電子情報通信学会技術研究報告原稿用紙
一般(様式 1)
社団法人 電子情報通信学会　　信学技報
THE INSTITUTE OF ELECTRONICS,　　IEICE Technical Report
INFORMATION AND COMMUNICATION ENGINEERS

IEC 62856 Open systems dependability の背景と今後
－合意形成，説明責任，障害対応，変化対応－

木下 佳樹†‡　　武山 誠†‡

†神奈川大学理学部情報科学科　〒259-1293 神奈川県平塚市土屋 2946
‡神奈川大学プログラミング科学研究所　〒259-1293 神奈川県平塚市土屋 2946
E-mail:　{yoshiki, makoto-takeyama}@kanagawa-u.ac.jp

あらまし　IEC TC56 Dependability による IEC 62853 *Open systems dependability* 開発は，2017 年 11 月現在 AFDIS (Approved for Final Draft International Standard)段階にあるプロジェクトである. 本稿は最新の FDIS 候補草稿に基づいて, この標準を概観する.

キーワード　open system; open systems dependability; dependability case

An overview of IEC 62856 Open systems dependability
－Consensus Building, Accountability Achievement, Failure Response and Change Accommodation－

Yoshiki KINOSHITA†‡　　Makoto TAKEYAMA†‡　and　Jiro TSUSHIN‡

† Department of Information Sciences, Faculty of Science, Kanagawa University　2946 Tsuchiya, Hiratsuka, 259-1293
‡ Research Institute for Programming Science, Kanagawa University　2946 Tsuchiya, Hiratsuka, 259-1293
E-mail:　{yoshiki, makoto-takeyama}@kanagawa-u.ac.jp

Abstract　IEC 62853 Open systems dependability, which is being developed by IEC TC56 at the stage of AFDIS (Approved for Final Draft International Standard) as of September 2017, is overviewed based on its committee draft for vote (CDV).

Keywords　open system; open systems dependability; dependability case

1. はじめに

たいていのシステムは，複雑でしかも時につれて変化するので，全体を完全に制御する利害関係者がいない．しかも，システムは異なる利害関係者に対しては違った姿を現す．このようなシステムをとらえるために，オープンシステムの概念が導入された．オープンシステムとはその範囲や機能，構造が時とともに変化し，また視点が異なると異なる記述がなされるようなシステムだと定義する．オープンシステムのディペンダビリティは，想定外の事象が発生し，システムに関する情報が不完全にしか与えられなくても，期待されるサービスを続ける能力である．国際標準 IEC 62853 *Open systems dependability* は，オープンシステムのディペンダビリティ管理のためのガイダンスを提供するべく，開発が進められており，その開発段階は 2017 年 11 月現在，AFDIS (Approved for Final Draft International Standard)である．IEC 62853 はディペンダビリティ要求を，ISO/IEC/IEEE 15288 *System life cycle processes* に規定されたライフサイクルプロセスの上の四つのプロセスビューとして規定する．その四つのプロセスビューとは合意形成，説明責任達成，障害対応，変化対応である．以下ではオープンシステムのディペンダビリティに対するこのアプローチを概観する．

IEC 62853 開発は，研究プロジェクト「利用者志向ディペンダビリティの研究」(2008 – 2014)（科学技術振興機構 CREST「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」研究領域）の活動の一部であり，著者らは IEC TC 56 Dependability の IEC 62853 の開発プロジェクトチーム PT4.8 Open Systems Dependability のプロジェクトリーダ（第一著者）およびプロジェクトチームメンバ（第二著者）として，この標準の開発に中心的役割を果たしてきた．

2. オープンシステム・ディペンダビリティ

2.1. オープンシステム特有のディペンダビリティ課題

IEC によるディペンダビリティの定義は「要求され

たように要求された時に遂行する能力」である(IEC 60050-192:2015, 192-01-22). ディペンダビリティの定義は他にも広く受け入れられているものがないではないが，我々は IEC の定義を採る.

