MATLAB EXPO

セキュアコーディングを実践する
ー セキュリティ関連のソリューション紹介 ー

アプリケーションエンジニアリング部
田中 康博

MathWorks®

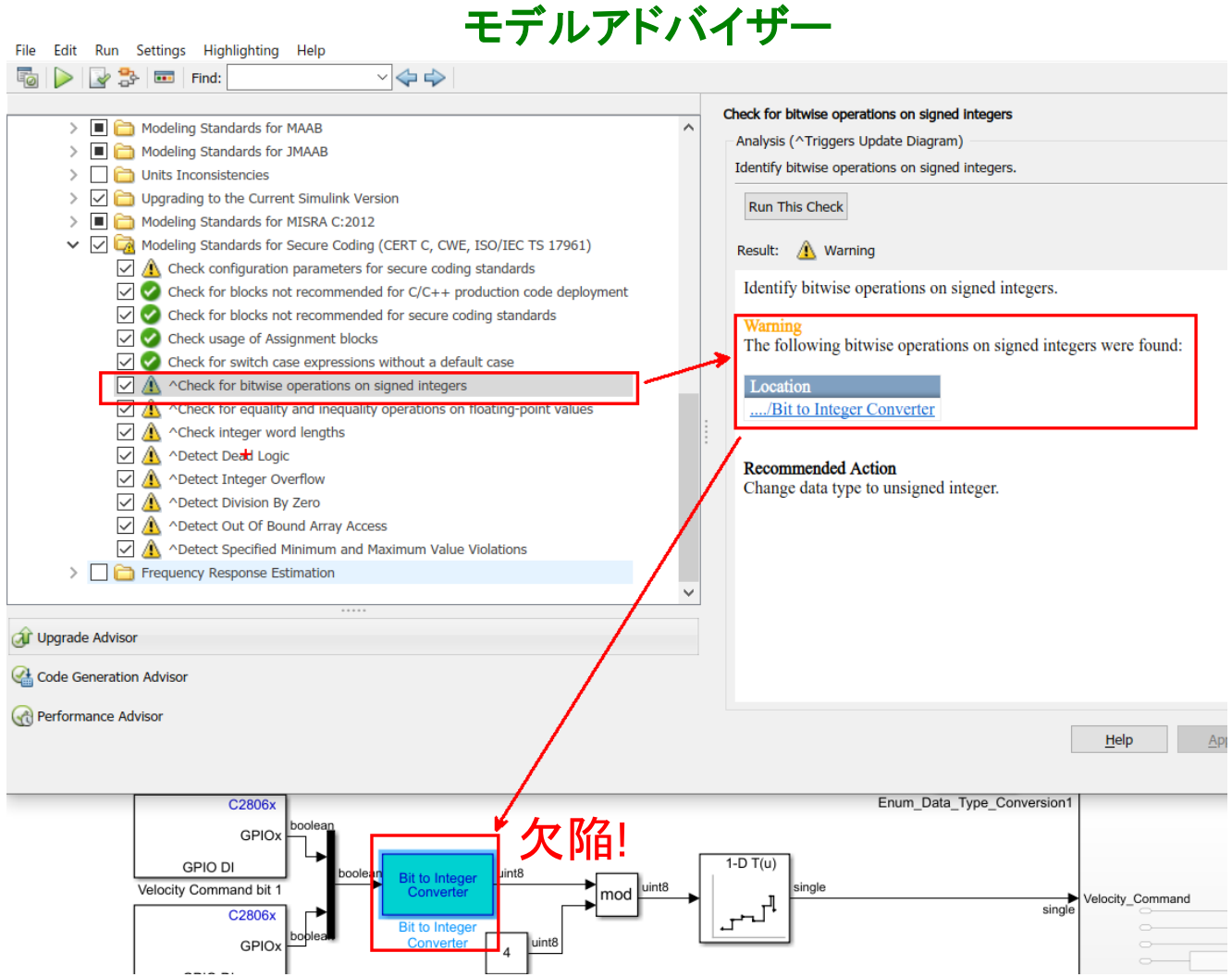
セキュリティ関連のソリューション紹介

セキュリティ関連のソリューション紹介 ― モデリングガイドライン

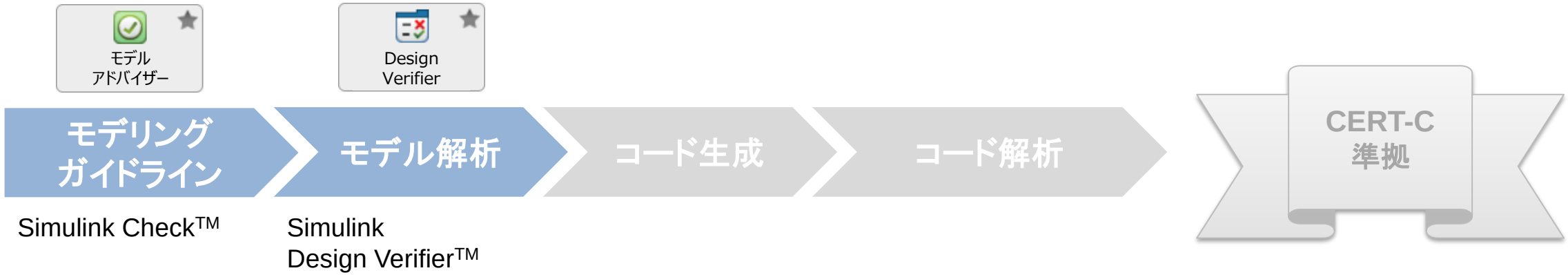
Simulink Check™

モデルのセキュリティ標準への準拠性を検証 (1)

- 概要:
  - セキュアコーディングのためのモデリング標準からの逸脱を特定
- モデルアドバイザーでのチェック:
  - CERT C, CWE, ISO/IEC TS 17961
- 結果:
  - 基本的な欠陥の削除
  - 生成コードのセキュリティ標準への準拠性を低下させる可能性のあるブロックの削除やパラメーターの見直し



