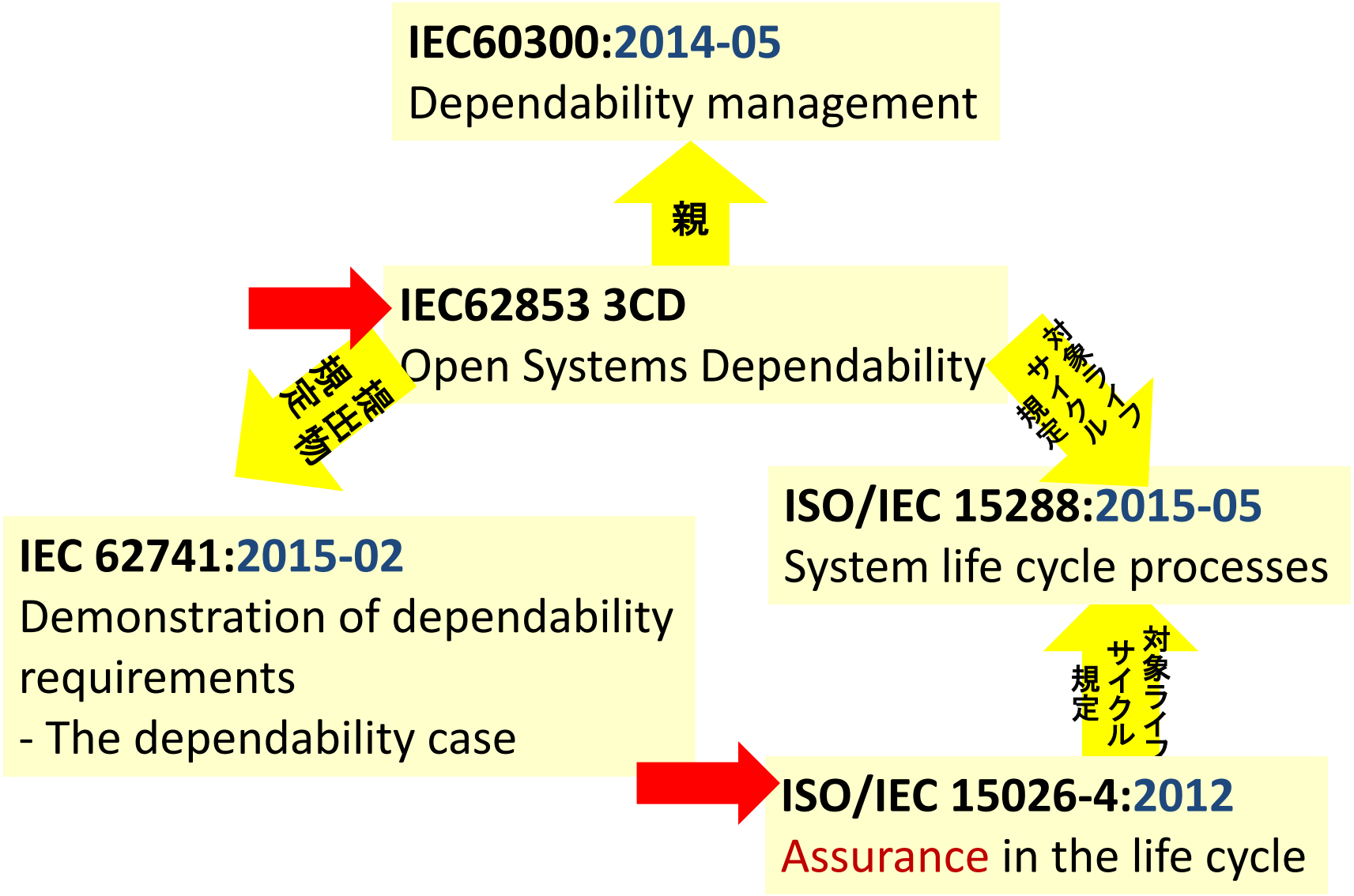
Open Systems Dependability 関連 国際標準の動向

2015-03-16

DEOS協会　標準化部会
神奈川大学 理学部 情報科学科
木下佳樹

IEC 62853 と関連標準



IEC 62853 草稿の現状

- 2015-04-15: 3nd CDへの各国コメント締切
- 2015-07-20: コメント集計、エディタに送付
- 今後の見込み
  - 2016-04: 3rd CD コメント集計
  - 2016-05: TC56 WG4 meeting; 3rd CD コメント解決
  - 2016-06: CDV 配布
  - 2016-09: CDV コメント集計
  - 2016-10: TC56 WG4 meeting; CDV コメント解決
  - 2016-01: FDIS 配布
  - 2017-10: 出版

IEC 62853/Ed1.0 3CD の目次

1. Scope
   対象を明確にする
2. Normative references
   本規格が準拠する他の規格など
3. Terms and definitions
   用語定義
4. Open systems dependability
   OSD概念の解説
5. Conformance
   OSD達成主張のために求められる提出物: 7章達成を主張する dependability case
6. Process views for achieving OSD
   OSD達成のために実現しなければならないプロセスビュー