システム障害やシステムおよび環境の変化のもとでも絶えずサービスを提供するためには，ディペンダビリティ管理活動がシステムライフサイクルのいたるところで遂行されなければならない.

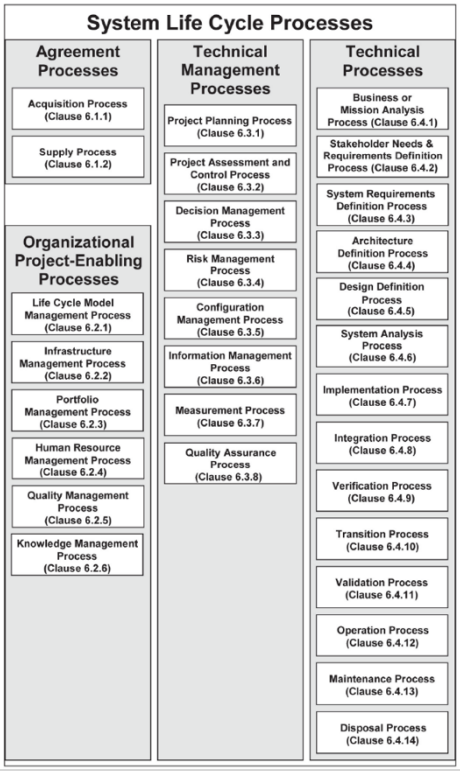

図 1　ISO/IEC/IEEE 15288 が規定するシステムライフサイクルプロセス

オープンシステムのディペンダビリティ達成のためには，システムライフサイクルの様々な局面で，絶えず改善活動がなされる必要がある．オープンシステムの仕様は本質的に不完全なものでしかありえない．したがって，ディペンダビリティ達成の最終目標は，仕様の正しい実現ではなく，説明責任の達成におかれるべきである．システムの制御の中枢がどこにも存在しないため，説明責任達成のために必要な活動は，システムライフサイクルの様々な局面に現れる．そのため，説明責任達成は，決して自明なことではない.

説明責任はシステムへの信頼と信用に直結する．信頼や信用は主観的なものだが，ディペンダビリティにおいて本質的な属性である．システムが障害から技術的に回復しても，説明責任が果たされず，人々の信頼が失われると，規制や世論他の社会的な要因のせいでサービス提供を再開できなくなってしまう場合がある.

オープンシステムは常に変化するので，利害関係者間のディペンダビリティ管理に関する合意も，常に見直され続けなければならず，必要に応じて改訂されるべきものである．ディペンダビリティ管理に関する合意の改訂につれて，説明責任の利害関係者への割り当ても改訂されなければならない．さらに，この過程全体が明確に定められているばかりでなく，それ自体を対象とした利害関係者間の合意がえられていなければならない.

説明責任は障害対応においても重要である．SoS (System of Systems)において，全体システムのディペンダビリティは部分システムの説明責任に支えられる．部分システムの障害があっても，その情報を他の部分システムに与えることによって障害の影響を緩和させることのできる場合もある.

「システムの目的，目標，環境および性能の変化に対応し，説明責任を達成し続けて，期待されるサービスを要求されたように要求された時に提供する能力」という，オープンシステムに特に必要となるディペンダビリティ能力をオープンシステム・ディペンダビリティという.

オープンシステム・ディペンダビリティ向上のためのシステム管理への要求を次節に記す.

2.2. オープンシステム・ディペンダビリティ管理のための四つの活動

IEC 62853 CDV は，オープンシステムがディペンダブルにするためにはシステムライフサイクルにおいて利害関係者に次の四つの活動を可能にしなければならない，と要求している.

合意形成　システム，その目的，目標，機能，環境およびこれらの変化について議論をする際の枠組を確立し,それをすべての利害害関係者に理解させること，その枠組でこれらについての共通の理解と明示された合意事項を確立し記すこと，さらに共通の理解と合意を状況の変化に応じて維持管理すること.