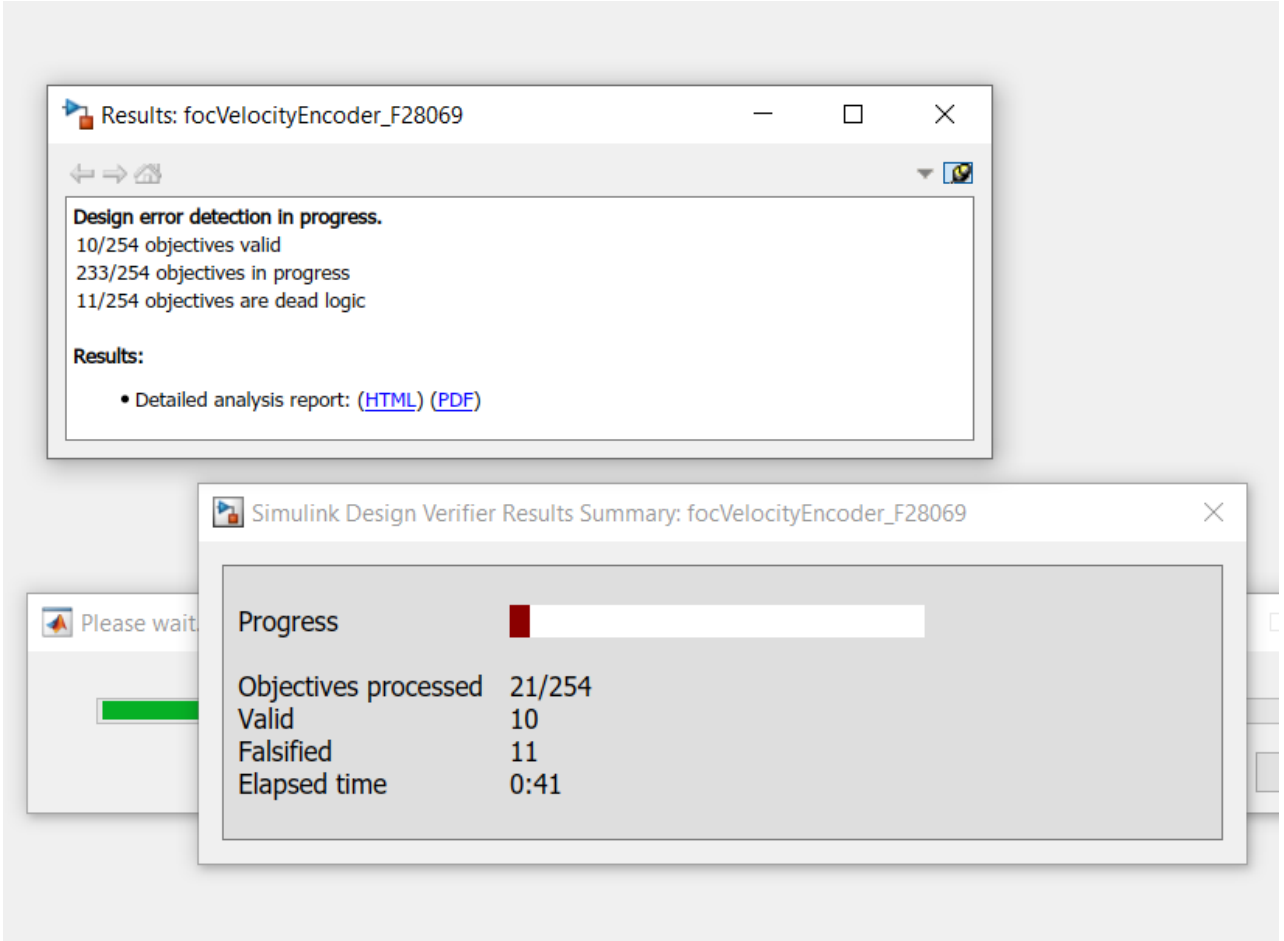
セキュリティ関連のソリューション紹介 ー モデル解析



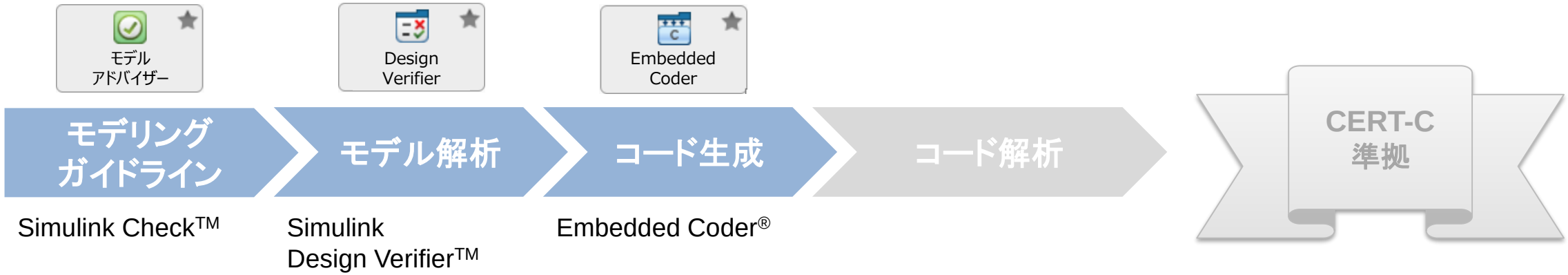
モデルのセキュリティ標準への準拠性を検証 (2)

- 概要:
  - モデルの潜在的な設計エラーを特定
- 検出される設計エラー:
  - ゼロ除算, 整数オーバーフロー, 範囲外配列アクセス
  - デッドロジック
  - 浮動小数点の問題 (NaN / 非正規浮動小数点)
  - 指定された最小値と最大値の違反
  - データストアのアクセス違反
- 結果:
  - 設計エラーの削除 / 正当化

