

TOSVERT™ VF-S15

---

VF-S15 Safety function manual

---

"Original instructions"

**Toshiba Industrial Products and Systems Corporation**

## — Contents —

<u>Important information</u> .....	1
I. Safety Information.....	2
II. About the book.....	3
1. Before you begin.....	5
1.1 Safety instructions .....	5
1.2 Qualification of personnel and use .....	7
2. Overview .....	8
2.1 Introduction .....	8
2.2 Standards and Terminology.....	9
2.3 Basics .....	10
3. Description .....	12
3.1 (STO) Safe Torque Off.....	12
3.2 (SS1) Safe Stop 1 .....	12
4. Incompatibility with safety functions.....	14
4.1 Limitations .....	14
5. Safety monitoring .....	16
5.1 Detected fault given by the drive .....	16
6. Technical data .....	17
6.1 Electrical Data .....	17
6.2 Safety function capability.....	18
6.3 Several certified architectures .....	20
6.4 Process system SF - Case 1 .....	21
6.5 Process system SF - Case 2.....	22
6.6 Process system SF - Case 3.....	23
7. Services and maintenance.....	24
7.1 Maintenance .....	24

## **Important information**

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither manufacture nor any of sales or distributors shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Toshiba software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.



# I. Safety Information

## Important Information

### NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.




#### Explanation of markings

Marking	Meaning of marking
 Warning	Indicates that errors in operation may lead to death or serious injury.
 Caution	Indicates that errors in operation may lead to injury (*1) to people or that these errors may cause damage to physical property. (*2)

(\*1) Such things as injury, burns or shock that will not require hospitalization or long periods of outpatient treatment.

(\*2) Physical property damage refers to wide-ranging damage to assets and materials.

#### Meanings of symbols

Marking	Meaning of marking
	Indicates prohibition (Don't do it). What is prohibited will be described in or near the symbol in either text or picture form.
	Indicates an instruction that must be followed. Detailed instructions are described in illustrations and text in or near the symbol.
	-Indicates warning. What is warned will be described in or near the symbol in either text or picture form. -Indicates caution. What the caution should be applied to will be described in or near the symbol in either text or picture form.

### PLEASE NOTE

The word "drive" as used in this manual refers to the controller portion of the adjustable speed drive as defined by NEC.

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Toshiba for any consequences arising out of the use of this product.

## II. About the book

### At a Glance

#### Document Scope

The purpose of this document is to provide information about safety functions incorporated in VF-S15. These functions allow you to develop applications oriented in the protection of man and machine.

#### Validity Note

This documentation is valid for the VF-S15 drive.

VF-S15 listed on Table 1 incorporate the safety function STO and SS1.

Table 1

Input voltage class	Inverter type
3-phase 200V to 240V	VFS15-2002PM__/-W1/Y-A*
	VFS15-2004PM__/-W1/Y-A*
	VFS15-2007PM__/-W1/Y-A*
	VFS15-2015PM__/-W1/Y-A*
	VFS15-2022PM__/-W1/Y-A*
	VFS15-2037PM__/-W1/Y-A*
	VFS15-2055PM__/-W1/Y-A*
	VFS15-2075PM__/-W1/Y-A*
	VFS15-2110PM__/-W1/Y-A*
	VFS15-2150PM__/-W1/Y-A*
1-phase 200V to 240V	VFS15S-2002PL__/-W1/Y-A*
	VFS15S-2004PL__/-W1/Y-A*
	VFS15S-2007PL__/-W1/Y-A*
	VFS15S-2015PL__/-W1/Y-A*
	VFS15S-2022PL__/-W1/Y-A*
3-phase 380V to 500V	VFS15-4004PL__/-W1/Y-A*
	VFS15-4007PL__/-W1/Y-A*
	VFS15-4015PL__/-W1/Y-A*
	VFS15-4022PL__/-W1/Y-A*
	VFS15-4037PL__/-W1/Y-A*
	VFS15-4055PL__/-W1/Y-A*
	VFS15-4075PL__/-W1/Y-A*
	VFS15-4110PL__/-W1/Y-A*
	VFS15-4150PL__/-W1/Y-A*

3-phase 380V to 500V	VFS15-4004PL1__/-W1/Y-A*
	VFS15-4007PL1__/-W1/Y-A*
	VFS15-4015PL1__/-W1/Y-A*
	VFS15-4022PL1__/-W1/Y-A*
	VFS15-4037PL1__/-W1/Y-A*
3-phase 525V to 600V	VFS15-6015P__/-W1/Y-A*
	VFS15-6022P__/-W1/Y-A*
	VFS15-6037P__/-W1/Y-A*
	VFS15-6055P__/-W1/Y-A*
	VFS15-6075P__/-W1/Y-A*
	VFS15-6110P__/-W1/Y-A*
	VFS15-6150P__/-W1/Y-A*

(\*)The references followed by “Y-A38”, “Y-A65”, “Y-A66” and “Y-A67” don’t conform.

#### Related Documents

Title of Documentation	Reference Number
VF-S15 Instruction manual (Japanese)	E6581610
VF-S15 Instruction manual (English)	E6582175
VF-S15 ATEX Guide	E6581861

# 1. Before you begin




## 1.1 Safety instructions

The information provided in this manual supplements the product manuals.



Carefully read the product manuals before using the product.

Read and understand these instructions before performing any procedure with this drive.



