D-Caseのこれまで、現在、これから

名古屋大学情報連携統括本部
情報戦略室
松野裕

自己紹介

- 2006.3 東大博士課程修了後、東北大PD
- 2008.10 - 2010.3 産総研木下チーム
- 2010.4 - 2012.3 東大石川チーム
- 2012.4 - 横国大倉光チーム・名古屋大山本グループ

内容

- はじめに: D-Caseのきっかけ
- アシュアランスケースについて
- これまでと現在
- これから
- まとめ

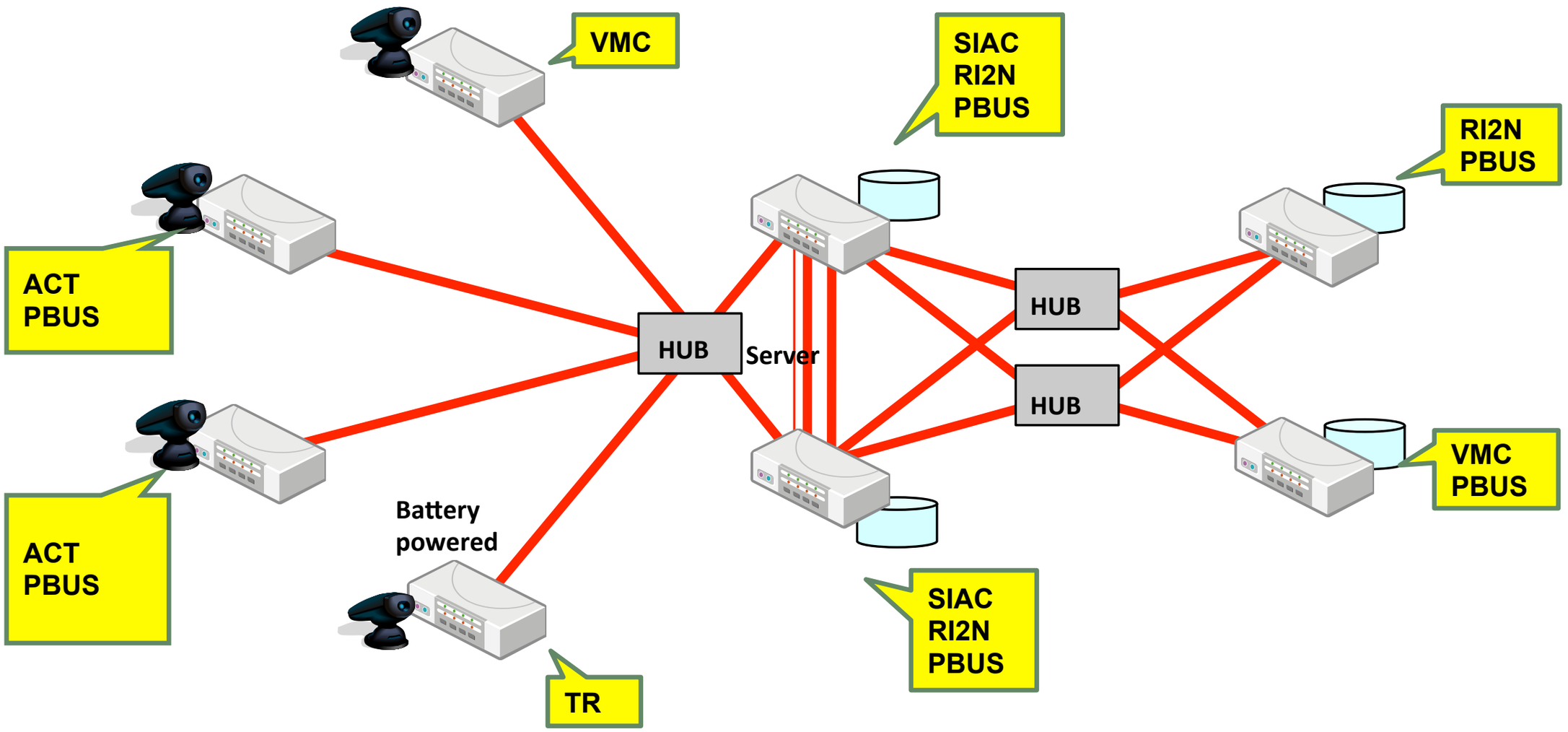
D-Caseのきっかけ

- DEOS(Dependable Embedded Operating System for Practical Use)では組み込みOSを中心とした研究開発を行なっていた
  - 研究チームはOS要素技術を開発し、組み込みOSに統合しようとしていた
- 2009年9月DEOS中間成果報告会が行われた