設計エラー検出



セキュリティ関連のソリューション紹介 ― コード生成



Simulink Check™

Simulink
Design Verifier™

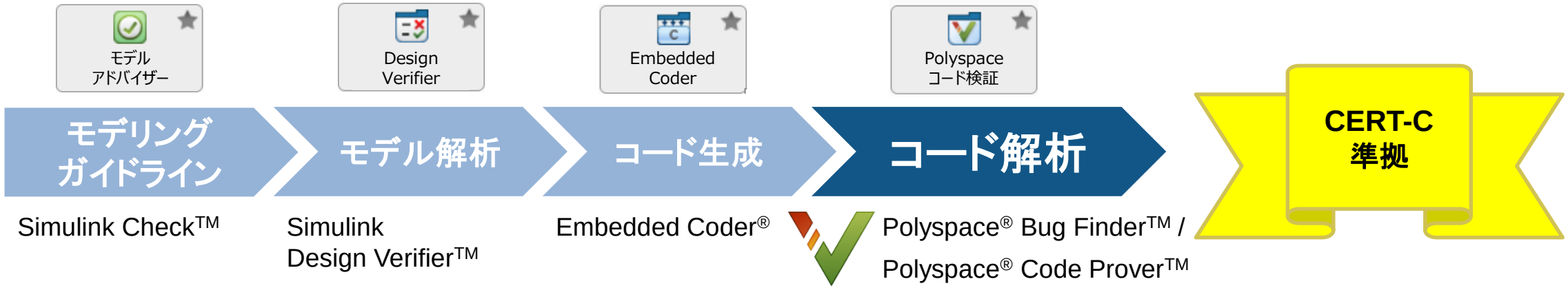
Embedded Coder®

セキュリティ標準のためのコードを生成

- モデルアドバイザーによるEmbedded Coderのパラメーターの提案
  - 浮動小数点演算子、再帰検出、オーバーフロー処理など
- ユーザーの希望がセキュリティ標準から逸脱する可能性がある
  - 既定のパラメーター動作：調整可能 (ファイルスコープ)
  - CERT-C DCL19-C. (関数スコープ)
    - Minimize the scope of variables and functions
- ユーザーはモデルに手書きコードを含めることができる
  - セキュリティ標準に準拠していない可能性がある

