Young, A., & Walker, A. (2017). Improvements in Functional Safety of Automotive IP Through ISO 26262:2018 Part 11. In J. Stolfa, S. Stolfa, R. V. O'Connor, & R. Messnarz (Eds.), Systems, Software and Services Process Improvement: 24th European Conference, EuroSPI 2017, Ostrava, Czech Republic, September 6–8, 2017, Proceedings (pp. 547–556). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-64218-5_45

Improvements in Functional Safety of Automotive IP through ISO 26262:2018 Part 11

Alison Young, Alastair Walker

Lorit Consultancy, Scotland
alastair.walker@lorit-consultancy.com

Abstract. In early 2018, the second edition of ISO 26262:2018[1] automotive functional safety standard, is due for release. At the time of writing, the draft international standard (DIS) version is out for comment and review. One significant change over the original version of the ISO 26262:2011[2] standard is part 11, which brings detailed information to support semiconductor manufacturers develop ISO 26262 compliant intellectual property (IP). In the original version, information available to semiconductor companies was limited, this forthcoming release will bring significantly more information to support semiconductor and silicon IP suppliers. In the areas of digital and analogue components, programmable logic devices (PLD), multi-core processors and sensors. Tips, recommendations and practical examples are illustrated. However, there are certain areas that still not well represented, diagnostic coverage for analogue components for example is not defined in detail and there is a shortage of supporting information. Part 11 could also provide more worked examples to give design and functional safety teams a better insight into estimation techniques. The final draft international standard (FDIS) is due for publication in autumn 2017, and certain aspects of part 11 will be enhanced.

Keywords: Functional safety, Intellectual Property, Diagnostic Coverage, Dependent Failures Analysis, transient faults

1 Introduction

When ISO 26262:2011 was released, it brought a lot more information than was in IEC 61508[3] covering the areas of system, hardware and software development, to support design and functional safety teams in the automotive industry. However, for many semiconductor suppliers, the information represented in the first edition of ISO 26262 did not capture the requirements or consid-erations that are relevant to them in comparison with original equipment manufacturers (OEMs) and design teams at tier 1 or 2 level suppliers.

As many semiconductor devices are developed as Safety Element out of Context (SEooC) the end application is unknown and assumptions on the final implementation, safety goals and Automotive Safety Integrity Levels (ASIL) need to be made. While design teams implementing the Item can define and assess system level safety mechanisms and diagnostic coverage it is not so easy for semiconductor suppliers. Many concerns for semiconductor manufacturers are centred around transient failures of components, something that was not well addressed in the first edition of ISO 26262, equally part 11 brings enhanced information to support dependent failures analysis (DFA).

Part 11 would also be a very useful reference source for teams in the aviation industry as it expands greatly on some of the topics covered in DO-254[4]

In this paper, the solutions proposed in the DIS ISO 26262:2018 are reviewed and discussed in terms of how they enhance the detail and act as an adjunct to the first edition.

2 ISO 26262 part 11 concepts

2.1 Transient fault quantification

There is a good comparison between the suggested techniques in part 5 and part 11 of ISO 26262 and more over part 11 can also provide additional information for teams designing products that are not deemed to be IP.

Good references are made in part 11 to JEDEC[5] standards for understanding failure mechanisms and reliability of semiconductors additionally, equally the introductions to reliability standards, IEC TR 62380[6], SN 29500[7] and FIDES[8] also very informative.

Conversely part 11 repeats a number of topics that are addressed in other parts of ISO 26262 and relates them to IP, the size of part 11 could have been restricted if the information was referenced from other parts of the standards e.g. Section 4.10 Interfaces within distributed developments.

.

2.2 Component package failure rate

Section 4.6.2.2 of part 11 discusses the strengths and weaknesses of different reliability standards in relation to component package failure rates, it also addresses considerations relating to the device packaging and pins, topics that are not easily understood nor addressed to any great extend in the original version of ISO 26262.

2.3 Permanent base failure rate calculation using industry sources

Part 11 addresses the topic of base failure rate distribution in a concise manner, introducing the reader to the techniques for calculation of failure rates based on die and package. The die calculation methods using either area or number of equivalent gates. Figure 2.3 illustrates the typical factors contributing to the hardware component failure rate.

