IEC 62853 *Open systems dependability* 要点と今後の展開

2018-06-05

ディペンダビリティ技術推進協会　オープンシンポジウム

神奈川大学　理学部　情報科学科

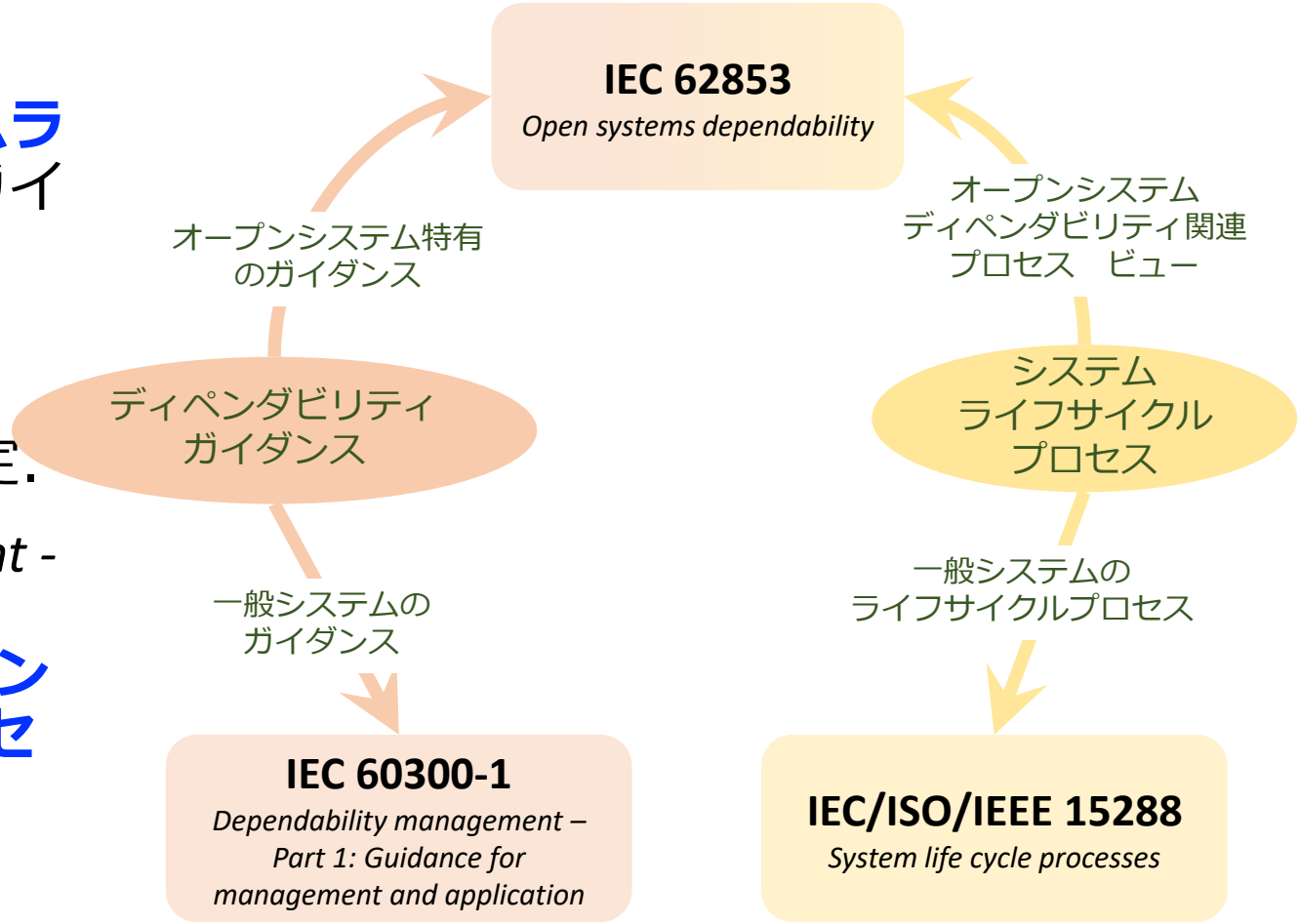
IEC TC 56 *Dependability* WG 4 *Information systems* Convenor

