DEOS関連国際標準の動向（IEC62853:Open systems dependability）

第二回 DEOS協会オープンシンポジウム

2015-06-17

DEOS協会標準化部会
http://deos-standard.progsci.info.kanagawa-u.ac.jp/

OSD 標準

- Open systems dependability (OSD) とは？

  変わり続けるシステムに対するディペンダビリティの新しい概念

  DEOS技術の根幹

- OSDの標準とは？

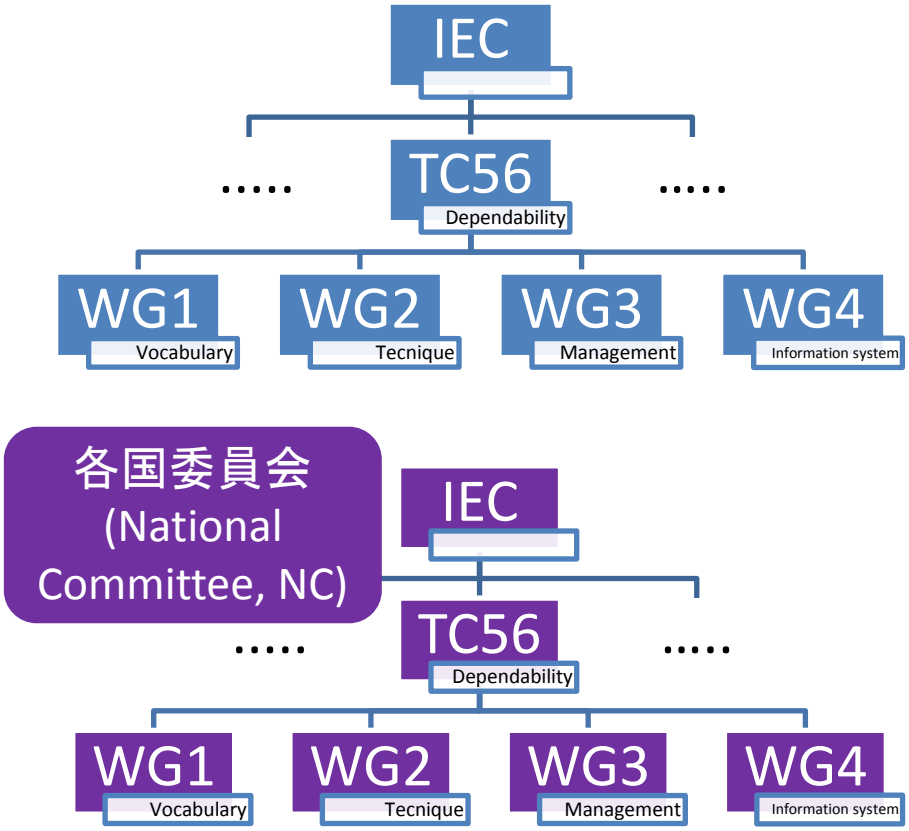
  「システムライフサイクルがOSDを達成する」ための要件を規定する標準。

  　要件　＝　requirements　あるいは　要求事項

  IEC 62853 Open systems dependability として国際標準の制定が進行中。

  　IEC TC56 Dependability PT4.8 Open systems dependability

国際標準制定の組織と作業過程



- New Work Item Proposal (NWIP)
  - 投票により承認
- Working Draft (WD)
  - Editor間で回覧→コメント収集→処理→次の草稿
- Committee Draft (CD)
  - 各国に配布→コメント収集→コメント処理→次の草稿
- Committee Draft for Vote (CDV)
  - 各国に配布→賛否投票＋コメント収集、処理
- Draft International Standard (DIS)
- Final DIS (FDIS)

IEC 62853 規格制定作業の現状

- 混乱を避けるため、制定中の国際規格草案は、公開されない。IEC 62853 も例外に非ず。
- 近況:

  IEC 62853/Ed1.0 2CD が各国委員会に配布された。

  各国委員会からのコメント送付の締切: 2015-07-17

  2015-10-19 – 23: IEC TC56 全体集会において、各国からのコメントの処理を決定する

  決定されたコメント処理に沿って次の草稿を準備する。

  これを繰り返し、2016-12 に規格出版の予定。

IEC 62853/Ed1.0 2CD 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. Requirements for OSD
   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 + 8章達成を主張するassurance metacase
6. Process views and assurance metacases
   本規格の基本概念
7. 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
8. Assurance metacases for achieving open systems dependability
   OSD達成のために用意しなければならないアシュランスメタケース

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

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

IEC 62853/Ed1.0 2CD の内容

IEC62853 2CDはシステムライフサイクルがOpen systems dependability (OSD) を持つための要件を定める規格（の案）

どんな要件？

- 4つのプロセスビューが提供されていることを主張するディペンダビリティケースがあることと

  Consensus Building,
  Failure Response,
  Accountability Achievement,
  Change Accommodation