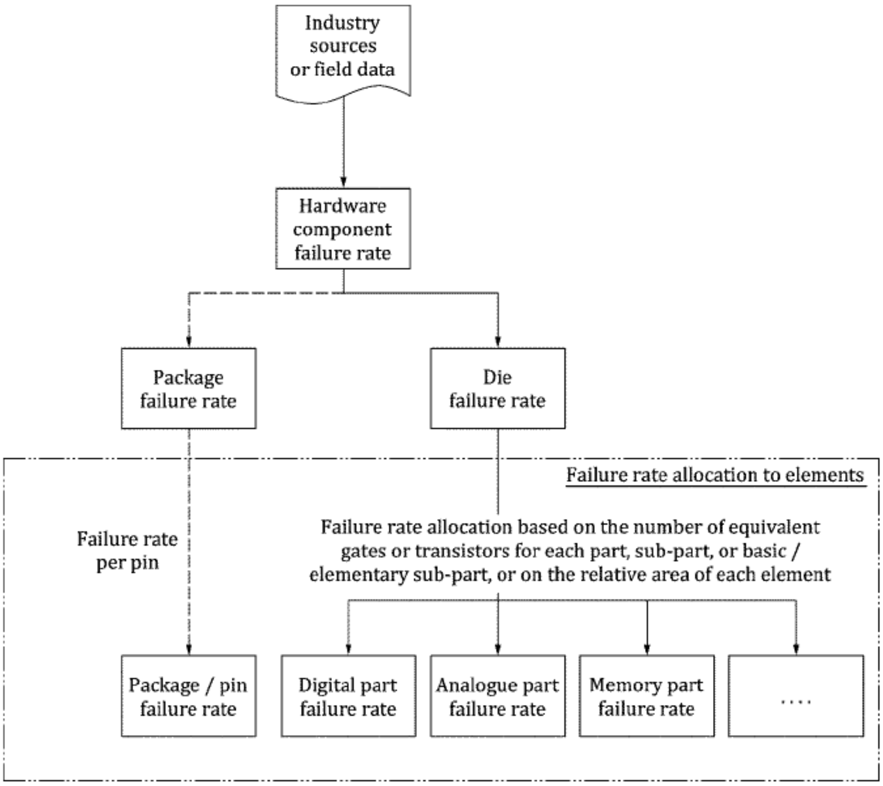


Fig. 1. Base Failure Rate Distribution

Section 4.6.3.5, introduces the topic of Multi-Chip Modules, but does not unfortunately give much guidance on what this referring to.

2.4 Diagnostic coverage

Part 11 is still weak in supporting the definition of analogue diagnostic coverage, this is conceded in the document that accurate estimation of analogue diagnostic coverage is not easily achieved. The techniques used in other standards such as the ISO 13849-1[9] are potentially superior, where application specific examples of diagnostic coverage are given in Annex E, this however would be more complex to realise in the wide variety of automotive applications. There are better examples of calculating diagnostic coverage for digital components e.g. the Direct Memory Access (DMA) controller given in Annex A.

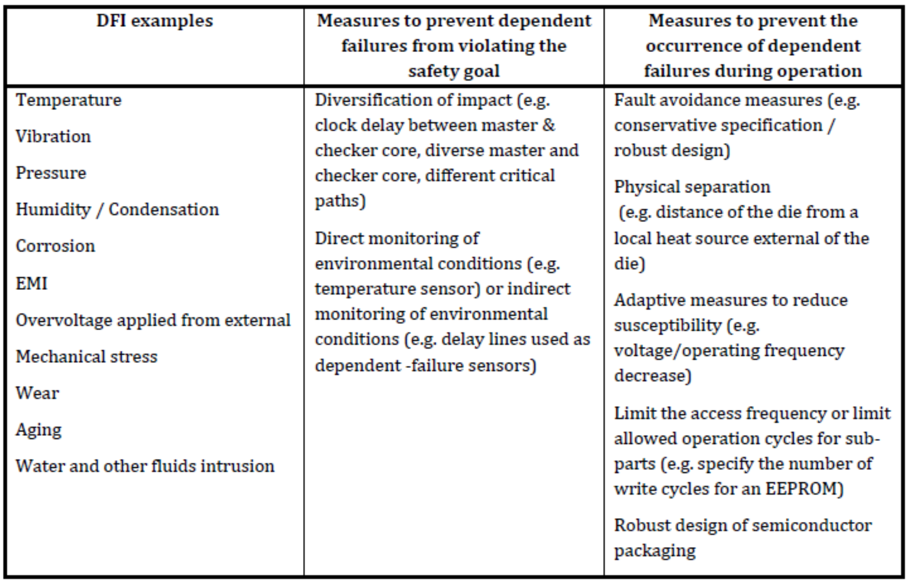
2.5 Dependent failures analysis (DFA)package failure rate