説明責任遂行　利害関係者間の合意の各項目について，その不達成が利害関係者および一般社会に与える影響を明示すること．これには，合意不達成の場合に説明責任を持つ利害関係者とその者が負う補償の明示が含まれる．これによって，各利害関係者による合意達成への最善の努力が促され，同時に，合意不達成の場合の補償を得る保証が得られる.

障害対応　障害に対して，その場の状況に最も適切な形で，直ちに対応して期待されるサービスをできるだけ提供し，中断と損害を極小にするための計画および実行.

変化対応　要求，環境，目的，目標の変化があってもシステムを「目的にかなった」状態に保つこと.

これら四つの活動は互いに他に依拠しあいながら進む．合意形成は他の活動の根拠を与える．説明責任

達成は形成された合意の実施を担保するとともに，障害対応や変化対応による活動を知らしめることによってシステムに対する社会からの信頼と信用を促進する．障害対応は説明責任達成のために必要な情報を与え，障害再発防止のための変化対応活動を開始させる．変化対応は，合意形成を再開して環境等の変化を共通理解と明示的合意に反映させる．合意形成で得られる合意は常に，絶え間ない更新の必要にさらされるシステムのスナップショットと考えるべきものである．

3. ISO/IEC/IEEE 15288 が提供するシステムライフサイクルプロセス

ISO/IEC/IEEE 15288 *System life cycle processes* は 30 のシステムライフサイクルプロセスを規定している．プロセスは四つのプロセスグループに分かれる: 合意プロセス，組織プロジェクト支援プロセス，技術管理プロセスと技術プロセスの四つである．プロセスは以下によって規定される．

- プロセス名: プロセス全体の範囲を規定する名前が与えられる．
- 目的: プロセス遂行のゴールを記述する．
- アウトカム: プロセスの実行の結果が良好であるときに得られる，システムの状態．
- アクティビティ: 互いに関連するいくつかのタスクの集まり．タスクはアウトカム達成のための要求，推奨あるいは許される活動である．

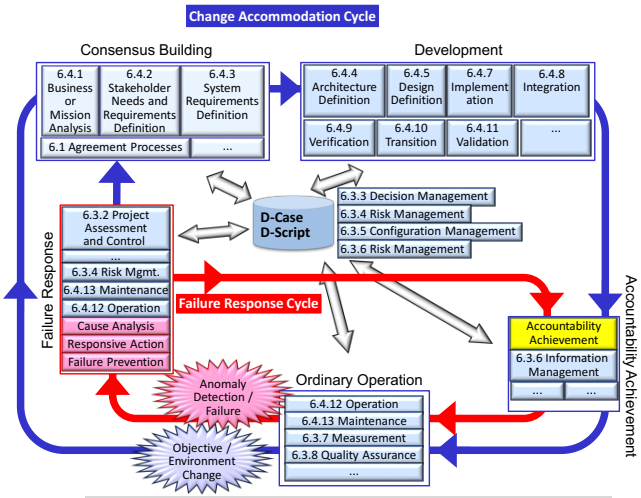

図 2　DEOS ライフサイクルプロセス

「システムライフサイクルプロセス」を，プロセスのつなぎ方,つまり「システムライフサイクルモデル」と区別することが大切である．ISO/IEC/IEEE 15288 はシステムライフサイクルモデルを提供しているわけではなく，その部品となるライフサイクルプロセスを提供する．それらを water flow で繋いでもスパイラルで繋いでもアジャイルで繋いでも 15288 に違反するわけではない．IEC 62853 も，システムライフサイクルモデルは規定しない．しかし主要な参照例として DEOS ライフサイクルモデル (DEOS LCM – 文献[2]で「DEOS プロセス」と呼ばれているもの)附属書で取り上げている．

ISO/IEC/IEEE 15288 のシステムライフサイクルプロセスは，繰り返して，しかも再帰的に適用されることが想定されている．例えば検証プロセス(Verification Process)はシステムの様々なレベル(アーキテクチャ定義，設計定義，実装，組み立て設置(integration))で繰り返し適用されることが想定されている．

