CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Prior Use for Non-Programmable and Fixed Program Language Devices for IEC 61511-1:2016 + A1:2017

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members a guideline on demonstrating Prior Use for Devices of a Safety Instrumented Function.

It is not the intention of this document to replace any existing corporate policies or processes. The intent is to determine the process by which a user can review equipment to support a claim of Prior Use.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of how to demonstrate a Prior Use claim for non-programmable and fixed program language sensors, final elements and logic solvers of a Safety Instrumented Function.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline - Prior Use for non-programmable and fixed program language devices for IEC 61511-1:2016 + A1:2017".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

Reference should be made to IEC 61511-1: 2016 + A1: 2017, *Functional safety - Safety instrumented systems for the process industry sector*, which provides detailed information relating to the demonstration of Prior Use.

This guidance is not intended to be an authoritative interpretation of the law; however Competent Authority (CA) inspectors may refer to it in making judgements about a duty holder's compliance with the law. This will be done in accordance with the CA's published enforcement policies (refer to www.hse.gov.uk/pubns/hse41.pdf) and it is anticipated that this document will facilitate a consistent national approach.

It should be understood however that this document does not explore all possible options for demonstrating Prior Use, nor does it consider individual site requirements. Following the guidance is not compulsory and duty holders are free to take other action.

Contents

1. EXECUTIVE SUMMARY

For a Safety Instrumented Function designed to achieve a specific Safety Integrity Level, IEC 61511 requires that potential random and systematic failures of the subsystems (sensors, logic solver and final elements) and the complete integrated loop be fully assessed.

This guidance has been developed to provide information on demonstrating Prior Use for non-programmable and fixed program language (FPL) devices that may be used within a subsystem. It should be read in conjunction with the CDOIF guidance on the functional safety management of installed Safety Instrumented Systems, for the integration of these devices into a Safety Instrumented Function.

The target audience for this guidance are those with experience in functional safety and a knowledge of IEC 61511.

A working group was commissioned under CDOIF to develop this guideline to assist users in preparing a case for demonstration of Prior Use. This is not intended to be prescriptive in defining the mechanism by which Prior Use should be demonstrated, but aims to highlight key factors that should be considered.

2. INTRODUCTION AND SCOPE

Prior Use is a documented assessment by an end user that a device is suitable for use in a SIS based upon operational experience in a similar operating environment. This assessment should demonstrate that the device meets functional and integrity requirements, including that the systematic faults are sufficiently low.

The definition of Prior Use is provided in section 3.2.51 of IEC 61511-1 with requirements for Prior Use within clause 11.5.3 and 11.5.4.

In order for a Safety Instrumented Function to meet its integrity requirements it must have both sufficient systematic safety integrity and sufficient hardware safety integrity as shown in figure 1. One of the options to meet systematic safety integrity is to comply with the requirements based upon Prior Use.

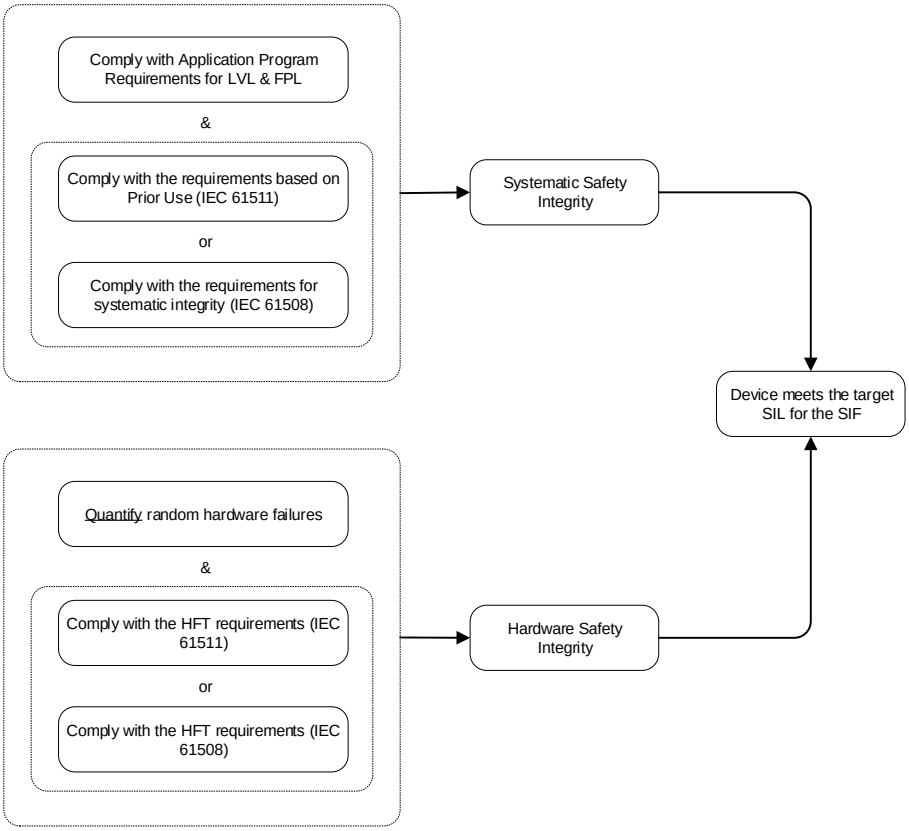

Figure 1 – Requirements to achieve a specified SIL (IEC 61511)

This guidance is only applicable for non-programmable and FPL devices, in accordance with IEC 61511-1 clause 11.5.3 and 11.5.4.

This guidance is only applicable for non-programmable and FPL devices for use in SIL1 or SIL2 applications.

2.1. Concept of Prior Use

Within the chemical and downstream oil industries there are a number of devices that are used within Safety Instrumented Functions that do not have evidence of compliance to IEC 61508 (e.g. statement of compliance from the manufacturer or a certificate of compliance from a certification body). In these cases a Prior Use demonstration is required.

The device Safety Manual provided by the Original Equipment Manufacturer (OEM), which is a compliance requirement in IEC 61508 (see IEC 61508-2; Annex D), provides details to an end user that the device hardware and software has been designed in a systematic way. For example, it has followed a design lifecycle, appropriate competence of people designing the device has been assured, etc. The end user then has confidence that the systematic faults have been minimised and that random hardware failures are as described and can be used as the basis for failure data calculations.

A demonstration of Prior Use should aim to provide an equally effective alternative with respect to ensuring that systematic dangerous failures are sufficiently low and that random hardware failures are as described and can be used as the basis for failure data calculations.

Circumstances when a Prior Use demonstration may be required:

1. For installed systems where no certification exists, however, the device has a reliable track record (and the end user wants to demonstrate that it remains fit for purpose).

2. For new systems where a certified device exists but the end user has good reason to use another non-certified device that has a reliable track record (and wants to record and demonstrate that track record before using it in a new SIF)

3. For new systems where no suitable certified device exists (and the end user wants to build up a Prior Use demonstration)

The concept of Prior Use is based on the device history and on significant documented experience with a device in a given application. It is used to demonstrate that there are sufficiently low dangerous random hardware and systematic failures concerning the intended application (see IEC 61511-2 clause A.11.5.2.1).

If the Prior Use option is adopted it has to be demonstrated, as per figure 1, that the device:

- has a sufficiently low likelihood of systematic faults (refer to section 3.1 and 3.2)

- is sufficiently reliable so as to achieve the overall target PFDavg or dangerous failure rate requirement for the SIF (refer to section 3.3, 3.4 and 3.5);

- meets the architectural constraints requirements (refer to section 3.3, 3.4 and 3.5);

2.2. Example Scenario

The following figure shows two example scenarios of a high level trip for an above ground storage tank. The high level trip could be configured as either:

- Scenario 1, a simple level switch, non-programmable
- Scenario 2, a radar level transmitter, Fixed Program Language device