The DFA section of part 11 provides guidelines for the identification and analysis of possible common cause and cascading failures between given elements, the assessment of their risk of violating a safety goal (or derived safety requirements) and the definition of safety measures to mitigate such risk if necessary. This is done to evaluate potential safety concept weaknesses and to provide evidence of the fulfilment of requirements concerning independence or freedom from interference identified during coexistence analysis (see ISO 26262-9:2018, Clause 6).

Section 4.7.4 of part 11 also addresses the topic of the difference between common cause failures and cascading failures in semiconductor devices and highlights that in a given failure scenario the differentiation is not always possible or useful. This is a distinct difference from other parts of ISO 26262.

The Dependent Failures Initiator (DFI) represents the root cause of dependent failures in safety scope. A list of DFI is provided as a starting point, considering different systematic, environmental and random hardware issues see Figure 2.5 for the table of environmental issues.

A good definition of the relationship between DFA and safety analysis is given: While the safety analysis primarily focuses on identifying single-point faults and dual/multiple-point faults to evaluate the targets for the ISO 26262 metrics and define safety mechanisms to improve the metrics if required, the DFA complements the analysis by ensuring that the effectiveness of the safety mechanisms is not affected by dependent failures initiators.



DFI examples	Measures to prevent dependent failures from violating the safety goal	Measures to prevent the occurrence of dependent failures during operation
Temperature Vibration Pressure Humidity / Condensation Corrosion EMI Overvoltage applied from external Mechanical stress Wear Aging Water and other fluids intrusion	Diversification of impact (e.g. clock delay between master & checker core, diverse master and checker core, different critical paths) Direct monitoring of environmental conditions (e.g. temperature sensor) or indirect monitoring of environmental conditions (e.g. delay lines used as dependent -failure sensors)	Fault avoidance measures (e.g. conservative specification / robust design) Physical separation (e.g. distance of the die from a local heat source external of the die) Adaptive measures to reduce susceptibility (e.g. voltage/operating frequency decrease) Limit the access frequency or limit allowed operation cycles for sub-parts (e.g. specify the number of write cycles for an EEPROM) Robust design of semiconductor packaging

Fig. 2. Systematic dependent failures initiators due to environmental conditions

2.5.1 DFA workflow

Part 11 gives a very good approach to identifying DFI, if the DFI is adequately captured, identifying the necessary safety mechanisms and ensuring these are also adequate. The techniques listed could benefit teams working on automotive systems which are not necessarily restricted to semiconductors or IP.