これは草稿の目次です。
出版される規格は、これとは異なるのが普通で、場合によっては大幅に異なる可能性があります

A) (informative) Relationship to other standards on dependability
B) (informative) Example lifecycle models with open systems dependability
C) (informative) An example template for dependability cases
D) (informative) Systems concepts and dependability of systems
E) (informative) Role of contingency planning in open systems dependability
F) Boundaries of accountability within an open system

ISO/IEC 15026-4
Assurance in the life cycle

- **ライフサイクルを通じたアシュランス達成のためのガイダンス**

  OSDの考えが埋め込まれている

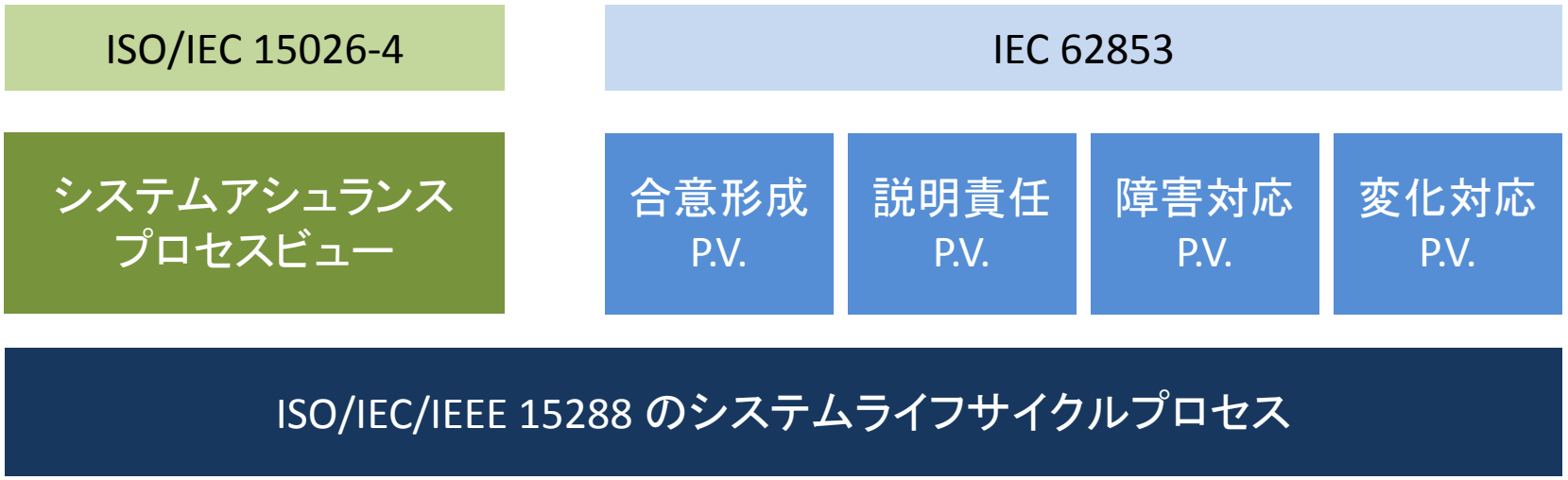
  Scope (of 15026-4)

  This part of ISO/IEC 15026 gives guidance and recommendations for **conducting selected processes**, activities and tasks for systems and software products **requiring assurance claims** for properties selected for special attention, called critical properties. This part of ISO/IEC 15026 specifies a property-independent list of processes, activities and tasks to achieve the claim and show the achievement of the claim. This part of ISO/IEC 15026 establishes the processes, activities, tasks, guidance and recommendations in the context of a defined life cycle model and set of life cycle processes for system and/or software life cycle management.

ISO/IEC 15026-4:2012 の内容

- ISO/IEC/IEEE 15288 System life cycle processes 上に **system assurance process view** を規定

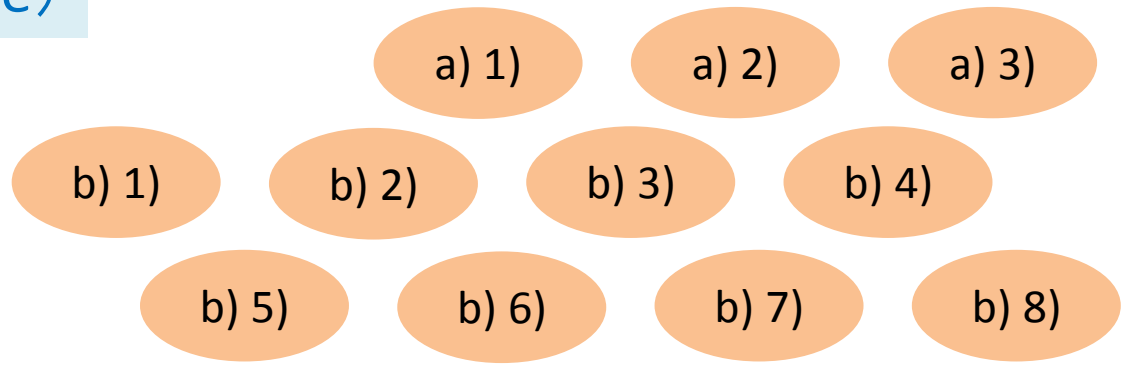
  Cf. IEC 62853 は 15288 上に 4つのプロセスビューを規定する