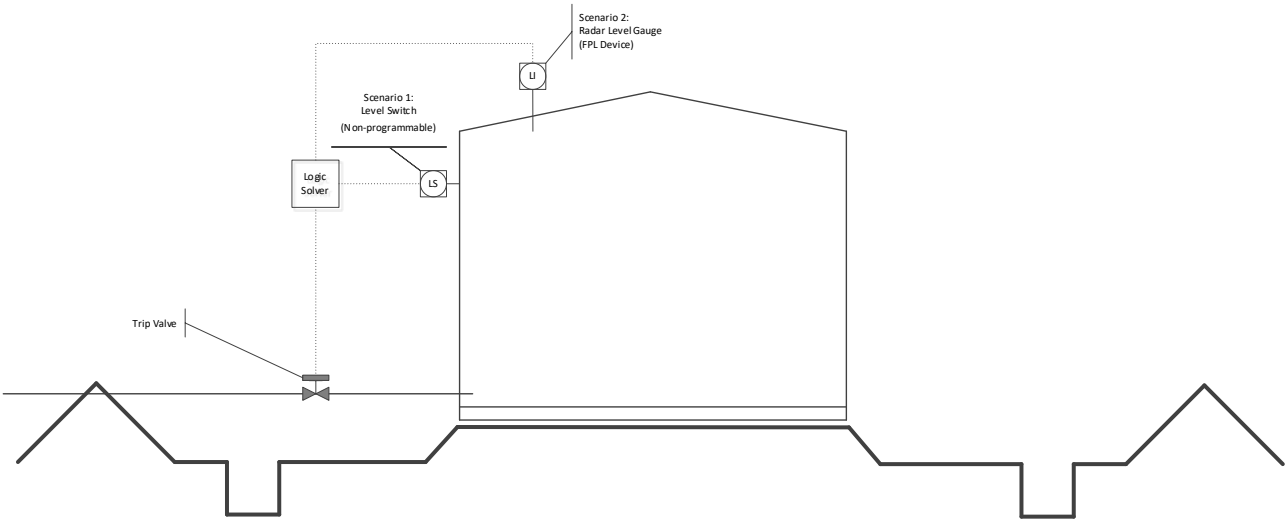

Figure 2 – Example scenario

Using this guidance

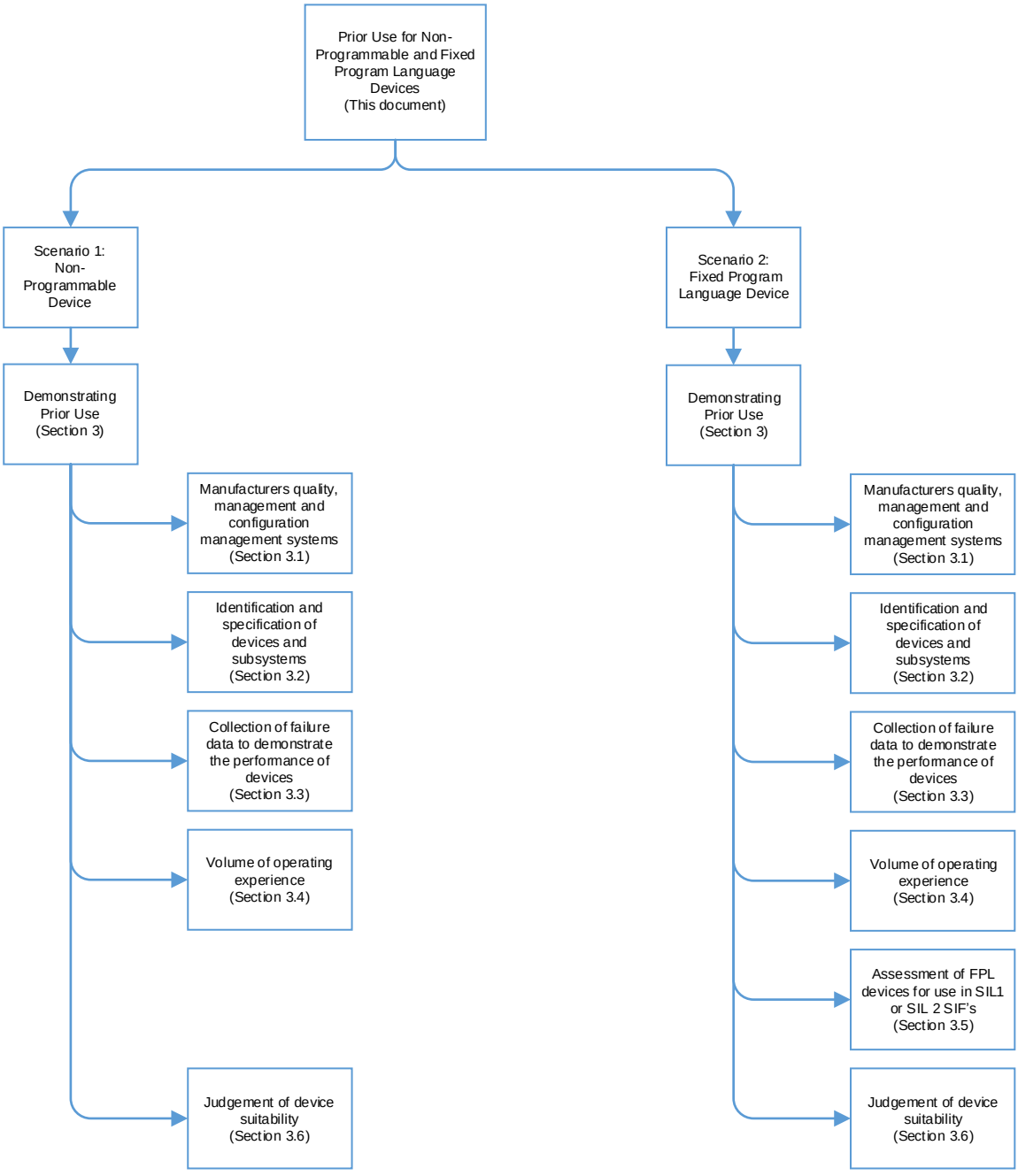

Figure 3 – Using this guidance

3. DEMONSTRATING PRIOR USE

IEC 61511 Prior Use requirements are based upon providing evidence that devices are suitable for use in a SIF (dangerous random hardware and systematic faults have been reduced to a sufficiently low level compared to the required safety integrity requirements).

The level of detail required in the assessment should be in accordance with the complexity of the device and the required SIL of the Safety Instrumented Function.

In order to evaluate if a device can be considered for inclusion in a Safety Instrumented Function based on Prior Use, and to provide the evidence, the following requirements must be met, and a judgement made by the user on the suitability of the installed device for the SIF in question:

- The manufacturer of the device has recognised quality management and configuration management systems in operation (Refer to section 3.1).
- The device has an identifiable specified functionality required for inclusion in the SIF (Refer to section 3.2).
- The device has been used before in an equivalent (or near equivalent) process operation (which may be either safety or non-safety related) (Refer to section 3.3).
- The device has been used in sufficient volume to gain realistic and reliable operating experience (Refer to section 3.4).
- Where the device is programmable using a FPL and is for use in SIL1 or SIL2 applications, the device configuration and use has been considered (Refer to section 3.5)
- Using the above evidence the end user will be required to make a judgement as to whether the device is suitable for the application based on the evidence gathered. For further information refer to section 3.6.

This demonstration of Prior Use suitability is an end user activity with respect to a specific Safety Instrumented Function application. Where a single device is used in multiple SIFs, there is likely to be an overlap in the information required for a Prior Use demonstration. In these cases, it may be beneficial to firstly conduct the Prior Use demonstration for a single device, then review and update this as necessary for each specific SIF.

3.1. Manufacturer's quality, management and configuration management systems

In order to assess the suitability of the device by Prior Use, IEC 61511-1 Clause 11.5.3.2 requires evidence of consideration of the manufacturer's quality, management and configuration management systems in order to minimise systematic failures. The intent of this evidence is to establish that the device was manufactured to a good standard and that it can be operated and maintained appropriately throughout the life of the SIF.

There are potentially two routes by which this aspect can be supported:

1. Assessment of the manufacturer's systems by the user of the device to establish all of the following:

    a. the manufacturer has a quality management system in place;

    b. the manufacturer has been manufacturing equipment of this type (not necessarily this model) for a significant number of years;

    c. the manufacturer has been supplying to the user's industry (or closely related industries) for a significant number of years;

    d. the device has been manufactured in appreciable numbers over an appreciable time period (i.e. it is not a "special" or "limited run" device);

    e. the manufacturer applied relevant national or international product standards to design and manufacture of the device;

    f. installation, operating and maintenance manuals for the device are available;

    g. the manufacturer has procedures in place for revision control for modifications to the device;

    h. the manufacturer has procedures in place for returns and equipment failure assessments that require them to take appropriate action;

    i. the manufacturer has processes to deal with any obsolete devices, for example a migration path to a new device;

    j. the manufacturer has procedures for dealing with device recalls or safety modifications;

    k. the manufacturer has procedures in place for assessing equipment failure data for the device.[1] This should include procedures for identifying modification required due to hardware or systematic failures.

    Some of these requirements may be demonstrated by a manufacturer's quality certificate and policy which covers the device from first manufacture to present day (such as ISO 9001). Even where compliance to ISO9001 is demonstrated, the end user should satisfy themselves that all of the above requirements are met.

2. Where the manufacturer is no longer trading, or relevant records required for 1 above cannot be obtained, the user may collect evidence or make statements to establish all of the following:

    a. the manufacturer had been manufacturing equipment of this type (not necessarily this model) for a significant number of years;

[1] NOTE: Obtaining this failure data is not a substitute for user collected operating experience as required unless the manufacturer can show compliance to IEC 61508-2, in which case Prior Use is not required to show device suitability.

b. the manufacturer supplied to the user's industry (or closely related industries) for a significant number of years;

c. any "special" or "limited run" device features are documented and understood with respect to failure modes;

d. the end user has sufficient information to identify the device model and version;

e. the end user has sufficient operating and maintenance information to carry out successful operation and any envisaged maintenance to the device;

f. the end user has a documented, credible plan in place to manage device failure:

- repair the device; or,
- following an assessment of the failure mechanism, effect repair of the SIF by replacing the device either:
  - with an identical device, for example from spares holding (considering obsolescence issues) or
  - with a functional equivalent which can be shown to be suitable for use in the relevant SIF as part of a management of change process (either through its own Prior Use assessment or compliance with IEC 61508-2 & -3) for the foreseeable life of the SIF.