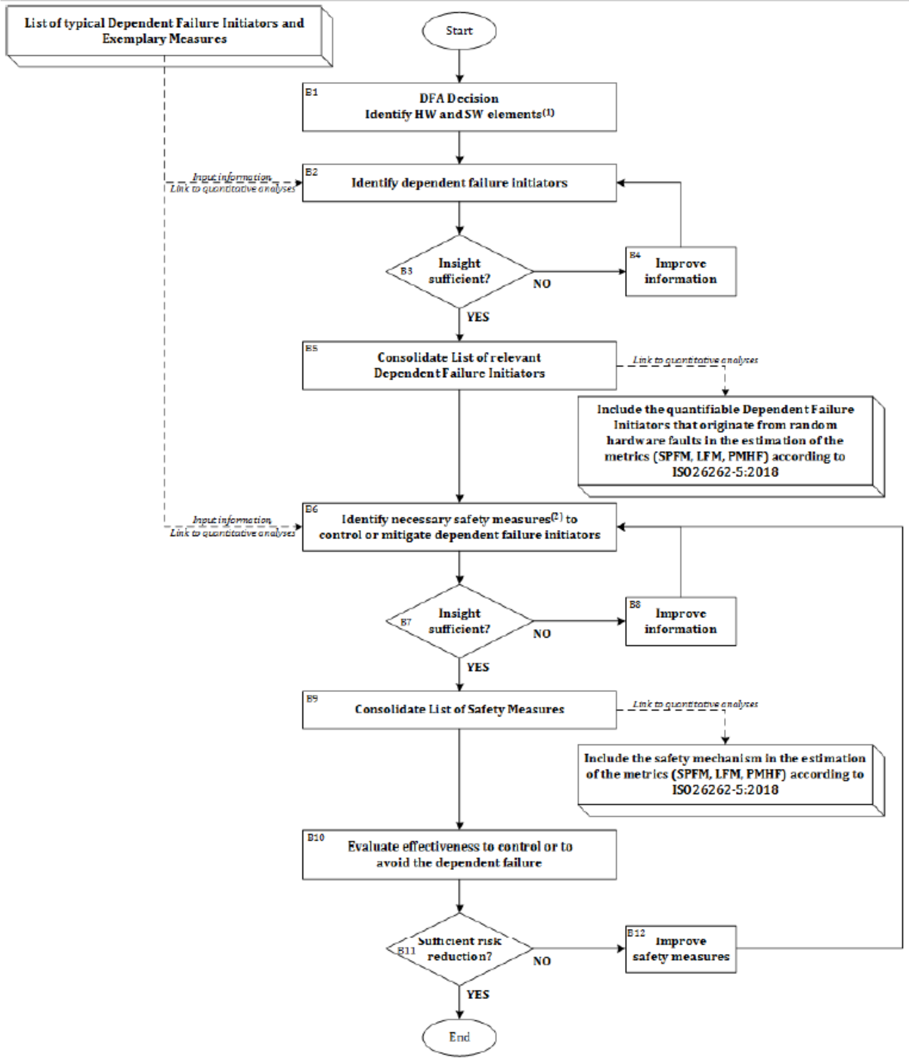


Fig. 3. Dependent failures analysis workflow

2.6 Fault injection

Good guidance is given in part 11 on the potential benefits and usage of fault injection, e.g. on verifi-cation planning, and techniques. Where part 11 is maybe a bit weaker as on the definition of when and how often to use fault injection testing i.e. more to verify the effectiveness of safety mechanisms rather than to justify diagnostic coverage.

3 Semiconductor technology categories and use cases

3.1 Digital components

The handling of digital components and memories is arguably the strongest area in part 11. Detailed definition and guidance on fault models of components such as memories, failure modes of common digital blocks, transient analysis and estimation of diagnostic coverage are documented. For teams developing purely digital components part 11 is an extremely helpful reference. Part 11 also supports the processes and is a suitable adjunct to the information already documented in part 5 of ISO 26262.

3.2 Analogue & mixed signal components

Regarding analogue components there is good coverage of potential failure modes in part 11, particularly in Table 35. Likewise, the discussions on Analogue Single Event Transients (ASET) are very good. The weakness in part 11 is the lack of information on diagnostic coverage. Annex D gives a good example of a quantitative analogue assessment, however under and overvoltage detection is given 99.9% diagnostic coverage, without any rationale on how this was calculated. Typical examples of circuits and the estimated or calculated diagnostic coverage would be very helpful.

3.3 Programmable logic devices (PLD)

The lifecycle mapping of PLDs as indicated compares well with the SEooC mapping given in ISO 26262, showing clearly the hardware assumptions generated by the PLD manufacturer, that must be validated by the PLD user. Part 11 documents a good relationship between PLD die failure rates and IEC TR 62380, giving com-plete examples of FIT rates based on logic, memory etc. and giving derating figures. Also, there are good references to JESD89A[10] for transient fault considerations.

