Software Technology

Prof. Mike Hennell
Technical Director

LDRA Testbed®, IEC 61508 and DO-178B/C

アジェンダ

- IEC 61508 、DO-178B/C **スタンダードへの準拠**
- MISRA **ガイドライン** for C、C++
  - **主な目的は組込みシステムの信頼性向上**
- CERT C **セキュアコーディングスタンダード**
  - **主な目的はあらゆるシステムのセキュリティ向上**
- IPA/SEC **国産スタンダード**
  - **あらゆるシステムの信頼性、メンテナンス性、ポータビリティ、スタイル**
- LDRA Testbed **の機能性･能力**

IEC 61508 Requirements

- IEC 61508 は主にプロセス志向のガイドラインであるが V&V に対する規定もある
- その [IEC98, Part 3, 条項 7.9.2.7]には V&V 活動として コード検証、ソフトウエアモジュールテスト、 インテグレーションテストなどが含まれる

Table III. IEC 61508 recommendations for code verification

- 推奨される 5つの主なカテゴリは

1. フォーマルプルーフ (形式検証)
2. 確率論的テスト (ランダム実行など)
3. 静的解析
4. 動的テストとその解析
5. ソフトウエア複雑度の尺度

- これらテクニックに関してはスタンダード内に追加の表がある

IEC 61508

- SIL（安全性レベル）によって各テクニックは 分類される
  - 推奨、推奨しないのどちらでもない
  - 推奨しない
  - 推奨
  - 強く推奨
- 問題なのは特定のアプリやSILに対して、どのテクニックが推奨されるのか、されないのかを決定できる仕組みが無いこと

DO-178B/C Requirements

- DO-178B/C も主に目標達成を念頭にしたプロセス志向のスタンダード　そして該当する様々な手法によって達成される
- 検証の目標については、別表 A7 に要約されている
- 主な目標は、ソフトウエアが要件を満たしていることと、安全性に影響を及ぼす全ての要素が考慮されていることの証明

DO-178B/C Verification

- バイナリ（あるいは同等な）レベルで要件を満たしていることを証明しなければならない　そして要件に関わらないコードが有ってはならない
- 各要件から関連するコードに直接トレースできること
  また全てのコードは要件にトレースできること
- SIL同様クリティカリティに応じたカバレッジ尺度が動的解析に求められる
  最もクリティカルなレベルAからEまでの5段階　レベルCが最も一般的

DO-178B/C Verification

- レベルAでは完全な分岐のテストと
  複雑な論理条件には MCDCカバレッジが必要
- コードはプログラミングスタンダードに準拠していること
- どのスタンダードを施行すべきかは言及していない
  しかしベストプラクティスのスタンダードが期待される
- 最も良く採用されているのはMISRA あるいはその派生

Software Faults ソフトウエアの欠陥

- IECスタンダードや DO-178B/Cの目的は、残存するソフトウエアの欠陥を、信頼度要求事項（SILのレベル）に応じて保証すること
- ここでソフトウエアの欠陥とは“要求される振る舞い”からの逸脱

Software Faults ソフトウエアの欠陥

- ソフトウエアの欠陥は以下のいずれかに分類：
  - アプリに特化した欠陥
    - 特定のアプリケーションドメインのみに関連する欠陥（ブレーキ作動の失敗）
  - テクニカルな欠陥
    - 基本的にどのようなアプリでも欠陥となる（配列境界エラー、不当な配列参照）

Static Analysis and Dynamic Analysis

- 静的解析ツールはテクニカルな欠陥検出に向く
  - これらの欠陥は言語、プログラミング上の問題
- 動的解析は基本的にアプリケーションの欠陥検出に向く
- 動的解析といくつかの形式的手法のみ
  アプリケーションの欠陥を検出することが出来る
- これはアプリケーションの仕様である要件を明確に用いることで

Static Analysis Limitations

- どのような静的解析でも
  またいくつかの形式手法でも全欠陥を検出することは保証できない
- チューリングマシンの停止性問題）に帰結
  「（任意の）プログラムにバグがないか判定できるプログラム」は存在しない
- 全ての欠陥を検出できない
  偽陽性メッセージの生成という結論になる　そして完全ではない

Dynamic Analysis

- 動的解析は全ての起こり得る欠陥を検出できる
- 問題は、欠陥が露呈される条件が複雑となり、通常計り知れない
- 一般に動的解析は 多様なカバレッジ尺度の到達目標で実践的に行える

LDRA Testbed

- LDRA Testbed は静的解析、動的解析の両方を提供
- 形式手法を用いて様々な解析を実施
  - システムワイドなデータフロー解析
  - システムワイドなポインタ解析
  - システムワイドなファイル操作の解析
  - システムワイドな配列境界解析
  - 実行不可能なコードを検出 (システム・プロシジャ内)
  - 無効なコードを検出 (システム・プロシジャ内)
  - インフォメーションフロー解析 (プロシジャ内)
- フォーマルメソッド (形式手法) がDO-178Cで公式に認識されている