### ■ HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

 Warning	
 Prohibited	<ul style="list-style-type: none"> <li>• Many parts of this drive, including the printed circuit boards, operate at the line voltage. DO NOT TOUCH. Use only electrically insulated tools. Failure to follow this instruction will result in death or serious injury.</li> <li>• DO NOT touch unshielded components or terminal strip screw connections with voltage present. Failure to follow this instruction will result in death or serious injury.</li> <li>• DO NOT short across terminals PA/+ and PC/- or across the DC bus capacitors. Failure to follow this instruction will result in death or serious injury.</li> </ul>
 Mandatory action	<ul style="list-style-type: none"> <li>• Read and understand this manual before installing or operating the drive. Installation, adjustment, repair, and maintenance must be performed by qualified personnel. Failure to follow this instruction will result in death or serious injury.</li> <li>• The user is responsible for compliance with all international and national electrical code requirements with respect to grounding of all equipment. Failure to follow this instruction will result in death or serious injury.</li> <li>• Before servicing the drive:               <ul style="list-style-type: none"> <li>- Disconnect all power, including external control power that may be present.</li> <li>- Place a "DO NOT TURN ON" label on all power disconnects.</li> <li>- Lock all power disconnects in the open position.</li> <li>- WAIT 15 MINUTES to allow the DC bus capacitors to discharge.</li> <li>- Measure the voltage of the DC bus between the PA/+ and PC/- terminals to ensure that the voltage is less than 42 Vdc.</li> <li>- If the DC bus capacitors do not discharge completely, contact your local Toshiba representative. Do not repair or operate the drive.</li> </ul> </li> <li>• Install and close all covers before applying power or starting and stopping the drive. Failure to follow this instruction will result in death or serious injury.</li> </ul>



### ■ UNINTENDED EQUIPMENT OPERATION

 Warning	
 Mandatory action	<ul style="list-style-type: none"> <li>• Read and understand this manual before installing or operating the drive. Failure to follow this instruction will result in death or serious injury.</li> <li>• Any changes made to the parameter settings must be performed by qualified personnel. Failure to follow this instruction will result in death or serious injury.</li> </ul>



## ■ DAMAGED DRIVE EQUIPMENT

 Warning	
 Prohibited	<ul style="list-style-type: none"> <li>Do not operate or install any drive or drive accessory that appears damaged. Failure to follow this instruction can result in death, serious injury, or equipment damage.</li> </ul>



## ■ LOSS OF CONTROL

 Warning	
 Mandatory action	<ul style="list-style-type: none"> <li>The designer of any wiring scheme must consider the potential failure modes of control channels and, for certain critical control functions, provide a means to achieve a safe state during and after a channel failure. Examples of critical control functions are emergency stop and overtravel stop. Failure to follow this instruction can result in death, serious injury, or equipment damage.</li> <li>Separate or redundant control channels must be provided for critical control functions. Failure to follow this instruction can result in death, serious injury, or equipment damage.</li> <li>Each implementation of a control system must be individually and thoroughly tested for proper operation before being placed into service. Failure to follow this instruction can result in death, serious injury, or equipment damage.</li> <li>System control channels may include links carried out by the communication. Consideration must be given to the implications of unanticipated transmission delays or failures of the link. Failure to follow this instruction can result in death, serious injury, or equipment damage.</li> </ul>

## ■ INCOMPATIBLE LINE VOLTAGE

 Caution	
 Mandatory action	<ul style="list-style-type: none"> <li>Before turning on and configuring the drive, ensure that the line voltage is compatible with the supply voltage range shown on the drive nameplate. The drive may be damaged if the line voltage is not compatible. Failure to follow this instruction can result in injury or equipment damage.</li> </ul>

## ■ RISK OF DERATED PERFORMANCE DUE TO CAPACITOR AGING

 Caution	
 Mandatory action	<ul style="list-style-type: none"> <li>The product capacitor performances after a long time storage above 2 years can be degraded. In that case, before using the product, apply the following procedure:           <ul style="list-style-type: none"> <li>*Use a variable AC supply connected power input terminals.</li> <li>*Increase AC supply voltage to have:               <ul style="list-style-type: none"> <li>- 25% of rated voltage during 30 min</li> <li>- 50% of rated voltage during 30 min</li> <li>- 75% of rated voltage during 30 min</li> <li>- 100% of rated voltage during 30 min</li> </ul> </li> </ul> </li> <li>Failure to follow this instruction can result in injury or equipment damage.</li> </ul>



---

## 1.2 Qualification of personnel and use

---

### Qualification of personnel

Only appropriately trained persons who are familiar with and understand the contents of this manual and all other pertinent product documentation are authorized to work on and with this product. In addition, these persons must have received safety training to recognize and avoid hazards involved. These persons must have sufficient technical training, knowledge and experience and be able to foresee and detect potential hazards that may be caused by using the product, by changing the settings and by the mechanical, electrical and electronic equipment of the entire system in which the product is used.

All persons working on and with the product must be fully familiar with all applicable standards, directives, and accident prevention regulations when performing such work.

### Intended use

The functions described in this manual are only intended for use with the basic product; you must read and understand the appropriate product manual.

The product may only be used in compliance with all applicable safety regulations and directives, the specified requirements and the technical data.

Prior to using the product, you must perform a risk assessment in view of the planned application. Based on the results, the appropriate safety measures must be implemented.

Since the product is used as a component in an entire system, you must ensure the safety of persons by means of the design of this entire system (for example, machine design).

Operate the product only with the specified cables and accessories. Use only genuine accessories and spare parts.

Any use other than the use explicitly permitted is prohibited and can result in hazards.

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel.

The product must NEVER be operated in explosive atmospheres (hazardous locations, Ex areas).

---

## 2. Overview

---



---

### 2.1 Introduction

---

The safety function incorporated in VF-S15, allow you to develop applications oriented in the protection of man and machine.

Safety integrated functions provides the following benefits:

- Additional standards-compliant safety functions
- Replacement of external safety equipment
- Reduced wiring efforts and space requirements
- Reduced costs

The VF-S15 drives are compliant with normative requirements to implement the safety function.

