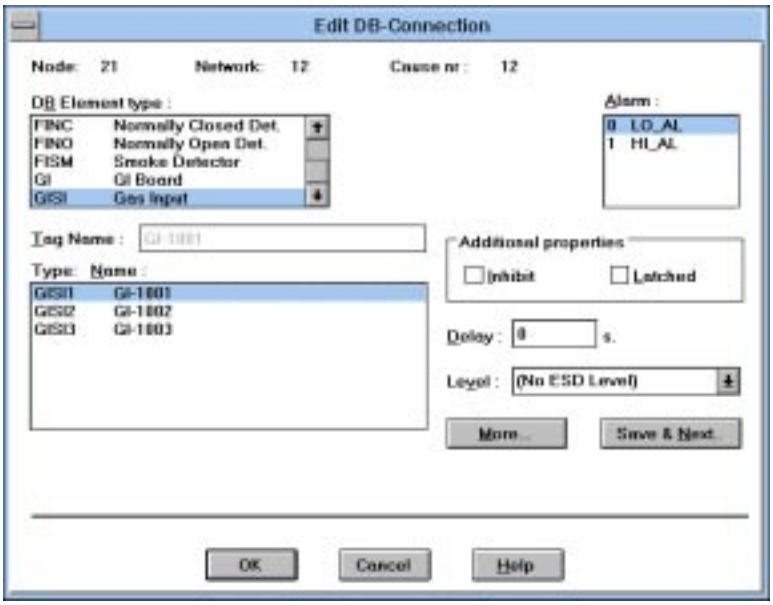

Figure 2-11. Cause definition dialog box.

2.4.6 Safeguard Configuration Builder

Safeguard Configuration Builder is a tool used to configure the parameters that control the start-up and monitoring of safety functions as well as Cause & Effect communication. After the user selects various parameters from drop-down menus and lists, the tool will automatically generate the necessary configuration file.

2.5 Communication software and functions

2.5.1 MasterBus 300

Outline description

MasterBus 300 is used to interconnect Advant Station 500 Series and MasterGate 230/1 stations in a plant network. In a control network MasterBus 300 is used to interconnect Advant Station 500 Series, MasterView 800/1 Series, Advant Controller -and Safeguard 400 Series, MasterPiece 200/1, and MasterBatch 200/1 stations. It provides high-speed, high-performance communication over medium distances.

MasterBus 300 is based on the IEEE 802.2 class 1 connection-less unconfirmed data link service protocol, and IEEE 802.3 CSMA/CD (Carrier Sense Multiple Access/Collision Detection) medium access control. In short this means that there is no specific master station, but all stations have equal access to the bus. A connection-oriented transport protocol according to ISO class 4 ensures flow control and reliability.

Network configurations

Up to 45 stations can be connected to a MasterBus 300.

The following figure shows an example of a control network configuration based on MasterBus 300.

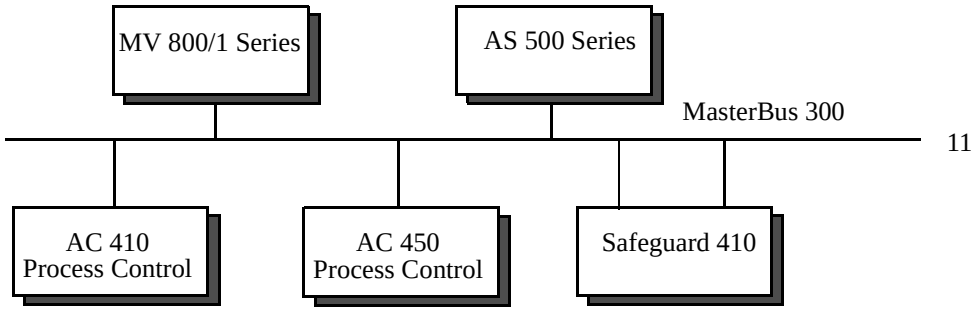

Figure 2-12. Control and safety network with MasterBus 300

To ensure availability of data communication also when a cable or a communication unit fails, MasterBus 300 can be duplicated. This is illustrated in the figure below. Note that all stations are connected to both buses to achieve fully redundant communication links.

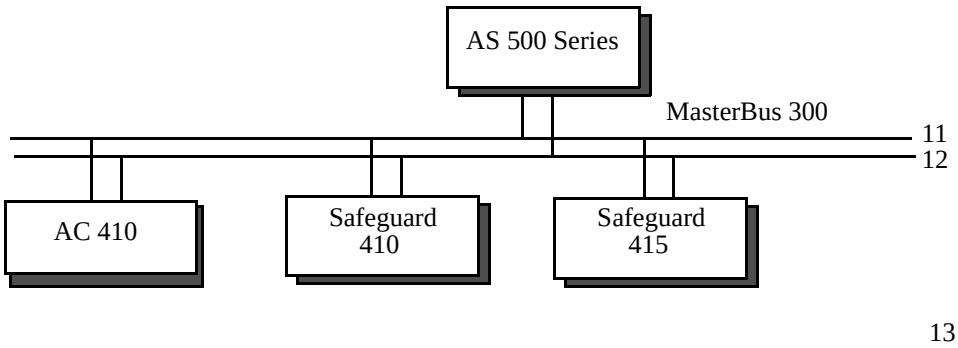

Figure 2-13. Control and safety network with redundant MasterBus 300

NOTE

For proper safety system integrity, a redundant communication system is required.

Performance

The transmission rate is 10 Mbits/second. This gives an effective data transfer rate of approximately 2000 packets/second, where the length of each packet is up to 300 bytes. This capacity is sufficient for all situations that can occur in an Advant OCS network with up to 45 stations.

2.5.2 RCOM/RCOM+

Outline description

RCOM/RCOM+ (Remote COMmunication) provides multi-drop, point-to-point or telecommunication capabilities (dial-up connections, e.g. over public telephone networks).

Traffic on an RCOM/RCOM+ link is controlled by a master station. Direct communication is possible only between the master and the slaves.

Stations connected via RCOM/RCOM+ appear in the Advant OCS system as stations in a MasterNet local control network.

The difference between RCOM and RCOM+ is that RCOM uses the Break character to alert a slave, while the RCOM+ uses a special character combination, up to 24 DAT's and a safer check sum calculation (CRC 16).

RCOM+ is used together with modems that do not reproduce the Break character. In communication with MasterPiece 40 and MasterPiece 200/1 RCOM shall be used.

The following RCOM/RCOM+ functions are examples of functions performed in master mode:

- Polling of event from the slaves
- Read and Write command to the salves
- Clearing of the event queues and Setting of the clocks in the slaves
- Blocking and Deblocking of the slaves.

The data transfer is performed using packets of data (Data Sets). Time stamped events can be transferred from slave to master.

Up to 8 slave nodes can be connected in an RCOM/RCOM+ configuration for Safeguard 400 Series.

Performance

RCOM/RCOM+ operates at a speed up to 19 200 bps. The communication speed and data throughput depends on the physical media for communication and the controller in which the module is mounted.

2.5.3 MVI-MODBUS

Outline description

The Gould Electronics MODBUS communication protocol can be used when the Safeguard or Advant OCS system communicates with other systems. The connection is of point-to-point or multi-drop type and the board can act as master or slave. Both RTU (that is binary) and ASCII modes are supported.

Equipment requirements

Safeguard 400 Series must be equipped with a communications submodule in order to use the MVI-MODBUS protocol. The submodule can be of the type CI534V02 or CI532V02.

Network configuration

The transmission speed is up to 19200 bits/s Traffic on the MVI-MODBUS link is controlled by the master station. Direct communication is only possible between the master and the slaves. Safeguard 400 Series can act as both a master or as a slave station.

2.5.4 AF 100

Outline description

Advant Fieldbus 100 is a high speed communication link intended for communication between an Advant Controller - and Safeguard 400 Series, Advant Controller 110, Advant Controller 70, Advant Controller 31-S, S800 I/O Station, AdvaSoft for Windows and other equipment adapted for the bus. Besides the ABB control products, converters for motor drives can be connected to the bus. Units connected to the bus are denoted stations.

Advant Fieldbus 100 is a high-performance bus specifically designed for real time applications. It features reliable, cyclic (deterministic) data transfer (using Data Set Peripherals), cyclic data transfer between S800 I/O station(s) to an Advant Controller -and Safeguard 400 Series as well as event-driven background transfer of service data.

Cyclic data is deterministic in time and size.

Advant Fieldbus 100 is mainly installed with electrical medium, coaxial or twisted pair.
To allow distances longer than 700 meters (coax) respectively 750 meter (twisted pair), optical medium is used.

Bus lines may be single or redundant, when redundant lines are used all parts of the bus must be redundant. When optical media is used redundant lines can not be used. If redundant lines are used, the communication interfaces monitor the two lines and automatically select the “working line” in case of a fault in the bus interface or a broken cable.

Advant Fieldbus 100 features a master scheme, distributed to one or several communication interfaces on the bus, such interface is denoted Bus Administrator (BA). One of the Bus Administrators is master, while the others are back ups. The master Bus Administrator controls the traffic on the bus, concerning the master scheme, by polling data to be sent.

The communication module in the controllers supports the exchange of data by cyclic data communication and the message transfer.

Network configurations

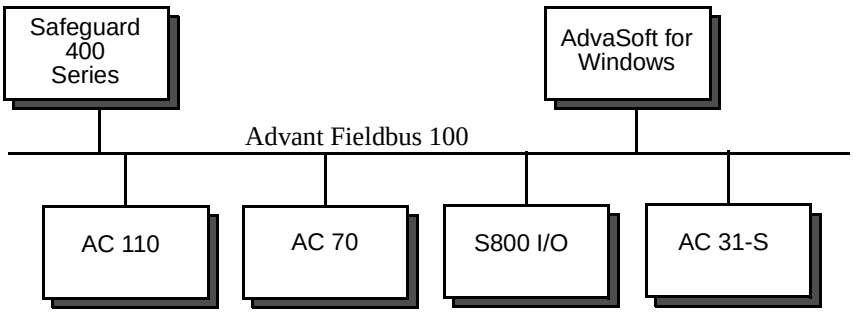

Figure 2-14. Advant Fieldbus 100

On Advant Fieldbus 100, service data is transferred in background mode and is automatically initiated when required. It does not disrupt or delay cyclic data communication.

Up to 80 stations can be connected to a bus.

Performance

The transmission rate is 1.5 Mbit/second. Cyclic communication is user configured by means of Cyclic Data Packets (CDPs), each corresponding to a Data Set Peripheral. Cyclic data packets are configured to be transferred on the bus with cycle times of 1, 2, 4, 8,...,4096 ms and with size of 2, 4, 8, 16, and 32 bytes. Cyclic Data Packets are broadcasted on the bus. Cyclic data transmission can use up to 75% of the total bus capacity. The remaining 25% is reserved for message transfer. If not used for cyclic data, up to 50% of the bus capacity can be used for message transfer. Message transfer is used for e.g. event handling or remote access.

Any unit on the bus can be removed from the bus and be replaced without disturbing other stations on the bus or their communication with each other. Communication with a reconnected unit is resumed automatically.

2.6 Application Software

2.6.1 General

In order to make application engineering less complicated, ABB has assembled a series of application units, which enable the user to configure operator station displays and application logic through the use of display elements, dialogs and user elements (which are PC elements specific to the application in question). Application Units generally consist of:

- Display Elements and Dialogs for applications specific to Safeguard for the Advant Operator Workplace. These display elements and dialogs are not included in the Safeguard option in the Operator Workplace.
- User elements are the preferred library of elements for safety-specific application logic. The elements are predefined by means of the UDPC (User defined PC elements) utility. The term ‘User Elements’ (abbreviated UE) is used to distinguish these elements from standard PC elements.
- User defined events are event texts.
- A manual, which describes and lists all features and aspects of the application unit in detail, and instructs the user in how to configure it.

2.6.2 Application unit

A number of application solutions are available as re-usable application units that contains presentations, dialogs, user defined PC elements accompanied by a manual that describes the parameterization and use.

- Fire & Gas
- Shutdown
- High integrity dual loop control (HIDL)

2.6.2.1 Fire & Gas

Safeguard Fire & Gas protection technology, as a part of the ABB Safety concept, is an integral part of ABB’s open control systems. Fire and gas protection is implemented by integrating modern certified products for fire & gas detection, and using standardized, high performance plant network solutions in combination with Safeguard 400 Series controllers. The application unit for fire and gas protection contains elements and instructions designed to allow uncomplicated configuration of fire and gas protection systems.

2.6.2.2 Shutdown

Shutdown, whether Emergency Shutdown or Process Shutdown, is a vital part of contemporary safety technology. The application unit Shutdown is designed to supply application-specific user elements, display elements, dialogs and instructions on how to structure the cause & effect logic.

2.6.2.3 High Integrity Dual Loop

The application unit High Integrity Dual Loop is an extension of the functional unit AO (Analog Output), making it possible to implement analog outputs in dual systems, with 0-20 mA electrical output interface. Also included is the possibility for implementing control loops with the functional unit PIDCON in dual systems. The application unit HIDL comprises necessary functions for presentation, operation and maintenance of a control loop.

- Scanning of inputs from analog transmitters
- Control loops including PIDCON
- Analog outputs
- Monitoring of output loop for loop faults
- Internal board testing and fault detection
- Single/dual switch over functions
- Operator station functions.

Chapter 3 Hardware Functions

3.1 General Information

Safeguard 400 Series consists of Safeguard 410 and Safeguard 415. Safeguard 410 is a compact 1 rack (per branch) version and Safeguard 415 can be configured with up to 3 racks (per branch). The controllers are based on Advant Controller 410.

The hardware consists of processor modules, sub-modules, sub-racks, and power supplies. The central sub-rack differs slightly for Safeguard 410 and Safeguard 415 (bus expansion included for Safeguard 415), but the processor modules are identical.

The Safeguard 400 Series complies with the design standard 1oo2D (one out of two) and 1oo1D (one out of one), two of the designated architectures for safety systems defined by the IEC 61508, the international standard for functional safety.

The main difference between 1oo1D (also known as Single Safeguard) and 1oo2D is:

- 1oo2D has two independent controller branches for processing and diagnostics of the signals.
- 1oo1D has one controller branch for the same purpose.

3.1.1 Safeguard 410

The processor module and S100 I/O cards in Safeguard 410 are fitted into the same central S100 I/O sub-rack. The processor module used is named PM150V08 and has the following characteristics:

1. The CPU board contains a Motorola MC68020 processor and dynamic read/write memory (RAM) with ECC (Error Correction Circuit). The memory houses the system software as well as the user application. The CPU board is delivered with PM150V08 which is a 8 MB dynamic read/write memory version.
2. One slot for flash memory Program Card holding the safety system software.
3. Two RS-232-C ports dedicated for printer and MasterView 320
4. One port dedicated for connection of Advant Station 100 Series Engineering Stations
5. Four slots for communication sub-modules, two slots are configured with MB300 interface.
6. Direct access to Fireguard and Autronica addressable detector systems connected via the communication sub-module slots.