Whichever of these routes is taken, evidence should also be sought (from the manufacturer or otherwise) as to what safety alerts, modifications, changes, etc. have occurred through the life of the device so as to establish whether the user's current knowledge of the risks of using the device is as complete as possible.

3.2. Identification and specification of the devices or subsystems

An assessment should be made between the functionality required (in the context of the requirements of the SIF(s) as defined in the Safety Requirements Specification (SRS)) and the device capabilities and limitations.

The overall capability of the device should be fully defined, together with the limitations that would impact how the device can be used within a SIF (i.e. required device functionality and environmental limitations). This should include but not be limited to:

- The identity of the device – manufacturer, type / model, version etc.
- The functional specification of the functions capable of being performed and their limitations, for example:
  - Operating range if applicable.

- Relevant process conditions, e.g. temperature, pressure, viscosity, chemical properties, etc.
- Relevant environmental conditions, e.g. vibration, EMC, extremes in temperature, etc.
- Installation requirements, including any manufacturer's specification (e.g. electrical supply, instrument air, hydraulic requirements, process connection), etc..
- Maintenance, inspection and proof test requirements, including any diagnostic features based on manufacturer's requirements and / or relevant good practice.
- Any requirements to address known systematic failures.

- The failure modes of the devices for each of the functions that is capable of being performed and any associated diagnostic functionality, including failures that can be detected by diagnostics external to the device.

In order for end users to manage Prior Use devices used in safety applications a recommended approach is to create an approved vendor document that lists "SIF approved devices". This document details the types of devices assessed by the end user for Prior Use (following this guidance) and lists the approved manufacturers / vendors that these shall be procured from. If there are any restrictions in terms of operating location or service, these should also be identified within the document. If this approach is used it should address the above points, be managed, monitored and updated regularly.

If an approved SIF device list is used then it should also include failure rate data.

Once the device capabilities and limitations have been specified, this should be checked against the requirements of each SIF that uses the device to ensure that the device provides the necessary functionality and integrity. For example – that the device response time meets the SIF requirements specification such that the SIF can respond within the process safety time.

3.3. Collection of failure data to demonstrate the performance of the devices or subsystems in similar operating profiles and physical environments

It is conceivable that a device is to be included into a SIF because it is already providing that functionality in a satisfactory manner, albeit that it has not been shown to be compliant with the requirements of IEC 61508. The device may have also been extensively used in equivalent (or near equivalent) applications at many other facilities.

Where this is the case, relevant and sufficient failure data should be available in order to confirm that the device has provided service under the conditions which will be demanded by the SIF and to identify any conditions which may be different to that which the device has previously been exposed. The failure data that should be available is discussed in Appendix A.

The following should be collected in order for the end user to make this assessment:

- Device failure data records (refer to the guidance provided in EEMUA 222 and HSE OG54 for further information relating to device failure data records), Additional guidance is available on proof testing which may provide further information on the data to be collected from failures.

- Records of any modifications that have been necessary to the device

- Records of any failures, and for systematic failures how these were addressed

  Note: There should be a reliable system in place to detect and record failures to ensure confidence in the failure records. Failures should be readily categorised in terms of safe/dangerous, revealed/unrevealed, the failure type and cause. All failures should be recorded consistently (refer also to Appendix A). If historical data of random hardware failures cannot be categorised into safe/dangerous, revealed/unrevealed then all the failures should be treated as dangerous unrevealed failures.

Generic failure data or failure data provided by the manufacturer should not generally be used as this does not demonstrate qualitative suitability under the user's operating conditions nor does it support a failure rate that relates to the user's operating conditions. If generic or manufacturer's failure data is used reference should be made to the caveats provided in Appendix A.

Note that however the failure data is determined, it should be credible, traceable, documented, justified and based on field feedback from similar devices used in a similar operating environment.

3.4. Volume of the operating experience

It is expected that, if the device is to be demonstrated to be suitable using the Prior Use approach, it will have had significant and reliable service in equivalent (or near equivalent) operations – refer to Appendix A.3 for information on the confidence of failure data. The following sources may be considered in order for the end user to make this assessment:

- the number of devices;

- the number of years that the device has been used in equivalent (or near equivalent) applications at a facility;

- the different applications for which the device has been used at a facility, where this is relevant to the Prior Use assessment;

- whether the device has been used at other of the user's facilities, so long as there is confidence in the operating environment and experience data reported by that facility.

In the case of field devices (for example, sensors and final elements) fulfilling a given function, this function is usually identical in safety and non-safety applications, which means that the device will be performing in a similar way in both type of applications. Therefore, consideration of the performance of such devices in non-safety applications may be included in the overall volume of operating experience.

However, non-safety related data is comparable to safety related data only where the application is similar in terms of duty and environment on both the wetted and non-wetted parts of the device (for example process fluid characteristics [clean, dirty, viscous], temperature, corrosiveness, indoor or outdoor service).

If an approved SIF device list is used then it should only include devices that have significant and reliable operating experience and devices should be removed when they show a history of not performing in a satisfactory manner.

3.5. Assessment of FPL devices for use in SIL1 or SIL2 SIFs

Devices programmable using a Fixed Programming Language present additional failure modes associated with their configuration and the software implementing their functionality, over and above those for a non-programmable device. Whilst the operating experience required for sections 3.3 and 3.4 is relevant to these failure modes, specific systematic failures can be introduced through inappropriate configuration in a FPL that will not necessarily be revealed through operating experience.

When considering the operating experience of a FLP programmable device, devices should normally only be considered to be identical (and hence relevant for operating experience collection) if they are both devices that are physically the same and they have the same firmware version.

Where there are multiple firmware versions among the population being considered for prior use, users must carry out an impact analysis on the differences between the firmware versions. This shall include a proportionate review of the manufacturer's change management evidence associated with the firmware revisions e.g. reason for the change(s), specification, regression testing etc. If the impact analysis determines that the differences between the firmware versions do not have an adverse effect on the SIF application, the relevant firmware versions can be included in the prior use demonstration.

Evidence must be collected regarding all possible functions (for example configurable options and settings) of the device, including those that are not used in the SIF application in question. For each function, the user must document:

- whether the function is in use;
- confirm that the function is correctly programmed for the SIF application (i.e. that the fixed programming parameters are suitably specified) if it is in use;
- confirm that the function is correctly disabled if it is not in use;
- confirm that the function is unlikely to interfere with the SIF application if it is not in use.

The above may simply consist of a table of the device functions, their configuration, and a logic argument regarding unused functions and their likelihood to interfere.

- In understanding whether or not unused programmable functions can affect the SIF application there may be benefit in reviewing other applications around the site where the same devices are used but with some of these programmable functions

activated. This may assist the user in making a judgement of suitability provided these functions can be demonstrated to have no impact of the safety functionality of the device. Refer to Appendix C for an example Parameter Checklist.

When considering the functions of the device, the full range of parameters that can be configured in the FPL need to be considered, including but not limited to those associated with interface (input/output) signals, modes of operation and processing functions, even if not associated directly with the SIF in question.

The user should also document whether particular functions used in the application in question are sufficiently unique to this application to invalidate the collection of data as required by section 3.3.

This analysis requires access to data needed to confirm the field configuration of the device. This may require consultation with the Original Equipment Manufacturer and/or investigation of programming by the user.

Following the guidance in this section is not sufficient to show that a FPL device is suitable for use in SIL3 applications. Refer to BS EN 61511-1 11.5.4.4.

3.6. Judgement of device suitability

Based on the evidence collected for the Prior Use demonstration, the end user should make a judgement on the suitability of the device for a particular application. The judgement should demonstrate that:

- there is confidence that the device was designed in a systematic way to control systematic faults through the device history, versions and modifications.
- there is confidence in the random hardware failure data collected.
- known systematic failures have been addressed
- requirements associated with FPL programmable devices have been addressed

If the device is deemed to be suitable a statement should be provided to that effect, i.e. that the device is suitable for use in a SIF for a specified application and that the Prior Use evidence provided is sufficient to meet the Prior Use requirements of IEC 61511-1.

From the outcome of the assessment, an action plan may be developed for the device, for example to:

1. replace the device with a certified device (as part of a scheduled plan)
2. limit the use of the device to particular situations
3. carry out additional work to improve the Prior Use demonstration, e.g. collect more data, carry out a Failure Mode Effects and Criticality Analysis (FMECA) etc.
4. identify any measures (e.g. increased maintenance, inspection and proof testing) required, e.g. whilst the Prior Use demonstration is being improved.

The statement of suitability, action plan along with the information gathered in sections 3.1 to 3.5 above should be maintained as part of the device's Safety Manual and subject to management of change.

Appendix A Random Hardware Failure rate calculations

The demonstration of Prior Use by the end user involves the recording of failure information. This recording of failure information provides the opportunity to determine appropriate failure data for the devices or devices to be used in SIFs.

A.1 Sources of Failure Data

Where an end user has limited operational data, or there is uncertainty regarding the robustness of the operational data for a device, there are other sources of random (not systematic) failure data that might be considered. These may include:

- Manufacturers failure rate data
- Generic failure rate data, from sources such as EEMUA, FARADIP, OREDA etc.

However, great care should be taken when using any of these other sources. Firstly, manufacturers will almost certainly have no direct experience of the use of the items under conditions similar to those of the end user. Furthermore, the data provided by manufacturers is often simply a synthesised prediction of performance that they are hoping for from the product.