#### Safety function as per IEC 61800-5-2

<b>STO</b>	<b>Safe Torque Off</b> The function purpose is to bring the motor into a no torque condition so it is relevant in terms of safety since no torque is available at the motor level. Power modules are inhibited and the motor coasts down or prohibits the motor from starting.
<b>SS1</b>	<b>Safe Stop 1 Type C</b> (initiates the STO function after and application specific time delay) SS1 consists of : <ul style="list-style-type: none"> <li>• Monitored deceleration of the movement according a specified time delay.</li> <li>• STO (triggered after time delay has been reached.)</li> </ul>

## 2.2 Standards and Terminology

Technical terms, terminology and the corresponding descriptions in this manual are intended to use the terms or definitions of the pertinent standards.

In the area of drive systems, this includes, but is not limited to, terms such as "safety function", "safe state", "fault", "fault reset", "failure", "error", "error message", "warning", "warning message", etc.

Among others, these standards include:

- IEC 61800 series: "Adjustable speed electrical power drive systems"
- IEC 61508 series Ed.2: "Functional safety of electrical/electronic/programmable electronic safety related systems"
- EN 954-1 Safety of machinery - Safety related parts of control systems
- EN ISO 13849-1 & 2 Safety of machinery - Safety related parts of control systems

### CE Declaration of Conformity

The EC Declaration of Conformity for the EMC Directive can be obtained in CD-ROM (E6581624).

### ATEX certification

The ATEX certificate can be obtained with VF-S15 ATEX Guide.

### Certification for functional safety

The integrated safety function is compatible and certified following IEC 61800-5-2 Ed.1 Adjustable speed electrical power drive systems – Part 5-2 : Safety requirements – Functional IEC 61800-5-2 as a product standard, sets out safety-related considerations of Power Drive Systems Safety Related "PDS (SR) s" in terms of the framework of IEC 61508 series Ed.2 of standards.

Compliance with IEC 61800-5-2 standard, for the following described safety function, will facilitate the incorporation of a PDS(SR) (Power Drive System with safety-related functions) into a safety-related control system using the principles of IEC 61508, or the ISO 13849-1, as well as the IEC 62061 for process-systems and machinery.

The defined safety functions are:

- SIL 2 capability in compliance with IEC 61800-5-2 and IEC 61508 series Ed.2.
- Performance Level "d" in compliance with ISO 13849-1.
- Compliant with the Category 3 of European standard ISO 13849-1 (EN 954-1).

Also refer to Safety function capability, page 17.

The safety demand mode of operation is considered in high demand or continuous mode of operation according to the IEC 61800-5-2 standard.

The certificate for functional safety can be obtained with this manual.

## 2.3 Basics

### Functional Safety

Automation and safety engineering are two areas that were completely separated in the past but recently have become more and more integrated.

Engineering and installation of complex automation solutions are greatly simplified by integrated safety functions.

Usually, the safety engineering requirements depend on the application.

The level of the requirements results from the risk and the hazard potential arising from the specific application.

### IEC 61508 standard

The standard IEC 61508 "Functional safety of electrical/electronic /programmable electronic safety-related systems" covers the safety-related function. Instead of a single component, an entire function chain (for example, from a sensor through the logical processing units to the actuator) is considered as a unit. This function chain must meet the requirements of the specific safety integrity level as a whole. Systems and components that can be used in various applications for safety tasks with comparable risk levels can be developed on this basis.

### SIL - Safety Integrity Level

The standard IEC 61508 defines 4 safety integrity levels (SIL) for safety functions. SIL1 is the lowest level and SIL4 is the highest level. A hazard and risk analysis serves as a basis for determining the required safety integrity level. This is used to decide whether the relevant function chain is to be considered as a safety function and which hazard potential it must cover.

### PFH - Probability of a dangerous Hardware Failure per Hour

To maintain the safety function, the IEC 61508 standard requires various levels of measures for avoiding and controlling detected faults, depending on the required SIL. All components of a safety function must be subjected to a probability assessment to evaluate the effectiveness of the measures implemented for controlling detected faults. This assessment determines the PFH (probability of a dangerous failure per hour) for a safety system. This is the probability per hour that a safety system fails in a hazardous manner and the safety function cannot be correctly executed. Depending on the SIL, the PFH must not exceed certain values for the entire safety system. The individual PFH values of a function chain are added. The result must not exceed the maximum value specified in the standard.

SIL Safety Integrity Level	Probability of a dangerous Failure per Hour (PFH) at high demand or continuous demand
4	$\geq 10^{-9} \dots < 10^{-8}$
3	$\geq 10^{-8} \dots < 10^{-7}$
2	$\geq 10^{-7} \dots < 10^{-6}$
1	$\geq 10^{-6} \dots < 10^{-5}$

## PL - Performance level

The standard IEC 13849-1 defines 5 Performance levels (PL) for safety functions. “a” is the lowest level and “e” is the highest level. Five level (a, b, c, d, e) correspond to different values of average probability of dangerous failure per hour.

Performance level	Probability of a dangerous Hardware Failure per Hour
e	$\geq 10^{-8} \dots < 10^{-7}$
d	$\geq 10^{-7} \dots < 10^{-6}$
c	$\geq 10^{-6} \dots < 3 \cdot 10^{-6}$
b	$\geq 3 \cdot 10^{-6} \dots < 10^{-5}$
a	$\geq 10^{-5} \dots < 10^{-4}$

## HFT - hardware detected fault tolerance and SFF - Safe Failure Fraction

Depending on the SIL for the safety system, the IEC 61508 standard and SFF, Safe Failure Fraction requires a specific hardware detected fault tolerance HFT in connection with a specific proportion of safe failures SFF (safe failure fraction).

The hardware detected fault tolerance is the ability of a system to execute the required safety function in spite of the presence of one or more hardware detected faults.

The SFF of a system is defined as the ratio of the rate of safe failures to the total failure rate of the system.