ディペンダビリティ技術推進協会　標準化部会　主査

木下佳樹

IEC 62853 *Open systems dependability* とは? —1. Scope より

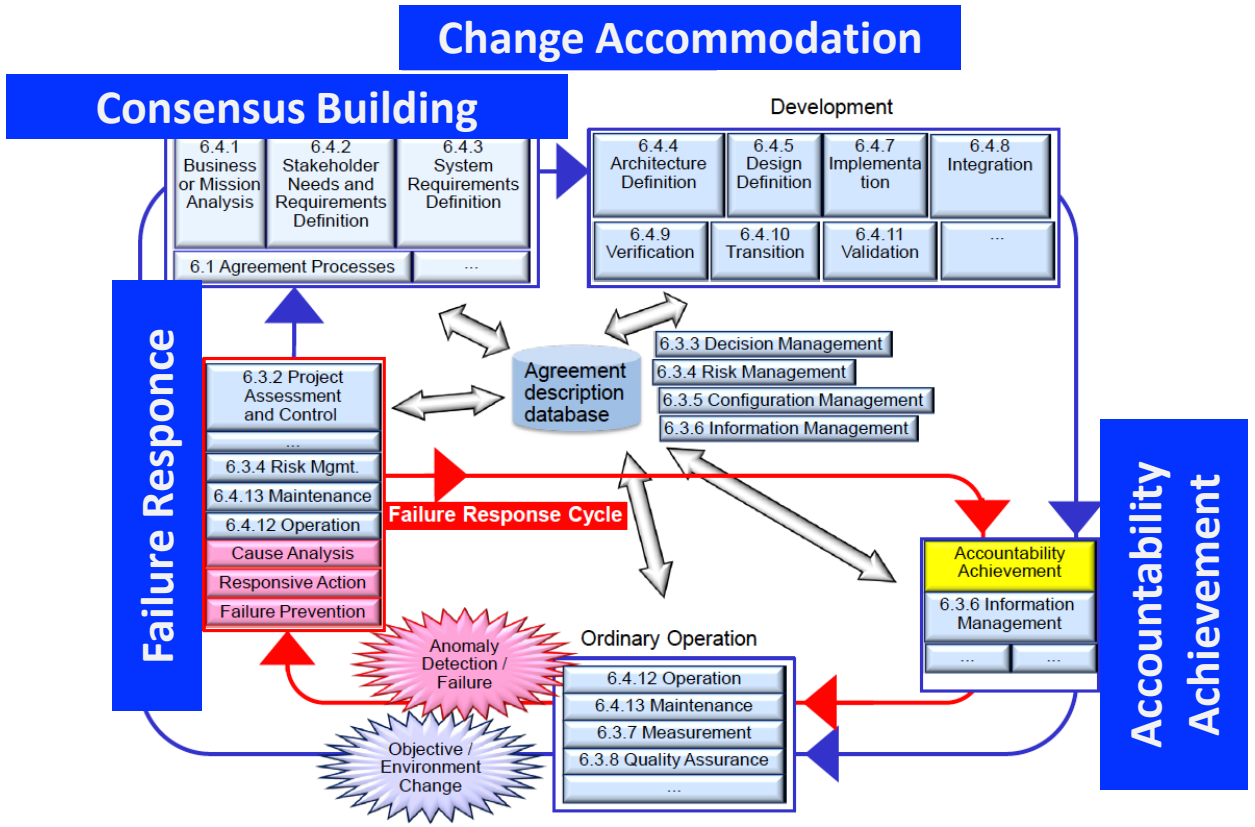
- オープンシステムの**ディペンダビリティ達成**のために必要な，**システムライフサイクルへの要求**に関連するガイダンスを規定する.
- システムライフサイクルは **ISO/IEC/IEEE 15288 *System life cycle processes*** が規定しているものを想定.
- IEC 60300-1 *Dependability management - Part 1: Guidance for management and application* が規定する**一般のディペンダビリティ管理の上**に，4つの**プロセスビュー**として要件を付け加える.