3.1.2 Safeguard 415

The processor module and S100 I/O cards in Safeguard 415 are fitted into the same central S100 I/O sub-rack. Safeguard 415 can be equipped with two additional S100 I/O sub-racks. The

processor module used for Safeguard 410 /415 are identical and have the same characteristics except for point 6 which will be as follows:

6. Direct access to up to 54 S100 I/O cards (or 52 I/O cards in a certified system) located in the central S100 I/O sub-rack and two S100 I/O sub-rack.

3.1.3 Input/Output hardware

In Safeguard 400 Series two different I/O systems are utilized, local and distributed. The local I/O system is named **S100 I/O** and distributed I/O system is named **Addressable detector systems** and have the following characteristics:

- **S100 I/O** is a board based I/O system. The I/O boards are placed in I/O sub-racks. The process cables are connected to connection units which are connected via dual standard cables to the I/O boards in each branch of the Safeguard 400 Series.
- **Addressable detector systems** is an addressable fieldbus based fire system for fire data acquisition. The fire detectors are connected on addressable loops which are terminated in Fire local panels. The fire units are connected via dual RS232 based protocol links to sub-modules in the CPU-unit in each branch of the safety system

3.2 S100 I/O

The S100 I/O system is used for Safeguard 400 Series

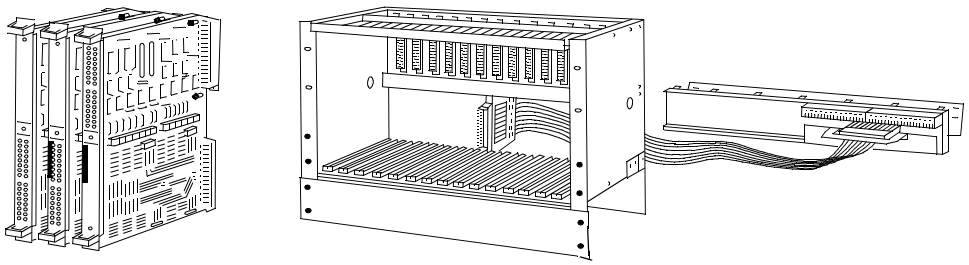

Figure 3-1. Sub-rack configuration

The S100 I/O system consists of I/O boards with 4 to 32 channels, depending on type. The boards are placed in I/O sub-racks with the following dimensions:

Width: 482,6mm (19”)

Height: 347mm (13.7”) (including cable duct)

Depth: 335mm (13.2”)

The sub-racks are mounted in cabinets and are fitted with guide bars for I/O boards and other plug-in units. Each board is connected to the back plane of the rack. One or several connection units with screw terminal blocks for connection of the process cables are provided for each I/O board. The connection units are connected with the I/O board via standard cables and are normally mounted in the rear part of the cabinet.

The connection units have additional terminals for power distribution to sensors and actuators. For analog inputs the connection units also include current shunts. This feature makes it possible to exchange analog input boards without breaking any current loops.

Digital I/O boards have LED indicators showing the status of each channel. Analog input units have a LED indicating completion of each A/D conversion.

Diagnostic functions are executed for all I/O boards at system start-up and during normal operation. Any fault detected is indicated by a LED on the I/O boards face plate, and by a system error message reported to Advant Station 500 Series Operator Stations or to Advant Station 100 Series Engineering Stations connected to the controller concerned.

The analog input signals are protected against over-voltage and hf-filtering by the connection unit. A low-pass filtering amplifier with programmable gain and A/D conversion is handled on the AI-board. The amplifier can be programmed to handle a wide range of voltage and current inputs, 4-20mA, 2-10mA, 0-±10mA, 0-10V, 0-±10V, 0-5V, 0-±5V and so on depending of type of I/O-board and connection unit.

For some of the digital input boards local time tagging on the input board are available for process events, thus providing a very good time resolution.

I/O boards can be exchanged while the system is running. New boards and functions can be added while the system is in operation.

The total range of safety I/O sets in S100 I/O are presented in tables in Section 4.4, Reference Guide.

3.2.1 Input subsystem

The local input subsystem are S100 I/O input cards mounted in the S100 I/O sub-rack. Local inputs are available in the following types:

1. DSAI 160 for the following type of signals:
    a. Normally-Open (NO) - loop monitored digital inputs (contacts)
    b. Normally-Closed (NC) - loop monitored digital inputs (contacts)
    c. Smoke/heat detectors with electrical reset pulse
2. DSAI 165 for electro-catalytic gas detectors directly connected
3. DSAI 130 (analog inputs, differential 12 bit), current or voltage loop
4. DSAI 133 (analog inputs, single ended 12 bit), current or voltage loop
5. DSAI 133N (safety analog inputs, single ended 12 bit), current or voltage loop
6. DSAI 110 (analog inputs, single ended 8 bit), current or voltage loop
7. DSDI 110A (digital input, scanning or interrupt controlled) 24 VDC
8. DSDI 110N (safety digital input, scanning or interrupt controlled) 24 VDC

All boards, except for points 7 and 8, are essentially analog in nature and use voltage level to detect the field signal status, such as Normal, Alarm and fault conditions, as well as value for the gas detectors and analog input sensors.

A common termination unit distributes loop power and provides signal termination, signal conditioning (e.g. current shunt) and signal splitting.

The signals are split to dual input boards, one in each safety controller, via separate cables. The input board uses high input resistance, typically more than 1 Mohm to prevent computer or board malfunctions from reaching the termination unit and hence affect the input signal or the other safety controller.

In the case of Single Safeguard, there is only one cable, and one input board.

Intrinsically safe field devices

For connection of intrinsically safe field devices in explosive hazard area, safety barriers are used. The input stage must be used with zener type (passive) AC barriers to allow the loop monitoring current to flow from the termination unit through the field device.

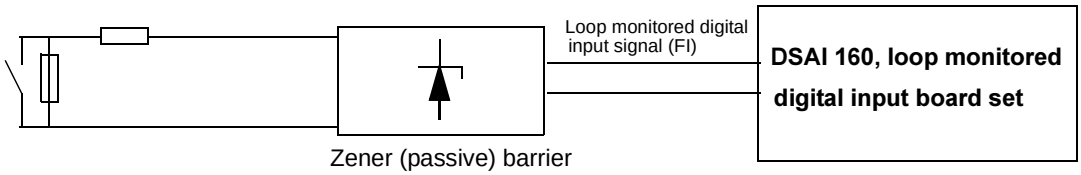

Figure 3-2. Loop monitored digital input with zener barrier.

If galvanic isolation barriers are used, the signal path will only be monitored from the barrier to the input board. In such applications, a galvanic barrier with loop monitoring connected to two digital inputs may be used

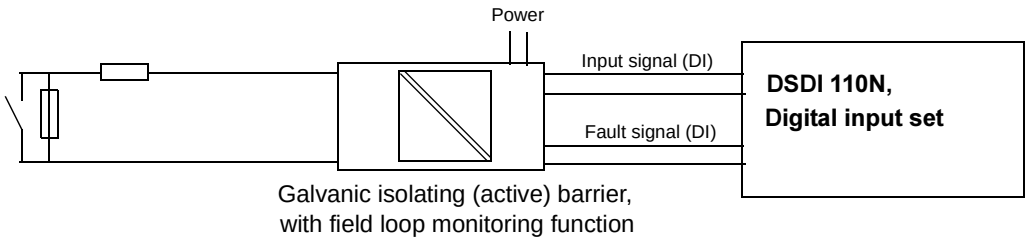

Figure 3-3. Digital input with galvanic isolation barrier

3.2.1.1 DSAI 160, loop monitored digital inputs

The loop monitored digital input set uses the 12 channel analog input board DSAI 160, and the termination board DSTD 170 with signal splitting. The signals are balanced differential ± 12VDC used for detection of the various faults and alarm conditions. The field power are supplied through the termination board and can be single or redundant.

The loop monitored digital input set is intended for

- Safety critical voltage free field contacts such as level/pressure switches or push-button.

NOTE

For loop monitoring purposes an end of line resistor and a serial resistor must be mounted in the NO/NC field contact. See Table 4-20 for ordering details on standard end of line and serial resistors.

- Conventional electronic heat, smoke and fire detectors.

In those cases where the field device has additional status or test contacts, these could be wired to status digital inputs.

The DSAI 160 has indicators on the front for common board fault and operation as well as indication of status, inhibit and loop fault individually for each channel.

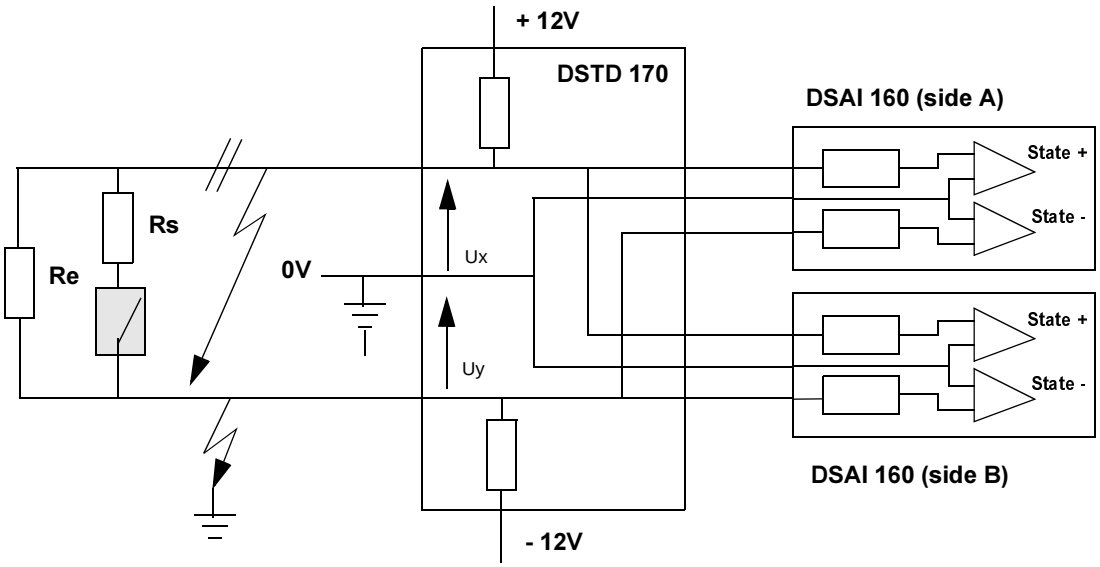

Figure 3-4. Principle diagram for DSAI 160 input set

The loop monitored digital inputs also allow several normally open contacts in parallel. This is primarily applicable for fire detection, where the input stage also provides reset for smoke detectors.

End of line and intermediate resistors are used to provide defined voltage levels that are detected by the input boards to reflect switch status and loop failure mode (cable break or short circuit). The balanced ± 12 V loop power allows earth fault detection without loss of contact status.

3.2.1.2 DSAI 165, Gas Inputs, catalytic detectors

The DSAI 165 board set allows direct connection to 3 or 4 wire electro-catalytic gas detectors (pellistors.). The unit comes complete with current generators as well as software function for calibration of the detector, and thus needs **no** external circuitry except the pellistor itself.

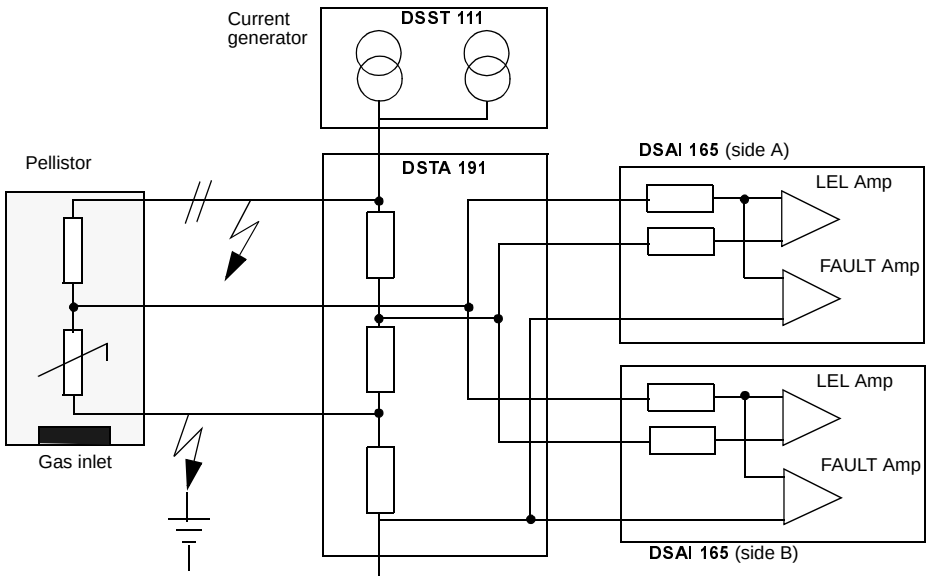

Figure 3-5. Principle diagram for DSAI 165 input set

The input stage accepts zero point and selectable test gas low explosive limit value during calibration and calculates the calibration correction values. Limit values can be set to prevent calibration when detector response is outside a given range, e.g. to prevent calibration of a contaminated pellistor. As an added feature, the firmware also calculates the normalized detector sensitivity to determine when the detector needs replacement. The interface can be programmed for different manufacturers' detectors and allows setting of system parameters such as detector warm up time.

The bridge voltage is converted to represent the gas concentration (% LEL) and checked against limits L and H. The input stage supports latched alarms and input inhibit functions.

With the DSAI 165, loop fault types are not separated, but appear as a common loop fault status for each channel, covering cable break, short circuit and earth fault.

The DSAI 165 has indicators on the board front for common board failure, operation and individual (per channel) indication of low limit alarm, high limit alarm, inhibit and loop fault.

3.2.1.3 DSAI 130, Analog Inputs

DSAI 130 is an analog input board, used with connection unit DSTA N001 or DSTA N002. The design of the two connection units are the same. The loop signals are connected to the connection unit. This unit contains terminals for connection of 16 differential 12-bit analog

input signals, as well as power distribution for field devices. Depending on which level of certification is required, the DSAI 130 input board can be configured in different ways.

3.2.1.4 DSAI 133, Analog Inputs

DSAI 133 is a 32 channel analog input board, which can also be used in pairs, for a redundant connection. It is used with DSTA 002A and DSTK 152.

3.2.1.5 DSAI 133N, Safety Analog Inputs

The Safety Analog Input (SAI) board used with Safeguard 400 Series is DSAI 133N.This is based on the DSAI 133 for the standard S100 I/O system. The connection units are made with dual connections. The DSAI 133N board is used with connection unit DSTA N040 (shunt resistor 2x125 ohm in series) which includes logic board DSTA N041.