According to IEC 61508, the maximum achievable SIL of a system is partly determined by the hardware detected fault tolerance HFT and the safe failure fraction SFF of the system.

IEC 61508 distinguishes two types of subsystems (type A subsystem, type B subsystem). These types are specified on the basis of criteria which the standard defines for the safety-relevant components.

SFF	HFT type A subsystem			HFT type B subsystem		
	0	1	2	0	1	2
< 60%	SIL1	SIL2	SIL3	-	SIL1	SIL2
60% ... < 90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
60% ... < 99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
$\geq 99\%$	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

## Detected fault avoidance measures

Systematic errors in the specifications, in the hardware and the software, usage detected faults and maintenance detected faults of the safety system must be avoided to the maximum degree possible. To meet these requirements, IEC 61508 specifies a number of measures for detected fault avoidance that must be implemented depending on the required SIL. These measures for detected fault avoidance must cover the entire life cycle of the safety system, i.e. from design to decommissioning of the system.

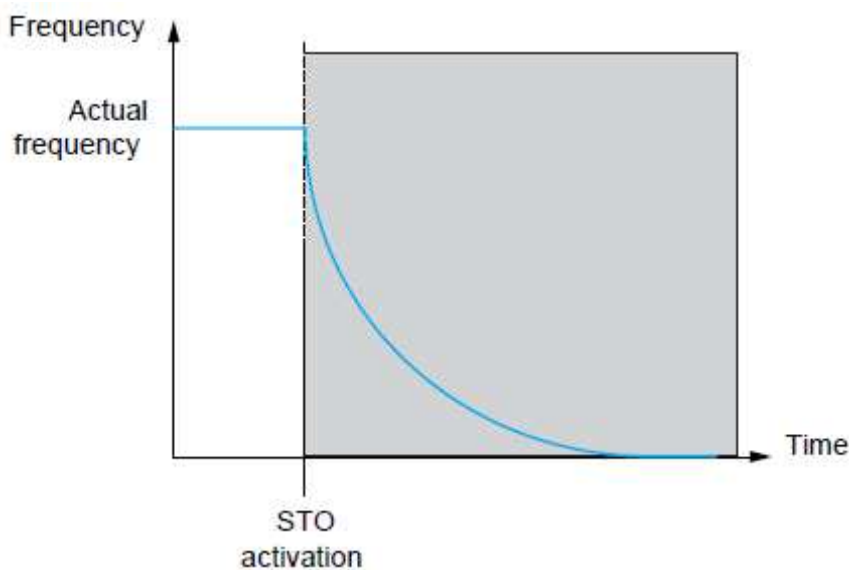
## 3. Description

### 3.1 (STO) Safe Torque Off

The purpose of this function is to bring the motor into a no torque condition with motor coasts down or prohibits the motor from starting. So it is relevant in terms of safety since no torque is available at the motor level.

The logic input "STO" is always assigned to this function.

The STO status is accessible with the drive.



#### STO Normative reference

The normative definition of STO function is in §4.2.2.2 of the IEC 61800-5-2:

"Power, that can cause rotation (or motion in the case of a linear motor), is not applied to the motor. The PDS(SR)(Power Drive System with safety-related functions) will not provide energy to the motor which can generate torque (or force in the case of a linear motor).

NOTE 1 This safety function corresponds to an uncontrolled stop in accordance with stop category 0 of IEC 60204-1.

NOTE 2 This safety function may be used where power removal is required to help prevent an unexpected startup.

NOTE 3 In circumstances where external influences (for example, falling of suspended loads) are present, additional measures (for example, mechanical brakes) may be necessary to help prevent any hazard.

NOTE 4 Electronic means and contactors are not adequate for protection against electric shock, and additional measures for isolation may be necessary."

#### Safety function (SF) level required for STO function

<b>Configuration</b>	<b>SIL</b> <i>(Safety Integrity Level)</i> according to IEC 61508	<b>PL</b> <i>(Performance Level)</i> according to ISO-13849
STO with or without Preventa module	SIL2	PL "d"

The Preventa module is required for the machine environment because:

- For the machine environment (IEC60204-1 & Machine Directive), reset shall not initiate a restart in any cases. One of the most stringent case is when STO is activated, then the power supply is switch off. In this case, if STO is deactivated during the loss of supply, the motor do not have to restart automatically. The Preventa module can prevent a spurious restart in the previous condition. So the Preventa module is mandatory for machine applications.
- E\_stop of several BDM in a PDS: the Preventa module has some safety outputs for application which requires one or several safety outputs.

For other environments, the Preventa module is not required, except if the application requires it: System fallback position.

## 3.2 (SS1) Safe Stop 1

This function, SS1 Type C, by consist of STO function and application specific delay is used to stop the motor. STO is initiated after an application specific safe time delay.

The behavior at the activation and deactivation of the SS1 function depends on the type and setting of application specific safety relay.

### SS1 Normative reference

The normative definition of SS1 function is in §4.2.2.2 of the IEC 61800-5-2:

“The PDS(SR)(Power Drive System with safety-related functions)

Type C. initiates the motor deceleration and initiates the STO function after an application specific time delay.”

NOTE This safety function corresponds to a controlled stop in accordance with stop category 1 of IEC 60204-1.

In accordance with the IEC 60204-1, the SS1 function generates a stop category 1 for the PDS generates a stop category 0 after:

- The motor stop ( when the motor is below a specified limit )
- or an application specific time delay

### Safety function (SF) level required for SS1 function

<b>Function</b>	<b>Configuration</b>	<b>SIL</b> <i>(Safety Integrity Level)</i> according to IEC 61508	<b>PL</b> <i>(Performance Level)</i> according to ISO-13849
SS1 Type C	STO with Preventa module	SIL2	PL "d"

---

# 4. Incompatibility with safety functions

---

---

## 4.1 Limitations

---

### Type of Motor

STO can be used with synchronous and asynchronous motors.