どんな要求か？

以下の四つの要求を process view と呼ばれる過程として規定

- 合意形成
  - Consensus Building
- 説明責任遂行
  - Accountability Achievement
- 障害対応
  - Failure Response
- 変化対応
  - Change accommodation



合意形成の過程

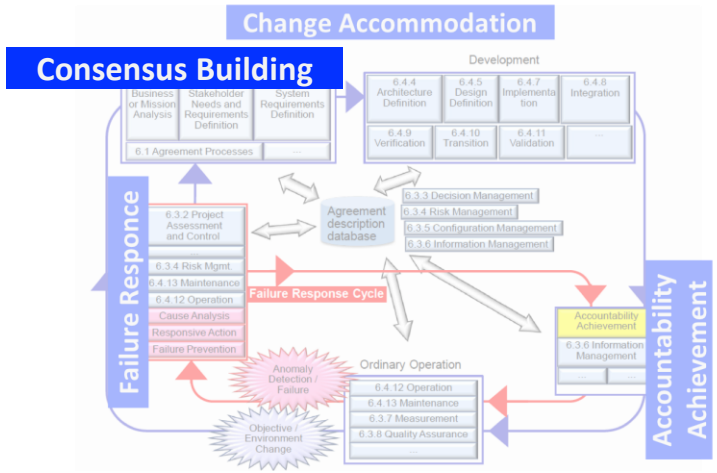
ステークホルダ間の合意形成

stakeholder = 利害関係者，当事者

- **明示的な合意**，及びシステムとその変化に関する**共通理解**を確立する過程

合意

- **明示的合意**
  - ＝契約
- **共通理解**
  - 暗黙の了解事項を含む
  - 想定外の事態への対処の根拠



説明責任遂行の過程

品質保証から説明責任へ

- **明示的合意の不履行**の，当事者や社会への**影響**を明示する過程

  責任者による**損害補償義務**も明示されること．この明示がシステムについての**合意事項改善**，システムへの**信頼と確信の維持**，想定される被害への**補償の確保**などにつながる．

合意不履行

- **関係者に起因**
  経営判断，事故など
- **関係者以外に起因**
  自然災害，事故など

説明責任 ⊇ 補償義務

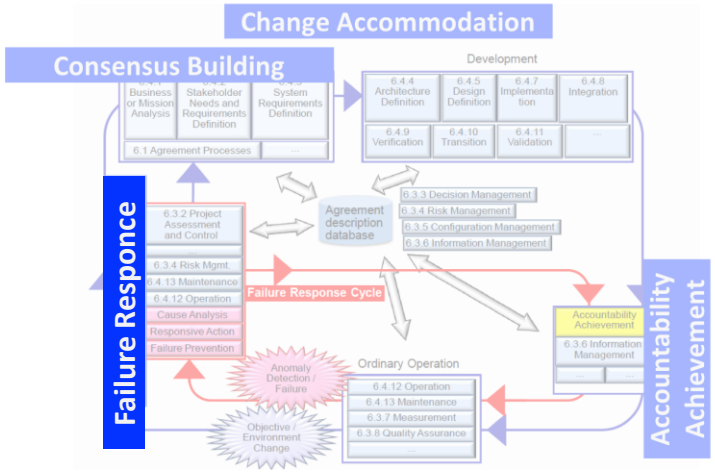
- 合意事項改善
- 信頼と確信の維持
- 被害への補償の確保

障害対応の過程

- 障害に際しても，**状況に応じてできるだけサービスを続け，被害と中断を最小**にする過程.