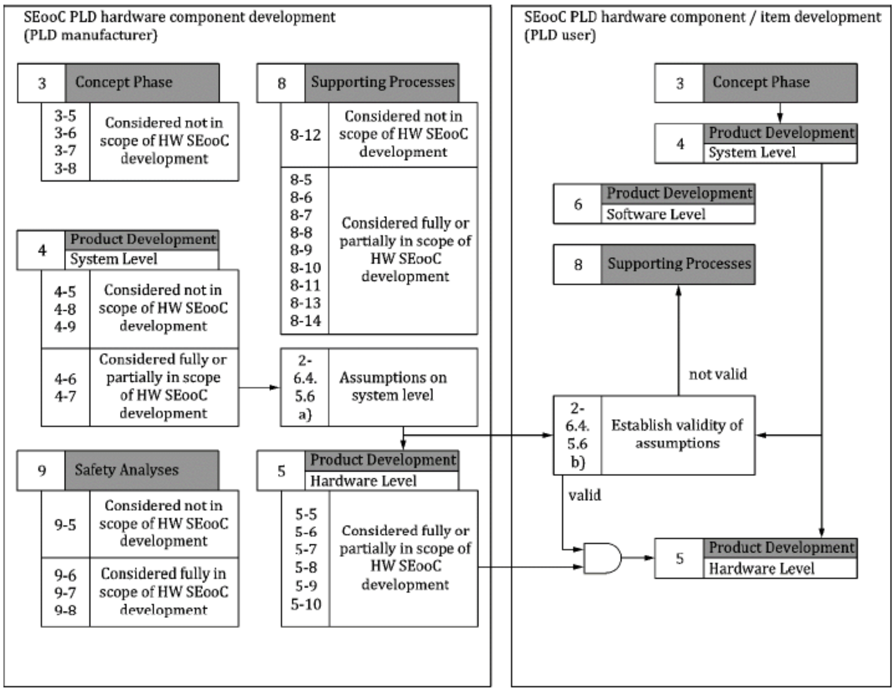


Fig. 4. ISO 26262 Lifecycle Mapping to PLD

3.4 Multi-core

The analysis of multi-core components gives a good overview of simplistic multi-core applications and supports this well with decomposition discussions. However, this section of part 11 does not elaborate on the techniques such as software lock-step or loosely coupled lock-step, as these are deemed to be out with the scope of part 11. As microcontroller technology advances, we now have standard automotive devices with 3 or more cores [11]. How these cores interact and are assessed in the context of functional safety requires a significantly more detailed evaluation than that given in part 11. Part 11 does give an introduction to the topic of multi-core components as indicated in Figures 3.4.1 and 3.4.2 below.

Multi-core component type	Description
Homogeneous multi-core component	Homogeneous multi-core components include only identical PE
Heterogeneous multi-core component	Heterogeneous multi-core components have non-identical PEs, typically with different Instruction Set Architecture (ISA)

Fig. 5. Types of multi-core components

As described in section 5.4 of part 11, shared resources are a known DFI. For a software element, a shared resource can be a hardware element (e.g. RAM, cache) as well as a software element (e.g. drivers). Within a multi-core the issue caused by shared resources (e.g. memory, time, execution or exchange of information interferences) can be resolved by assigning the corresponding software elements to independent programmable elements (PE) without the same shared resources. Other issues (e.g. shared memory, commonly used software elements) are addressed analogously to a single core system (e.g. memory encapsulation via MPU by the OS, developing the commonly used software elements compliant with the initial ASIL). Techniques such as hypervisors[12],[13] can help to achieve software partitioning, are introduced, but the reader of part 11 would require much more detailed investigation to establish the benefits.

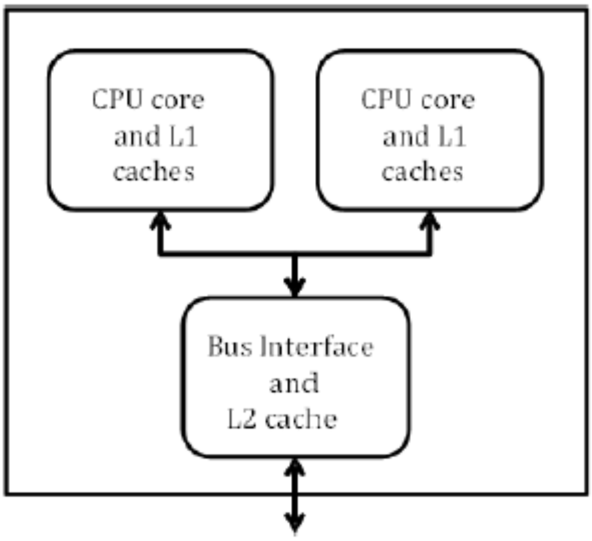


Fig. 6. Generic diagram of a dual-core system

3.5 Sensors & transducers

Section 5.5 gives a good general overview of sensors, failure modes, production processes. Several examples are given of different stages of a Micro Electro Mechanical Systems (MEMS) functional safety evaluation, looking at the safety analysis, safety measures, DFA and specific failures of the component parts. This section does give a good introduction to the topics but again very much at an introductory level.