- 上記のディペンダビリティケースに関する5つのメタアシュランスケースがあること

  大幅な変更の可能性あり

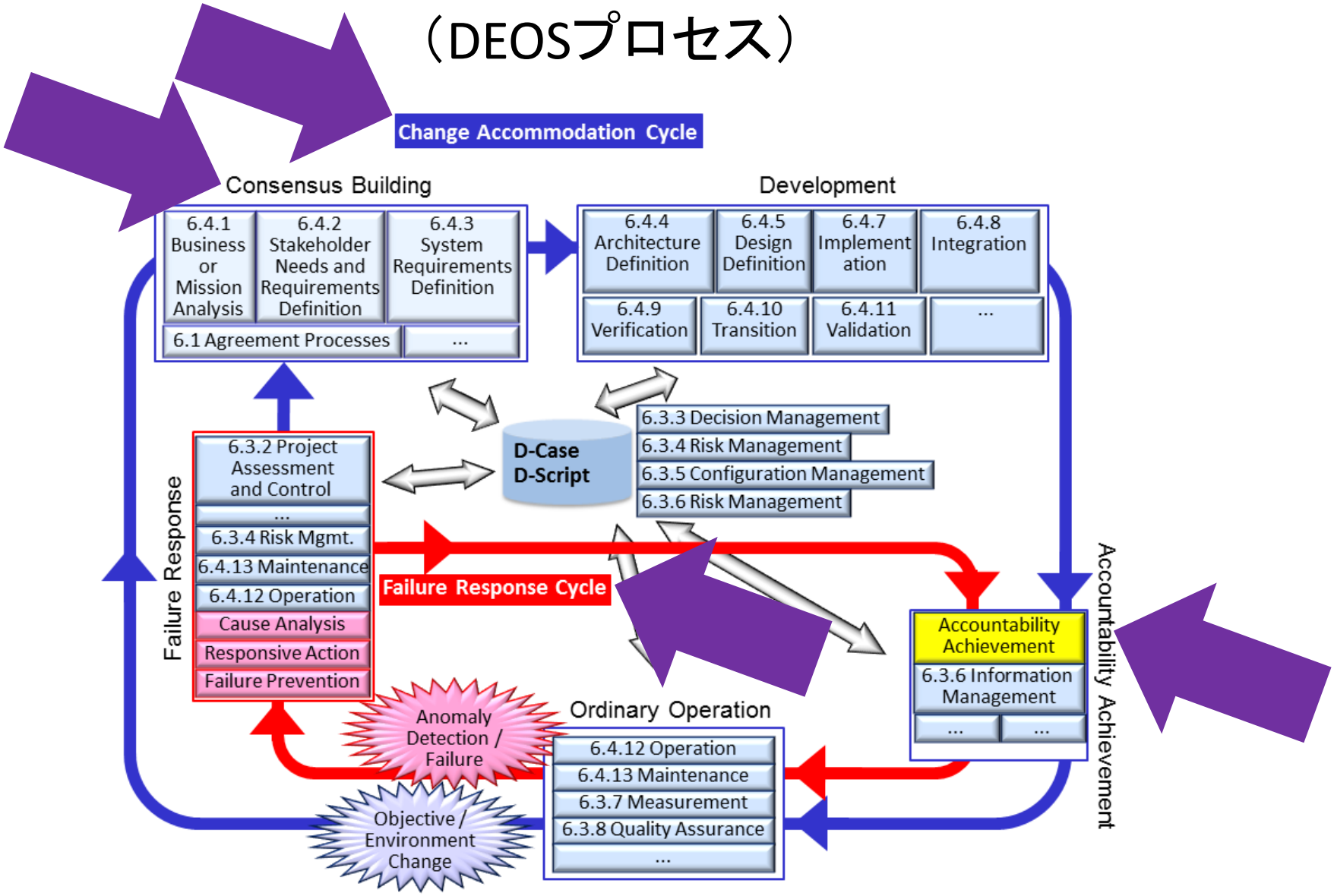
  Internal Consistency,
  Validity,
  Confidence
  External Consistency,
  Adequacy,

プロセスビューとは？

- ISO/IEC 15288によりシステムライフサイクルのプロセスが規定されている。
  - Process – activity – task と階層的に規定されている。
  - 重要: 15288はプロセスにどんなものがあるかを規定するのみ。プロセスをどのように組み合わせ、どんな順番で行うかを決めるのは **life cycle model**。
- 場合によっては、特定の技術的観点に関連するprocess, acdtivity, task を一ヶ所に集めるのが適切な場合がある。そのようにしてprocess, activity, task を集めたものがプロセスビューである。