プロセスビュー

目的（purpose）

アウトカム



15288 プロセス

			Proj. assess. proc.
Acquisition proc.	Supply proc.	Quality mng. proc.	Proj. Plan. proc.
Decis. mng. proc.	Quality assur. proc.	Stkhld needs & req. def. proc.	Sys req def proc.

7 Assurance guidance and recommendations for selected processes

7.1 Introduction

Clause 7 cites the activities and tasks from the Agreement, Project, and Technical categories of processes in ISO/IEC 15288:2008 and in ISO/IEC 12207:2008 that require extension or special interpretation when a defined level of assurance is to be demonstrated. Assurance-claim-related guidance and recommendations are provided for performing these activities and tasks to achieve the outcomes of the process views. This guidance and recommendations assume and depend upon the full application of ISO/IEC 15288 and 12207 as indicated in clause 3. The processes not cited in this clause are considered adequate as defined in ISO/IEC 15288:2008 and ISO/IEC 12207:2008 to achieve the claims for the critical properties.

7.2 Acquisition process

The Acquisition Process (ISO/IEC 15288:2008, 6.1.1 and ISO/IEC 12207:2008 6.1.1) obtains a product or service in accordance with the acquirer's requirements. When the acquisition is for a system element, this process should ensure that all requirements for achieving of showing the achievement of any assurance claim associated with that system element is passed to the supplier through the agreement.

7.2.1 Relevant activities and tasks

Systems Assurance Process View	Software Assurance Process View
c) Initiate an agreement 1) Negotiate an agreement with the supplier. d) Monitor the agreement. 1)Assess the execution of the agreement. 2)Provide data needed by the supplier and resolve issues in a timely manner.	6.1.1.3.4 Contract agreement. 6.1.1.3.4.2 The acquirer shall then prepare and negotiate an agreement with the supplier that addresses the acquisition requirements, including the cost and schedule, of the software product or service to be delivered. The contract shall address proprietary, usage, ownership, warranty and licensing rights associated with the reusable off-the-shelf software products. **6.1.1.3.5 Agreement monitoring.** **6.1.1.3.5.1** The acquirer shall monitor the supplier's activities in accordance with the Software Review Process and the Software Audit Process. The acquirer should supplement the monitoring with the Software Verification Process and the Software Validation Process as needed.

7.2.2 Assurance guidance and recommendations

The project should ensure that the agreement considers the variables and their values of the critical properties for the system element being acquired. The agreement should include integrity requirements (i.e., guarding against counterfeit parts, tampering, system elements with vulnerabilities, and revealing of confidential information including information about vulnerabilities to ensure that what is received is what is expected. The project should derive the claims for the system element being acquired from the system's assurance claims and incorporate them into the request for the supply of the system element. In addition, the project should incorporate the following considerations into the negotiations and the agreement with the supplier:

a) Confidence that the appropriate controls regarding dependability (e.g., trustworthiness) of their personnel and those of their associated organizations are effectively implemented.

b) Confidence that the supplier guards against counterfeit parts, tampering, and other threats to system or product integrity as well as against revealing confidential information.

c) Confidence that the system element transferred, received, and, to the extent practicable, installed and operated, is the one intended.

d) Confidence that the product development environment has appropriate resources in place to protect the integrity of the product and its critical properties during development.

e) Confidence that the system or software development life cycle model chosen by the supplier is appropriate to the nature of any assurance claims to be achieved.

f) Confidence that the appropriate controls regarding implementation of safety requirements and the achievement of system safety integrity requirements are effectively implemented.

The project should revisit the approaches to showing achievement of claims when considering an acquisition from a new supplier to ensure that the new supplier does not deny required information, enable a new threat, or undermine the safeguards already in place to protect the system.

The project should submit a request for proposal (RFP) that can be correctly understood by the supplier and other stakeholders and establish a procedure for resolving problems and changing the agreement. Upon a change of agreement, the project should ensure that the stakeholder requirements defined in the Stakeholder Requirements Definition process are the starting point of the change. The project should consider a multi-stage agreement when appropriate.

ISO/IEC 15026-4 改訂の計画

- 15026-4:2012は15288:2008に基づく
  ➔15288:2015の出版により改定の必要
- ISO/IEC JTC1 SC7 WG7 にて

  2015-11　改訂のエディタに木下佳樹を指名、NWIP (New Work Item Proposal) およびWD (Working Draft)作成を依頼。

  2016-05　NWIPを審議

おわり