LDRA Testbed

- **広範なプログラミングガイドラインをサポート**
  - MISRA C (1998 and 2004) and C++ (2008)
  - JSF++ AV
  - CERT C Secure Coding Standard
  - IPA/SEC C (from Japan)
  - MISRA C (2011) is on its way!
  - Others
- **システムワイドな複雑度解析**
  - **コントロールフローの複雑度**
  - **プログラミング構造の複雑度**
  - **データフロー複雑度**

Future Directions for programming standards

2つの主な傾向

- **セキュリティリスクに対するルールの強い要望　米国政府にて主導**
- **ツールの欠陥検出能力を向上させるルールの追加**
- **2つ目に関してゼロディフェクトソフトウエアの実現可能性は一般的になりつつあり、いくつかのクラスのソフトウエアでは既に実現できている**
- MISRA **は積極的に両方に取組んでいる**

Future Directions for programming standards

- CERT セキュアコーディングイニシアティブ (米) 活動継続中
- C 標準の正式なCERT サブセットを ISO C コミュニティと開発中
- 更なる精度向上を目指して洗練され続けている
- MISRA はこれら全てのグループと協力し
  ツールで解析可能なルールを抜粋している

- LDRA はこれらグループに参加し、厳密なルール定義に貢献している

Dynamic Analysis

- 動的解析の完全な要件に対するトレーサビリティをサポート

- 以下のカバレッジレベルに対応

  – ステートメント
  – ブランチ
  – MC/DC モディファイド・コンディション・デシジョン
  – LCSAJ リニア・シーケンス・アンド・ジャンプ

- ソースコード、オブジェクトコードレベルの両方をカバレッジ解析

Dynamic Analysis

- 動的解析はホスト上、シミュレータ、ターゲットで実行可能
- ターゲットの制約はツールの様々な機能で支援可能
- 例えば I/Oやメモリ領域、CPUパワーの制限など

Tool Qualification

- ツールのクォリフィケーションはツールの有効性を実証するプロセス
  例えば、所要のタスクを課して所要の検証データを得ること
- DO-178C ではツールクォリフィケーションプロセスの仕様を規定
- DO-178C では最終コードに欠陥をもたらす可能性のあるツールと
  検査のためのツールを区別
- DO-178B 対応で進化してきた LDRA のようなツールへの
  クォリフィケーションは本質的に変わりない

Tool Qualification

- LDRA はDO-178B、DO-178C の両方に対して
  全面的なツールクォリフィケーションパッケージを提供
- このクォリフィケーションプロセスは、ツールクォリフィケーションを規定しない IEC61508 でも受け入れられている
- LDRA ツールスイートは、1989年に高信頼性航空機搭載ソフトウエア（レベル A）で初めてクォリフィケーションされた
- LDRA は、100 以上の DO-178B レベルA プロジェクトで採用され、相当数に上るDO-178B に関わるプロジェクトを支えている

Software Technology

Traceability
トレーサビリティについて

Professor Mike Hennell
Technical Director

Compliance コンプライアンス・準拠

IEC61508 スタンダードでは、“このスタンダードに準拠するには、所要の基準・条件（安全性レベルなど）に応じて要件を満たしていることを証明すること。それゆえ各条項や補足事項は全ての目標が満たされていること” と記載されている。

現実的には、標準への準拠を証明するために IEC61508 の全ての要件がどのように満たされたかを列挙することを必要とする。これは IEC61508 準拠のために開発される製品、および準拠を謳いたい特定アプリケーションの両方に適用される。

Compliance コンプライアンス・準拠

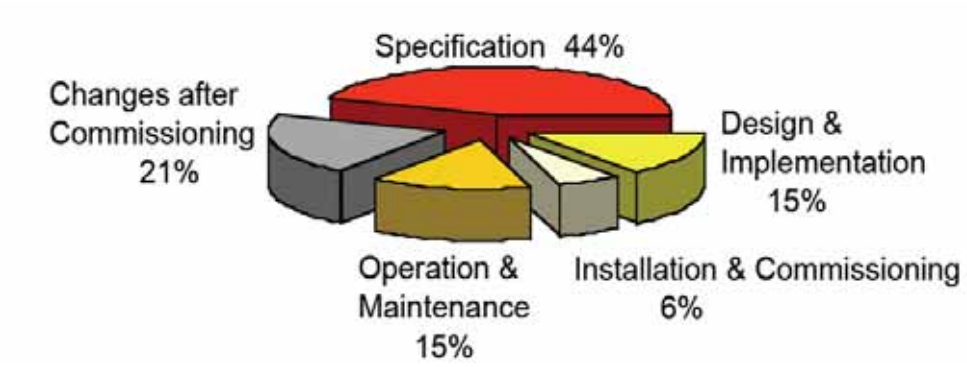
IEC61508 はスタンダードであるが法令ではないので、準拠が必須ということではない。しかしながら多くの場合、準拠はベストプラクティスであることと認められ、責任問題を追及されるような場合に引き合いに出すことが出来る。また多くの国家が IEC61508 あるいはその多くの部分を安全規定として直接盛込んでいる。その観点からすれば、法的な効力を有するといえる。そして多くの産業界や政府機関向けの安全装置、システム、サービスは、本質的に IEC61508 の準拠が求められる。それゆえ IEC61508 はスタンダードではあるが、広く支持されて準拠が法的に求められることが多い。