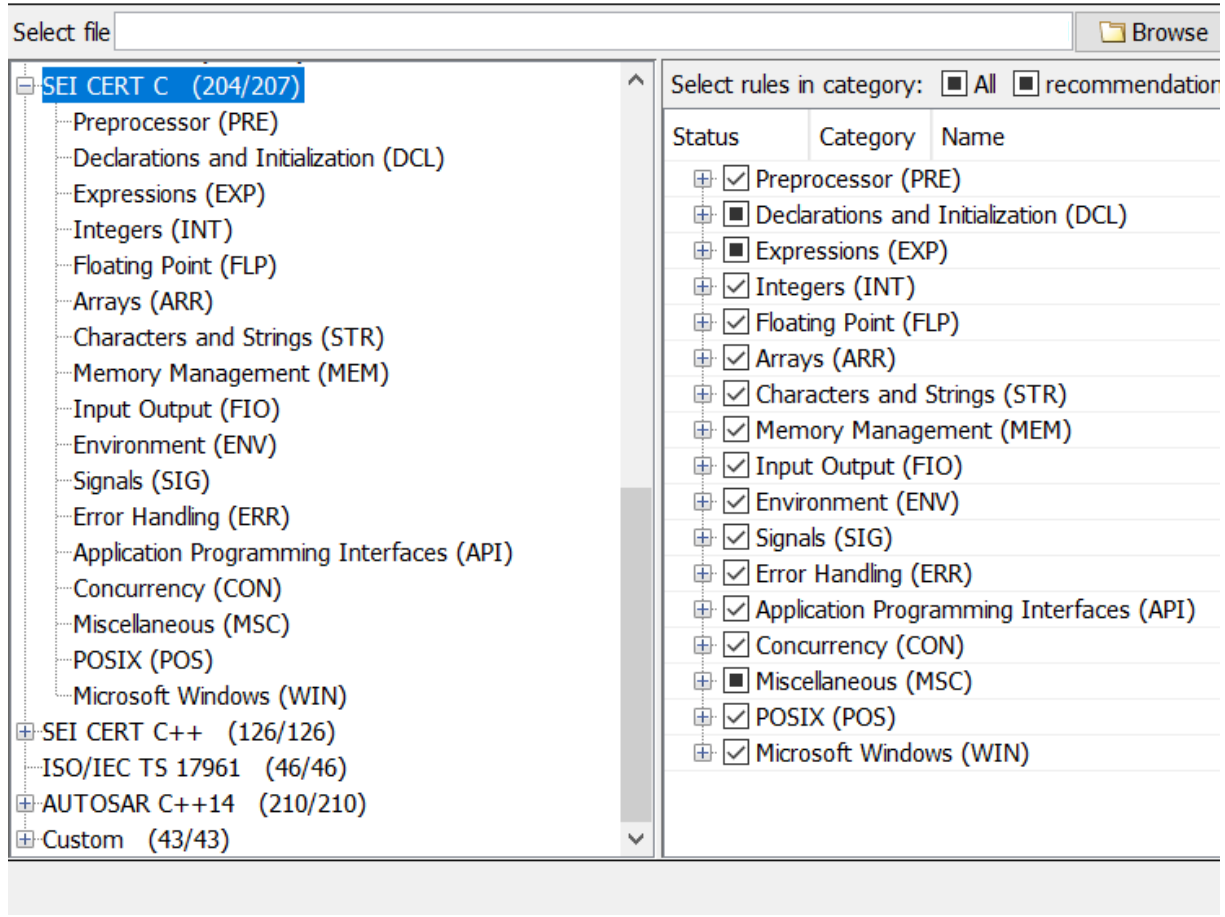
Polyspace Bug Finder ヘルプドキュメント

セキュリティ関連のソリューション紹介 ― コード解析

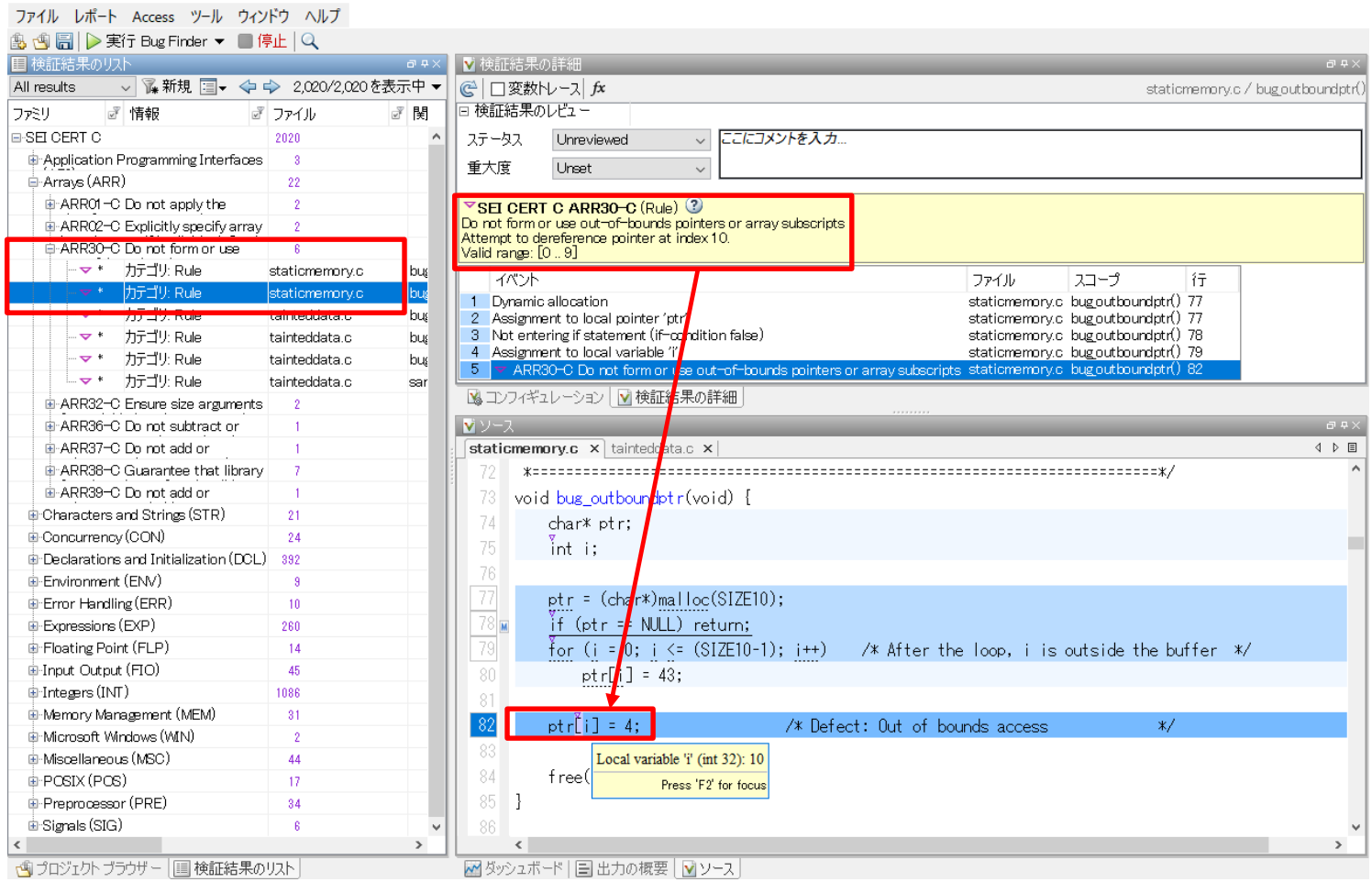


コードのセキュリティ標準への準拠性を検証 (1)

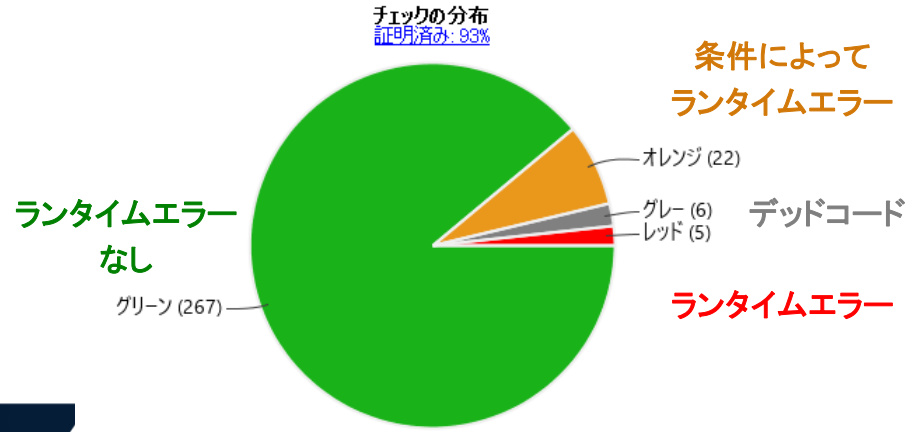
- コードレベルで最終チェック
  - ルールはコードに対してのみ定義される
  - 手書きコード (S-function など)
- セキュアコーディングチェッカー
  - CERT-C/C++
  - ISO/IEC TS 17961
  - MISRA-C:2012 Amendment 1
- CWEチェックのための解析フィルター



コードのセキュリティ標準への準拠性を検証 (2)