### Prerequisites for using safety functions

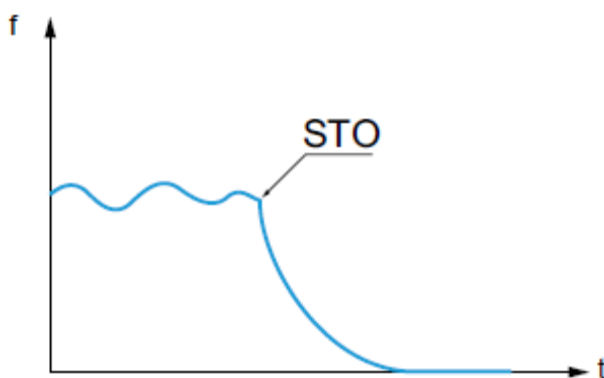
Some parameters have to be fulfilled for a proper operation:

- Motor size is adequate to the application and is not in the limit of its capacity
- Speed drive size has been properly chosen for the electrical mains, sequence, motor and application and it is not in the limit of their catalogued capacities.
- If required, the adequate options are used. Example: like dynamic brake resistor or motor inductor.
- The drive is properly setting up for the right speed loop and torque characteristics for the application; the speed profile of the reference is mastered by the drive control loop.

### Allowed and unallowed application for safety function

#### Allowed application

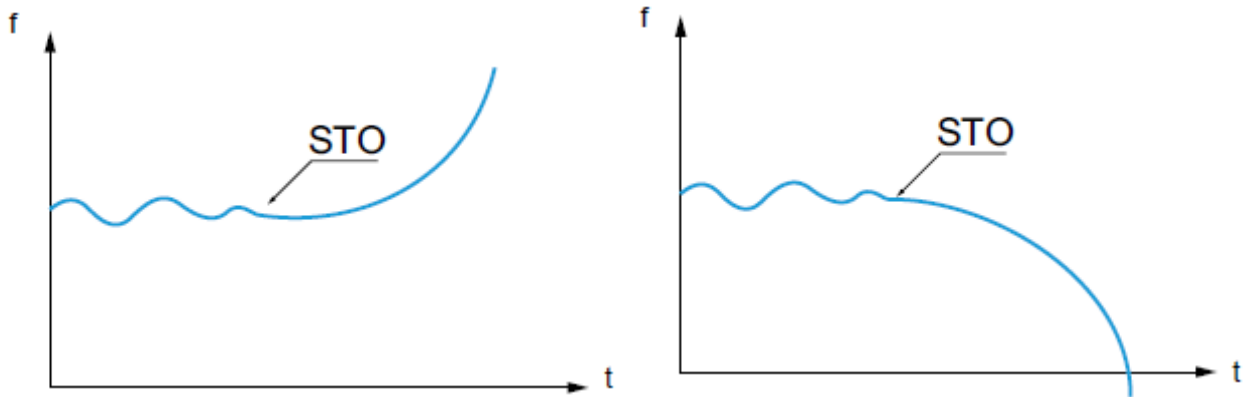
Allowed sharp of stop after STO request or freewheel stop





### Unallowed application

Application with acceleration of the load after shut down of the drive or where there are long/permanent regenerative braking cycles are not allowed. Unallowed sharp of stop after STO request or freewheel stop.



Examples: vertical conveyors, vertical hoist, lifts or winders.

### Priority between safety functions

STO has the higher priority. If the STO function is triggered, a safe torque off is managed whatever the others active functions.

---

## 5. Safety monitoring

---

---

### 5.1 Detected fault given by the drive

---

When fault is detected on safety function drive trips in [PrF]. Drive can only be reset by a power OFF/ON.

## 6. Technical data

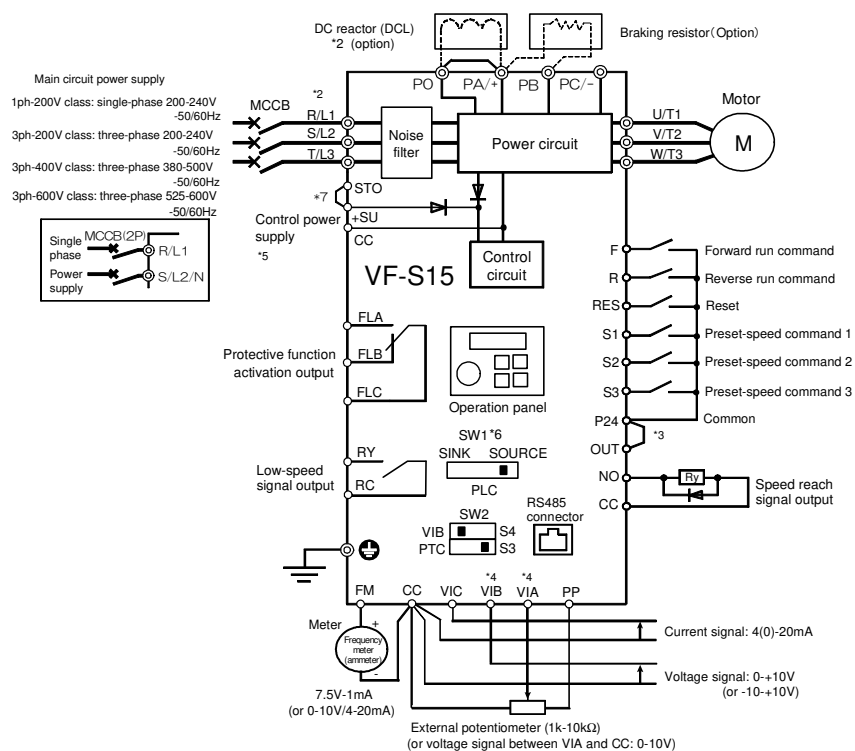
### 6.1 Electrical Data

The Logic inputs and Logic outputs of the drive can be wired for logic type 1 or logic type 2.