Requirements Traceability 要件のトレーサビリティ

安全なライフサイクル要求事項 (条項7)

安全なライフサイクルは、認識して-評価し-設計して-証明する (“identify – assess – design - verify”) といったロジカルな閉ループを成す。
安全関連システムのリスクが削減される最適なデザインは、プロセスに必要なリスク低減策とマッチするということ。

Causality of Defects 欠陥の原因



システム障害となる原因の調査結果：HSE “Out of Control.”

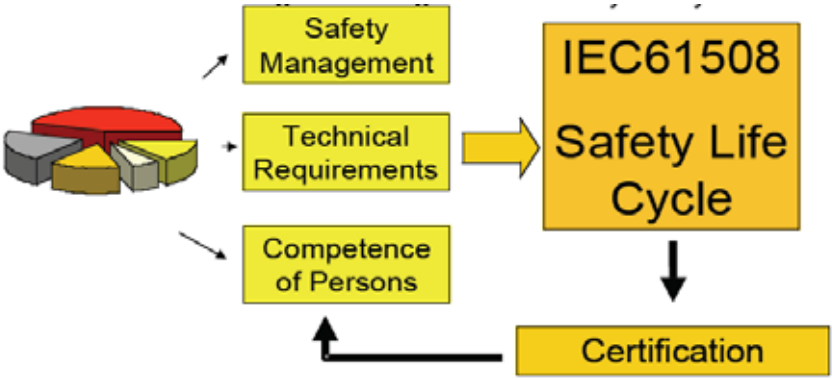
産業向け制御機器の事故原因の分析から多くの事故が仕様に関わっていることがわかる -すなわち要件定義とトレーサビリティ

Traceability for Independence インデペンデント独立性

機能安全の査定 (Clause 8)

Part1では、IEC61508 で求められる機能安全の査定活動についても記載している。査定の目的は安全性システムが、求められる安全性レベルであることを調査すること。一人以上の有資格者が関わって機能安全の査定を実行されること。個々の担当者は機能安全の査定対象から適切な独立関係にあること、SILのレベルや関わる重要性に応じて。

HSE Recommendation HSE の推奨



Business Benefits of Traceability トレーサビリティの効果 (ビジネス)

- 製品が顧客需要を満たすことのチェックを可能にする
  - 機能性
    - 要求される能力・機能
  - 特徴
    - 使い易さ
    - ルックアンドフィール (見た目の良さ)
  - 特性
    - 電子
    - 機械

Business Benefits of Traceability トレーサビリティの効果 (ビジネス)

マーケット駆動の開発をファシリテート (円滑に) する

- 要件の導出
  - マーケット分析
  - 製品仕様
  - 製品開発
- 要件ベースのテスト
- 要件ベースの製品実証

Business Benefits of Traceability トレーサビリティの効果（ビジネス）

開発･製造エコシステムの管理

- 製品の製造には必要となるコンポーネントがある
- 顧客により発見される欠陥を無くし改善できる
  - トレーサビリティにより要件とコードのリンクを提供
- 複製には開発プロセスの再現が必要なので、開発プロセスの再利用ができれば飛躍的なコスト削減となり、また最終製品の一貫性を維持することにも貢献する

Business Benefits of Automated Traceability

自動化されるトレーサビリティの効果（ビジネス）

- **要件の再利用を円滑化**
  - 新製品開発に既存製品を活用できる
  - 望まないものを除外できる
  - 飛躍的に開発コストと市場投入までの時間を削減

Finally

- SECのコーディングスタンダードは
  一般的にシリアスな20のプログラミングエラーを公開
- LDRA Testbed スイートはこれら全てを検出可能

Conclusion

- LDRA ツールスイートはDO-178B/C　や
  IEC 61508　で求められる主要なテスト手法を全てサポート
- 全SILレベルに対するエビデンスを完全に提供できる唯一のツール
- セーフティクリティカル、ミッションクリティカルなソフトウエアで35年以上広く用いられてきた実績

Q&A

Any Questions?