  ➔ ISO/IEC/IEEE 15288:2015 System life cycle processes, Annex E Process views

DEOS ライフサイクルモデル
（DEOSプロセス）



DEOSの四プロセスビュー

- Consensus building process view
  要件定義及びその実現に関する合意形成
- Accountability achievement process view
  システムについての説明責任遂行
- Failure Response process view
  障害対応。障害への短期的対応
- Change accommodation process view
  変化対応。故障への中長期的な対応、環境変化への対応など

注意：　通常のシステムライフサイクルに必要なもの（通常の運用プロセスなど）を、ここに再掲する必要はない。

これらのプロセスビューは、OSD達成のために必要な事柄を、ISO/IEC/IEEE 15288 に定められた通常のシステムライフサイクルプロセスに付け加えるもの。

"DEOS process"
➔ DEOS life cycle model

DEOS用語 vs 国際標準用語: いわゆる "DEOS process" は、ISO国際標準でいう life cycle model であって、process ではない。➔ 若干混乱している

process

set of interrelated or interacting activities that transforms inputs into outputs
[ISO9000:2005]

life cycle model

framework of processes and activities concerned with the life cycle that may be organized into stages, which also acts as a common reference for communication and understanding
[ISO/IEC/IEEE 15288:2015]

∴ IEC62853草稿のなかでは、"DEOS process" に相当する DEOS life cycle model が例として紹介されている。

stage

- ISO/IEC/IEEE 15288 には process に加えて stage がある。

  stage

  period within the life cycle of an entity that relates to the state of its description or realization

  Note 1 to entry: As used in this International Standard, stages relate to major progress and achievement milestones of the entity through its life cycle.

  Note 2 to entry: Stages often overlap.

- DEOS の四大要素は、stage であり process view でもある。

  四大要素: "consensus building", "accountability achievement", "failure response", "change accommodation"

再掲

IEC 62853/Ed1.0 2CD の内容

IEC62853 2CDはシステムライフサイクルがOpen systems dependability (OSD) を持つための要件を定める規格（の案）

どんな要件？

- 4つのプロセスビューが提供されていることを主張するディペンダビリティケース

  Consensus Building, Accountability Achievement, Failure Response, Change Accommodation

- 5つのメタアシュランスケース

  Internal Consistency, External Consistency, Validity, Adequacy, Confidence

ディペンダビリティケースとは？

- D-Caseのこと、と思ってほぼ間違いない。
- アシュランスケースのうち、
  - 安全性に関する主張をするもの：安全ケース
  - ディペンダビリティに関する主張をするもの：ディペンダビリティケース
  - セキュリティに関する主張をするもの：セキュリティケース

再掲

IEC 62853/Ed1.0 2CD の内容

IEC62853 2CDはシステムライフサイクルがOpen systems dependability (OSD) を持つための要件を定める規格（の案）

どんな要件？

- 4つのプロセスビューが提供されていることを主張するディペンダビリティケース

  Consensus Building, Accountability Achievement, Failure Response, Change Accommodation

- 5つのメタアシュランスケース

  Internal Consistency, External Consistency, Validity, Adequacy, Confidence

メタアシュランスケースとは？

- 62853 Clause 7の四つのプロセスビュー達成を主張するディペンダビリティケースが、粗末なものでなく、一定の品質を持っていることを主張（要求）しておきたい。
- そのためには、ディペンダビリティケースに関するアシュランスケースを書けばよい。

  ふつう、アシュランスケースはシステムに関して書かれるが、ディペンダビリティケースのような文書に関するアシュランスケースもあり得る。
- ディペンダビリティケース（ディペンダビリティケース）に関するアシュランスケースなので
  メタアシュランスケースとよぶ。

標準化部会講演会のお知らせ

2015-07-21 (火)

神奈川大学KUポートスクエア（みなとみらい）

http://deos-standard.progsci.info.kanagawa-u.ac.jp/

大芦誠(日本規格協会)

サービス化する経済における標準化

武山誠（神奈川大学）

DEOSライフサイクルモデルについて

木下佳樹(神奈川大学)