SW1	Active state
SINK	Output draws current (Sink) Current flows to the input
SOURCE	Output supplies flows from the input Current Current (Source)

Signal inputs are protected against reverse polarity, outputs are short-circuit protected. The inputs and outputs are galvanically isolated.

\* Terminals are shorted between STO and +SU as a default setting.



## 6.2 Safety function capability

**Safety functions of PDS (SR) are part of a global system.**

If qualitative and quantitative objectives of safety set by the final application requires to make some adjustments to use the safety functions in a safe way, then the integrator of the BDM is responsible of these complementary evolution (for example management of the mechanical brake on the motor).

Also, the output information generated by the utilization of safety functions (default relay activation, relay of brake logic command, errors codes or information on the display, ...) aren't considering safety information.

### Machine application

Function	STO	SS1 type C
	STO with Preventa XPS AF or equivalent	STO with Preventa XPS ATE or XPS AV or equivalent
IEC 61800-5-2 / IEC 61508 /	SIL2	SIL2
IEC 62061 (1)	SIL2 CL	SIL2 CL
EN 954-1 (2)	Category 3	Category 3
ISO 13849-1 (3)	Category 3 PL "d"	Category 3 PL "d"
IEC 60204-1	Category stop 0	Category stop 1

(1) Because the standard IEC 62061 is an integration standard, this standard distinguishes the global safety function (which is classify SIL2 for VF-S15) from components which constitute the safety function (which is classify SIL2 CL for VF-S15)

(2) According to table 6 of IEC 62061 (2005)

(3) According to table 4 of EN13849-1 (2008)

### Process application

Function	STO	SS1 type C
	STO	STO with Preventa XPS ATE or XPS AV or equivalent
IEC 61800-5-2 / IEC 61508 /	SIL2	SIL2
IEC 62061 (1)	SIL2 CL	SIL2 CL

(1) Because the standard IEC 62061 is an integration standard, this standard distinguishes the global safety function (which is classify SIL2 for VF-S15) from components which constitute the safety function (which is classify SIL2 CL for VF-S15)

### Input signals safety functions

Input signals safety functions	Units	Value for STO
Logic 0 (Ulow)	V	< 2
Logic 1 (Uhigh)	V	> 17
Impedance (24V)	kΩ	1.5
Debounce time	ms	< 1
Response time of safety function	ms	< 10

### Synthesis of the dependability study

Function	Standard	Input	STO input
STO	IEC 61508 Ed.2	SFF	96.7%
		PFD10y	6.24.10 <sup>-4</sup>
		PFD1y	6.16.10 <sup>-5</sup>
		PFHequ 1y	7.04 FIT (1)
		Type	B
		HFT	1
		DC	93%
		SIL capability	2
	IEC 62061 (2)	SIL CL capability	2
	EN 954-1 (3)	Category	3
	ISO 13849-1 (4)	PL	D
		Category	3
		MTTFd in years	16200

(1) FIT : Failure In Time = Failure/10<sup>9</sup> hours

(2) Because the standard IEC 62061 is an integration standard, this standard distinguishes the global safety function (which is classify SIL2 for VF-S15) from components which constitute the safety function (which is classify SIL2 CL for VF-S15)

(3) According to table 6 of IEC 62061 (2005)

(4) According to table 4 of EN13849-1 (2008)

Preventive annual activation of the safety function is recommended. However the safety levels are reached with lower margins without annual activation.

For the machine environment, Preventa module is required for the STO function. To free from the Preventa module, the "Restart" function parameters have to be part of the safety function. Please refer to the Preventa usefulness details.

NOTE: The table above is not sufficient to evaluate the PL of a PDS. The PL evaluation has to be done at the system level. The fitter or the integrator of the BDM has to do the system PL evaluation by including sensors data with numbers from the table above.

---

## 6.3 Several certified architectures

---

NOTE: For the certification relative to functional aspects, only the PDS(SR) (Power Drive System with safety related functions) will be in consideration, and not the complete system in which fits into to help to ensure the functional safety of a machine or a system/process.

Here are the architectures certified:

- Process system SF - Case 1
- Process system SF - Case 2
- Process system SF - Case 3