The AI-board database configuration is equal to DSAI 133. Channel 32 is used by the SAI software for test values to indicate if field values or test values are applied on the other 31 channels.

The loop signals are connected to the connection unit. This unit contains:

- Terminals for connection of 31 single ended analog input signals. Power distribution for field devices.
- The logic board is equipped with circuits for generation of test signals, as well as logic which controls the sequential alternation between field values and test values.

The input board DSAI 133N contains:

- The hardware used is based upon a standard DSAI 133 board, with 32 channels. The AI-board starts to synchronize with the input channel test sequence as soon as the start-up phase is finished. When it is synchronized with the connection unit, cyclic diagnostics will be executed.
- Software to distinguish between test values and field values. The field values are updated every 248 ms.

The operation of the analog input board is monitored. The monitoring task executes with a cycle of one second.

3.2.1.6 DSAI 110, Analog Inputs

DSAI 110 is an input board, used with connection unit DSTA N012 or DSTA N013. The loop signals are connected to the connection unit. This unit contains terminals for connection of 32 single ended 8-bit analog input signals, as well as power distribution for field devices.

3.2.1.7 DSDI 110A, Digital Inputs

The DSDI 110A digital input set uses the standard, 32 channels 24VDC, DSDI 110A digital input boards and a DSTD N007 termination board with signal splitting. The field power are supplied through the termination board and can be single or redundant.

The digital input sets are used for digital signals such as status signals and non-safety critical signals.

3.2.1.8 DSDI 110N, Safety Digital Inputs

The Safety Digital Input (SDI) board used with Safeguard 400 Series is DSDI 110N.This is based on the DSDI 110A for the normal S100 I/O system. The connection units are made with dual connections. The DSDI 110N board is used with connection unit DSTD N030 with one or two logic boards DSTD N031.

The DI-board database configuration is equal to DSDI 110. Channel 32 is used as the test indication signal between the connection unit and the input board.

The loop signals are connected to the connection unit. This unit contains:

- Terminals for connection of 31 field input signals. Power distribution for the field devices.ï
- The field termination unit is equipped with logic boards for generation of test patterns. It can be configured with one or two logic boards. One logic board is used in single controller systems. With two logic boards, each board is generating independent test signals for each controller in a dual system. A yellow LED indicates that the test is running.

The input board DSDI 110N contains:

In addition to the verification of the test patterns from the connection unit, the digital input board performs several internal diagnostics.

3.2.2 Output Subsystem

The local output subsystem consists of S100 I/O output cards mounted in the S100 I/O sub-rack. Local outputs are available in the following types:

1. Master Vote 3000 safety digital outputs (24 VDC)
    a. Normally Energized (NE) outputs for e.g. shutdown valves
    b. Normally De-energized (ND) outputs for e.g. fire protection devices
2. DSDO 110 non fail-safe digital outputs, transistor type, for status outputs. (relay output)
3. DSDO 115 non fail-safe digital outputs, relay type, for status outputs. (24 VDC)
4. DSAX 110 analog I/O for PID control in high availability control systems
5. DSAO 130 analog output signals.

3.2.2.1 Master Vote 3000, safety digital outputs

The Master Vote 3000 output stage is a safety output unit designed to reduce output spurious trips to a minimum, while at the same time guaranteeing executive action on demand. The Master Vote 3000 units are designed to support extended and independent self-testing and monitoring functions, including associated field devices such as cables and actuators. The

system incorporates a fail-to-safe isolate function, and offers true output state read-back and continuous loop fault monitoring.

The Master Vote 3000 functions handle:

- One out of two output voting (1oo2D) in normal operation for Normally Energized (NE) and Normally De-energized (ND) signals.
- Performs active testing and diagnosis on itself and the processing units to control fault tolerant and fail-to-safe fall-back.
- Permits isolation of one branch for maintenance operations.
- Tests and/or read-back the field output loops to provide information on internal and external component malfunctions.

Normally Energized (NE) outputs power the field device during normal operation. Power is interrupted to cause shutdown action. These outputs are used for shutdown valves, fire dampers and similar devices where fail-to-safe action is required. The fail-to-safe action is to de-energize.

Normally De-energized (ND) outputs control field devices that are not powered during normal operation. Power is applied to cause action. These outputs are used for fire fighting, and alarming devices that do not require action on failure to take place. The fail-to-safe action is to remain de-energized.

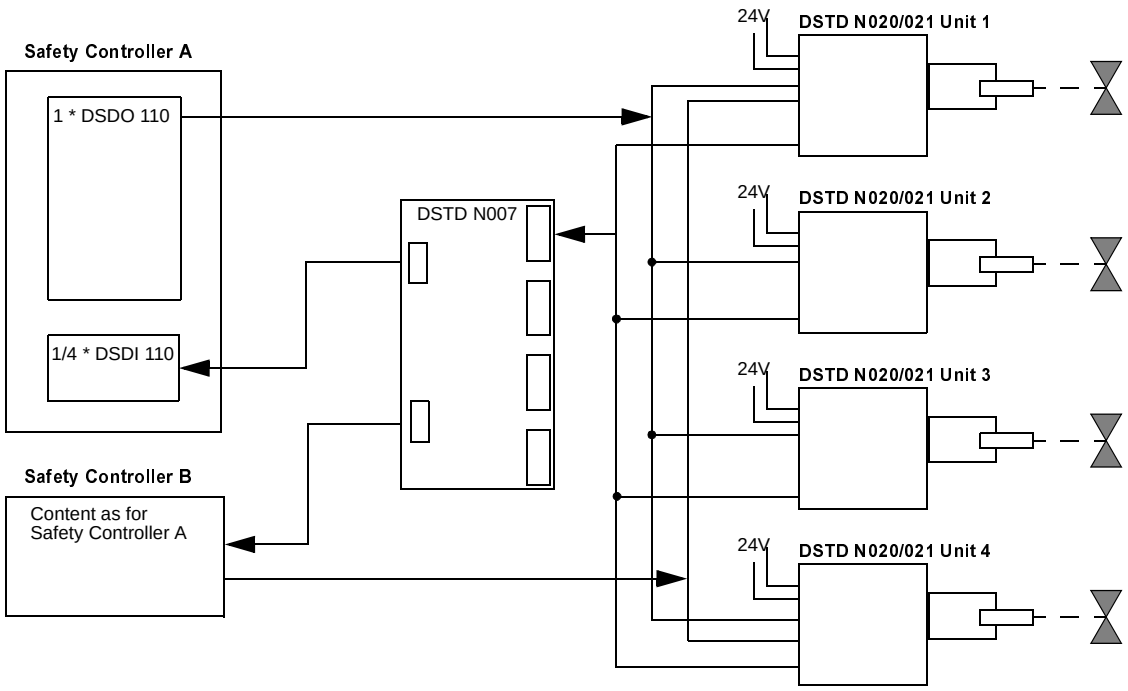

Figure 3-6. Master Vote 3000 Output Set for 1oo2D Systems

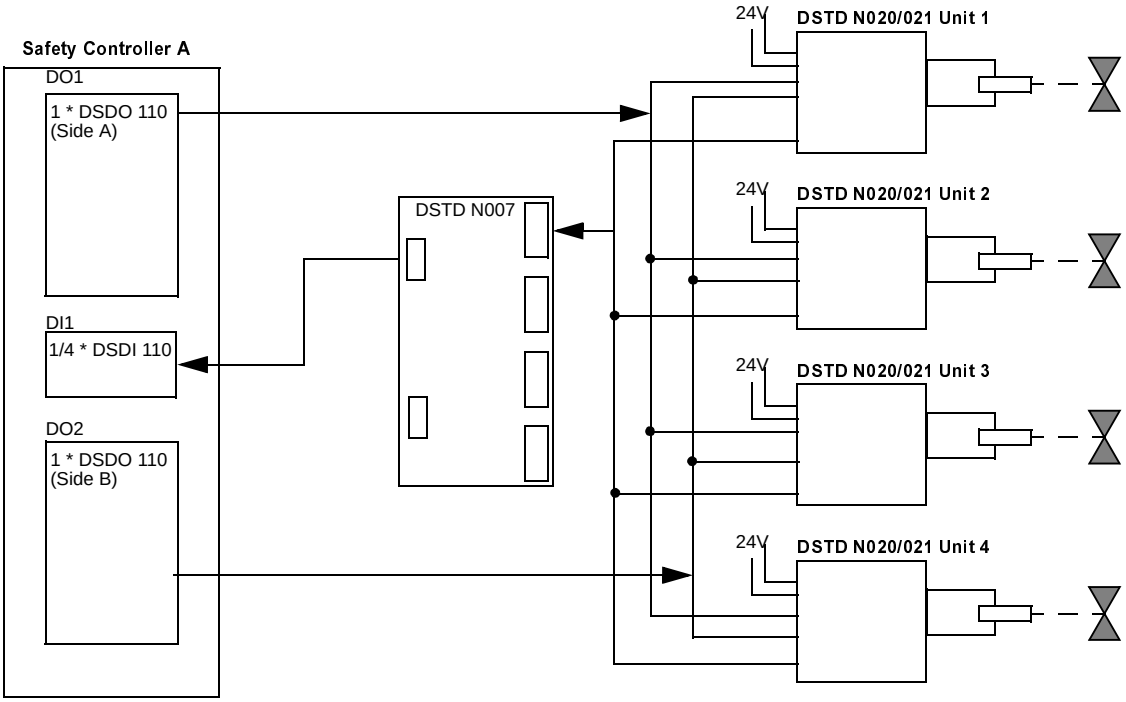

Figure C-7. Master Vote 3000 Output Set for 1oo1D Systems

The following hardware is required for a standard NE or ND Master Vote 3000 output set:

1. Two DSDO 110 digital output card with 32 channels, one in each controller side, for controlling four output stage termination units.
2. Four termination units, DSTD N020 for NE outputs or DSTD N021 for ND outputs. Each termination unit provides 7 field output channels. The termination units are connected to the digital output card with a 40-pole/split to 4x10-pole ribbon cable.
3. Two DSDI 110 digital input card with 32 channels per 16 termination units (that is per 4 Master Vote 3000 output sets) one in each controller side with one common termination unit DSTD N007, for the Master Vote 3000 output test program. Each termination unit gives 2 status feedback signals, one for channel test monitoring and one for isolate monitoring.

Normally Energized Outputs

The following figure gives an overview of the basic operation for a Normally Energized (NE) output.

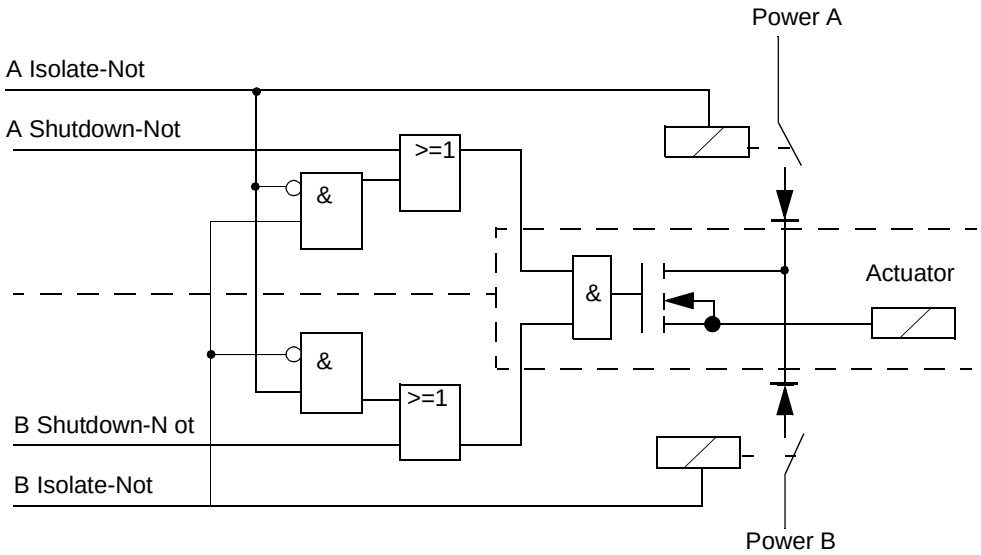

Figure 3-8. Master Vote 3000 Normally Energized principle

NOTE

In Single Safeguard systems, Side A and B are controlled by consecutive bioards in the same controller.

A logic state table for this circuit describes its operation. A/B Isolate-N (ISO-A, ISO-B) and A/B Shutdown-N (SD-A, SD-B) are the isolate and shutdown inputs from Safety Controller A (SCA) and Safety Controller B (SCB) respectively. The logic is negated, that is low (or zero) represents the activate signal state

The Master Vote 3000 has two power interrupting relays in the output power supply, controlled directly from the A/B Isolate-N. This allows either computer to disable its power feed to the unit. The function is used de-energize the output in case of a driver short circuit, or to isolate one system side for maintenance (Maintenance Bypass).

Normally De-Energized Outputs

The following figure gives an overview of the basic operation for a Normally De-energized (ND) Output.:

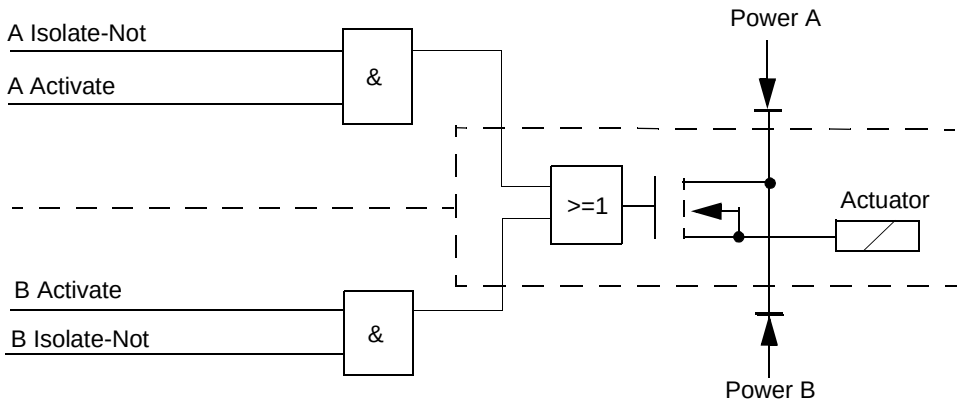

Figure 3-9. Master Vote 3000 Normally De-energized principle

NOTE

In Single Safeguard systems, Side A and B are controlled by consecutive bioards in the same controller.

A logic state table for this circuit describes its operation. A/B Isolate-N (ISO-A, ISO-B) and A/B Activate (ACT-A, ACT-B) are the inputs from Safety Controller A (SCA) and Safety Controller B (SCB) respectively. The isolate signal logic is negated (that is low is the active state).

Master Vote 3000 Options

For details see description in Section 2.1.6.2, Output testing.

Manual release

The Master Vote 3000 termination unit includes external output connections for hard-wired activation of the individual ND outputs. In this configuration, a hard-wired activation command will directly bypass the logic and cause a direct activation. Read-back and testing will detect the presence of a hard-wired command action.

