Title: MTTF (MEAN TIME TO FAIL) data for Standard drives, High performance AC drives, Servo drives and DC drives.

Summary of Contents

This information is provided to assist in reliability and availability analysis and/or safety system design when using Control Techniques variable speed drives. The data is provided without any warranty or undertaking beyond the scope of any independent verification or certification as stated in the text. The text explains the origins of the data and the steps which have been taken to ensure its accuracy.

General failure data

Field failure rates

The MTTF estimated from the field failures for all reasons is given in the table below. This data was calculated for products manufactured between the dates shown in the table, from the total number of failures 12 months after the date of manufacture. A cautious estimate of 2,880 running hours per year has been applied.

Product	MTTF (h)	λ (h^{-1})	Manufacturing period
Standard AC drives	1,194,232	0.84×10^{-6}	Apr '14 to Jun '14
High performance AC drives	669,540	1.49×10^{-6}	Apr '14 to Jun '14
Single axis servo drives	327,273	3.05×10^{-6}	Oct '07 to Jun '10
Multi-axis servo drives	242,017	4.13×10^{-6}	Oct '07 to Jun '10
DC drives	293,878	3.40×10^{-6}	Jan '09 to Sep '11

These values include failures for reasons which include damage caused by errors in installing and commissioning[1]. Failure rates for correctly installed and commissioned drives would be expected to be substantially lower. On the other hand, in considering drive availability, allowance should be made for the fact that the drive contains comprehensive protection facilities which mean that it is likely to trip in the event of various unexpected occurrences such as excessive temperature, impact loading etc. These do not represent a drive fault but still they may result in a loss of availability unless some form of automatic trip recovery process is in place. Drive trips which occur for valid reasons do not constitute failures, but may have a serious impact on availability.

This data can be used in assessing reliability and availability of systems using these drives. It is not recommended that it be used for safety analysis, because the probability of a systematic fault is higher than that of a random hardware failure. The drive uses complex hardware (ASICS and LSI semiconductor devices) and firmware which might contain systematic faults which have not been revealed by testing, or which might be misunderstood or misapplied by the system designer. For this reason, it is the policy of Control Techniques Ltd that its products should not be used to carry out safety functions except where they have been specifically designed for the purpose and such use is clearly authorised by Control Techniques Ltd. The only onboard function which is intended for use in safety functions is **Safe Torque Off** (previously referred to as **Secure Disable**). The Unidrive M10X, M20X, Commander SK, Multiax and DC drives offer no safety functions.

In analysing a system which uses a drive and has a possible functional safety impact, it should be assumed that the drive is capable of all failure modes associated with its functions, i.e. that the torque or speed or direction could fail to follow the input requests in any mode consistent with the inherent limits of the drive (i.e. rated current and power), and that outputs and indications could fail to give correct values.

It is not possible to provide PFH data for non-safety functions according to EN 61800-5-2 etc. and there can be no SIL value. When using EN ISO 13849-1:2006 for safety-related machinery design, a value of 10 years is suggested for $MTTF_d$ of a component of one channel (clause 4.5.2 option c).

<u>Calculated failure rates</u>
No calculated failure rate data is provided (i.e. data calculated using FMEA from standard component failure databases). The reasons for not providing this data are:

- Lack of valid data or analysis processes for major key components such as IGBT, ASIC etc.
- Lack of valid data for modern manufacturing processes – e.g. fine-pitch surface-mounting components
- A general lack of confidence in the validity of conventional FMEA analysis of complex, highly-integrated and firmware-based systems

[1] Service returns where no fault is found in a full functional test, or where obvious damage has been caused by the installer, are excluded.

Safety-related failure data – Safe Torque Off (Secure Disable)

The Unidrive SP drive product incorporates the Safe Torque Off (Secure Disable) function – referred to as **STO** in the remainder of this document. This has been assessed according to the following standards for safety-related control functions using electrical or electronic equipment. Note that in all cases the requirements of the European EN standards and the corresponding international IEC or ISO standards are identical. In order to make the information most general the international standards are referred to by preference, but in relation to the EU Machinery Directive it is the EN standards which are applicable. They can in practice be treated as interchangeable.