Secondly, with the generic failure rates to be found in databases there is no guarantee that the device that the end user is considering will be similar in performance to the database figure. Any use of generic data should have appropriate justification for its appropriateness and should be regarded as a provisional figure until real experience is available to support or reject the figure.

Whilst other sources of data are useful for comparative purposes or whilst data is being gathered, end users own failure data should be used to calculate random hardware failure rates with prior use demonstrations. This represents the failure data of a given device in a given service and operating environment – see also A.4 below.

A.2 Recording Failure Information

One mechanism to gather failure rate data for a device is through analysis of records held within a maintenance management system (or equivalent), which should indicate the number of devices in use, the period of time the device has been in use for and the record of any failures and failure modes during that time. The end user should have confidence in their maintenance management system to ensure that records are kept correctly and are up to date. As discussed in Section 3, the system should sufficiently reliable to be able to accurately detect and record failures to ensure confidence in the failure records. Failures should be readily categorised in terms of safe/dangerous, revealed/unrevealed, the failure type and cause.

The failure recording method should consider collecting information covering: repair time; type, nature and location of the fault; environmental conditions; actions taken to replace or repair; person involved; equipment used; spares required and the time from installation until the failure.

For field equipment such as sensors and final elements, the function of the device is usually the same whether the device has been used in a safety or non-safety application;

therefore, failure data from both applications is acceptable. Non-safety related data is comparable to safety related data only where the application is similar in terms or duty and environment on both the wetted and non-wetted parts of the device (for example process fluid characteristics [clean, dirty, viscous], temperature, corrosiveness, indoor or outdoor service).

Where failure data has been obtained from a maintenance management system, periodic reviews of the data applicable to the device should be performed after it has been deemed suitable for a Prior Use claim, for example as part of periodic review and Functional Safety Assessment stage 4. This will provide additional evidence of suitability and provide a mechanism by which previously unidentified failure modes can be detected.

A.3 Confidence of Failure Data

It is essential that the persons carrying out the assessment are competent in the various activities required.

The assessment must demonstrate a confidence that the device is fit-for-purpose for use within the Safety Instrumented Function, this must also include assurances of the operating conditions and environment together with any ancillary equipment which may be required for or have an effect on the failure data of the device

In order to demonstrate confidence in the results of the assessment, all stages (collecting, reviewing, analysing and calculating) that provide the failure data should be sufficiently detailed, comprehensive and fully auditable, where assumptions have been made, they should be substantiated with supporting information. The source of any calculation methods used should be referenced and shown to be appropriate for the assessment.

It should be noted that the methods used to determine failure data from actual failure records are always calculated predictions based upon assumptions and limited operational time. The methods used to determine the failure data must be appropriate to the data available to give confidence that the resulting failure data is sufficiently conservative.

For example, if a large number of device failures (n) have been recorded then, based on the assumption of constant failure rate, the simple formula

$$\lambda = n/T$$

can be used to calculate the dangerous failure rate based on observed site failure data, where: λ is the observed dangerous failure rate, n is the number of dangerous failures found in t operational hours, T is the cumulative time of N devices over time t, i.e. T=Nt. E.g. using n=10, N=10, t=10 then λ=0.1 failures per year.

Where the number of failures is small, even zero, then it will necessary to make a statistical interpretation of the failure data and again for the reasons of simplicity to assume a constant failure rate. IEC 61511-2 proposes that the Chi-square test is a suitable method in this case using an upper bound confidence of 70%.

A worked example using this method is given in Appendix C.

A.4 Other considerations for determining failure data

Where evidence derived from an end user maintenance management system is insufficient or not available, the end user may consult with other end users (for example through trade bodies such as EEMUA) to ascertain if failure data is available from similar applications on other sites.

Should suitably credible, traceable and justified failure rate and failure modes still not be available from these other sources, the end user may consider using other available failure data, such as generic failure data, manufacturer's failure data or data determined from a failure mode analysis (e.g. Failure Modes Effects Analysis (FMEA) / Failure Modes, Effects and Criticality Analysis (FMECA) / Failure Modes, Effects and Diagnostic Analysis (FMEDA)).

Use of generic or manufacture's data may also be considered as a baseline for comparison against user collected data.

Any failure mode analysis (FMEA / FMECA / FMEDA) should only be completed by a suitably independent and competent person. Even then, there is no guarantee that any failure rate derived from such an exercise will match eventual experience.

The challenge, where non site-specific failure data is to be used, is to demonstrate that the values selected are appropriate for the site in question.

In reality, this means using, for example, conservative failure data based upon generic data and / or (possibly de-rated) manufacturer's / analysis data for PFDavg calculations and then planning to record site-specific data followed by a review to determine whether the data used is sufficiently conservative. The prior use demonstration will only be fully complete when the data used has been shown to be appropriate once operational experience has been gained.

Appendix B Example of failure data collection and analysis

Data Gathering of Failure Data

Twelve vibrating fork level switches has been utilised throughout the Tank Farm area in safety applications since 2010 up to and including 2020.

The following table provides an extract of all failures, random and systematic, involving the 12 point devices as well as the associated radar level indicators from 2010 to 2020. It is assumed in this example all devices were installed in 2010.

When collecting failure data, each failure should be categorised as either a **Systematic Failure** or **Random Hardware Failure**. Systematic failures should be eliminated or other appropriate measures should be taken to manage the risk. Random hardware failures should subsequently be used in calculating the failure rate for the device.

From the information in this example, the collection, analysis and quantification of the failure data can be reviewed in appendix C

Tag Number	Failure Record	Date	Duty	Service	Classification	Failure	Reason for Failure	Event	SD	SU	DD	DU	Remarks	Maintenance Repair	Time to Repair
LS_001 (Switch)	2008/03	13/03/ 2008	Tank 301 High Level Trip	Diesel	Clean	Corrosion of Tines causing loss of mass and increased frequency	Systematic failure	Fail dangerous				1	Corrosion not noticed during visual inspection. safety related issue as device does not detect increased level. **Systematic failure-Dangerous Undetected**	Device replacement	<8 hrs
LS_005 (Switch)	2009/02	16/02/ 2009	Tank 305 High Level Trip	Diesel	Clean	Tine sheared	Random failure	Fail to danger, detected by diagnostic			1		Mechanical failure increased detected by diagnostics – safety related. **Random failure**.	Device replacement	<8 hrs
LS_011 (Switch)	2009/09	21/09/ 2009	Tank 311 High Level Trip	Diesel	Clean	Incorrect setting of parameters in device head and switch	Systematic failure	Possible dangerous failure				1	Failure would only be detected during Proof test. **Systematic failure - Dangerous Undetected.**	Routine Maintenance – Proof Test	<1 hr
LI_006 (Radar)	2010/12	18/12/ 2010	Tank 306 High Level Trip	Gasoline	Clean	Incorrect setting of dielectric constant in Radar Device	Systematic failure	Fail dangerous				1	Failure would only be detected during Proof test. **Systematic failure - Dangerous Undetected**.	Routine Maintenance – Proof Test	<1 hr
LI_016 (Radar)	2011/01	03/01/ 2011	Tank 316 High Level Trip	SCB	Clean	Corrosion leading to Radar Antenna break away	Systematic failure	Fail dangerous				1	Corrosion not noticed during visual inspection. safety related issue as device does not detect increased level. **Systematic failure-Dangerous Undetected**	Device replacement	<8 hrs
LI_009 (Radar)	2011/07	12/07/ 2011	Tank 309 High Level Trip	Additive	Clean	In correct selection of frequency parameter	Systematic failure	Possible dangerous failure				1	Failure not noted during simulation type proof test, only detected during physical filling test. **Systematic failure - Dangerous Undetected**..	Device replacement With correctly specified frequency parameters	<48 hrs

Calculations – Random Hardware Failures

There are many sources and techniques for performing failure data calculations. Various formulae and techniques can be found in IEC 61508, IEC 61511, ISA-TR84.00.02-2015 and IEC ISO 14224. There are also many technical publications on failure data assessments which provide further calculations.

Recording of Systematic Failures and Prior Use Demonstrations

Details of systematic failures observed over a period of time can be used as part of the evidence to support a Prior Use demonstration. During the observed period of time it would be expected that all failure mechanisms of the device would be recorded. It is likely this will include both random and systematic failures. The table above shows details of both types of failures. It would be expected that systematic failures would be analysed at the time of detection and in most cases it should be possible to implement measures to eliminate the failure mechanisms. If the failure mechanism is eliminated then it should not be included in the overall failure data calculations moving forward. However, in some cases it may not be possible to fully eliminate the systematic failure mechanism, e.g. it may be specific to that application. This could result in an overall increased failure rate of the device for that application. In that case the contribution of the systematic failure should be added to the random failure rate to provide an overall dangerous failure rate for the device.

Records kept should include the actions taken to eliminate the systematic failure mechanism – this should be included within the device's Safety Manual. In cases where it is accepted as an additional failure rate then full justification should be provided.

A full example of all aspects related to a Prior Use justification is provided in Appendix C.