3.2.2.2 DSDO 110/115, Digital Outputs

The DSDO 115 digital output set consist of standard, 32 channels, DSDO 115, digital output boards and a, DSTD N007, termination board with signal splitting. The 24 VDC transistor outputs are short circuit proof and can supply maximum 150 mA pr. channel.
The field power are supplied through the termination board and can be single or redundant.

The DSDO 110 digital output set consist of standard, 32 channels, DSDO 110, digital output boards and four, DSTD N010, termination boards with signal splitting.
The potential free relay outputs can break loop voltage from 24 VDC to 250 VAC.

The safety digital output sets are used for status indication and other non-safety critical signals.

3.2.2.3 DSAX 110, Analog Outputs/Inputs

Analog outputs are normally a process control function.

The Application Unit HIDL (High Integrity Dual Loop) is a method for implementing analog outputs and PIDCON (PID controller) in dual nodes when this is required for high availability control systems. The hardware needed to include this function is the DSAX 110 safety analog output and control set, which consist of the standard DSAX 110 analog input/output board with the connection unit DSTA 001A, and an additional control board AXTX N001.

3.2.2.4 DSAO 130, Analog Outputs

Analog outputs are normally a process control function.

The DSAO 130 analog output set consist of standard, 16 channels DSAO 130, analog output boards and DSTA N180 termination boards without signal splitting. Additional master/slave switch-over relay for loop control is required. The 8 bit analog outputs can either be 0-10 VDC or 0-20 mA. The field power are supplied through the termination board and can be single or redundant for both termination boards.

The analog output sets are used for status indication and other non-safety critical signals

3.3 Addressable detector systems

For ordering details on Fireguard and addressable fire detectors please contact ABB Industri AS, Norway.

3.3.1 Fire detection

The addressable fire inputs are connected via a fire panel. The fire alarm panel communicates with the Safeguard 400 Series. It is fully integrated with high functionality as a part of ABB Safety, and is connected through a link to each safety controller in the Safeguard 400 Series.

NOTE

Optical isolators or modems must be installed on communication links between Safeguard 400 Series and the Fireguard (or Autronica).

For ordering details of Fireguard and Autronica communication software please refer to Table 4-15, Software options.

3.3.1.1 Fireguard

Analogue heat, smoke (ionization and optical), manual call points and flame are all fire detectors which can be connected to the Fireguard fire alarm panel manufactured by Eltek. Each Fireguard contains 2 or 4 addressable loops with a maximum of 99 detector addresses per loop. The Fireguard can handle detectors in both non-hazardous and hazardous areas.

3.3.1.2 Autronica BS-100

Addressable fire inputs can also be connected via an Autronica BS-100 addressable fire alarm panel which also is supported by an individual protocol.

3.4 External Watch Dog

The function of the External Watch Dog is to interrupt the control power to the Master Vote 3000 termination units. It is only required if the controller is located in an installation which is unmanned for periods longer than the degraded mode time. The safety outputs from Master Vote 3000 are switched off if the External Watchdog is not triggered by the application engine.

3.5 Advant Engineering Workplace

Advant Engineering Workplace establishes the engineering environment for the AdvaBuild Engineering Software under Windows NT. Further engineering products can be added and extend the basic functions of the Advant Engineering Workplace by controller configuration functions and computer aided electrical engineering functions.

- Advant Station 130 Engineering Station for Windows NT
  - a ruggedized PC (Personal Computer) with AMPL Control Configuration software including options On-line Builder and AMPL PC, and DB Element Libraries for off-line engineering, on-line programming, maintenance and fault tracing of Advant OCS. Ideal for field work.
- Advant Station 100 Series Engineering Board
  - an ISA board which allows use of an appropriate IBM compatible PC together with AMPL Control Configuration products similar to an Advant Station 100 Engineering

station for off-line engineering, on-line programming, maintenance and fault tracing of Advant OCS.

3.6 Advant Operator Workplace

Advant Operator Workplace with AdvaCommand for UNIX and Windows NT represents a new approach to supervision and control of industrial processes. It does not only provide the capability to communicate with the process but also with other computers and systems outside the automation system. This information integration capability makes it possible to view both administrative data and process control data on the operator workplace.

Unix Hardware

Advant Operator Workplace for Unix is available as:

- Advant Station 520, a desktop workstation

It is based on the Hewlett-Packard 9000/700 series workstation with the HP-UX 10.20 operating system and it can have one or two monitors. It is equipped with a real-time accelerator board, including an optionally redundant interface to MasterBus 300/300E, ensuring real-time performance and response.

Each station constitutes one workplace. A workplace is equipped with one or two monitors, a operator keyboard or/and a standard QWERTY keyboard, a track ball or/and a mouse. There are also two models of track balls

- the standard unit with push-buttons for basic command entry - straight from the track ball
- the enhanced unit for a wider range of operator interaction.

Windows Hardware

Advant Operator Workplace for Windows NT shall run on a powerful PC workstation for Windows NT that combines real-time performance with an open system technology. The PC workstation hardware forms a base for the operator workplace.

The workstations used for Advant Operator Workplace for Windows NT should be equipped with a real-time accelerator board including an optional, redundant interface for connection to MasterBus 300/300E

NOTE

For continuously updated and more detailed information on which PC workstations ABB recommends for AdvaCommand for Windows NT, please contact your local ABB sales department.

3.7 Communication hardware

3.7.1 MasterBus 300

Physically MasterBus 300/300E is a multi-drop link built in segments with coaxial cable. The maximum length of one segment is 500 m (1640 ft.). A larger distance can be covered by connecting several coaxial segments with repeaters, if required with special point-to-point link seg-

ments between two repeaters, as shown in Figure 3-10. The maximum resulting cable length between any two stations on the bus, including repeaters and possible link segments between repeaters, is then five segments or 2500 m (8200 ft.) when using coaxial cable. Of these five segments, a maximum of three may be coaxial segments, the rest of the segments are link segments.

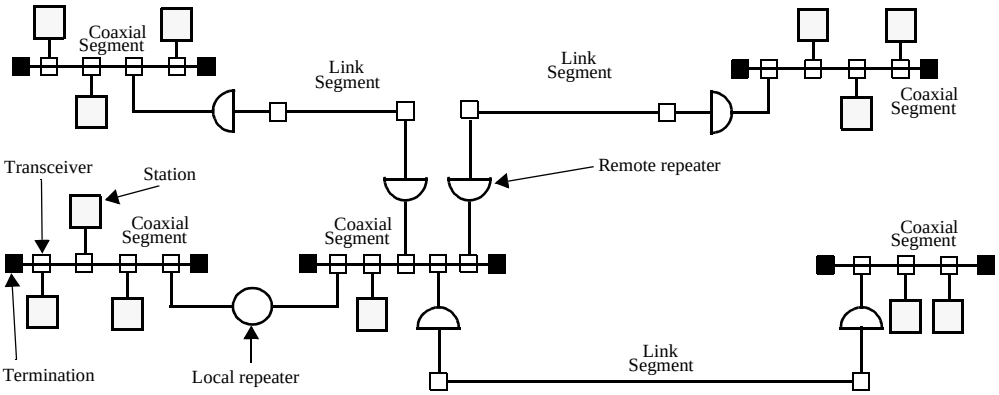

Figure 3-10. Using repeaters to extend the range of MasterBus 300

By using fibre optic cable in the link segments the maximum distance between two stations can be extended to 3500 m (11480 ft.). A fibre optic link segment can be maximum 1km (3280 ft.).

The distance between two stations can be increased even further by using an active star coupler. With active star couplers and fibre optic cables the maximum distance between two stations is 4500 m (14760 ft.). Active star couplers are supplied by other vendors than ABB.

Outdoor installation of bus cables requires special considerations. Please refer to the MasterNet User's Guide.

For ordering details of MasterBus 300/300E communication units, connection units, cables and transceivers, please refer to Table 4-17 in the Reference list section of this guide.

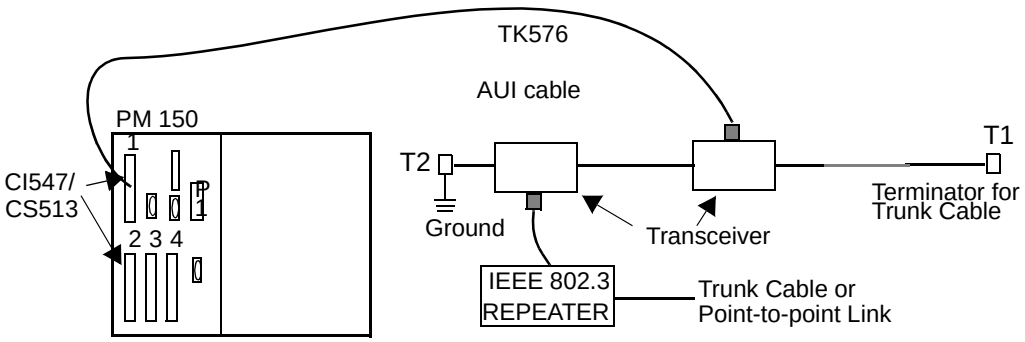

Figure 3-11. MB 300/300E Hardware in a Safeguard 400 Series controller

CI547

The CI547 communication interface is a replacement for CS513, the MasterBus 300 communication interface for Advant Controllers. Unlike CS513, CI547 contains its own microprocessor (CPU). This will reduce the load of the main CPU, since the load is independent of the number of nodes in the network. All routing messages will now be handled by the communications board directly.

3.7.2 RCOM/RCOM+

RCOM/RCOM+ links are connected to the controller by means of the communication board CI532V01 for Advant Controller 400 Series and Advant Controller 110.

Physical configuration

Physically RCOM/RCOM+ conforms to the CCITT recommendation V.24. The maximum permissible distance between end nodes, and other configuration details such as multi-drop, point-to-point or dial-up connections, depend on the choice of modem and cabling. The transmission speed depends on chosen hardware. The maximum RCOM/RCOM+ transmission speed is 19200 bits/s.

3.7.3 MVI-MODBUS

The MultiVendor Interface for Safeguard 400 Series is designated CI532V0X or CI534V0X, where “X” is a character indicating the communication protocol.

Physical configuration

Physically the MVI links conform to the CCITT recommendation V.24. Each Multi Vendor Interface has two communication channels with full IBM-PC modem support. The connection is a DE9S connector with a DTE interface. The maximum permissible distance between end nodes and other configuration details depend on the choice of modems and cabling.

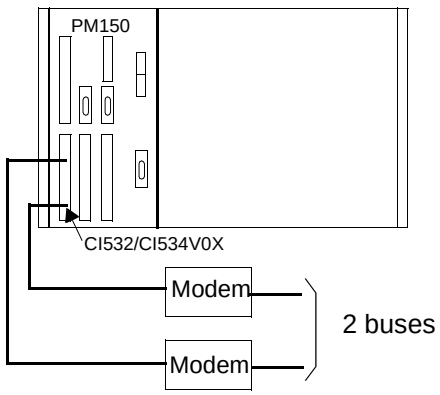

Figure 3-12. Safeguard 400 Series communication on MODBUS

3.7.4 AF100

The Advant Fieldbus 100 (AF 100) is a high performance fieldbus which is used for communication between Safeguard 400 Series and AdvaSoft for Windows and equipment developed and sold by other suppliers. Distributed S800 I/O stations can be connected via Advant Fieldbus 100.

Up to 80 nodes (79 AC 110, AC 70, AC 31-S, or S800 I/O Station) can theoretical be connected to one bus. For twisted pair cable theoretical 32 stations can be connected to each segment.

The bus has a theoretical maximum bus length of 2000 m (6561 ft.) but the actual bus length is depending on which transmission media is used. Three types of transmission media, coaxial cable, twisted pair (twp) cable and optical fibre are supported. The bus can be build up by several segments. Different segments are interconnected with the modems TC513 respectively TC630.

The cable types to use are:

- Coaxial cable, up to 300 m (984 ft.) per segment - RG59 B/U, 75Ω, Connectors: BNC
- Coaxial cable, up to 700 m (2296 ft.) per segment - RG11 A/U, 75Ω, Connectors: BNC
- Twisted pair cable, up to 750 m (2460 ft.) per segment, Communication media according to IEC 1158-2 fieldbus standard.
  Twisted pair cable used:
  Trunk cable: Belden - 1634, IBM type 1, 2 pair.
  Drop cable: Belden - 1642A, IBM type 6, 2 pair
  Connectors: e.g. Phoenix Combicon MSTB 2.5/4-ST-5,08
- Optical fibre allows the total bus length to be, up to 1700 m (5576 ft.).
  Dual 62.5/125µ or 100/140 Multimode graded index type,
  Connectors: Multimode ST Style.

Chapter 4 Product Configuration and Documentation

4.1 Application Program Configuration

The database contains a record (also called an object) for each of the many I/O points in the process. Configuration is done in the AdvaBuild Function Chart Builder.

The function blocks are used to provide extended basic treatment, such as handling of coincidence conditions, and design of typical solutions for protection systems (halon, deluge, sprinkler, water spray and so on) and actuator devices (sectioning ESD valves, blowdown valves and so on).

The cause and effect logic is designed with logic function elements (such as AND, OR) from the AdvaBuild Function Chart Builder or as a cause & effect logic matrix in the AdvaBuild Safety Builder.

The AdvaBuild Function Chart Builder is available for the Advant Station 500 and 100 Series Engineering station.

The AdvaBuild Safety Builder is available for the Advant Station 100 Engineering station.

4.1.1 Tools and procedures

The configuration tools comprise:

- AdvaBuild Function Chart Builder (FCB) that is used to
  - generate function block macros.
  - generate the application program and database
  - generate User Elements.
- AdvaBuild Safety Builder, an optional cause and effect application editor, that produces the cause and effect table.
- Target system functions in the AdvaBuild On-Line Builder, for up and downloading the application as well as measurement of system performance, fault tracing and so on
- Utilities, such as standard or custom import/export filters.
- The application source code files that are contained in a project library.

When configuring the system, one can choose three different procedures:

1. When design basis documentation is machine readable, it can be directly imported to source code format via import/export filters. Additional entry of function block macros is done in the Function Chart Builder (FCB). Set up of test programs, additional database data and verification of C&E data is performed with the Safety Builder
2. When design documents are on paper format, the cause & effect chart and database contents is built in the Safety Builder.

3. If the logic is not cause & effect oriented, import and configuration (application control program and database entry) is performed with the Function Chart Builder.

Database and AMPL storage formats and down-loads are reversible, so resident data in the target system may be loaded back to the FCB and even exported to an external system.

The operator station is configured with AdvaBuild on the operator station itself.

4.2 System configuration

The Safeguard 400 Series is delivered in standard 1 to 5 cabinet arrangements. The cabinet type is RM500 Series.