IEC/ISO	EN	Title
-	EN 954-1:1997	Safety of machinery - safety related parts of control systems - general principles for design
IEC 61508	EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems (Seven parts)
IEC 62061:2005	EN 62061:2005	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC 61800-5-2:2007	EN 61800-5-2:2007	Adjustable speed electrical power drive systems – Safety requirements - Functional
ISO 13849-1:2006	EN ISO 13849-1:2006	Safety of machinery. Safety-related parts of control systems. General principles of design.

The purpose of this safety function is, on request, to prevent the drive from generating torque in the motor. For an explanation and application guidance on this function, please refer to the relevant User Guides.

STO has been independently assessed and certified by BGIA **http://www.dguv.de/bgia/en/index.jsp** which is a notified body under the EU Machinery Directive. The main standard applied is EN 61800-5-2:2007 which is a specific standard for adjustable speed drives. BGIA have also provided certification according to EN ISO 13849-1:2006.

IEC 61800-5-2 is based on the principles given in IEC 61508, using the basic parameters of SIL and PFH_D. For applications where standards IEC 62061, IEC 61508 or others derived from IEC 61508 are applied, these standards are compatible and inter-operable. For this reason no statement of conformity with these standards is given, because conformity with IEC 61800-5-2 gives all of the information required.

STO was designed to meet EN 954-1 at category 3. The main requirement of this category is that no single fault shall cause a loss of the safety function, and that most faults shall be revealed. It is also necessary to avoid unproven or complex techniques, or stored-program devices, which are not easily amenable to failure analysis using a qualitative FMEA. This is achieved using a single input channel and a circuit which uses only simple discrete electronic components, in an arrangement which ensures that all single component failures result in the drive being disabled. The requirements of category 3 are actually exceeded since additionally, no combinations of two component failures result in a loss of the safety function.

Since the drive is a sub-system which is intended for incorporation into a complete control system which may include a safety-related control system, safety data is required for the drive in order to permit analysis of the complete system. The following data has been based both on the independent assessment done by BGIA and by analysis carried out within Control Techniques Ltd using the FMEDA analysis tool provided by the independent organisation Exida.

Because **STO** uses simple discrete electronic components and does not depend on software or complex integrated circuits, it is amenable to FMEA using well-established databases. The component failure database applied was Siemens SN 29500.

In addition to the FMEDA, hardware fault injection tests have been carried out to validate the assumptions made regarding failure modes.

Data	Description	Value from BGIA	Value from CT	Notes
Data according to IEC 61800-5-2 also applies for IEC 62061 and IEC 61508 (series):				
PFD	Probability of failure on demand	-	-	Not applicable, since **STO** operates in continuous demand mode[2]
T_1	Diagnostic test interval	-	-	Not applicable, **STO** is effectively self-testing and does not rely upon diagnostic tests
	Sub-system type	A	A	Low complexity
HFT or N	Hardware fault tolerance	0	0	Single channel
SFF	Safe failure fraction	100%	99.7%	BGIA value considers first fault only. CT considers sequences of faults.
λ_D PFH_D[3]	Hardware failure rate per hour in dangerous direction	$< 10^{-8}$	8×10^{-10}	BGIA value considers a first fault only and is a default minimum value. CT value includes sequences of faults.
SILCL	SIL claim limit	3	3	Because of the single channel input, in practice the system SIL achieved may be restricted to 2.
	Fault reaction	Drive remains disabled in the presence of the *enable* command. Internal state can be monitored through a parameter.		
Data according to EN ISO 13849-1:2006:				
PL	Performance level	e	e	
$MTTF_d$	Mean time to failure in dangerous direction	10^4 yr	10^5 yr	Clause 4.5.2 of the standard limits $MTTF_d$ to 100 years for individual channels. Because of the verified high SFF of STO, it can be treated as a single component under Table D.1.
T	Mission time	20 yr	20 yr	
MTTF	Mean time to failure (both safe and dangerous directions	-	10 yr	According to clause 4.5.2 c) of EN ISO 13849-1:2006

[2] It is assumed that when called for, if the safety function fails to operate then a hazard is very likely to occur, and that the function will be called for many times in a year of operation. This is the most severe requirement, typical of machinery safety applications, and a requirement of IEC 62061 and IEC 61800-5-2.

[3] According to IEC 61800-5-2 the parameter is PFH, i.e. the probability of failure of the safety function. This can cause confusion since in the other standards it is referred to as PFH_d, i.e. the probability of failure of the system in the dangerous direction.