Appendix C Worked Example of Prior Use Demonstration

As a result of a functional safety review of Tank Farm operations an operator is required to demonstrate that an installed Tank overfill system can achieve a target Safety Integrity Level (SIL) of 1. The existing system has been subjected to a review by site engineering and the decision is to replace the existing relay logic solver device with an IEC 61508 compliant device that is SIL1 capable. Fortunately the existing final element valve assembly (Actuator, Solenoid Valve and Valve Body) has an IEC 61508 assessment stating that the valve assembly is suitable for use in a SIS up to SIL2.

The existing system consists of Two tank sensors a high level probe (Non Programmable) and a Radar level gauge (FPL Device) neither are certified devices and therefore the operator wants to build up a prior use demonstration against IEC 61511 Clause 11.5.2, 11.5.3 and 11.5.4 prior use requirements to evaluate that the devices have a sufficiently low likelihood of systematic faults and are sufficiently reliable so as to achieve the overall target PFDavg or dangerous failure rate requirement for the SIF while meeting the architectural constraints requirements.

The high level probe device is a point level switch and was manufactured in 2010 and the OEM vendor states it has a useful life of 15 years and the OEM will no longer support the product from 2025. 12 similar devices were purchased and installed in May 2010 as a part of the same Tank Farm level switch upgrade..

The Radar level gauge is a time of flight analogue device and was also manufactured in 2010 and the OEM vendor states it has a useful life of 20 years and the OEM will no longer support the product from 2030. 12 similar devices were purchased and installed in May 2010 as a part of the same Tank Farm level monitoring upgrade

The following tables provide an example Prior Use assessment (completed in 2020) for a SIL1 system (higher SILs would require proportionately more robust demonstrations) which details the review process that the company followed and the evidence used to fulfil the Prior Use requirements.

Manufacture's Quality, Management and Configuration Management Systems (Refer to section 3.1)

Requirement	Evidence
Assessment of the manufacturer's systems by the use of the device to establish all of the following; a. the OEM has a quality management system in place; b. the OEM has been manufacturing equipment of this type (not necessarily this model) for a significant number of years; c. the OEM has been supplying to the user's industry (or closely related industries) for a significant number of years; d. the device has been manufactured in appreciable numbers over an appreciable time period (i.e. it is not a "special" or "limited run" device); e. the OEM applied relevant national or international product standards to design and manufacture of the device; f. installation, operating and maintenance manuals for the device are available; g. the OEM has procedures in place for revision control for modifications to the device; h. the OEM has procedures in place for returns and equipment failure assessments that require them to take appropriate action;	The following is an example of argument / justification for an IEC 61511-1 Clause 11.5.2 and 11.5.3 prior use requirement and the type of evidence that would support the demonstration. a. The OEM has a current ISO9001:2015 certificate reference OEM_QP_2015, the original QMS certificate was issued in 2000 and has been renewed as required and covers the date of manufacture of the device. The OEM was audited in 2010 and again in 2015 reference audit report AR_AVL_123_2015 Revision A b. The OEM has been manufacturing level probes since 2000, the OEM ceased producing the device under review in 2012 replacing it with device of similar construction with enhanced firmware features. c. The OEM has been supplying to the process industry and specifically to Tank Farm Operators since 2000. d. The probe type under review was manufactured for 7 years from 2006 to 2012 and the OEM records show 8000 where supplied, but, cannot guarantee all have been put in to service. e. The device is designed for use in a hazardous environment and as such designed and constructed to meet the relevant 2006 EU Directives and IEC/ISO standards as listed in the OEM device operating and maintenance manual reference: LP-2006-20 Issue 01. f. The device operating and maintenance (O&M) manual ref: LP-2006-20 Issue 01 is available. g. The O&M manual has a revision history and parts configuration management list included. The device was IP rating of the device was changed in 2008 from IP54 to IP55. In 2010 the colour of the device head was changed from blue to yellow. The assessor does not consider that these changes effect the PU history. h. The OEM has a customer complaint and returns service, but, due to the nature of the process market and the potential health risks due to poor decontamination have never received a returned device from the operator or any similar site. The OEM has stated that when a device is returned it is assessed and where appropriate the findings are shared through a safety bulletin with agents and companies who have procured the

Requirement	Evidence
	devices directly from the OEM. The OEM has no record of a safety bulletin being issued for the device under review.
i. the OEM has processes to deal with any obsolete devices, for example a migration path to a new device;	i. The OEM has stated the device has a useful life of 15 years and will no longer be supported from 2025. The OEM ceased producing the device under review in 2012 replacing it with device of similar construction and size with enhanced firmware features. The new device is considered a direct replacement and can be purchased to the same specification and flange sizing to the device under review. This Prior Use assessment does not consider the suitability of the replaced device.
j. the OEM has procedures for dealing with device recalls or safety modifications;	j. Refer to h. above. Notifications of safety modifications are sent out through a safety bulletin with agents and companies who have procured the devices directly from the OEM. The OEM has no record of a safety bulletin being issued for the device under review
k. the OEM has procedures in place for assessing equipment failure data for the device.	k. Refer to h. The OEM has stated that when a device is returned it is assessed and where appropriate the findings are shared through a safety bulletin. The OEM has no record of a safety bulletin being issued for the device under review.

Identification and Specification of the Devices or Subsystems (Refer to section 3.2)

Requirement	Evidence
An assessment should be made between the functionality required (in the context of the requirements of the SIF(s) as defined in the Safety Requirements Specification (SRS)) and the device capabilities and limitations.	Site Engineering have developed a SRS (document reference: T306_LS_001_SRS Revision A) for the device under review which is generally in accordance with IEC 61511 Clause 10.3.2 requirements. The overall Tank Farm systems have been subjected to an Functional Safety Assessment Stage 4 in accordance with CDOIF "Functional Safety Management of Installed Safety Instrumented Systems" reference T306_FSAS4R_001 Revision A
The overall capability of the device should be fully defined, together with the limitations that would impact how the device can be used within a SIF (i.e. required device functionality and environmental limitations). This should include but not be limited to:	The proposed High Level SIF is a simplex architecture (1oo1) consisting of the Probe T306_LS_001 (Sensor Subsystem) , Relay T306_HLR_001 (Logic Solver Subsystem) and Air Fail Closed Spring Return Quarter Turn Ball Valve Assembly T306_XCV_001 (Final Element Subsystem). The device is a point level switch, when not covered by the liquid, the level probe vibrates at its natural frequency and is monitored by an integral detection circuit, when the liquid rises and covers the probe the frequency of oscillation drops and on detection changes the output state to the relay that goes open circuit causes the solenoid to change state releasing the air and the spring drives the inlet valve to Tank T306 closed stopping the filling of the tank.
a. The identity of the device – manufacturer, type / model, version and firmware version etc.	a. The device type is a vibrating fork level probe manufactured by Acme Limited model HLS-00Z version A, with firmware version B, switching the load via 2 potential-free simultaneously changeover contacts. For safety applications specific terminals are instructed by the OEM for safety models and these will be used for this device as well and have been added to the devices safety manual documentation.
b. The functional specification of the functions capable of being performed and their limitations, for example: • Operating range if applicable. • Relevant process conditions, e.g. temperature, pressure, viscosity, chemical properties, etc. • Relevant environmental conditions, e.g. vibration, EMC, extremes in temperature, etc. • Installation requirements, including any manufacturer's specification (e.g. electrical supply, instrument air, hydraulic requirements, process connection), etc.	b. The probe is designed to operate as a high level liquid detection device only, the output is direct switching onto the relay circuit. • The probe is top inserted into the tank and trips at 90% liquid level (Equivalent height 7.6m with volume 42.08m^3) with switch position set to >0.5 g/cm^3 • T306 operates at ambient pressure and temperature conditions, chemical properties are listed on the COSHH Data Sheet reference: SDS-0123 Rev: C • Humidity up to 100%, Shock and vibration as per IEC60068, EMC as per EN 61326, temperature extremes only as UK ambient temperature conditions • The installation is as per OEM installation and commissioning manual reference: LP-2006-19 Issue 00, the device is flange mounted with no temperature spacer required. The probe length is 380mm from flange face to tip, there are no contamination issues or special conditions for top entry installation, the electrical supply is within OEM voltage tolerance, ingress protection is IP55.