障害対応

- **サービス継続**
  - ダウングレード運転？
- **被害を最小に**



状況に応じて

合意からの逸脱を含む
←共通理解，説明責任

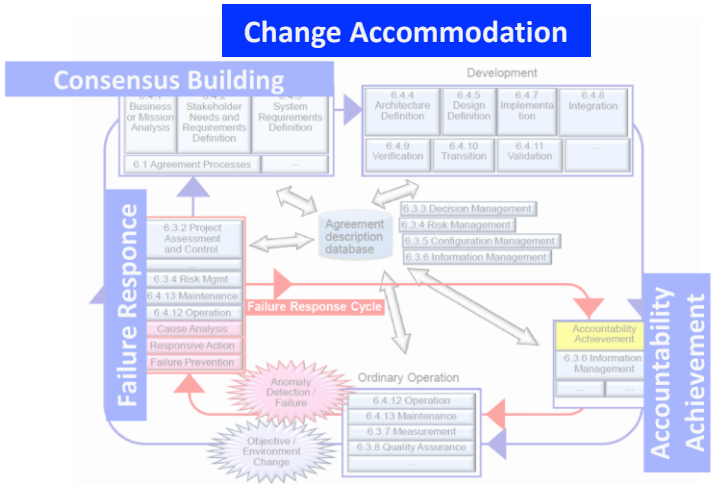
修復／新版開発の必要性判断

変化対応の過程

- 環境，要求，目的の**変化**があってもシステムが**目的にかなっている**状態を保つ過程

変化

- **環境**
  マーケット，関連法規，部品供給, etc.
- **要求**
  部品仕様，性能要求，etc.
- **目的**
  経営ポリシー，用途変更，etc.