Single cabinet

The single cabinet contains two central sub racks in the upper half of the hinged frame, each containing CPU, memory and communication as well as space for a limited number of I/O boards and is normally used for Safeguard 410. Both the system and the field power supply racks are located in the lower part of the frame. The connection units for field inputs as well as for field outputs are located in the rear mounting plane.

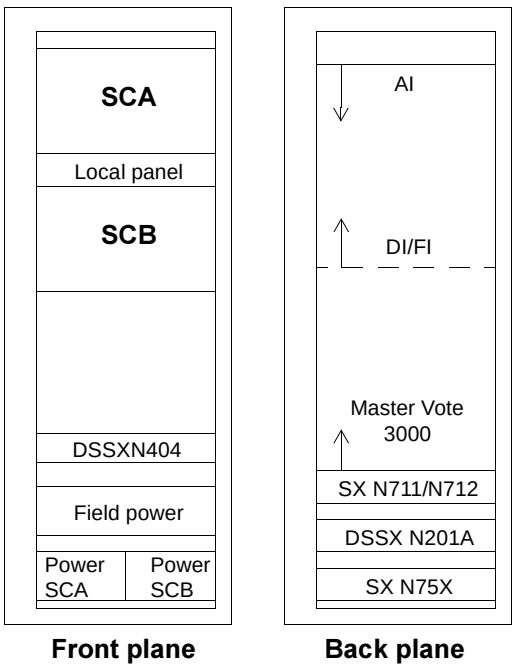

Figure 4-1. Single cabinet configuration(1)

(1) In certain cases (TÜV-certified systems), DSSXN404 can be replaced with SXN414

NOTE

In Single Safeguard systems (1oo1D), the section marked SCB will not be present.

Double cabinet

The double cabinet solution is used when the Safeguard 410 has a full I/O configuration, or when the Safeguard 415 is used.

Cabinet No. 1 contains two central sub racks, each containing CPU memory and communications as well as room for input boards, systema dn field power supply racks, tha connection unit for main supply and the power distribution unit for input termination units. This cabinet is primarily intended for field input connection units.

In Safeguard 415, Cabinet No. 2 contains the first I/O subracks, and in both the 410 and the 415 it contains an optional field power supply rack and power distribution unit for outputs, as well as connection units for Master Vote 3000 output modules.

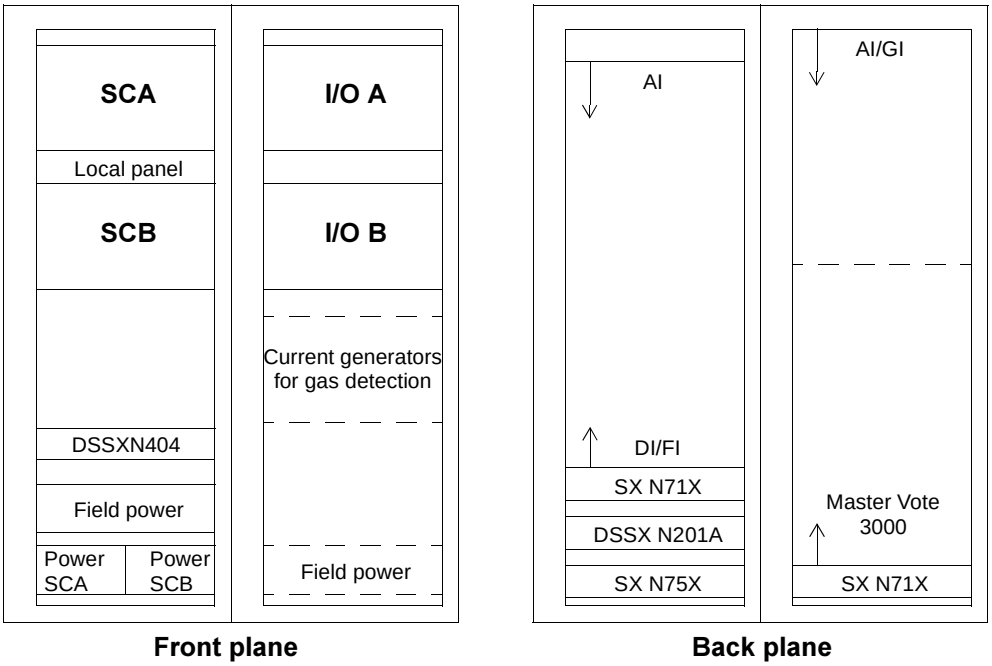

Figure 4-2. Double cabinet configuration(1)

(1) In certain cases (TÜV-certified systems), DSSXN404 can be replaced with SXN414

Additional I/O Cabinet

An additional I/O cabinet would contain an I/O sub-rack with a set of field power distribution units. Extra cabinets can be added to accommodate the field termination units.

NOTE

In Single Safeguard systems (1oo1D), the sections marked SCB and I/O B will not be present.

4.2.1 Safeguard 410/415 basic unit

The basic unit for Safeguard 410/415 consists of units according to the table below:

Table 4-1. Basic unit Safeguard 400 Series

Safeguard	Units(1)	Description
410/415	2 (1)* PM 150V08	Processor module with 8 Mbyte RAM
410/415	4 (0)* CS 513 or 4 (0)* CI 547	Redundant MasterBus 300 sub-modules
410/415	2 (1)* DSRF 185	I/O sub-rack for S100 I/O & process module
410/415	2 (1)* DSSR 122	Voltage regulator, 24 V/5 V
410/415	2 (1)* SB 171	Battery back-up charger unit
410/415	2 (1)* SB 520	Battery unit
410/415	1 (1)* DSHM 202	Local maintenance panel
410/415(2)	1 (0)* DSSX N404	Internal Supervision Distr.Unit
410/415(3)	1 (0)* SX N414	Internal Supervision Distr. Unit w/ watchdog function
415	2 (1)* DSTK 281	Bus extension cable for connection to DSTC 175 and to accommodate connection between extension rack 1 and central S100 I/O rack.
415	2 (1)* DSTC 175	Termination unit for supervisory signals.
410/415	1 * Documentation	3BNP000432R301 Safety Manual
410/415	Necessary parts	Delivery binders, service shelf, socket outlet etc.

(1) Numbers in parentheses concern Single Safeguard only
(2) Recommended standard installations.
(3) For unmanned installations, refer to Section 3.4, External Watch Dog.

The processor unit battery back-up are supplied by the SB 520 battery unit through the battery back up charger unit SB 171. The battery back-up time is minimum 4 hours.

For longer application back-up time, refer to PCMCIA PROM cards listed in Table 4-17. The PROM cards can be used to store system software or application programs.

The processor module PM150V08 have four slots for sub-modules built in. It can be equipped with sub-modules in accordance with the table below. The maximal number of sub-modules and sub-module buses allowed in processor module are also specified.

NOTE

The Safeguard 400 Series processor module is equipped with two MasterBus 300 sub-modules (CI 547/CS 513) each, leaving two free sub-module slots for additional communication.

Table 4-2. Available Sub-modules for PM150V08

Description	Consists of	Max. No. of modules	Buses per module	Max. No. of buses
Serial communication	CI 531 (1)	2	2	4
MasterBus 300	CS 513	2	1	Total 2
MasterBus 300E	CS 513	2	1	
MasterBus 300	CI547	2	1	Total 2
MasterBus 300E	CI547	2	1	
RCOM/RCOM +	CI 532V01	2	2	Total 4
MVI-MODBUS	CI 532V02	2	2	
MVI-MODBUS	CI 534V02	2	2	
Advant Fieldbus 100	CI 520	2	1	2

(1) This sub-module is used for RS232 communication to Fireguard and Autronica remote addressable systems

4.2.2 Safeguard 415 extension S100 I/O racks

The extension S100 I/O rack 1 and 2 for Safeguard 415 consists of units according to the tables below..

Table 4-3. S100 I/O extension rack 1 for Safeguard 415

Units	Description
2 * DSRF 182	I/O sub-rack 1 for S100 I/O
2 * DSSR 122	Voltage regulator, 24 V/5 V
2 * DSBC 173N 2 * DSBC 172N	Bus extension board for I/O sub-rack. Bus extension board for CPU-rack
2 * DSTK 183 2 * DSTK 281	Bus extension cable to accommodate connection between extension I/O rack 1 and central rack.

Table 4-3. S100 I/O extension rack 1 for Safeguard 415

Units	Description
2 * DSTK 185	Bus extension cable for connection between extension I/O rack 1 and central rack.
2 * DSTC 176	Bus termination unit.

Table 4-4. S100 I/O extension rack 2 for Safeguard 415

Units	Description
2 * DSRF 182	I/O sub-rack 2 for S100 I/O
2 * DSSR 122	Voltage regulator, 24 V/5 V
2 * DSBC 173N	Bus extension card for I/O sub-rack
2 * DSTK 183	Bus extension cable to accommodate connection between extension I/O rack 1 and 2.
2 * DSTK 185	Bus extension cable for connection between extension I/O rack 2 and 1

Table 4-5. Bus supervision units

Units	Description
2 * DSBS 116N	Bus supervision units

Table 4-6. Remote S100 I/O basic unit for Safeguard 415 w/ fiberoptic comm.

Units	Description
2 * DSRF 182	I/O sub-rack 2 for S100 I/O
2 * DSSR 122	Voltage regulator, 24 V/5 V
2 * DSBC 173N	Bus extension card for I/O sub-rack
1 * DSSXN404	Internal supervision distribution kit
1 * DSSXN407	CPU/run distribution kit
2 * DSTK 183	Bus extension cable to accommodate connection between extension I/O rack and modem.

Table 4-6. Remote S100 I/O basic unit for Safeguard 415 w/ fiberoptic comm.

Units	Description
2 * TK 575	Bus extension cable for connection between extension I/O rack and modem.
2 * TC 561	Fiberoptical modem

Table 4-7. Bus extension kit when using one I/O-rack

Units	Description
2 * DSBC172N	S 100 I/O Bus extender board
2 * TC 560	Fiberoptical modem
1 * DSSX N405	CPU/run-distribution
1 * RA 543	Modem bracket
2 * TK 580	Cables

Table 4-8. Bus extension kit when using two I/O-racks

Units	Description
2 * TC 560	Fiberoptical modem
1 * TK 560	Interconnector
1 * RA 543	Modem bracket
2 * TK 580	Cables

4.2.3 Available I/O unit positions

The following number of board positions are available: (Most article numbers take one slot in each redundant pair, thus the numbers can be added and compared with available slots below)

Table 4-9. I/O board capacity for Safeguard 410 and 415

Sub-rack set number	Description	No. of I/O slots
1	Central S100 I/O sub-rack for Safeguard 410 with CPU including memory and communication	15 (Certified system: 14)
1	Central S100 I/O sub-rack for Safeguard 415 with CPU including memory, communication and bus extension card	14
2	S100 I/O sub-rack no. 1 for Safeguard 415	20 (Certified system: 19)
3	S100 I/O sub-rack no. 2 for Safeguard 415	20 (Certified system: 19)

This means that the maximum number of I/O cards for Safeguard 410 are 15, and 54 for Safeguard 415. For certified systems the numbers are 14 and 52, respectively.

4.2.4 Capacity and performance

The following two tables define the maximum number of the various types of S100 I/O cards and the maximum number of the various signals allowed for a Safeguard 400 Series unit.

Table 4-10. S100 I/O and signal capacity in Safeguard 400 Series

Signal type	HW-capacity Max. S100 I/O Boards	SW-capacity Max. Signals
Gas inputs	32 (1)	618
Fire inputs	32(2)	862
Analog input	32(2)	910
Digital inputs inclusive status DI for Master Vote 3000 output set	48	2300
Digital output inclusive outputs for Master Vote 3000 output set	48	1489
Analog output	32(1)	963

(1) This total is a sum of gas input and analog output S100 I/O boards

(2) This total is a sum of fire input and analog input S100 I/O boards

Table 4-11. Master Vote 3000 Output set capacity

Safeguard type	Channel test type	HW-capacity Max. Output sets	SW-capacity Max. Signals
Single	Slow scan	10	280
	Fast scan	5	140
Dual	Slow scan	20	560
	Fast scan	10	280

For memory and load calculations, refer to the Safeguard 400 Series Safety Manual.

4.2.5 Master Vote 3000 output system configuration

Normally Energized (NE) or Normally De-energized (ND) Master Vote 3000 is ordered in sets of 28 output channels. For Dual Safeguard, each set consists of one output board (1 board slot) for each of the two controllers and four Master Vote 3000 units. For Single Safeguard, each set consists of exactly the same components, except that the two output boards are mounted into the one controller. Each Master Vote 3000 unit requires physically one third DSRA 111 Mounting bar. One SXN71(x) field power distribution unit per 2 Master Vote output sets (if 1+1 redundant) are also required. If N+1 redundant, one SXN71(x) is required per 4 Master Vote output sets.

For each **four** board sets, (that is 112 channels) one digital input board for test signals is required. Each uses one half DSRA 110 Mounting Bar as for most other I/O board set termination units.

If the ‘read-back’ option is required, one ‘loop status’ board is needed for each Master Vote 3000 board set (of 28 channels).

4.2.6 Addressable fire input configuration

The Safeguard 400 Series remote inputs can be physically connected on addressable loops to Autronica BS-100 or Fireguard ANX95i fire alarm panels for fire detection. Each panel has a connection to each of the controllers in the Safeguard 400 Series on the CI 531 sub-module. A maximum combination of four fire alarm panels can be connected to one Safeguard 400 Series unit, meaning two CI 531 sub-modules per safety controller.

4.2.7 MB 300 network configuration

The Safeguard 400 Series is used with Master Bus 300 and can be configured for single or redundant buses. To maintain the availability of the safety system it is strongly recommended that a redundant MasterBus 300 network and a redundant connection (one connection to each MB 300) for both safety controllers in the Safeguard 400 Series is implemented.

NOTE

To support this recommendation, Safeguard 400 Series is configured with a redundant MasterBus 300 interface connection as a standard. See Basic unit Safeguard 400 Series Table 4-15 above.

The network does not affect basic system operation and is not necessary for operation of a Safeguard 400 Series unit, however the network is used to update system status between branches after maintenance or other system restart actions. The network is used to exchange operator information with AS 500 series operator stations during normal operation.

If the user application is made dependent upon MB 300 communication, e.g. through the Cause & Effect remote shutdown function between Safeguard 400 Series units, a redundant MB300 network must be used to obtain a tolerance against single fault throughout the safety system.

Thus network reliability and availability should be designed on requirements for operator information availability, not system reliability.

The Safeguard 400 Series can share operator stations and networks in Advant OCS (Master). To take full advantage of the Integrated system design, such a connection is often recommended.

Safeguard 400 Series avoids “contamination” (corruption) of the safety system with a number of control mechanisms built into the network. Since the ABB Master Net is a full ISO/OSI 7-layer model implementation, these checks are layered so that even if erroneous information should enter the system on a lower level, it will be detected and discarded on some higher level.