Requirement	Evidence
• Maintenance, inspection and proof test requirements, including any diagnostic features based on manufacturer's requirements and / or relevant good practice.	• The device details have been entered into the maintenance management system as asset number P3_T306_LS_001, the visual inspection interval is set to 12 months and the function test to 14 months. Both the existing inspection and function test procedures are based on the OEM O&M manual ref: LP-2006-20 Issue 01 and the OEM installation and commissioning manual reference: LP-2006-19 Issue 00. A SIF proof test has been developed for the SIF loop document reference: SIF_T306_LS_001_PT Revision 0 and is also based on the OEM manuals. The proof test includes testing of the diagnostics as the OEM instructions. The probe will be removed and submerged in water 1 g/cm^3 (for switch requirement density >0.5 g/cm^3) for the proof test and therefore proof test coverage for the switch will initially be set to 100% for the sensor subsystem PFDavg calculation.
• Any requirements to address known systematic failures.	• Identified systematic failures include: - Potential use of incorrect fuse size (0.5A slow-blow fuse required), label added to system to ensure correct fuse used. - OEM has identified the influences of process operating conditions on device performance characteristics and these have been considered in the design. - High viscous liquids can cause switching delays, the current process liquid is not considered highly viscous, but a change of characteristics would be checked by process design. - Non alignment of metal housing cap and fixing with locking screw with potential for liquid ingress and damage. Cap must be removed to access test button to activate device function test and dip switches. Checking of fixing requirement included in annual visual inspection procedure. - Configuring dip switch for min safety mode instead of max safety mode. . Checking of dipswitch position included in proof test and visual inspection procedure. - Corrosion, corroded forks will increase the vibration frequency causing a spurious trip of the inlet valve and raising a diagnostic fault alarm. HSE rr823 provides guidance on potential effects of operational deterioration in ageing plant and provides guidance. During the Proof test and inspection the probe is removed and will inspected at that time for corrosion and deterioration effects - Not sufficient capable cable length allowed for removal of the probe for testing, this was confirmed during installation and no changes have been made. - The above functional capabilities and limitations have been added to the device's safety manual documentation

Requirement	Evidence
c. The failure modes of the devices for each of the functions that is capable of being performed and any associated diagnostic functionality, including failures that can be detected by diagnostics external to the device.	c. The device is capable of two failure modes max (high trip) or min (low trip). The proof test covers the OEM test sequence for high level detection including wiring check. Removing and lowering the probe into an equivalent liquid causes the contacts to open breaking the circuit and SIF to trip. Removal of the device from the liquid causes the contacts to close and the SIF can be reset. No external diagnostics are available for this device. The device has no integral diagnostic features'.
d. Approved vendor document that lists "SIF approved devices" including approved manufacturers / vendors that these shall be procured from. If there are any restrictions in terms of operating location or service, these should also be identified within the document. If this approach is used it should address the above points, be managed, monitored and updated regularly.	d. An approved vendor list has been created for the site, document reference AVL_SIS_001 Revision D, the probe OEM is included on the list and the new model is certified under IEC 61508 and therefore can be replaced following normal change control procedures. No restrictions are in place for this vendor in terms of operating location, servicing is provided by the local OEM office. The list is managed by and all approvals are through the Site Engineering Manager only.
e. If an approved SIF device list is used then it should also include failure rate data.	e. 12 devices were purchased and installed in May 2010 as a part of the Tank Farm level switch upgrade. This equates to approximately 1051200 (120 years) operational hours to date, excluding any downtime for bypasses, maintenance and testing. The site has recorded 2 safety related hardware failures and 1 Systematic Failure with a root cause analysis being carried out on all three, document references: RCA_HLS_124 Revision B, RCA_HLS_145 Revision D and RCA_HLS_170 Revision C. The RCA defines the failures as dangerous. Therefore based on the collected field data and an upper bound confidence of 70% the failure rate is 3.44E-06 Hours.
f. Once the device capabilities and limitations have been specified, this should be checked against the requirements of each SIF that uses the device to ensure that the device provides the necessary functionality and integrity. For example – that the device response time meets the SIF requirements specification such that the SIF can respond within the process safety time.	f. The SIF requirements are captured in the SRS (document reference: T306_LS_001_SRS Revision A) developed by Site Engineering for the device under review which is generally in accordance with IEC 61511 Clause 10.3.2 requirements which includes process safety and SIF response times. The device functional capability and limitations have been reviewed against the SIF requirements and are acceptable for the applications.

Collection of Failure data to demonstrate the performance of the Devices or Subsystems in similar Operating profiles and Physical environments (Refer to section 3.3)

Requirement	Evidence
It is conceivable that a device is to be included into a SIF because it is already providing that functionality in a satisfactory manner, albeit that it has not been shown to be compliant with the requirements of IEC 61508. The device may have also been extensively used in equivalent (or near equivalent) applications at many other facilities.	The level probe T306_LS_001 and 11 other probes were installed in 2010 to act as high level trip / alarm functions, although not previously designated as a SIF they have been extensively used in an equivalent SIF application “Tank Overfill”.
Where this is the case, relevant and sufficient failure data should be available in order to confirm that the device has provided service under the conditions which will be demanded by the SIF and to identify any conditions which may be different to that which the device has previously been exposed. The failure data that should be available is discussed in Appendix A.	12 installations equates to approximately 1051200 operational hours, excluding downtime for bypasses, maintenance and testing. The devices are inspected every 12 months and function tested every 14 months. 2 hardware failures and 1 systematic failure have been recorded, and defined as dangerous by RCA. Based on the field data and an upper bound confidence of 70% the failure rate is 3.44E-06 Hours (example calculation provided below)
The following should be collected in order for the end user to make this assessment: • Device failure data records (refer to the guidance provided in EEMUA 222 and HSE OG54 for further information relating to device failure data records), Additional guidance is available on proof testing which may provide further information on the data to be collected from failures. • Records of any modifications that have been necessary to the device • Records of any failures, and for systematic failures how these were addressed	With respect to the level probe for the SIL1 target and considering the 3 recorded failures (2 hardware and 1 systematic) the field experience required, based on a single sided confidence of 70%, the PFDavg for a Low demand mode of operation, with a Proof Test Interval of 8760 hours and if Proof Test Coverage was assumed to be 100%, using the ISA simplified equations for a single channel system would be 0.017 for the sensor. This falls within the SIL1 band based on the IEC 61511-1 Table 4 and the level sensor could therefore be considered suitable, with respect to random hardware failure rates only, for inclusion within a SIL1 Safety Instrumented Function subject to the overall PFD of the SIF being acceptable (which would be determined by PFD calculations in the usual way)
Note: There should be a reliable system in place to detect and record failures to ensure confidence in the failure records. Failures should be readily categorised in terms of safe/dangerous, revealed/unrevealed, the failure type and cause. All failures should be recorded consistently (refer also to Appendix A). If historical data of random hardware failures cannot be categorised into safe/dangerous, revealed/unrevealed then all the failures should be treated as dangerous unrevealed failures.	Since 2014, trip and SIF proof tests HSE OG54 guidance, failure modes are categorised in line with appendix 4. All failures are recorded by the tester using a set of key words and then analysed by Site Engineering before entry into the MMS as either dangerous, safe or systematic.
Generic failure data or failure data provided by the manufacturer should not generally be used as this does not demonstrate qualitative suitability under the user’s operating conditions nor does it support a failure rate that relates to the user’s operating conditions. If generic or manufacturer’s failure data is used reference should be made to the caveats provided in Appendix A.	No modification have been made to the devices to date.
Note that however the failure data is determined, it should be credible, traceable, documented, justified and based on field feedback from similar devices used in a similar operating environment	The recorded systematic failure was the non-alignment of the housing cap and rain water entering and causing the short-circuit of electronics and device to shut down. The cap was removed to access test button to activate device function test and dip switches. Checking the correct fitting of the cap and fixing of the locking screw is now included in the function test n procedure.

Below is an example calculation (completed in 2020) using the Chi-square test method, as proposed in IEC 61511 to determine the failure rate of the level switch, under Prior Use assessment, using an upper bound confidence of 70% to show how the failure data used in the above table may have been calculated.

As stated above, 12 similar devices were purchased and installed in May 2010, this gives an observed cumulative total of approximately 1051200 (120 years) operational hours to date, excluding any downtime for bypasses, maintenance and testing. During this time the site has recorded 2 safety related hardware failures assessed as dangerous failures.

As the number of dangerous failures is small, it has been decided by the team to make a statistical interpretation of the failure data and for the reasons of simplicity to assume a constant dangerous failure rate. IEC 61511-2 proposes that the Chi-square function ($\mathbf{X^2}$) is a suitable method and that an upper bound confidence of 70% would provide a suitable confidence in the calculated average failure rate.

In order to determine a value of $\mathbf{X^2}$ it is necessary to specify to parameters, the degrees of freedom (**df**) and the confidence level (α). These parameters are the two axis values for the columns used in the chi-square distribution tables to determine the value of X^2, in this case for 70% confidence interval, from the tables, the value is 7.23.

For the purpose of this example it has been assumed that the results of the end-users operating experience has resulted in the following data:

N = 12, is the number of level switches in the assessment

t = 87600 hours (2010→2020), is the observed operational time for one level switch

T = 1051200 hours, is the cumulative operational time (Nt) for all 12 level switches,

n = 2, is the number of dangerous failures found in T operational hours, and

df = 2(n+1) = 2(2+1) = 6 degrees of freedom

α = (1 – confidence level of the $\mathbf{X^2}$ distribution), which for a 70% confidence interval = (1-0.7) = 0.3

$\boldsymbol{\lambda_{70\%}}$ = Dangerous failure rate at a 70% confidence interval

Therefore for a sample of 2 (n) dangerous failures observed over a cumulated observation time of 1051200 (T) the upper bound confidence can be calculated by using the $\mathbf{X^2}$ function, where $\lambda_{70\%}$ can be evaluated by:

$$\lambda_{0,7} = \frac{1}{2T}\chi^2_{0,3,2(n+1)}$$

and there are 70% chances that the actual value is lower (i.e. better) than that. Using this approach, this confidence upper bound exists even if there had been no dangerous failures observed. It is always pessimistic compared to $\lambda_{average}$ but, it is increasingly accurate when T and/or n (and therefore df) increase (refer IEC 61511-2:2016 Appendix A.11.9.4)

In this case the dangerous failure rate at a 70% confidence interval will be:

$$\lambda_{70\%} = (1/2102400) \times 7.23$$

$$\lambda_{70\%} = 3.44E\text{-}06 \text{ per hour}$$

Therefore based on the collected field data and an upper bound confidence of 70% the dangerous failure rate is 3.44E-06 per hour

This dangerous failure rate can then be used to estimate an Average Probability of Failure on Demand (PFDavg) to determine if the level switch could be used as part of a SIF with a target Safety Integrity Level (SIL) of 1.