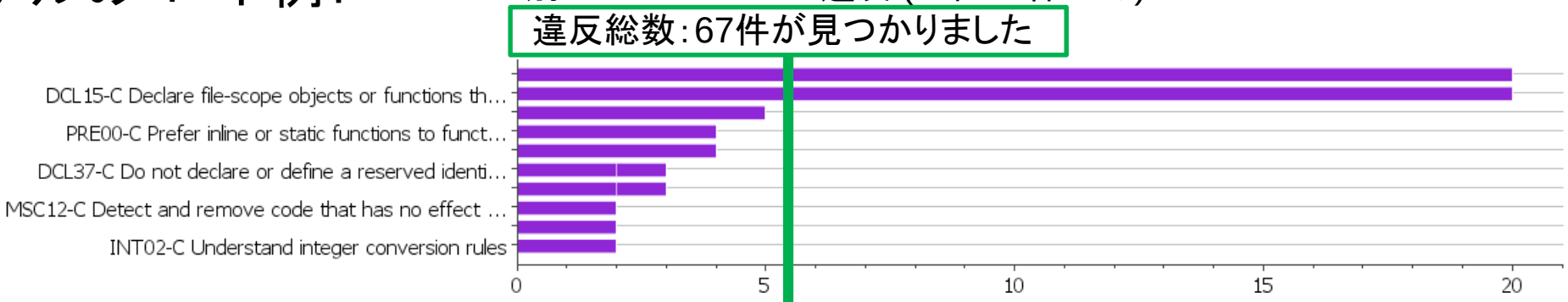
- デバッグ情報
  - 欠陥の原因特定、トレースバック
  - 変数の範囲/値
- **Polyspace Code Prover**
  - No False Negative
    - ランタイムエラーを検出
    - コードの安全性を証明



コードのセキュリティ標準への準拠性を定量化

未対応モデルのコード例：

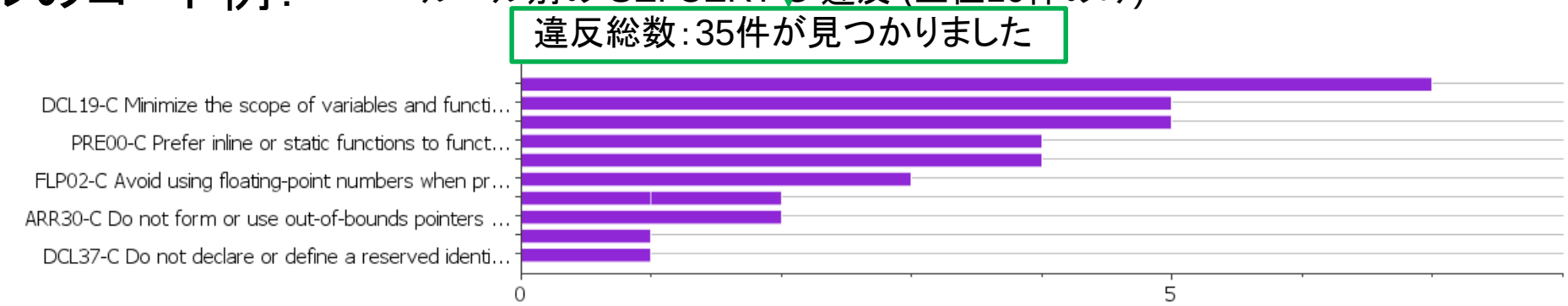
ルール別の SEI CERT C 違反 (上位10件のみ)