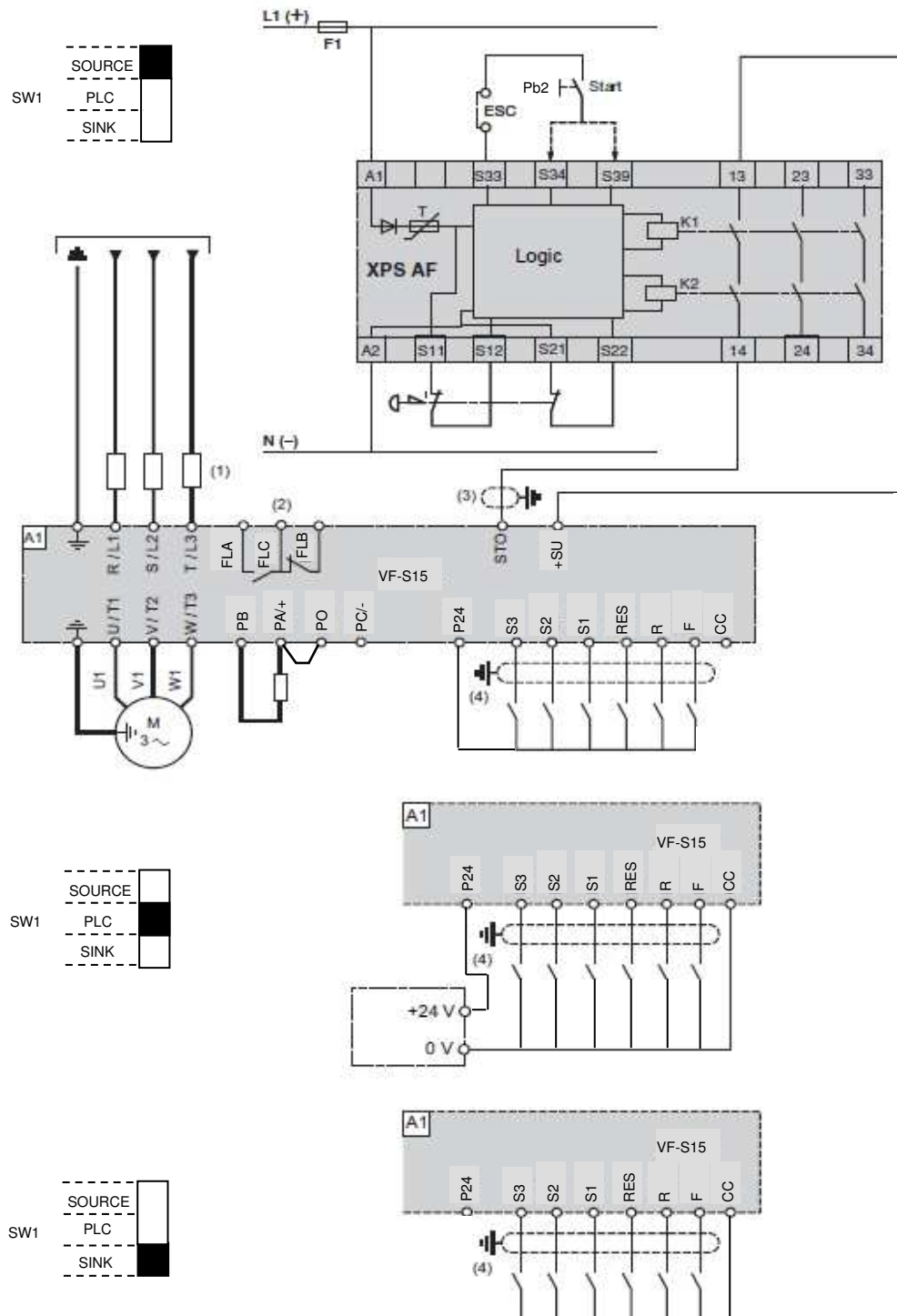
Safety functions of PDS(SR) (Power Drive System with safety-related functions) are part of a global system. If qualitative and quantitative objectives of safety set by the final application require to make some adjustments to use the safety functions in a safe way, then the integrator of the BDM (background debug module) is responsible of these complementary evolutions (for example management of the mechanical brake on the motor). Also, the output information generated by the utilization of safety functions (default relay activation, relay of brake logic command, errors codes or information on the display, ...) are not considering safety information.

## 6.4 Process system SF - Case 1

### Safety according to EN 954-1, ISO 13849-1 and IEC 60204-1 (Machine)

The following configurations apply to the diagram below:

- STO category 3 Machine with Safety controller module type Preventa XPS AF or equivalent