Some of these mechanisms are:

- The Physical and Data link layers uses a CSMA/CD protocol with CRC check-sum according to IEEE 802.3 and 802.2
- The transport layer is an ISO class 4 implementation with a calculated residual error rate of one message per 10^{14} messages.
- The application layer is protected by system authorization, as described under operator stations “System Security”.

In addition, to cause contamination, the message must contain meaningful information to the configured application. It can therefore be concluded that safety integrity cannot be disturbed by

other computers on the data highway. The operator can be prevented from performing illegal actions by proper configuration of system access rights.

Other forms of network contamination, such as computer virus cannot enter the control network or Safeguard 400 Series units due to the use of proprietary Network Protocols and Operating Systems on this level.

4.3 System Power Supplies and Distribution

The standard power for Safeguard 400 Series is configured with two power systems; one for system power and one for field devices. The power system is modularized with input voltages 18-72V DC, 110/230V AC or 110V DC and output voltages 24V DC 10A or ±12V DC 10A. The power system is prepared for redundant mains connections (Main I and Main II).

Mains and field distribution units are installed.

The mains distribution unit is designed for two incoming main supplies. The selection of the power rack type is dependent of the selected type of field power configuration.

4.3.1 System power supply

This provides power for the CPU and I/O racks as well as the internal control voltages for the Master Vote 3000 output units. Since the Safeguard 400 Series is a dual system, this in itself, gives redundancy in the power supply and each side is configured for the nominal current consumption, i.e. one module for the central rack only and two modules with up to two additional I/O racks.

NOTE

Single Safeguard, which has only one controller ‘side’, is nonetheless also equipped with redundant system power supplies, for safety reasons.

4.3.2 Field power supply

This must be configured in accordance with the project requirements and one or more racks can be used.

If it is necessary to split inputs and outputs, this is easily changed on the rack. Then the intention is that module one and two, four and five supply output power and module three and six supply input power.

Additional racks and modules can be added as needed.

4.3.3 Compact power supply

This one rack solution provides power for the central I/O racks as well as the internal control voltages for the Master Vote 3000 output units and field power.

Table 4-12. Power configurations

Description	Consists of
Main power distribution	
Main Power Distribution Basic mechanical details With space for: 2 * SXN75(x) + SXN760 or 1 * SXN711 + 1 * SXN712	1 * SX N700
Main Supply Distribution 24VDC 4 * C50A, 2 pole, MCB's	1 * SX N751
Main Supply Distribution 48VDC 4 * C25A, 2 pole, MCB's	1 * SX N752
Main Supply Distribution 115VAC 4 * C16A, 2 pole, MCB's	1 * SX N753
Main Supply Distribution 230VAC 4 * C10A, 2 pole, MCB's	1 * SX N754
AC Utility Voltage Distr. 1 * C6A, 2 pole, MCB and distribution connectors	1 * SX N760
Mains supply filters	
Filter 250V AC, 20 A	1 piece
Filter 250V AC, 55 A	1 piece
Filter 24/48/250V DC, 80 A	1 piece
CPU power racks	
6 slots for PMP3.00 power sub-rack for compact system 2*10A for CPU 2*10A (±12VDC) and 2*10A (24V DC) for field power	1 * RF 194K01
6 slots for PMP3.00 power sub-rack for medium sized systems 2*2*10A for CPU 2*10A (±12V DC)	1 * RF 194K02
6 slots for PMP3.00 power sub-rack for large systems 2*3*10A for CPU	1 * RF 194K03

Table 4-12. Power configurations (Continued)

Description	Consists of
Field power rack	
6 slots for PMP3.00 power sub-rack with 1:1 redundancy for field power	1 * RF 194K04
6 slots for PMP3.00 power sub-rack with N+1 redundancy for field power and dual mains with RF195 REL switchover unit	1 * RF 195K01

Table 4-13. Power modules

Description	Consists of
Dummy module inclusive circuit and plug for serial alarm strapping	1 * PMPDUMMY3.0
Power module 230V AC/24V DC -10A, no power factor correction(1)	1 * PMPE230K01
Power module 230V AC/±12V DC or 24V DC -10A, with power factor correction	1 * PMPSIC230K01
Power module 110V AC or DC/±12V DC or 24V DC -10A, with power factor correction	1 * PMPSIC110K01
Power module 18-72V DC/±12V DC or 24V DC - 10A	1 * PMPDC24K01

(1) This power module shall only be used for safety outputs (DSTD N020/N021).

Table 4-14. Field power distribution

Description	Consists of
Distribution unit for Field power, Field input voltage AI, FI, DI, GI and DO Intern. w/ 8 * K8A, 1 pole- MCB's, 0V and Mastervote contr. volt, distribution	1 * SX N711
Redundancy extension for Field power distr. unit SX N711 w/ 8 * K8A, 1 pole- MCB's	1 * SX N712

Table 4-14. Field power distribution

Description	Consists of
Field power distr.unit for AI/DI/FI/GI/DO. 1:1 red.: up to 20 AI/DI/GI/DO and 10 FI, total maximum 16 A N+1 red.: up to 30 AI/DI/GI/DO and 15 FI, total maximum 2*16 A	1 * DSSX N201A
Earth fault detection unit for balanced, floating 24V DC voltage	1 * DSSS N001

4.4 Reference Guide

This reference guide covers Safeguard 410 and 415 with S100 I/O. For ordering details refer to Price List 3BNP004143/A. Ordering details for fire & gas panels and field equipment are specified in Price List 3BNP000206 and 3BNP000207.

Items without Classification information, are items that obviously do not affect TÜV certification.

Table 4-15. Basic unit Safeguard 410/415

Description	Consists of	Article No.	Classification
General and normative requirements			
CE-Marking Safeguard 400 Series 1.5 - Cabinet mounted delivery		3BNP004340R1	Certified
CE-Marking Safeguard 400 Series 1.5 - Local assembly option		3BNP004341R1	Contact product responsible
Basic Unit for unmanned installations			
Safeguard 400 Series*1.5 - Basic unit with 1 CS513/TÜV Certification	2 * Standard AC410 Basic Units 2 * DSBS116N 4 * CS 513	3BNP004350R1	Certified
Basic Units for manned installations			
TÜV Certification for Safeguard 400 Series *1.5 numbers 3BNP004351R1 and 3BNP004353R1	2 * DSBS116N Document license	3BNP004111R4	Certified
Safeguard 400 Series*1.5 Basic unit /standard with CI547	2 * Standard AC410 Basic Units 4 * CI547	3BNP004351R1	Certified

Table 4-15. Basic unit Safeguard 410/415

Description	Consists of	Article No.	Classification
Safeguard 400 Series*1.5 /standard with CS513	2 * Standard AC410 Basic Units 4 * CS513	3BNP004353R1	Certified
Internal Supervision I/O kit, only required if External Watch Dog is used(1)	2 * DSDI 110A 2 * DSDO 110 1 * DSTD N007 2 * TK 711	3BNP004163R1	Certified

Table 4-16. Software options

Description	Consists of	Article No.	Classification
Cause & Effect matrix programming option *4.0/0. Required when Safety Builder is used.	2 * QC05-CEM11	3BNP000413R4	Certified
PC element library *11.0/0 for advanced process control	2 * QC01-LIB12	3BNP000455R4	Non-certified
Communication protocol *4.0/0 for Eltek ANX95E/i(1)	2 * QC05-FIE11	3BNP000427R4	Certified
Communication protocol *4.0/0 for Autronica BS-100/BS30(1)	2 * QC05-FIA11	3BNP000425R4	Certified
Safety I/O software module *4.0/0 for DSAI 133N and DSDI 110N	2 * QC05-SIO11	3BNP004152R4	Certified
Program module *11.0/0 for generation of User defined elements	2 * QC01-UDP11	3BNP000439R4	Certified
Local operator station interface *11.0/0	2 * QC01-LOS11	3BNP004129R4	Non-certified
System software backup card	1 piece	3BSE009724R1	

(1) QC05-FIE11 cannot exist in same system as QC05-FIA11 (and vice versa)

Table 4-17. Program Card

Description	Consists of	Article No.	Classification
MB510 Program Card Interface		3BSE002540R1	Certified
EQ_card: PCMCIA * 2MB Memory Card		3BSC630036R1	
EQ_Card: PCMCIA * 4MB Memory Card		3BSC630036R2	
EQ_Card: PCMCIA * 10MB Memory Card		3BSC630036R3	

Table 4-18. Communication

Description	Consists of	Article No.	Classification
MB300 equipment			
Tranciever set for thick MB300 LAN or GCOM comm. set or TCP/IP	1 * MB300K01	5730030-VN	Certified
5 m AUI cable assembly for transceivers	1 * TK 576V050	3BSC950055R1	Certified
15 m AUI cable assembly for transceivers Not certified for applications requiring EN54	1 * TK 576V115	3BSC950056R1	Certified
Tool Kit for tranciever installation	1 * MB300K02	5751029-2	
RS-232 equipment			
RS232 comm. interface Requires TC 710 and TK 710 or...(1)	2 * CI 531	3BNP000408R1	Certified
RS232 Fiber Op Modem	1 * TC 710	3BNP004154R1	Certified
Modem Cable for TC 710	1 * TK 710	3BNP004153R1	Certified

Table 4-18. Communication (Continued)

Description	Consists of	Article No.	Classification
Short distance modem for cable length < 10km 24VDC. Point to point < 1km 19200bps.	1 * TC 562	3BSC630049R1	Non-certified
Cable assemblies for CI 53x modem	1 * TK 595	3BSE006830R1	
RCOM+/RCOM Equipment			
RCOM+/RCOM Interface	2 * CI 532V07	3BNP000409R1	Non-certified
Short distance modem for cable. Length < 10km 24VDC. Point to point < 1km 19200bps	1 * TC 562	3BSC630049R1	Non-certified
Cable assemblies for CI 53x modem	1 * TK 595	3BSE006830R1	
MODBUS equipment			
MODBUS comm interface	2 * CI 532V02	3BNP000410R1	Certified
MODBUS comm interface Requires TC 710 and TK 710	2 * CI 534V02	3BNP004024R1	Certified
RS232 Fiber Op Modem	1 * TC 710	3BNP004154R1	Certified
Short distance modem for cable length < 10km 24VDC. Point to point < 1km 19200bps	1 * TC 562	3BSC630049R1	Non-certified
Modem Cable for FO-RS232	1 * TK 710	3BNP004153R1	Certified
Cable assembly, DE9 socket to DE9 pin, for CI 15x modems	1 * TK 595	3BSE006830R1	Non-certified
Advant Fieldbus 100 on Coax/Opto cable			

Table 4-18. Communication (Continued)

Description	Consists of	Article No.	Classification
Advant Fieldbus 100 comm.interface incl. sub modules, coaxial modems and drop cables	2 * CI 520 2 * TC 512 2 * TK 539	3BNP000463R1	Certified
AF100 Optical Modem	1 * TC 630	3BSE002253R1	Certified
Connection Kit	1 * AF100K03	3BSE006251R1	Certified
Terminator Kit		3BSE006244R1	Certified
Advant Fieldbus on twisted pair cable			
Advant Fieldbus 100 comm.interface incl. sub modules, coaxial modems and drop cables	2 * CI 520 2 * TC 512 2 * TK 539	3BNP000464R1	Non-certified
Connection kit 150 ohm incl.conn.unit terminator and drop cable	1* TC 505 1 * TC 501V150 1 * Drop cable	3BSE009616R1	Non-certified
Misc.Communication Equipment			
Capacitive de-coupler device for 4 cables	1 * TX 507	3BSE009892R1	
Capacitive de-coupler device for 8 cables	1* TX 507K01	3BSE009914R1	
Capacitive de-coupler device for 12 cables	3 * TX 507K02 Assembly kit	3BSE009915R1	
Capacitive de-coupler device for 16 cables	4 * TX 507K03 Assembly kit	3BSE009916R1	
Cable assembly DE9 socket - DB25 pin conn. of CI 53X modem	1 * TK 577	3BSE004650R1	
Short distance modem for cable length < 10km 24V DC. Point to point < 1km 19200bps 110/230V AC	1 * DSTC X008	5751030-1	Non-certified
Mounting plate for two modems/T-Boxes	1 * RA 543	3BSE004691R1	Certified

Table 4-18. Communication (Continued)

Description	Consists of	Article No.	Classification
Modem/T-Box sub-rack	1 * RF 541	3BSE003912R1	Certified
Voting unit for dual to single DC power lines	1 * SS 110	3BSE007698R1	Certified

(1) See Safety Manual 3BNP000432R201, Chapter 2.2

Table 4-19. Power systems

Description	Consists of	Article No.	Classification
Main Power distribution			
Main Power Distribution Basic mechanical details With space for 2 * SX N75X + 1 * SX N760	1 * SX N700	3BNP004192R1	Certified
Main Supply Distribution 24VDC Includes 4 * 50A MCB's	1 * SX N751	3BNP004196R1	Certified
Main Supply Distribution 48VDC Includes 4 * 25A MCB's	1 * SX N752	3BNP004197R1	Certified
Main Supply Distribution 115VAC Includes 4 * 16A MCB's	1 * SX N753	3BNP004198R1	Certified
Main Supply Distribution 230VAC Includes 4 * 10A MCB's	1 * SX N754	3BNP004199R1	Certified
AC Utility Voltage Distr. For Cubicle light and socket outlet	1 * SX N760	3BNP004195R1	Certified
CPU Power Racks			
Power subrack w/ six slots for PMP3.00, 2x10A for CPU, 2x10A for +/-12VDC, 2x10A for Field I/O (small systems)	1 * RF 194K01	3BNP000440R2	Certified

Table 4-19. Power systems (Continued)

Description	Consists of	Article No.	Classification
Power subrack w/ six slots for PMP3.00, 2x2x10A for CPU and 2x10A for ±12VDC (Medium systems)	1 * RF 194K02	3BNP000440R3	Certified
Power subrack w/ six slots for PMP3.00, 2x3x10A for CPU (Large systems)	1 * RF 194K03	3BNP000440R4	Certified
CPU Power Modules			
Dummy module incl. circuit and plug for serial alarm strapping	1 * PMPDUMMY3.0	3BNP000456R1	Certified
Power module 230VAC/24VDC -10A w/o power factor correction	1 * PMPE230K01	3BNP000503R2	Non-certified
Power module 230VAC/24VDC -10A with power factor correction	1 * PMPSIC230K01	3BNP000502R1	Certified
Power module 110VAC or DC/24VDC -10A with power factor correction	1 * PMPSIC110K01	3BNP000504R1	Certified
Power module 18-72VDC/24VDC - 10A	1 * PMPDC24K01	3BNP000505R1	Certified
Field Power Rack			
6 slots for PMP3.00 power sub-rack with 1:1 redundancy for field power	1 * RF 194K04	3BNP000440R5	Certified
6 slots for PMP3.00 Main Power rack N+1 redundant switch-over unit.	1 * RF 195K01	3BNP000444R2	Certified
Field Power Modules			
Dummy module incl. circuit and plug for serial alarm jumper function	1 * PMPDUMMY3.0	3BNP000456R1	Certified