For example, for a Low demand mode of operation, Proof Test Interval (Ti) of 10200 hours (14 months) and if Proof Test Coverage was assumed to be 100%, using the ISA simplified equations for a single channel system the estimated PFDavg would be:

$$\text{PFDavg (sensor)} = 0.5(\lambda_{70\%} TI) = 0.5(3.44E\text{-}06 \times 10200) = 0.017$$

This falls within the SIL1 band based on the IEC 61511-1 Table 4 and the level sensor could therefore be considered suitable, with respect to random hardware failure rates only, for inclusion within a SIL1 Safety Instrumented Function, subject to the overall PFD of the SIF being acceptable (which would be determined by PFD calculation in the usual way).

The Chi Square method is described in chapter 5 of 'Reliability, Maintainability and Risk Eighth Edition: Practical Methods for Engineers including Reliability Centred Maintenance and Safety-Related Systems' and IEC 61511-2:2016 Appendix A.11.9.4)

Volume of the Operating Experience (Refer to section 3.4)

Requirement	Evidence
It is expected that, if the device is to be demonstrated to be suitable using the Prior Use approach, it will have had significant and reliable service in equivalent (or near equivalent) operations – refer to Appendix A.3 for information on the confidence of failure data. The following sources may be considered in order for the end user to make this assessment: • the number of devices; • the number of years that the device has been used in equivalent (or near equivalent) applications at a facility; • the different applications for which the device has been used at a facility, where this is relevant to the Prior Use assessment; • whether the device has been used at other of the user's facilities, so long as there is confidence in the operating environment and experience data reported by that facility.	The volume of operating experience used for the Prior Use Assessment is based on the 12 devices installed in May 2010 as a part of the Tank Farm level switch upgrade. All of the devices operate on similar products, operating at ambient conditions with similar chemical characteristics: • 12 level probe devices are used as the basis of the prior use claim; • The number of years that the level probe device has been used in equivalent applications on the Tank Farm is 120 years; • This type level probe device is used in several different applications around the site but these are not considered as equivalent (or near equivalent) applications and therefore not relevant to this Prior Use assessment; • This type level probe device is used at several of our sites around the UK and Europe with similar operating and environmental conditions, but, there is not sufficient confidence in the operating environment and experience data reported by those sites to be included in this Prior Use assessment.
In the case of field devices (for example, sensors and final elements) fulfilling a given function, this function is usually identical in safety and non-safety applications, which means that the device will be performing in a similar way in both type of applications. Therefore, consideration of the performance of such devices in non-safety applications may be included in the overall volume of operating experience.	The level probe T306_LS_001 and 11 other probes were installed to act as high level trip / alarm functions, although not previously designated as a SIF they have been extensively used in an equivalent SIF application "Tank Overfill and therefore, consideration of the performance of these devices in non-safety applications is included in the volume of operating experience
However, non-safety related data is comparable to safety related data only where the application is similar in terms of duty and environment on both the wetted and non-wetted parts of the device (for example process fluid characteristics [clean, dirty, viscous], temperature, corrosiveness, indoor or outdoor service).	The volume of operating experience determined for a device to be included on the SIS approved vendor list document reference AVL_SIS_001 is based on the number of recorded failures and the equipment operational years inferred as that required to achieve the lower limit of the target SIL chapter 3 of *'The Safety Critical Systems Handbook' s'.*
If an approved SIF device list is used then it should only include devices that have significant and reliable operating experience and devices should be removed when they show a history of not performing in a satisfactory manner	The level probe T306_LS_001 and the associated 11 devices on the Tank Farm have generated 120 years of equipment operational years, excluding downtime for bypasses, maintenance and testing. This is significantly greater than the required field experience.

Assessment of FPL devices for use in SIL1 or SIL 2 SIFs (Refer to section 3.5)

Requirement	Evidence
Devices programmable using a FPL present addition failure modes associated with their configuration and the software implementing their functionality, over and above those for a non-programmable device. Whilst the operating experience required for sections 3.3 and 3.4 is relevant to these failure modes, specific systematic failures can be introduced through inappropriate configuration in a FPL that will not necessarily be revealed through operating experience. In order to demonstrate Prior Use for a FPL device, evidence must be collected regarding all possible functions of the device, including those that are not used in the SIF application in question. For each function, the user must document: a. whether the function is in use; b. confirm that the function is correctly programmed for the SIF application (i.e. that the fixed programming parameters are suitably specified) if it is in use; c. confirm that the function is correctly disabled if it is not in use; d. confirm that the function is unlikely to interfere with the SIF application if it is not in use. The above may simply consist of a table of the device functions, their configuration, and a logic argument regarding unused functions and their likelihood to interfere. When considering the functions of the device, the full range of parameters that can be configured in the FPL need to be considered, including but not limited to those associated with interface (input/output) signals, modes of operation and processing functions, even if not associated directly with the SIF in question. The user should also document whether particular functions used in the application in question are sufficiently unique to this application to invalidate the collection of data as required by section 3.3. Following the guidance in this section is not sufficient to show that a FPL device is suitable for use in SIL3 applications. Refer to BS EN 61511-1 11.5.4.4.	Site Engineering developed a “Checklist of Parameter settings” for each Radar device under review (T306_PSCL_001 Revision A) based on the OEM manual and set up instructions. For each Tank the “Required” and “Not Required” parameters were identified and required setting “1 or 0 / On or Off” or numerical value identified and entered into the Checklist. These have all been subjected to verification by a team independent of the development team and a training tool box talk prepared for the Maintenance Technicians to ensure the process is understood and followed during testing, repair or Management of Change. This process was carried out in order to demonstrate Prior Use evidence for the FPL device by first identifying all of the possible functions of the device, including those that are not used in the SIF application in question and then creating a checklist of how the System is to be set up including the non-used parameters. It was also important to include an independent verification step in the checklist to reduce the risk of a systematic error during and after the device set up. For each system, the process was: a. A checklist of Parameter settings has been developed for each Tank T306_PSCL_001 Revision A, The functions not used, e.g. “Tube diameter”, Bin Type”, “Filling speed solid” are clearly identified as not used for this application based on the devices OEM set up documentation. b. The checklist table of parameters is completed by the technician and then checked against the devices OEM set up documentation by the Maintenance Supervisor. Those parameters which are automatically set by the device are also checked at this time and if not used are disabled by setting the parameter to either 0 or “Off” as required. c. When parameterisation is completed the technician verifies against the checklist table of parameters that all parameters not used during process operations are also disabled, this is then checked by the Maintenance Supervisor that all non-used parameters are disabled by setting the parameter to either 0 or “Off” as required. d. The checklist of Parameter settings is reviewed against the Operating Mode of the Tank “High or Low”, Process conditions, Liquid and Tank Characteristics to ensure there is no interference with the SIF application.

Parameter Checklist (Refer to section 3.5)

Instrument ID: L101005 Serial Number: 34956AF4 Checklist Completed by NAME:_____SIGN:_____DATE:_____
Location ID: TF 04 TK101 Version: 16.3 Checklist verified by NAME:_____SIGN:_____DATE:_____
Application: Tank High Level Firmware Version: 8.4

Parameter	Description	Factory-default Setting	Configured Setting	Impact on SIF (Y/N)*
tREF	Tank Adjustment	nonE	nonE	Yes – Changes tank characteristics and will impact actual level recorded
SP1	Setpoint 1	50% VMR	35% VMR	Yes – adjusts the point at which output is switched causing trip function
rP1	Reset point 1	0.2 in (5mm) below SP1	0.4 in (10mm) below SP1	No – Hysteresis function is disabled
ASP2	Analogue start point	0% VMR	0% VMR	Yes – adjusts the analogue start value for the output from the transmitter, changing the actual level lo range reported
AEP2	Analogue end point	100% VMR	100% VMR	Yes – adjusts the analogue start value for the output from the transmitter, changing the actual level high range reported
dS1	Switch on delay	0.0	0.0	Yes – applies a delay to the output solenoid used for the trip functionality
Dr1	Switch off delay	0.0	0.0	No – applies a delay only to the off cycle of the solenoid, not used for trip functionality
LEnG	Probe length	nonE	1000 mm	Yes – adjusts the measured level from the radar probe.
Ou1	Output configuration	Hno	Hno	Yes – Hysteresis function, normally open, used within the logic for the high level trip in the logic solver
FOU1	Output logic	OFF	OFF	No – function not used
dAP	Damping function	0.0	0.0	No – function not used

Parameter	Description	Factory-default Setting	Configured Setting	Impact on SIF (Y/N)*
S.LVL	Simulation level	50% LEnG	35% LenG	No – used for simulation test only as part of calibration.
S.Tim	Simulation duration	3	3	No – used for simulation test only as part of calibration.
S.On	Simulation mode	OFF	OFF	No – used for simulation test only as part of calibration.