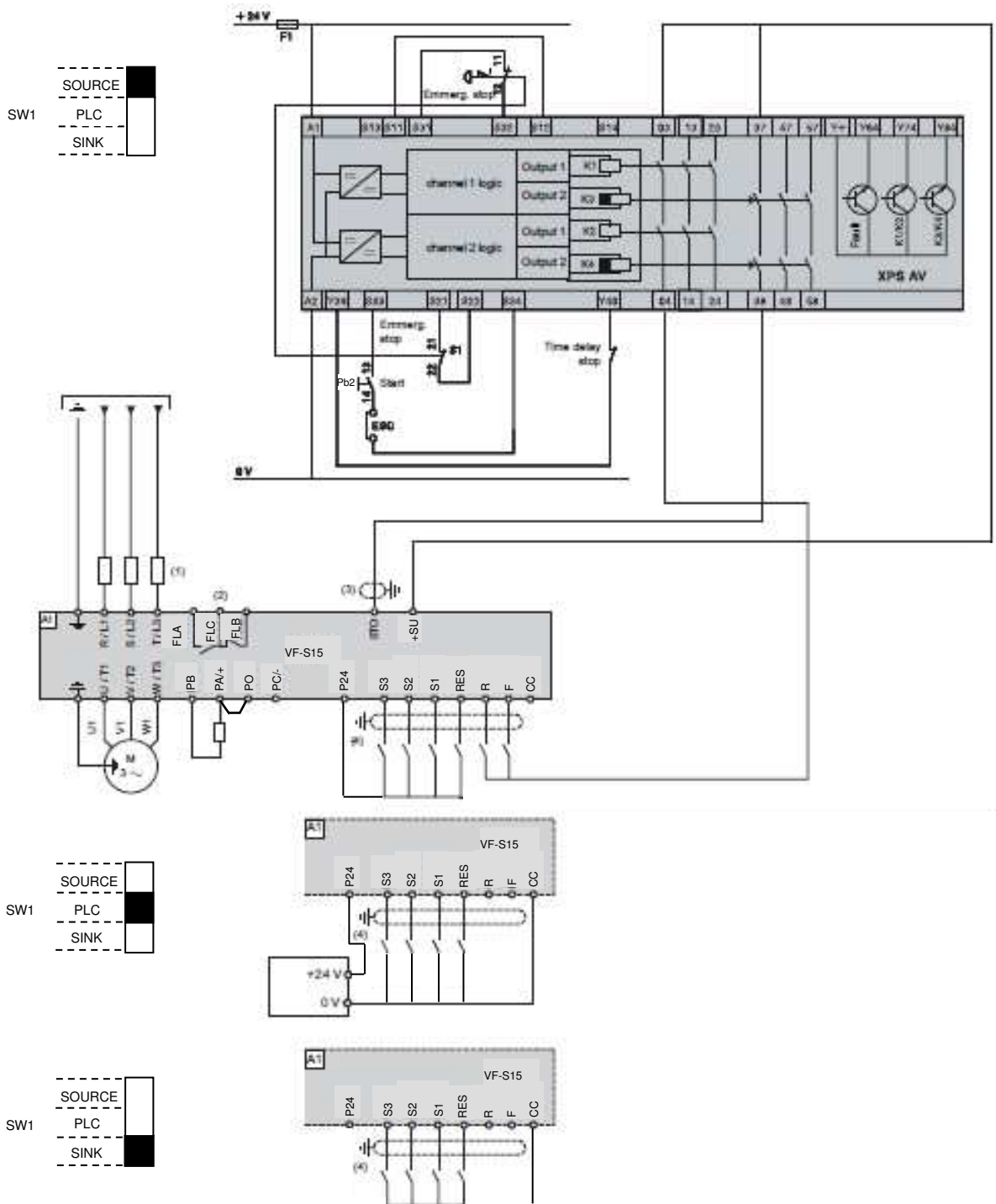


# 6.5 Process system SF - Case 2

Safety according to EN 954-1, ISO 13849-1 and IEC 60204-1 (Machine)

The following configurations apply to the diagram below:

- SS1 type C category 3 Machine with Safety controller module type Preventa XPS AV or equivalent



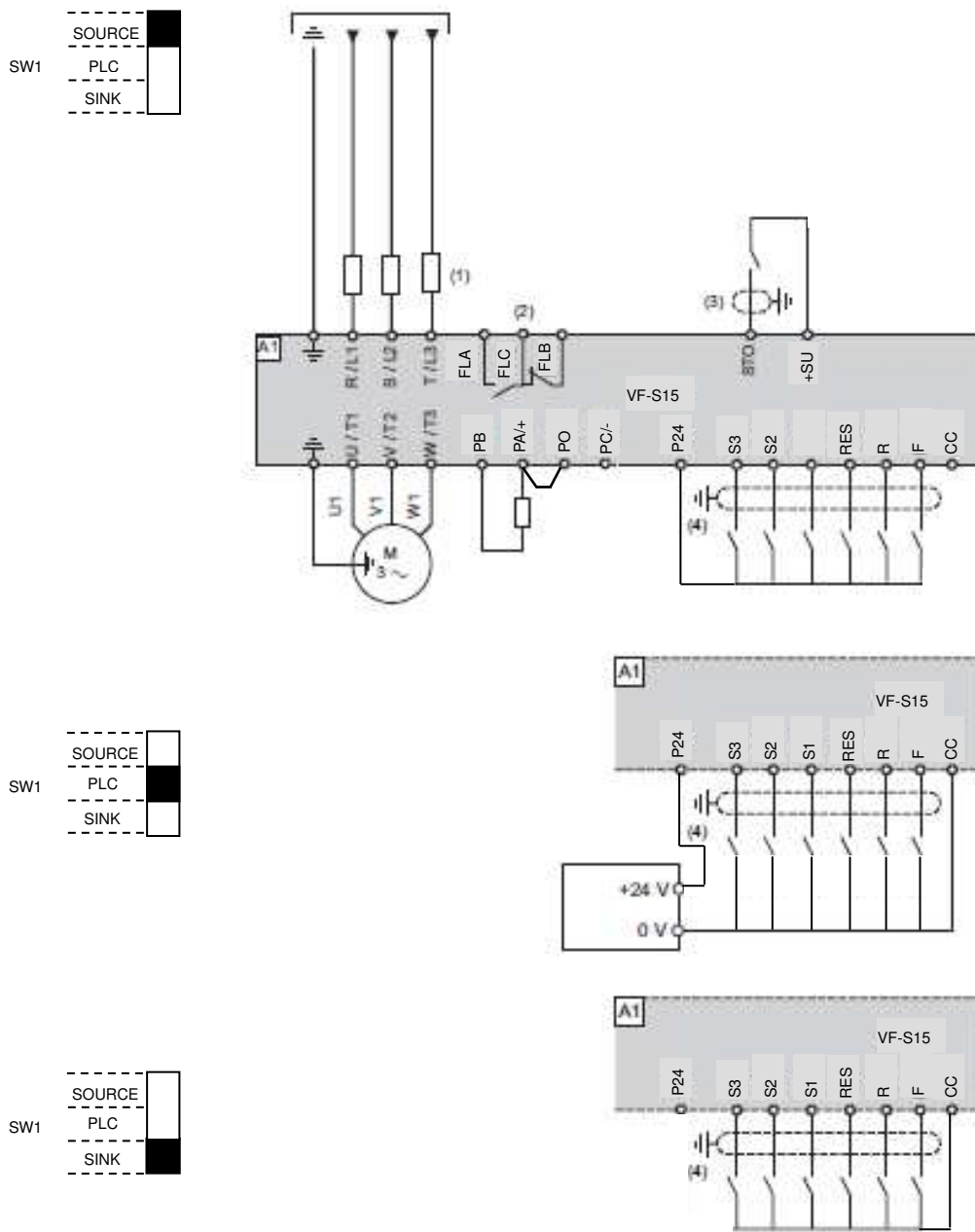


## 6.6 Process system SF - Case 3

### Safety according to IEC 61508

The following configurations apply to the diagram below:

- STO SIL 2 on STO (also SIL1)



---

## 7. Services and maintenance

---

---

### 7.1 Maintenance

---

For more product information, see the installation manual and programming manual from Toshiba.

#### **Preventive maintenance**

It is recommended to check each year the safety functions.

Example: Open the protective door to see if the drive stops in accordance with the safety function configured.

#### **Changing equipment of the machine**

Note: If you need to change any part of the machine out of VF-S15 (Motor, Emergency stop ...) you must redo the Acceptance test.