4. IEC 62853 アプローチ: プロセスビューによる実現

4.1. プロセスビューの概念

プロセスビューの概念は，ISO/IEC/IEEE 15288 の informative な附属書 E で導入されている．プロセスビューは，15288 でのプロセス間の区分に対して横断的な目的とアウトカムに関する．その記述は，新たにアクティビティとタスクを追加する替わりに，関連するプロセス達のどのアクティビティとタスクを如何に用いるとプロセスビューの目的とアウトカムが達成されるかを説明するガイダンスを含む．

従って，プロセスビューの記述は，目的，アウトカム，アウトカムを実現するプロセス，アクティビティおよびタスクの同定とそれらがアウトカムをどのように実現するのかの記述かならなる．プロセス等の典拠への参照もプロセスビューに含まれる．

IEC 62853 CDV は，第 2.2 にあげた四つの活動のそれぞれに対してプロセスビューを規定する．

4.2. 合意形成プロセスビュー

合意形成プロセスビューの目的は，システム，その目的，その目標，その環境，その性能，そのライフサイクルおよびこれらの更新に関する，利害関係者間の共通の理解と明示的合意の，確立と保守である．

システムに関して必要な明示的合意を完全にリストアップすることは不可能なので，想定外の自体への対処の根拠は，具体的な合意事項のリストではなく，それを生んだ利害関係者間に共通する理解に求める他ない．これが「共通理解」を「明示的合意」とは別に考える理由である．

共通の理解と明示的合意の確立に関して求められるアウトカムは，以下を含む．

- システムの利害関係者の同定
- 利害関係者間で共有される議論の枠組の確立（用語，依拠する外的規準等を含む.）
- システムの目的，目標，環境等とその変化に関する共通理解の確立
- 利害関係者間で利益相反を生じた場合の解決手段に関する事前合意

共通の理解と明示的合意の保守に関しては，以下を含む．

- 合意事項変更管理のポリシーの決定
- 事業目的，利害関係者のニーズ，システムおよびその環境等の変化に応じた合意の維持
- 合意達成過程自体のレビュー
- ディペンダビリティケースの策定と承認の責任の所在の明示
- 合意内容，合意形成過程の説明，および合意内容が適切かつ実行可能だと見なされた理由などのディペンダビリティケースへの記録

4.3. 説明責任達成プロセスビュー

説明責任達成プロセスビューは，明示的合意の破れが利害関係者に対してもたらすべき帰結・社会一般への影響を明確にし，確実なものとすることを目的とする．合意の破れは，利害関係者の都合による不履行だけでなく，自然災害のような避けられない理由によるも含む．

求められるアウトカムは以下を含む．

- システムライフサイクルの制御とリスク管理に関する主要な意思決定段階の同定(以下,「主要決定」は決定結果ではなく決定段階を指す)．
- 各主要決定の説明責任者の同定
- 明示的合意事項の各々について，その破れあるいは障害を生じうる主要決定の同定
- 各破れが説明責任を負わない利害関係者と社会に対して与える影響のアセスメント
- 各破れについて，説明責任者にもたらされるべき帰結と，非責任者および社会に対する救済とに関する合意
- 決定の影響結果の監視とアセスメント．期待外・予期外の結果を含め，ひろく行なう．
- 決定の影響結果を決定者および他の利害間関係者に情報提供するフィードバックループの確立
- 合意の破れが起きた際の，事前合意済みの救済の説明責任者による速やかな提供
- 説明責任者から他の利害関係者および社会一般への，十分かつ適切な情報の提供