Table 4-19. Power systems (Continued)

Description	Consists of	Article No.	Classification
Power module 230VAC/24VDC -10A no power factor correction TÜV-Certified for use with Master Vote outputs only	1 * PMPE230K01	3BNP000503R2	Certified
Power module 230VAC/24VDC -10A with power factor correction	1 * PMPSIC230K01	3BNP000502R1	Certified
Power module 110VAC or DC/24VDC -10A with power factor correction	1 * PMPSIC110K01	3BNP000504R1	Certified
Power module 18-72VDC/24VDC - 10A	1 * PMPDC24K01	3BNP000505R1	Certified
Field Power Distribution			
Field power distr.unit for AI/DI/FI/GI/DO. 1:1 red.: up to 20 AI/DI/GI/DO and 10 FI, total maximum 16 A N+1 red.: up to 30 AI/DI/GI/DO and 15 FI, total maximum 2*16 A	1 * DSSX N201A	3BNP000091R1	Certified
Distribution unit for Field power, Field input voltage AI, FI, DI, GI and DO Intern.	1 * SX N711	3BNP004193R1	Certified
Redundancy extension for Field power distr. unit SX N711	1 * SX N712	3BNP004194R1	Certified
Voting unit for dual to single DC power lines	1 * SS 110	3BSE007698R1	Certified
Earth fault det. unit for balanced floating 24V DC voltage	1 * DSSS N001	3BNP000183R1	Certified
Terminal Carrier for mechanical installation of 2 x DSSSN001		2664181-A	
Filters			

Table 4-19. Power systems (Continued)

Description	Consists of	Article No.	Classification
Main supply filter 250VAC, 20 A	1 piece	3BSC740007R1	Certified
Main supply filter 250VAC, 55 A	1 piece	3BSC740008R1	Certified
Main supply filter 24/48/250VDC, 80 A	1 piece	3BSC740009R1	Certified

Table 4-20. S100 I/O rack extensions

Description	Consists of	Article No.	Classification
I/O Subrack 1	2 * DSRF 182/ 2 * DSSR 122 2 * DSBC 172N/ 2 * DSBC 173N 2 * DSTK 281 2 * DSTK 183 1 * DSTK 185 2 * DSTC 176	3BNP00496R1	Certified
I/O Subrack 2	2 * DSRF 182/ 2 * DSSR 122 2 * DSBC 173N 2 * DSTK 185 2 * DSTK 183	3BNP000470R1	Certified
Dual set of DSBS 116N for I/O rack 2. Required when TÜV certification specified. Install in leftmost card slot in I/O rack #2.	2 * DSBS 116N	3BNP004128R1	Certified
I/O racks w/fiber optical comm.			

Table 4-20. S100 I/O rack extensions (Continued)

Description	Consists of	Article No.	Classification
Remote S100 I/O Basic unit for Safeguard 415 w/ fiberoptic comm.	2 * DSRF 182 2 * DSSR 122 1 * DSSX N404 1 * DSSX N407 2 * DSBC 173N 2 * DSTK 183 2 * TK 575 2 * TC 561 2 * DSTC 176	3BNP004116R1	Certified
Dual TC 560 set for installation in CPU cabinet when using one I/O-rack	2 * TC 560V01 1 * DSSX N405 1 * DSBC172N 1 * RA 543 2 * TK 575 2 * TX 560	3BNP004117R1	Certified
Dual TC 560 set for installation in CPU cabinet when using two I/O-racks	2 * TC 560V01 1 * TK 560 1 * RA 543 2 * TK 580	3BNP004130R1	Certified

:

Table 4-21. Input sets

Description	Consists of	Article No.	Classification
I/O input sets require DSSX N201A I/O output sets require SX N711 / SX N712			
Safety Digital Input 31 channel, 24V DC	2 * DSDI 110N 1 * DSTD N030 2 * DSTD N031 2 * DSTK 150	3BNP004156R1	Certified
Loop monitored digital input 12 channel	2 * DSAI 160 1 * DSTD 170 2 * DSTK 150	3BNP000024R1	Certified

Table 4-21. Input sets (Continued)

Description	Consists of	Article No.	Classification
End-of-line resistor unit 6,8K ohm/0,5W 25pcs.	RU1	3BNP000025R1	
Intermediate resistor unit 820 ohm/0,5W 25 pcs.	RU2	3BNP000026R1	
End-of-line/ intermediate resistor unit 6,8K ohm/820 ohm/0,5W 25pcs.	RU3	3BNP000148R1	
Gas input 12 ch. catalytic pellistor, combust. chamber type.	2 * DSAI 165 2 * DSST 111 1 * DSTA 191 2 * DSTK 150 2 * DSTK 166	3BNP000027R1	Certified
Current Generator rack w/power distr. & 10 slots for DSST 111 constant current generators. One rack per 5 * DSAI 165K01 input sets		3BNP000298R1	Certified
Safety Analog Input 31 ch., 12 bit, single ended 0-10V, 0-20mA	2 * DSAI 133N 1 * DSTA N040 1 * DSTA N041 2 * DSTK 152	2BNP004157R1	Certified
Analog input 16 ch. 12 bit, Diff.Input. 0 - +/- 10 V, 0 - +/- 20 mA	2 * DSAI 130 1 * DSTA N001 w/62.5 Ohm shunt 2 * DSTK 150	3BNP000028R1	Single loop: Non-interference Dual loop: Safety critical
Analog input 16 ch. 12 Bit, Diff. Input.0 - +/- 10 V, 0 - +/- 20 mA	2 * DSAI 130 1 * DSTA N002 w/250 Ohm shunt 2 * DSTK 150	3BNP000281R1	Single loop: Non-interference Dual loop: Safety Critical
Analog input 16 ch. 12 bit, diff. Input. 0 - +/- 10 V, 0 - +/- 20 mA	2 * DSAI 130 2 * DSTA N001 w/62,5 Ohm shunt 2 * DSTK 150	3BNP004118R1	Certified/AK4-SIL2

Table 4-21. Input sets (Continued)

Description	Consists of	Article No.	Classification
Analog input 32ch. 8 bit, single ended. 0 - +/- 10 V, 0 - +/- 20 mA	2 * DSAI 110 1 * DSTA N012 w/62.5 Ohm shunt 2 * DSTK 150	3BNP000029R1	Certified
Analog input 32ch. 8 bit, Single ended. 0 - +/- 10 V, 0 - +/- 20 mA	2 * DSAI 110 2 * DSTA N013 w/250 Ohm shunt 2 * DSTK 150	3BNP000283R1	Certified
Digital input 32 ch. 24V DC, scanning or interrupt.	2 * DSDI 10 1 * DSTD N007 2 * DSTK 150	3BNP000030R1	Certified
Analog input 32 ch., 12 bit, single ended 0-10V, 0-20mA	2 * DSAI 133 2 * DSTA 002A 2 * DSTK 152	3BSE008312R1	Certified

Table 4-22. Status outputs

Description	Consists of	Article No.	Classification
Digital output 32 ch. 24V DC 150mA Short circuit proof.	2 * DSDO 115 1 * DSTD N007 2 * DSTK 150	3BNP000031R1	Certified
Digital output 4x8 ch., 24-250V AC/DC 3A, relay	2 * DSDO 110 4 * DSTD N010 2 * DSTK 165	3BNP000032R1	Certified

Table 4-23. Master Vote 3000

Description	Consists of	Article No.	Classification
Max 4 Master Vote 3000 output sets pr. distribution unit (if 1:1 redundant). Max 6 Master Vote 3000 output sets pr. distribution unit (if N+1 redundant)			
Fail-safe NE output. 4x7 ch. 18-36 VDC 2A	2 * DSDO 110 4 * DSTD N020 2 * DSTK 165	3BNP000009R1	Certified

Table 4-23. Master Vote 3000

Description	Consists of	Article No.	Classification
Monitored ND output. 4x7 ch. 18-36 VDC 2A	2 * DSDO 110 4 * DSTD N021 2 * DSTK 165	3BNP000034R1	Certified
DI for Test Signals. One set/112 outputs.	2 * DSDI 110A 1 * DSTD N007 2 * DSTK 150	3BNP000035R1	Certified
Master Vote 3000 free configurable set			
DSTD N020, DSTD N021 and DSTD N010 are configurable in a free mix. Total max. quantity=4			
Master Vote auxiliary I/O boards.	2 * DSDO 110 2 * DSTK 165	3BNP004119R1	Certified
NE output unit. 24VDC/2A	1 * DSTD N020	3BSE003238R1	Certified
ND output unit. 24VDC/2A	1 * DSTD N021	3BSE003239R1	Certified
Relay output connection unit	1 * DSTD N010	3BNP000049R1	Certified
Read-back options			
Loop status from DSTD N020/ DSTD N021, 28 ch. 24V DC	2 * DSDI 110A 2 * DSTK 165	3BNP000051R1	Certified
Unit error from DSTD N020/ DSTD N021, one set/224 outputs.	2 * DSDI 110A 1 * DSTD N007 2 * DSTK 150	3BNP000053R1	Certified

Table 4-24. Analog output

Description	Consists of	Article No.	Classification
Analog output 16 ch. 8 Bit.0-10V/0-+20mA. Dual package w/ 2 single sets, separate term. units for each safety controller.	2 * DSAO 130 2 * DSTA N180 2 * DSTK 150	3BNP000466R1	Certified
Analog input/output 8 ch. in 8 ch. out. 0-10V 0-+20mA.	2 * DSAX 110 1 * DSTA 001A	3BNP000465R1	Certified

Table 4-25. Mounting bars and dummy boards

Description	Consists of	Article No.	Classification
Mounting Bars			
19” mounting bar for connection units, 3 module heights	1 * RA 120	3BSE005464R1	
19” mounting bar for 3 * Master Vote 3000 connection units, 4 module heights	1 * RA 111	3BNP000457R1	
Handle for board exchange, to facilitate mounting/dismounting in sub-racks	1 * DSRA 010	21880368-A	
Dummy boards			
4TE-width dummy board for Local assembly option	1 piece	29401767-57	

Table 4-26. Assembly

Description	Consists of	Article No.	Classification
Assembly and test of subrack by ABB. mech./cable/PCB/install. Inspection and testing.		3BNP000405R1	Certified

Table 4-27. Local assembly license

Description	Consists of	Article No.	Classification
Local assembly license.	1 * SG400LIC	3BNP000412R1	Non-certified

Table 4-28. RM 500 cabinets

Description	Consists of	Article No.	Classification
Additional cabinet items, such as lights and other accessories, order from MSN Select catalogue from ABB LV Systems AB, Sweden.			
RM5xx Cabinet IP21			
Cabinet with hinged frame IP21 ventilated Max. installed Heat Dissipation at 40/55 Deg. C: 900/450 W	1 * RM 517	3BSE16060R1	Certified
Cabinet with hinged frame IP21 ventilated. (not verified for CE mark)	1 * RM 547	3BSE016158R1	Non-certified
RM5xx Cabinetry IP41			
Cabinet with hinged frame IP41 ventilated Max. installed Heat dissipation at 40/55 Deg. C: 550/350 W	1 * RM 518	3BSE016061R1	Certified
RM5xx Cabinet IP54			

Table 4-28. RM 500 cabinets (Continued)

Description	Consists of	Article No.	Classification
Cabinet with hinged frame, IP54 sealed Max. installed Heat dissipation at 40/55 Deg. C: 450/200 W	1 * RM 519	3BSE016062R1	Certified
RM5xx Accessories			
Plate holder for front plate with customer designed text.		3BSE016259R1	
End panel for RM 500V2 cabinet.		3BSE016254R1	Certified
Shield plate		3BSE016257R1	Certified
Locking device		3BSE016258R1	
Mounting Sheet Powerr Filter 20A		3BSE016510R1	
Mounting Sheet Power Filter 55A		3BSE016511R1	
Mounting Sheet Power Filter 80A		3BSE016512R1	

Table 4-29. VSH 200 cabinets

Description	Consists of	Article No.	Classification
VSH 200 Cabinet IP21 Radio Proof			
VSH 200 Single cabinet Verified for CE Marking	1 * VSH 200	3BSE06070R1	Certified
VSH Accessories			
End plate	1 * VSH 200K30	3BSE006072R1	Certified
Cubicle lighting		SA362026-CM	
Galvanized isolation set		52820083-KX	
Bolt package	1 * RX 538	3BNP000484R1	

Table 4-29. VSH 200 cabinets (Continued)

Description	Consists of	Article No.	Classification
Conductive gasket	1 * RX 539	3BNP000485R1	
Mechanical details	1 * RX 540	3BNP000486R1	

Table 4-30. Cooling Fan

Description	Consists of	Article No.	Classification
Cooling Fan Unit for cabinets, 24 VDC	1 * DSRC113	52820083-LF	Certified

Table 4-31. Single System Items

Description	Consists of	Article No.	Classification
Basic Unit Set for local assembly			
Single Safeguard 400 Series*1.5 Basic Unit Items	1 * Standard AC410 Basic Unit	3BNP004354R1	Certified

Table 4-32. Single Software options

Description	Consists of	Article No.	Classification
Cause & Effect matrix programming option *4.0/0. Required when Safety Builder is used.	1 * QC05-CEM11	3BNP004356R4	
PC element library *11.0/0 for advanced process control	1 * QC01-LIB12	3BNP004360R4	
Communication protocol *4.0/0 for Eltek ANX95E/i(1)	1 * QC05-FIE11	3BNP004357R4	
Communication protocol *4.0/0 for Autronica BS-100/BS30(1)	1 * QC05-FIA11	3BNP004358R4	

Table 4-32. Single Software options

Description	Consists of	Article No.	Classification
Safety I/O software module *4.0/0 for DSAI 133N and DSDI 110N	1 * QC05-SIO11	3BNP004359R4	
Program module *11.0/0 for generation of User defined elements	1 * QC01-UDP11	3BNP004361R4	
Local operator station interface *11.0/0	1 * QC01-LOS11	3BNP004362R4	

(1) QC05-FIE11 cannot exist in same system as QC05-FIA11 (and vice versa)

Table 4-33. MB300 Communications options for Single Safeguard

Description	Consists of	Article No.	Classification
CI547 Communication Board for AC410 and MB300	1 * CI547	3BNP004429R1	
CS513 MB300 Communication Interface	1 * CS513K01	3BSE004772R1	

Table 4-34. Documentation

Title	Description	Article No.	Classification
Safeguard 400 Series Product Guide	This document containing a overview of the Safeguard 400 Series product and additional descriptions of Advant OCS 500 Operator -and 100 Engineering stations.	3BNP000431R301	
Safeguard 400 Series *1.5	Safety Manual.	3BNP000432R301	
S100 Safety I/O	Reference Manual	3BNP004030R1	
Safeguard 400 Series Hardware Units	Reference Manual for specific safety system hardware.	3BNP000499R1	