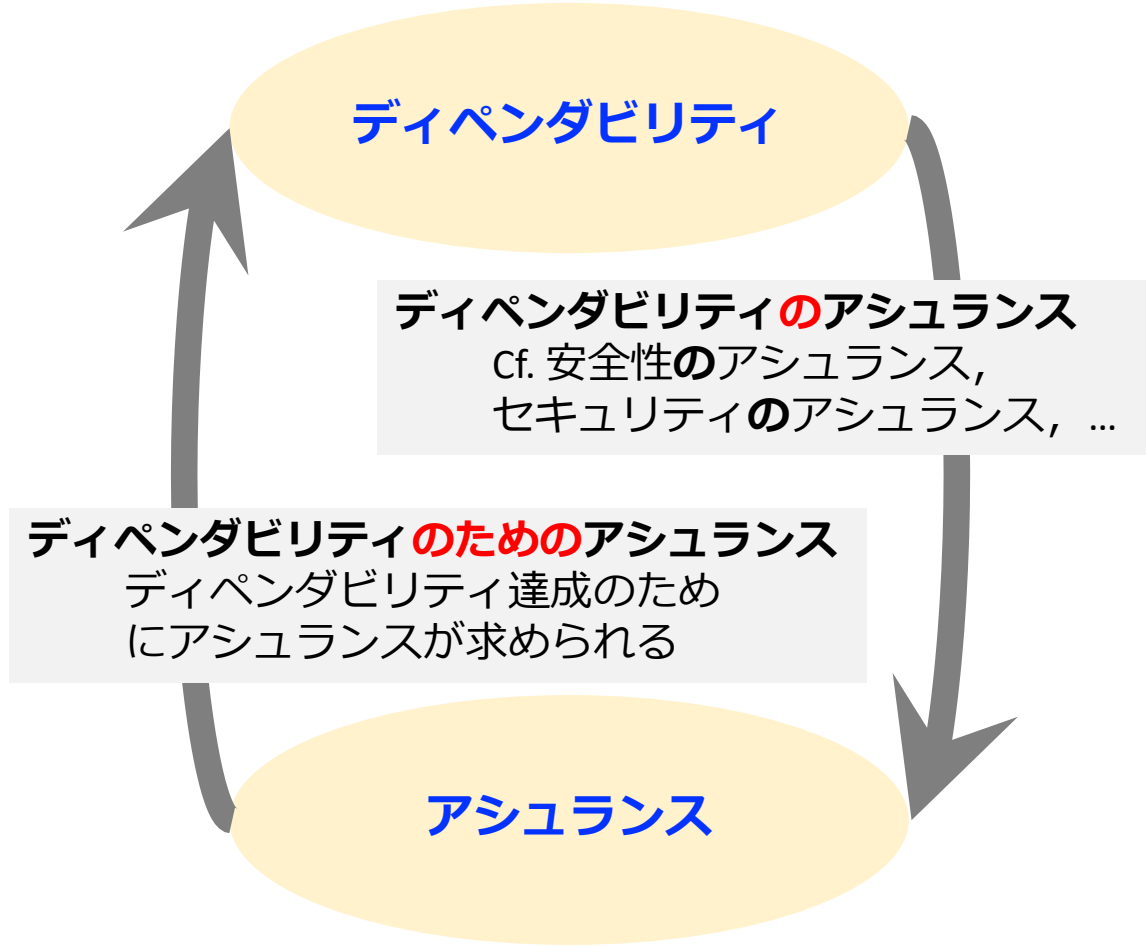
目的にかなった fit-for-purpose 状態を保つ

ディペンダビリティとアシュランス

ディペンダビリティとアシュランスの混同を避ける

国際標準体系における定義

- **Dependability** – ability to perform as and when required
  [要求されたとおり，要求された時に遂行する能力]
  (IEC 60050-192:2015)
- **Assurance** - grounds for justified confidence that a claim has been or will be achieved
  主張達成の(正当化された)確信の根拠
  (ISO/IEC 15026-1)



IEC 62853 制定への道のり: **CREST project**

科学技術振興機構 CREST 研究領域「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム 」

- OSDはこの研究領域の研究成果
  DEOS = Dependable Embedded Operating System
  ➔ DEOS = Dependability Engineering for Open Systems
- OSDの**研究と標準化が同時進行**
  - ➔ 研究領域**開始当初から標準化**を計画
    プロジェクト「利用者指向ディペンダビリティの研究」のミッションは標準化
  - ➔ 概念の吟味，**入念な仕上げへのIEC TC 56の貢献**は本質的.
  - ➔ 研究／標準化の同時進行は，**最近の世界的傾向**.

    Cf. "Assuring Autonomy" International Programme (Lloyd Registers Foundation/York Univ.)

    Cf. "Assurance of autonomous systems" Study Group Report (ISO/IEC JTC 1/SC 7)

Assuring Autonomy International Programme

Overview – January 2018

The Need: Current analysis methods and regulatory frameworks do not effectively address the technologies used by RAS, especially artificial intelligence (AI). Further the groups developing and deploying RAS are not always familiar with standard safety, assurance and regulatory practices. There is therefore a vital need for improvement in methods for assurance and regulation of RAS so they can catch up with, and positively influence, RAS developments and operations, thereby improving and assuring safety.

The Impact: The Programme will achieve wide impact via improved standards, regulatory frameworks, education and training, and public engagement. Ultimately the Programme will facilitate the introduction of RAS, in a safe and effective manner

Assuring Autonomy International Programme

verview – January 2018

s and autonomous systems (RAS) are already affecting society, and the foreseeable future. Use of RAS in areas such as transport and on safety and quality of life for a large proportion of the world's

s new risks. The Lloyd's Register Foundation *Foresight review of* ied that assuring and regulating the safety of RAS is currently the these new technologies.

d regulatory frameworks do not effectively address the technologies used by RAS, especially artificial intelligence (AI). Further the groups developing and deploying RAS are not always familiar with standard safety, assurance and regulatory practices. There is therefore a vital need for improvement in methods for assurance and regulation of RAS so they can catch up with, and positively influence, RAS developments and operations, thereby improving and assuring safety.