4.4. 障害対応プロセスビュー

障害対応プロセスビューの目的は，中断と被害を最小にしながら，最大限可能なサービスを状況に応じた方法で提供しつづけることである．

ガイダンスは障害を以下のように区分し，区分に応じたアウトカムの達成を求める．

- 予見し，事前に対処を計画するもの
- 予見するが，その可能性の低さやコスト面から対処の事前計画はしないと決めるもの
  （内，監視だけはするもの，監視もしないもの）
- 予見できないもの．（対処計画の予期外の失敗，可能性判断の失敗，等を含む）

求められるアウトカムは，準備，実行，障害対応の説明責任達成，および障害の経験に基づくシステムライフサイクルの改善などに関する．

障害対応の準備に関するものは，以下を含む．

- サービス継続を確実にするために保護しなければならない主要機能の同定
- 主要機能の保護のゴールの同定
- 主要機能に影響する fault，error，障害及びそれらの前兆（以下,「障害等」）の同定
- 同定された各障害等の影響解析（consequence 解析及び likelihood 解析）の遂行
- 同定された各障害等への対処のゴールの定義と合意
- 同定された各障害等の上記区分への区分け判断
- 事前計画すると決めた各障害等に対する特定の対応の開発，および，事前計画しないと決めたものに対するデフォールト対応の開発
- 障害一般からの被害を減少させる，特定の障害原因によらない包括的な方策の開発．

障害対応に実行に関するものは，以下を含む．

- 障害等の検出
- 原因解析および準備時の仮定の妥当性確認を含む影響解析の再実施
- 対処のゴールの，検出時の現状に応じた詳細化
- 特定の対応またはデフォールト対応の実施
- 事前計画のない障害等への事後的対応策定
- 対応自体による被害悪化やリスク増加の防止
- 周辺システムを含む全体としての被害の低減
- 対処のゴールに照らした対応のアセスメント

説明責任達成プロセスビューを呼び出しての障害対応の説明責任達成には，以下が求められる．

- 事前合意に基づいた損害の補償
- システムに対する確信と信頼の維持
- とられた対応に関する情報提供

変化対応プロセスビューを呼び出しての，障害の経験に基づくライフサイクル改善には以下が求められる．

- 改善のゴールにかんする合意

4.5. 変化対応プロセスビュー

変化対応プロセスビューは，要求，環境，目標や目的が変わっても，システムを「目的にかなった」（‘fit-for-purpose’）状態に保つことを目的とする．

「目的にかなった」状態にあることは，時点時点で変化する特定の目的より高次の目的となる．

求められるアウトカムは，以下を含む．

- 環境，仮定，リスク等に関する変化の認識と同定．
  予期外に検知された事象の原因たる変化の同定，

disruptive change の認識と管理を含む.

- 変化対応の準備: 'fit-for-purpose'への変化の影響のアセスメント，対応のゴールの定義，ゴールに関する合意形成と明示的合意の改訂.
- ゴールを満たす対応の開発，悪影響最小での適用
- 変化対応後のシステムの対応のゴールに照らしたアセスメント
- システムライフサイクルの絶え間ない改善
- 説明責任達成プロセスビューを呼び出しての変化対応の説明責任達成: 検知された変化と実施された対応間のトレーサビリティの維持，利害関係者と社会一般への対応の経緯と結果の説明

5. 適合性とディペンダビリティーケース

システムライフサイクルが IEC 62853 に適合していることを示すためには，前節の 4 つのプロセスビューのアウトカムをすべて達成していることを示すディペンダビリティケースが求められる.

仕様書などシステム自体の記述とは異なり，IEC 62853 の求めるディペンダビリティケースは，システムとそれを運用・改善するライフサイクルがどのような意味でディペンダブルといえる属性を持つのかを説明し論証する議論を記述する．これは，システムに対する利害関係者の確信／社会からの信頼の確保と，変化を含む長期的なシステムの成功に必要なものである.

ディペンダビリティケースの議論をどのように進めるかを例示する GSN のテンプレート (informative) が IEC 62853 の付録として提供されている．例えば，最上位の議論と，その直下の説明責任達成プロセスビュー達成に関する議論のテンプレートが以下のように与えられている．破線の方形については，さらに下位のテンプレートが与えられている.