Table 4-34. Documentation (Continued)

Title	Description	Article No.	Classification
Safeguard 400 Series Functional Units, Base functions	Describes the safety base functions included in the Safeguard 400 Series.	3BNP000433R301	
Safeguard 400 Series Functional Units, Cause & Effect matrices	Describes the Safety Builder tool and the Cause & Effect function.	3BNP000434R0101	
Safeguard 400 Series Functional Units, Addressable detection system	Describes the Fireguard and Autronica BS-100 addressable detection units.	3BNP000435R0101	
Safeguard 400 Series PC-Elements	Describes the safety PC elements.	3BNP000436R0101	
AdvaCommand User Interface, Safeguard Handler		3BNP000186R101	
Safeguard 400 Series Terminal Diagram Form package	Including Terminal Diagram Forms on paper A4 and in IGES format on 3.5” discetts.	3BNP000411R0001	
Advant Controller 410	User’s Guide	3BSE002414R501	
Installation Rules	User’s Guide Describes installation rules to ensure correct function in environments where disturbances are present.	3BSE009178R0001	
S100 I/O Hardware	Reference manual. Contains data sheets and a description of the S100 I/O system.	3BSE02413R0201	
AMPL Configuration	Advant Controller 400 Series Reference Manual	3BSE002417R601	
PC Elements	Advant Controller 400 Series Reference Manual	3BSE002418R501	

Table 4-34. Documentation (Continued)

Title	Description	Article No.	Classification
User Defined PC Elements	User's Guide	3BSE009739R0001	
Database Elements	Advant Controller 400 Series Ref. Manual/Rev. A	3BSE0014819R201	
AMPL Application Building	Reference Manual Describes in general terms how to create AMPL programs in the AC 400 Series.	3BSE003841R0001	
Masterview 320	User's Guide	3BSE003836R0001	
MasterNet	User's Guide	3BSE003839R0201	
GCOM Multidrop	User's Guide	3BSE000165R0001	
Advant Fieldbus 100	User's Guide	3BSE000506R701	
RCOM	Advant Controller 400 Series User's Guide /Rev:A Contains a technical description, instructions for installation, start-up, design and fault tracing of Remote COMmunication in AC410/450	3BSE000532R0001	
MultiVendor Interface-MODBUS /Rev.A	Advant Controller 400 Series User's Guide Contains a technical description, instructions for installation, start-up, design and fault tracing of MVI/MODBUS in AC410/450	3BSE000533R0001	
Multivendor Interface /MODBUS w/ MVB and CI534V02	Advant Controller 400 Series User's Guide	3BSE010719R0001	

Table 4-34. Documentation (Continued)

Title	Description	Article No.	Classification
EXCOM	User's Guide Contains a description of EXCOM, the necessary hardware and installation instructions. It describes all available services and their parameters. It also covers the subject of declaration of necessary variables, data types etc.	3BSE003835R0001	
MP280	Application Notes	7650060-201	
Functional Unit, Part 1	Common Properties User's Guide /Rev.A	3BSE003849R1	
Functional Unit, Part 2	AI, AO, DI, DO User's Guide /Rev.A	3BSE003850R0001	
Functional Unit, Part 3	User's Guide /Rev.A	3BSE003851R0001	
Functional Unit, Part 4	PIDCON, RATIOSTN, MANSTN User's Guide /Rev.A	3BSE003852R0001	
Functional Unit, Part 5	GENXXX, User's Guide /Rev.A	3BSE003853R0001	
Functional Unit, Part 6	MOTCON, VALVECON, User's Guide /Rev.A	3BSE003854R0001	
Interference-free electronics	Design and applications. Describes how to design circuit boards, electronics devices and systems with a high immunity to interference. It also deals with process adaption, communication and power supply with immunity to interference.	3BSE000877R0001	

Table 4-35. Documentation in Electronic Format

Description	Article No.	Classification
Preliminary Documentation	3BSE018003R1	
Issued Documentation	3BSE018006R1	
Operating of issued documentation	3BSE018007R1	

4.5 Advant Operator Interface Products

Advant Operator Workplace -with software AdvaCommand for Windows NT and AdvaCommand for UNIX- represents a new approach to supervision and control of industrial processes. It does not only provide the capability to communicate with the process but also with other computers and systems outside the automation system. This information integration capability makes it possible to view both administrative data and process control data on the operator workplace.

Figure 4-3. Advant Operator Workplace for UNIX, with two monitors

4.5.1 Product Benefits

Advant Operator Workplace can be connected to MasterBus 300 control networks, and communicate with Advant Controller 400 Series as well as with Advant Information Management Workplaces.

Advant Operator Workplace complies with the X Window System and the OSF/Motif Æ standards, making it possible to access and run applications in other stations throughout the network. For instance, to look up circuit drawings created and stored in an engineering station or view and edit data in product quality and business information systems.

Operator Interaction

Operator interaction by means of Human Machine Interface (HMI) equipment, ranging from low-cost to advanced operator workplaces featuring the latest technology in user interfacing, that is, high-resolution color graphics and windowing based on industry standards, such as X Window System and OSF/Motif.

4.5.2 Features

Some features of the Advant Operator Interface Products are:

- High resolution displays for presentation of process data.
- Trend presentation of historical data.
- Command entry to the process via mouse and keyboard -AdvaCommand for Windows NT
- Command entry to the process via mouse/trackball, function keyboard or a combination of both -AdvaCommand for UNIX
- Process alarms and events are time-tagged and presented for the operator in alarm and event lists and can also be announced audible to make the operator aware of it.
- Event messages and alarms can be grouped and gated in multitude of ways, ensuring that only relevant and primary events are brought to the operatorís attention.
- System status displays provides status information about the automation system with regards to all communication links, stations, peripheral equipment and process I/O boards.
- Process sectioning provides functions for dividing the process into sections and linking each workplace to the desired mix of process sections for supervision and control.
- Status lists is a list of process signals and objects matching search parameters supplied by the operator. Status lists are used to find process objects that are in a certain state or have something in common, for example, all blocked PID objects.
- Display Builder supports the creation of free-image displays for interactive monitoring and control.
- Station Backup function is used to backup applications in the own station.
- On-line Builder. Process controllers can be configured, debugged and documented on line from a window in the operator workplace.
- Trend presentation of historical data
- Central Backup function is used to backup applications in other stations of the system such as process controllers -AdvaCommand for UNIX.
- AdvaInform History. History is used for collection and long time storage of process data on the hard disk. These data can then be presented in Trend displays -AdvaCommand for UNIX.
- Display Distribution Services is used to manage displays in large networks. With this tool it is possible to have the display source code on one operator station and allow distribution of different sets of displays to any other operator station within the network.

4.6 Advant Engineering Products

Advant Engineering Products implement ABBís approach to a scalable automation project engineering. From the independent products needed for quick and efficient controller configuration, for example AMPL Control Configuration, to Advant Engineering Workplace which serves as an integrated platform for all the tools needed to manage, design, engineer, install, commission and maintain industrial automation plants with Advant OCS with maximum productivity and quality. The smaller independent products easily integrate into the total concept which addresses the needs of both the engineering and maintenance phases, which means that it offers important benefits to both application development and plant maintenance engineers.

4.6.1 Product Benefits

Advant Engineering Products support the different tasks in the engineering process. They do so by letting individual products be combined to fit the team of persons working with the whole range of the engineering, from single controller configuration to projects handling for a complete plant.

Object Oriented Engineering

The Advant Object concept is the common base for the set of tools providing efficient engineering methods to support process automation projects. Each project can be broken down into smaller and smaller components called Advant Objects. At the low level of the project structure these Advant Objects can be individual signals, connection terminals, motors, etc. Advant Objects are filled with information that describes different aspects of the corresponding real world object. These Aspects range from CAD drawings and functional descriptions to control programs. For easy access to the information there are different Views on the Aspects.

The ability to include dynamic data in the Aspects gives the concept a very high flexibility.

The fact that Advant Engineering Products and its components support this concept gives the engineer the means to handle projects of different size and scope in an efficient manner while maintaining high quality standards. Import of existing data into the engineering environment is well covered, allowing coexistence with existing tools and methods. To achieve a high engineering efficiency and quality one time data entry is supported.

Teamwork

Advant Objects promote teamwork of qualified personnel from different areas. By supporting multiple access to Advant Objects it is possible for several engineers to work with the Aspect of their speciality on the same object at the same time. By using the licensing flexibility, the individual workplaces can be tailored according to the needs of each engineer in the team.

Reuse

Engineering becomes more efficient when using Advant Objects. This is mainly due to good reuse support and extensive import functionality. Dynamic solutions in libraries can be merged with new engineering data., thereby creating completely new applications for the current project.

Lifetime Information Support

When the engineering is done and the plant is started, Advant Engineering Workplace acts as an excellent information data base. The possibility to add more Aspects to an Advant Object makes it is easy to keep the information updated and collect all the relevant information, about the object, in one place. This gives a certainty that, when needed, the information is accessible and complete.

Advant Engineering Products are designed to help engineers build and maintain industrial automation plants more efficiently, at lower costs and with better engineering quality. It does so by providing an integrating platform for all the disciplines, tools and tasks involved, throughout the life cycles of these plants. In short, Advant Engineering Products helps industrial automation engineers do a better job faster.

4.6.2 Advant Engineering Products

There are packages within Advant Engineering Products each built up by different tools. The tools, called Builders, are used for efficient entry of engineering data and graphical application programming of controllers. Since documentation is an important part in a project, functions for creation, managing, and printing of project documents are available. For electrical diagram handling there are products based on AutoCAD. There are also durable industrial PCs ideal for fieldwork.

Products which support Advant Objects running on Windows NT

- Advant Engineering Workplace, serves as a cooperation base for the engineering products
- AMPL Control Configuration, for configuration of Advant Controller 100 and 400 Series
- Computer Aided Electrical Engineering, for electrical CAD engineering
- Advant Station 100 Series Engineering Station, a durable PC for field work

NOTE

The minimum setup needed to configure an Advant Controller is AMPL Control Configuration.

4.7 Advant Engineering Workplace

Advant Engineering Workplace establishes the engineering environment for the AdvaBuild Engineering Software under Windows NT.

Further engineering products can be added and extend the basic functionality of the Advant Engineering Workplace. Together they can be run in a cooperating mode. These products are:

- AMPL Control Configuration
- Computer Aided Electrical Engineering (CAEE).

NOTE

The two products above are stand-alone products as well. Advant Engineering Workplace is not needed to run either of them but in the cooperating mode there

is more functionality and advantages, Figure 2-1 and Figure 2-2.

Two options which extend the functionality of Advant Engineering Workplace are available:

- Option Parameter Builder which handles the import and editing of engineering data used as parameters by the other AdvaBuild Engineering Software products.
- Option Document Builder which integrates office tools like Microsoft Word and Microsoft Excel with Advant Engineering Workplace. It also offers a document registry based on Microsoft Access. These features gives the user an excellent tool for the creation and administration of documents.

4.7.0.1 Product Benefits and Features

Some features of Advant Engineering Workplace, in cooperating mode together with the options:

- Multiple Structuring, that is, different views of the project
- Filter functions for easy retrieval of data
- Copy/Paste of Advant Objects including all its Aspects
- Automatic creation of parameterized Advant Objects from libraries and spread sheets gives extensive reuse support
- Dynamic documents, automatically updated when duplicated and given to another Advant Object
- Flexible parameter handling, where parameters are available for other Aspects
- Auto generated reports
- I/O allocation
- Printing

4.7.1 AMPL Control Configuration

AMPL Control Configuration is a suite of builders necessary to configure Advant Controller 100 and 400 Series with Master software. The products are based on Windows NT.

The option On-line Builder extends the functionality of AMPL Control Configuration by support of on-line configuration and download of Advant Controller 400 Series applications.

The set of available elements for Function Chart Builder is determined by libraries. AMPL PC and DB Element Libraries include the PC and DB Element Libraries and reference manuals for Advant Controller 400 Series (Advant Controller 410 and Advant Controller 450) and Advant Controller 100 Series (Advant Controller 160, Advant Controller 110, Advant Controller 70 and Advant Controller 55).

4.7.1.1 Product Benefits and Features

AMPL Control Configuration provides the following features:

- Administration of nodes, Circuits and Type Circuits simplifying project start-up and reuse

- Off-line editing with powerful cut/copy/paste
- On-line editing for rapid program modifications
- Target system control for easy testing of installed system
- Module diagnosis

In cooperating mode it supports much more features like:

- Support for the Advant Object concept including
  - parameterized data in Type Circuits used in Circuit aspects and DBElement aspects
  - efficient commands acting on sets of these aspects

4.7.2 Computer Aided Electrical Engineering

Electrical Diagram Builder - Wiring Builder is available for creation and administration of circuit diagrams, loop diagrams, connection diagrams, layout diagrams, I/O diagrams and overview diagrams and efficient handling and documentation of the plant wiring. As addition, CAEE Libraries contains symbol libraries and format libraries.

4.7.2.1 Product Benefits and Features

Computer Electrical Engineering provides, in cooperating mode together with the options, the following features:

- Support for the Advant Object concept including parameterized data
- Effective symbol handling for better reuse
- Extensive drawing help which shortens drawing time
- Semi-automatic allocation of connections to cables reduces work and mistakes
- Effective article import via standardized format to reduce work and mistakes
- System neutral, standardized description of engineered data to be imported and used by the customerís maintenance system

4.7.3 Advant Station 100 Series

Advant Station 100 Series Engineering Stations

Advant Station 100 Series Engineering Stations are durable PCs which satisfy the Advant OCS environmental specifications. Advant Station 100 Series Engineering Stations are ideal for fieldwork, including off-line engineering, on-line programming, maintenance and fault tracing.

The Advant Station 100 Series Engineering Stations are available in 2 different variants:

- Advant Station 120 Engineering Station for Windows NT (PCI)
- Advant Station 130 Engineering Station for Windows NT (ISA)

Advant Station 100 Series Engineering Boards

Advant Station 100 Series Engineering Boards allows the use of an appropriate IBM compatible PC together with AMPL Control Configuration products for on-line configuration of Advant Controller 400 Series. This will give a similar functionality to an Advant Station 100 Series Engineering Station.

The Advant Station 100 Series Engineering Boards are available in 2 different variants:

- Advant Station 100 Series Engineering Board (ISA)
- Advant Station 100 Series Engineering Board (PCI), which allows in addition direct connection to MasterBus 300.

4.7.3.1 Product Benefits and Features

In addition to the benefits and features for AMPL Control Configuration, Advant Station 100 Series Engineering Stations are very sturdy and can handle the rough treatment in the field. In a less hostile environment a PC together with any of the Advant Station 100 Series Engineering Boards can be used. If the Advant Station 100 Series Engineering Board (PCI) is used the configuration work can be made from the office via MasterBus 300.

3BNP000431R301

August 2000