The Assuring Autonomy International Programme: The Lloyd's Register Foundation and the University of

through the life of the programme.

Collaboration: A key to success of the programme is international collaboration; this will involve work with companies and universities and with other projects and programmes around the world.

The Outputs: The main output will be a Body of Knowledge (BoK), a wide-reaching, structured, curated

[1] http://www.lrfoundation.org.uk/news/2016/foresight-review-of-robotics-and-autonomous-systems.aspx

IEC 62853 制定への道のり: **国際標準活動**

標準団体の狭間にて．．．

「**情報技術のディペンダビリティ**」を所掌する標準化団体がない．

関連する現行標準団体

- **情報技術**：**ISO/IEC JTC 1** Information technology / **SC 7** Software and systems engineering

  WG 7 Life cycle management がシステムアシュランスを所掌．
  しかし，ディペンダビリティの専門家が少ない．リスクも．
- **ディペンダビリティ**：**IEC TC 56** Dependability

  WG 4 Information systems が情報システムを所掌．(convenor: 講演者)
  しかし，情報システムの専門家が少ない．

IEC 62853 *Open systems dependability* プロジェクトの現状

- 最新草稿
  FDIS (Final Draft International Standard)
  (2018-03-30 承認投票のため各国委員会に配布)
  IEC TC 56 内部文書 56_1772e_FDIS
- 現在のステージ
  BPUB (Being published)
  2018-05-18 上記FDISの出版が賛成19反対0棄権3で承認
- 次のステージ
  PPUB (Publication published)
  (anticipated 2018-06)
  (承認の日付(2018-05-18)から**6週間以内に出版**するのが規定)

IEC 62853 関連活動の今後

- IEC 62853 和訳
  - DEOS協会がFDIS草稿の**和訳を作成中**
  - **IEC標準翻訳本**出版へ（日本規格協会に働きかけ）
  - IEC 62853 の**JIS化**へ（関係方面に働きかけ）
  - 標準**和訳の意義**：新分野の技術用語／専門用語の日本語語彙構築
- オープンシステムディペンダビリティ 関連国際標準策定
  - IEC 60300-1 *Dependability management - Part 1: Guidance for management and application* への浸透: **OSD を標準的 dependability に**.
  - IEC 62853準拠のための各プロセスの**tangible提出物同定** (Information items/documents)
    - Cf. ISO/IEC/IEEE 15289 *Content of life-cycle information items (documentation)*
    - DEOS協会標準化部会の2018FY活動の主要テーマ
    - まず，DEOS協会文書➔次にTC 56 新規課題提案(NWIP)？
- **自律システム(AI)のアシュランス**研究，標準化
  - ISO/IEC JTC 1/SC 7 (ISO/IEC/IEEE 15026 *Systems and software asusrance – Parts 1 – 4.*

これ！

ISO/IEC/IEEE 15289
Content of life-cycle information items (documentation)

IEC 62853
Open systems dependability

ISO/IEC/IEEE 15288
System life cycle processes

おしまい

～ご静聴に感謝します～

IEC 62853 制定への道のり: 国際標準活動

- 標準化団体と技術委員会 (Technical Committees)
  - ISO/IEC JTC 1 Information technology / SC 7 Software and systems engineering
  - IEC TC 56 Dependability
- 標準化プロジェクトのステージ
  - NWIP (New Work Item Proposal) 2012-09-07/approved 2012-12-21
  - 1CD (draft Circulated as 1st Committee Draft) 2014-07-04
  - 2CD (draft Circulated as 2nd Committee Draft) 2015-04-17
  - 3CD (draft Circulated as 3rd Committee Draft) 2016-01-22
  - 4CD (draft Circulated as 4th Committee Draft) 2016-08-26
  - CCDV (draft Circulated as Committee Draft for Vote) 2017-05-12
  - FDIS (draft Circulated as Final Draft International Standard) 2018-03-30
  - IS (International Standard)