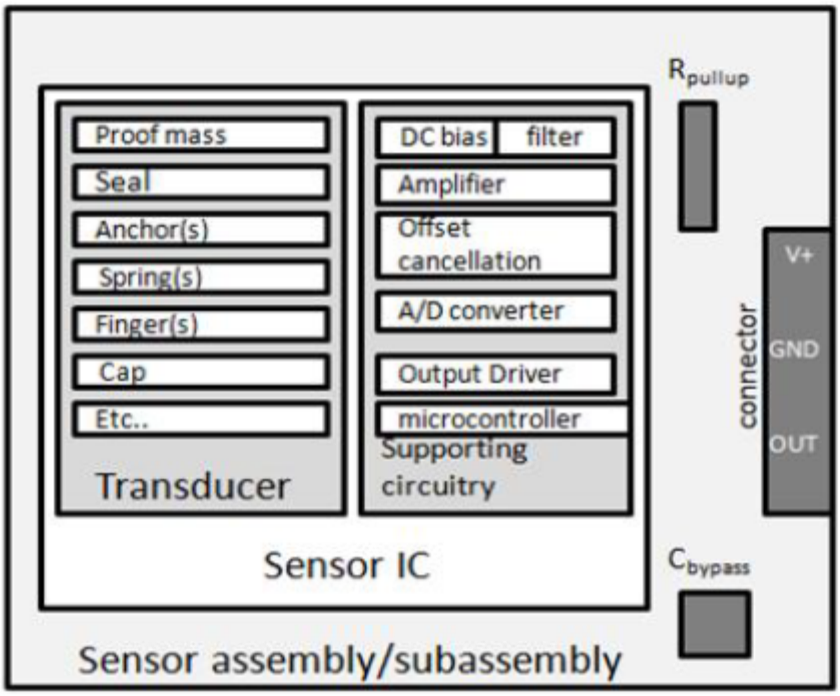


Fig. 7. Example of sensor complex hierarchical sensor

4 Conclusion and Future Work

ISO 26262:2018 gives additional supporting information to design and functional safety teams, in areas that were not too well supported in ISO 26262:2011, particularly how to evaluate hardware failure rates and DFA. Much of the additional information in part 11 focuses on introduction topics, rather than delving into subjects in more detail. Particularly the area of diagnostic coverage of analogue components is not well represented, and the 2011 version of the standard gave better support to teams in this area. Part 11 will generally be a helpful reference to design and functional safety teams and not only in the automotive sector, the aviation sector for instance could find this to be a valuable source of information

Lorit Consultancy in cooperation with partner organisations, is currently preparing training material based on the concepts in this paper. These shall be reviewed updated and expanded upon as the final version of part 11 is released.

References

1. ISO DIS 26262:2018 Road vehicles – Functional safety
2. ISO 26262:2011 Road vehicles – Functional safety
3. IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems
4. RTCA/D0-254:2000 Design Assurance Guidance for Airborne Electronic Hardware
5. JEDEC – Joint Electronic Device Engineering Council https://www.jedec.org/
6. IEC TR 62380 Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment
7. [Siemens SN29500 Component Failure Rate data (parts 1 to 14)
8. FIDES guide 2009 Edition A (September 2010), “Reliability Methodology for Electronic Systems”.
9. ISO 13849-1:2015 Safety of machinery – safety related parts of control systems – Part 1: General principles for design
10. [JESD89-2A JEDEC STANDARD Test Method for Alpha Source Accelerated Soft Error Rate
11. NXP MPC5746R – SPC5746R Microcontroller Data Sheet Rev. 5 10/2016
12. [Niimi, Y., et al., "Virtualization Technology and Using Virtual CPU in the Context of ISO 26262: The E-Gas Case Study", SAE Technical Paper, April 2013.
13. Bressoud, T.C., Schneider, F.B., “Hypervisor-based fault tolerance”, Proceedings of the fifteenth ACM symposium on Operating systems principles, 1995, pp.1–11.