*Does the configured parameter have an impact on the Safety Instrumented Function. Record justification for decision.

Judgement of Device Suitability (Refer to section 3.6)

Requirement	Evidence
Based on the evidence collected for the Prior Use demonstration, the end user should make a judgement on the suitability of the device for a particular application. The judgement should demonstrate that: • there is confidence that the device was designed in a systematic way to control systematic faults through the device history, versions and modifications. • there is confidence in the random hardware failure data collected. • known systematic failures have been addressed	The evidence collected for the Prior Use demonstration is filed in the "Prior Use Demonstration Dossier" document reference PLT3_HLS_PUD_001 Revision E, the assessor has reviewed the dossier and based on the evidence makes the following findings: • The OEM had a third party approved QMS in place at the time of device manufacture and the current QMS is ISO9001:2015 compliant. • Random hardware failure data collected is first analysed by site engineering before , entry into the MMS to ensure it is accurately described and valid, all data collected is based on field experience. The site engineering manager has oversight and all SIF failures are reviewed at a formal meeting held each month. • Systematic failures are recorded and analysed by site engineering using root cause analysis, the findings from the RCA are used to update / improve the relevant and associated procedures. All SIF procedures are subjected to a Safety Task Analysis review every 3 years. The site engineering manager has oversight and all SIF failures are reviewed at a formal meeting held each month
If the device is deemed to be suitable a statement should be provided to that effect, i.e. that the device is suitable for use in a SIF for a specified application and that the Prior Use evidence provided is sufficient to meet the Prior Use requirements of IEC 61511-1.	Based on the evidence collected for the Prior Use demonstration and filed in the "Prior Use Demonstration Dossier" document reference PLT3_HLS_PUD_001 Revision E, the assessor judges that the level probe device is suitable for use in a SIF for the specified application "Tank Overfill" in Plant 3 Tank Farm and that the Prior Use evidence provided is sufficient to consider the SIF Sensor Subsystem as SIL1 Capable for the SIF application.
From the outcome of the assessment, an action plan may be developed for the device, for example to: 1. replace the device with a certified device (as part of a scheduled plan) 2. limit the use of the device to particular situations 3. carry out additional work to improve the Prior Use demonstration, e.g. collect more data, carry out a Failure Mode Effects and Criticality Analysis (FMECA) etc. 4. identify any measures (e.g. increased maintenance, inspection and proof testing) required, e.g. whilst the Prior Use demonstration is being improved.	The suitability of the level probe for use as a SIF is limited to and for the specified application "Tank Overfill" in Plant 3 Tank Farm only. The device should not be considered suitable as a SIF Sensor Subsystem as SIL1 Capable for another SIF application unless evidence of a sufficient and suitable Prior Use Demonstration is developed for that application. The SIF must be proof tested in accordance with the SRS and the Proof test procedure, based on an interval of 14 months (as calculated by the PFD calculation ref. X). Visual inspections will be carried out at an interval of 12 months.
The statement of suitability, action plan along with the information gathered in sections 3.1-3.4 above should be maintained as part of the device's Safety Manual and subject to management of change.	The statement of suitability, action planning along with the information gathered in sections 3.1-3.4 above should be maintained as part of the device's Safety Manual and subject to management of change.

Appendix D Contents of a Prior Use Demonstration Dossier

IEC 61511 requires that for Installed systems, that have not followed IEC 61508 requirements, it needs to be shown that systematic faults are sufficiently low as not to be considered significant. The evidence to support this claim needs to be documented, for example as shown in appendix C in the form of a Prior Use Dossier with typical contents that may include the following sections:

1 **Manufacture's quality, management and configuration management systems**

1.1 OEM Quality Management and Certificate – *e.g. OEM_QP_2015*

1.2 Supplier Audit – *e.g. AR_AVL_123_2015 Revision* A

1.3 Approved Vendor List – *e.g. AVL_SIS_001 Revision D*

1.4 Functional Safety Management System

1.5 Operational Functional Safety Plan

2 **Identification and specification of the device or subsystems**

2.1 Safety Requirement Specification – *e.g. T306_LS_001_SRS Revision A*

2.2 OEM Operating & Maintenance Manual

2.3 OEM Installation & Commissioning Manual

2.3 Evidence of same devices operating in similar conditions – e.g. *SAP or similar*

2.4 Functional Safety Assessment Stage 4 – *e.g. CDOIF FSM of Installed SIS*

3 Collection of failure data to demonstrate the performance of the devices or subsystems in similar operating profiles and physical environments

3.1 Recorded Hardware failures, analysis and recommendation for improvement

3.2 Recorded Systematic Faults, analysis and recommendation for improvement

3.3 Basis of failure data collection and method of recording

3.4 Generic data used and justification

4 Volume of operating experience

4.1 Number of devices included in prior use demonstration

4.2 Number of years in equivalent (or near equivalent) applications in this facility

4.3 Number of years in equivalent (or near equivalent) applications in other facilities

4.3 Field data for equipment operations/demands or equipment operational hours

4.4 Average Probability of Failure based on field collected failure data

5 Assessment of FPL devices for use in SIL1 or SIL2 SIFs

5.1 Number of devices included in FPL prior use demonstration

5.2 Checklist of Parameter Settings – *e.g. T306_PSCL_001 Revision A*

5.3 Verified Checklist of Parameter Settings – *e.g. T306_PSCL_001 Revision A*

5.3 OEM Parameter Settings and Set Up Instructions for FPL

5.4 Lock Out Record for FPL devices

6 Judgement of device suitability

6.1 Statement of capability as a Safety Instrumented Function sub system

6.2 Achieved Safety Integrity Level

6.3 Findings and Recommendations

6.4 Action Plan

Appendix E Abbreviations

Abbreviation	Description
CA	Competent Authority
CDOIF	Chemical and Downstream Oil Industries Forum
EEMUA	Engineering Equipment and Materials Users Association
EMC	Electromagnetic Capability
FARADIP	Failure Rate Data in Perspective
FMEA	Failure Modes and Effect Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FMEDA	Failure Modes, Effects and Diagnostic Analysis
FPL	Fixed Program Language
FTS	Fail To Safe
HFT	Hardware Fault Tolerance
HSE	Health and Safety Executive
LI	Level Indicator
LS	Level Switch
MCC	Motor Control Centre
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
OEM	Original Equipment Manufacturer
PFD	Probability of Failure on Demand
PSLG	Process Safety Leadership Group
PTC	Proof Test Coverage
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirements Specification
TSA	Tank Storage Association
UKPIA	United Kingdom Petroleum Industry Association

Appendix F Other relevant publications

Further information relating to Prior Use can be found in the following publications

- IEC 61508 (2010), Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- IEC 61511 (2016), Functional safety - Safety Instrumented Systems for the process industry sector
- Safety and Environmental Standards for Fuel Storage Sites, Process Safety Leadership Group Final Report
- ISA-TR84.00.04, Guidelines for the Implementation of IEC 61511
- EEMUA 222, Annex F 'Application of IEC 61511 to Safety Instrumented Systems'
- HSE OG54 B 'Proof Testing of Safety Instrumented Systems in the Onshore Chemical/Specialist Industry'
- Chemical and Downstream Oil Industries Forum (CDOIF), Functional Safety Management of Installed Safety Instrumented Systems.
- Reliability, Maintainability and Risk Eighth Edition: Practical Methods for Engineers including Reliability Centred Maintenance and Safety-Related Systems ISBN 978-0-08-096902-2
- The Safety Critical Systems Handbook. ISBN 978-0-12-805121-4

Acknowledgements

This document was created as part of the Chemical and Downstream Oil Industry Forum Process Safety work stream.

CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Peter Davidson (Chair)	TSA
Dave Ransome	P&I Design Ltd.
Colin Easton	Prosalus
Dick Greenock	Prosalus
Jason Tack	Syngenta
Jon De Main	SABIC
Nic Butcher	HSE
Gerald Stewart	HSE
Steve Gregory	HSE
Jordan Smith	RAS
Scott Whiteside	Exxon Mobil
Pep Monk	Exxon Mobil
Paul Harvey	Exxon Mobil
Ron Bell	ESC
Paulo Oliveira	ESC
Jamie Walker	UKPIA
Nandish Velani	EEMUA
Edward Kessler	EEMUA
Paul Cram	Essar Oil

Revision History

Rev.	Section	Description	Date	Changed By
0	All	First Issue	30-June-2011	Peter Davidson
1	All	Updated following working group review	08-July-2011	Peter Davidson
2	All	Updated following working group second review	15-Nov-2011	Peter Davidson
3	All	Updated following comments received through CDOIF members and Competent Authority stakeholder reviews	20-April-2012	Alan G King, Dave Ransome, Peter Davidson
4	All	Updated following final stakeholder review	13-July-2012	Peter Davidson
5	All	Updated following comments from ESC	6-Aug-13	Peter Davidson
6	All	Updated to reflect IEC 61511 edition 2, added appendix for worked example	12-April-2019	Peter Davidson
7	All	Final Working Group comments included	26-October-2020	Peter Davidson
8	All	Updated to include requirements for FPL devices	04 Jan 2022	Peter Davidson
9	All	Stakeholder comments incorporated	04 April 2022	Peter Davidson