IEC 62853 オープンシステムズディペンダビリティの最新動向

神奈川大学プログラミング科学研究所他と共催

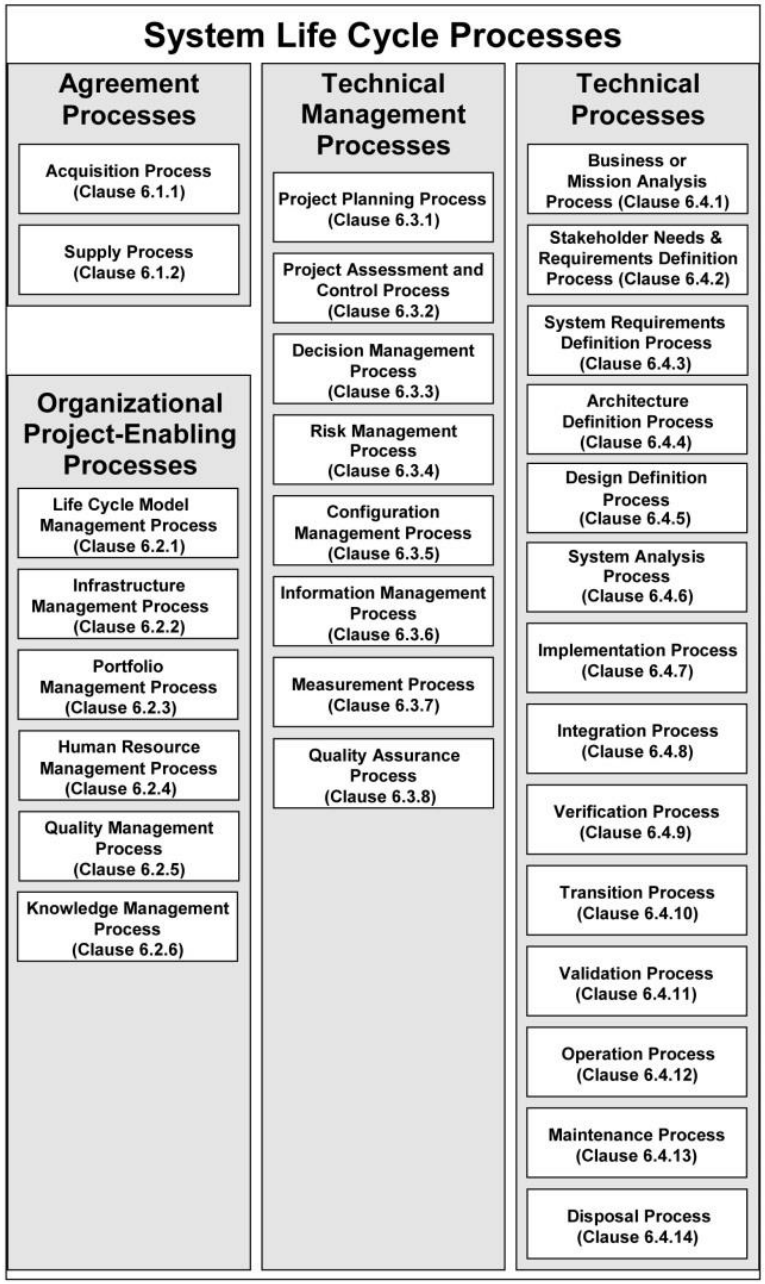
まとめ

- OSD 達成のための要件を規定する国際規格 IEC 62853 Open Systems Dependability 制定が IEC TC56 Dependability において進行中である。

  2016-12 発行予定
- 最新草稿における要件の内容は
  - 4つのプロセスビュー達成を主張するディペンダビリティケースがあることと

    Consensus Building, Accountability Achievement, Failure Response, Change Accommodation
  - 上記のディペンダビリティケースについての5つのメタアシュランスケースがあること。

大幅な変更の可能性あり


System Life Cycle Processes
Agreement Processes
Acquisition Process (Clause 6.1.1)
Supply Process (Clause 6.1.2)
Organizational Project-Enabling Processes
Life Cycle Model Management Process (Clause 6.2.1)
Infrastructure Management Process (Clause 6.2.2)
Portfolio Management Process (Clause 6.2.3)
Human Resource Management Process (Clause 6.2.4)
Quality Management Process (Clause 6.2.5)
Knowledge Management Process (Clause 6.2.6)
Technical Management Processes
Project Planning Process (Clause 6.3.1)
Project Assessment and Control Process (Clause 6.3.2)
Decision Management Process (Clause 6.3.3)
Risk Management Process (Clause 6.3.4)
Configuration Management Process (Clause 6.3.5)
Information Management Process (Clause 6.3.6)
Measurement Process (Clause 6.3.7)
Quality Assurance Process (Clause 6.3.8)
Technical Processes
Business or Mission Analysis Process (Clause 6.4.1)
Stakeholder Needs & Requirements Definition Process (Clause 6.4.2)
System Requirements Definition Process (Clause 6.4.3)
Architecture Definition Process (Clause 6.4.4)
Design Definition Process (Clause 6.4.5)
System Analysis Process (Clause 6.4.6)
Implementation Process (Clause 6.4.7)
Integration Process (Clause 6.4.8)
Verification Process (Clause 6.4.9)
Transition Process (Clause 6.4.10)
Validation Process (Clause 6.4.11)
Operation Process (Clause 6.4.12)
Maintenance Process (Clause 6.4.13)
Disposal Process (Clause 6.4.14)