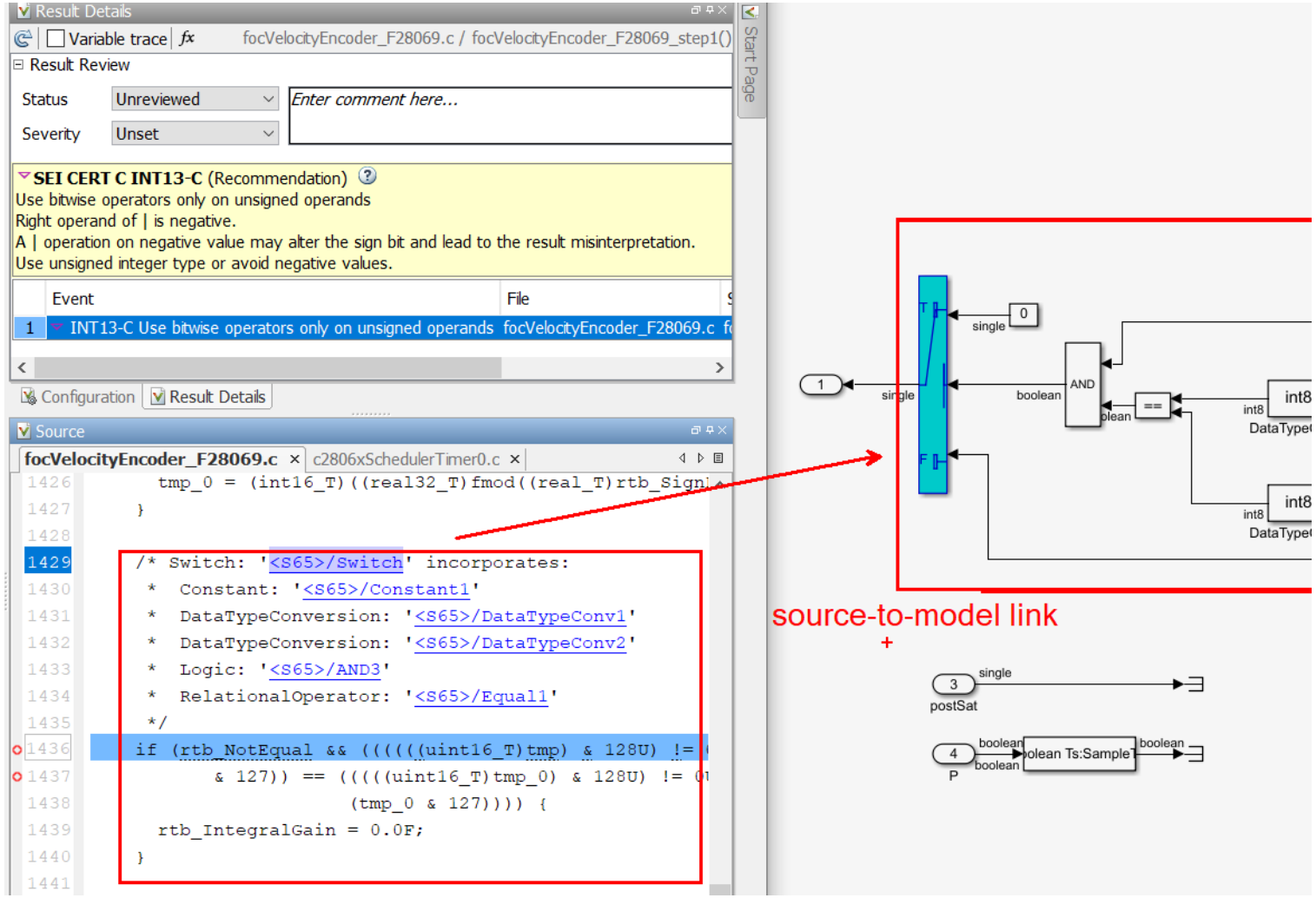
セキュアコーディング準拠への逸脱を削減

推奨モデルのコード例：

ルール別の SEI CERT C 違反 (上位10件のみ)



モデルとコード間のトレーサビリティ



- コードからモデルへジャンプできるハイパーリンク
- 双方向のトレーサビリティを確保

まとめ：セキュリティ関連のソリューション紹介

- モデルからコードまでのセキュアコーディングのサポート
- 開発の早期段階での設計チェック

Simulink Check

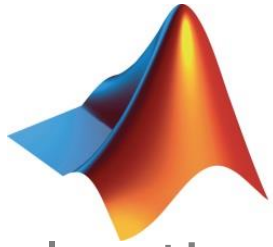
Simulink Design Verifier

- セキュアコーディングのためのコード生成の設定

Embedded Coder

- コードレベルで最終チェック
  - コード品質の定量化
  - 生成コード、S-Function、デバイスドライバなどの手書きコードなど

Polyspace Bug Finder / Polyspace Code Prover



MathWorks®

Accelerating the pace of engineering and science

© 2020 The MathWorks, Inc. MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See www.mathworks.com/trademarks for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.