6. IEC 62853 制定の現状と今後

2017 年 11 月現在，各国委員会に配布された最新の IEC 62853 草稿は CDV (Committee Draft for Vote) であり，BSi などから入手できる.（日本規格協会からは入手不可．CDV は，これを配布している national body とそうでないところが並存している状況である.）IEC 62853 の制定プロジェクトは AFDIS (Approved for Final Draft International Standard) 段階にあり，プロジェクトチームは 11 月中に FDIS 投票のための草稿を提出する見込みである．提出後 3 ヶ月の（フランス語への）翻訳期間を経て草稿は各国委員会による FDIS 投票に付され，2018 年半ばには投票結果が得られる見込みである．投票の結果承認されればその草稿が IEC 62853 FDIS として一般に入手可能なものとなる.

IEC 62853 は一般論であり，技術分野ごとに異なるディペンダビリティ要件に関する言及がない．今後，具体的な技術分野での適用を重ね，分野別のより具体的なガイダンスが策定されることが期待されている.

謝辞

IEC 62853 開発にあたって TC56 のプロジェクトチーム PT4.8 Open systems dependability のメンバーと交わした議論は有益であった．また，一般社団法人ディペンダビリティ技術推進協会標準化部会および技術部会のメンバーとは本標準案の基盤を提供する概念に関して数々の有益な議論を交わすことができた．以上記して感謝する.

文　献

[1] IEC 62853 *Open systems dependability*, Committee Draft for Vote (CDV), 2017.

[2] M. Tokoro (ed.), Open Systems Dependability – Dependability Engineering for Ever-Changing Systems, 2nd edition, CRC Press, 2015.

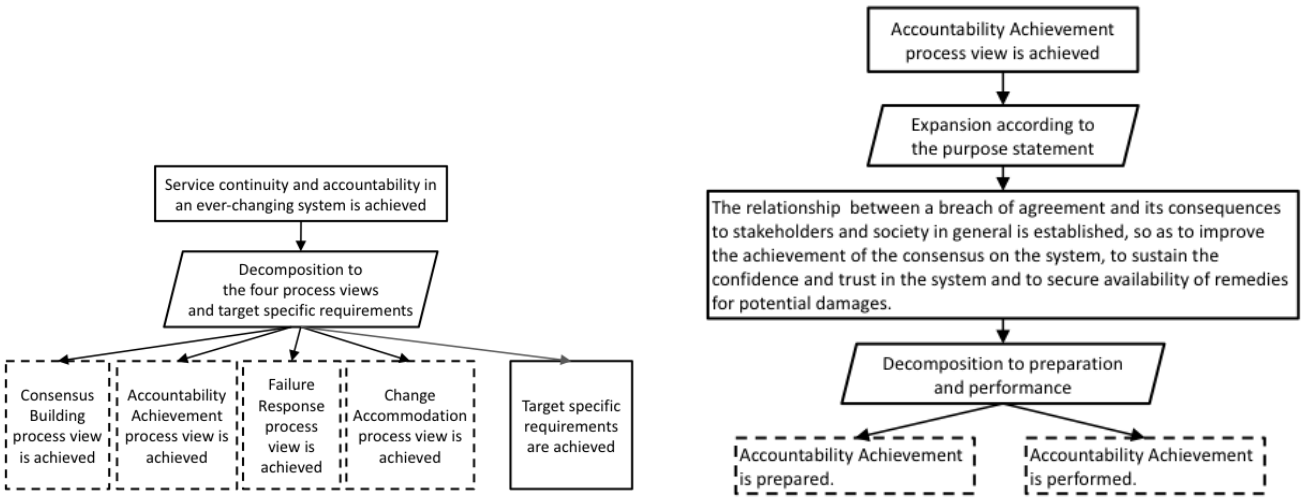

図 3 オープンシステムディペンダビリティを示す GSN テンプレート例 (IEC 62853 CDV より)