2009年9月
DEOS中間成果報告会

- 研究成果を統合してデモシステムを開発し、参加企業の方にDEOSがいかにディペンダブルで、価値があることを示す必要があった

遠隔監視サーバ
デモシステム



ACTやSIACは各研究チーム
で開発されたOS要素技術

中間成果報告会での課題

- デモシステムのディペンダビリティとは
- 各要素技術のディペンダビリティとは
- 類似技術との比較は、などなど

ディペンダビリティ
を説明するのは
難しい

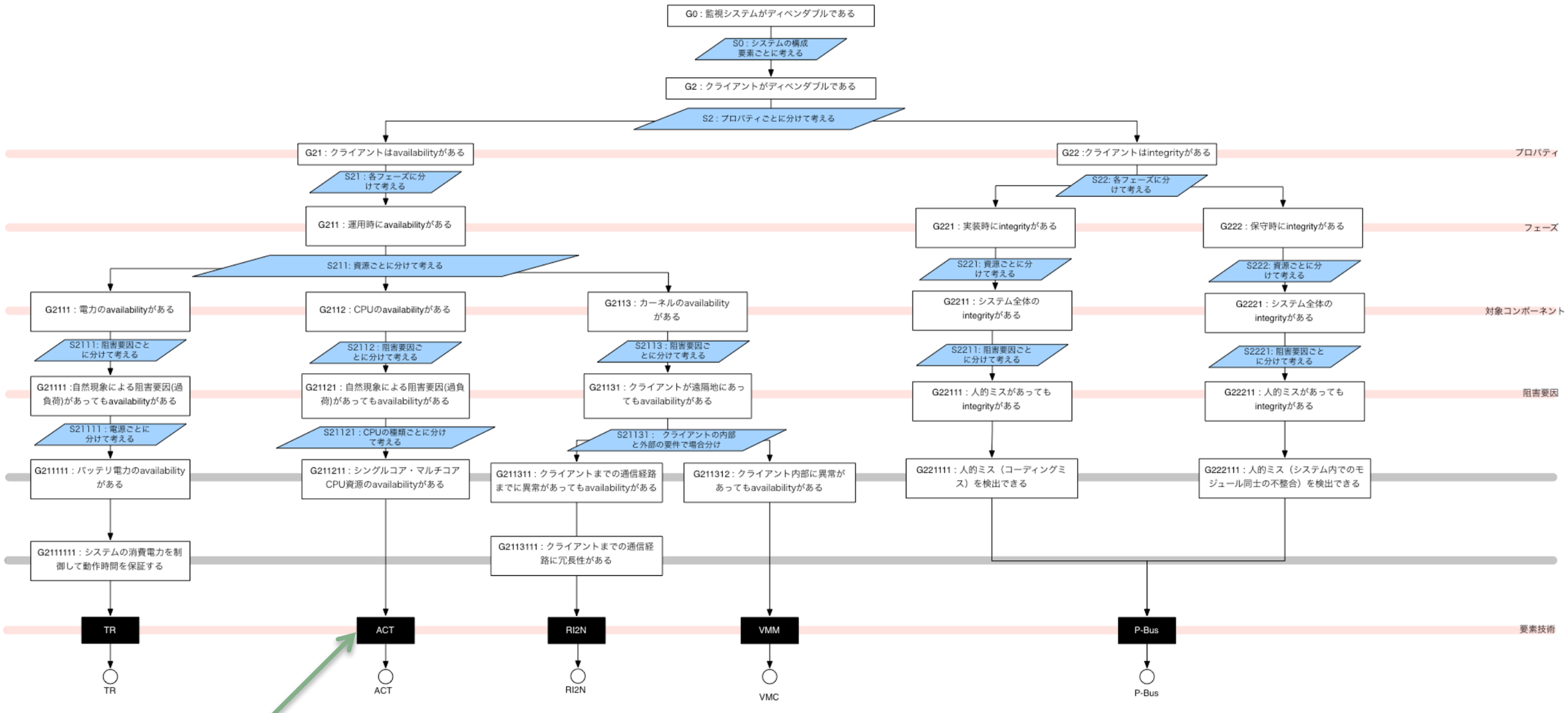
D-Caseの導入

- 産総研木下チームでは、海外調査旅行などを通じてアシュアランスケースの調査を行なっていた

- デモシステム、要素技術のディペンダビリティを説明することに有用でないかと導入した

  - D-Caseという名前がついた

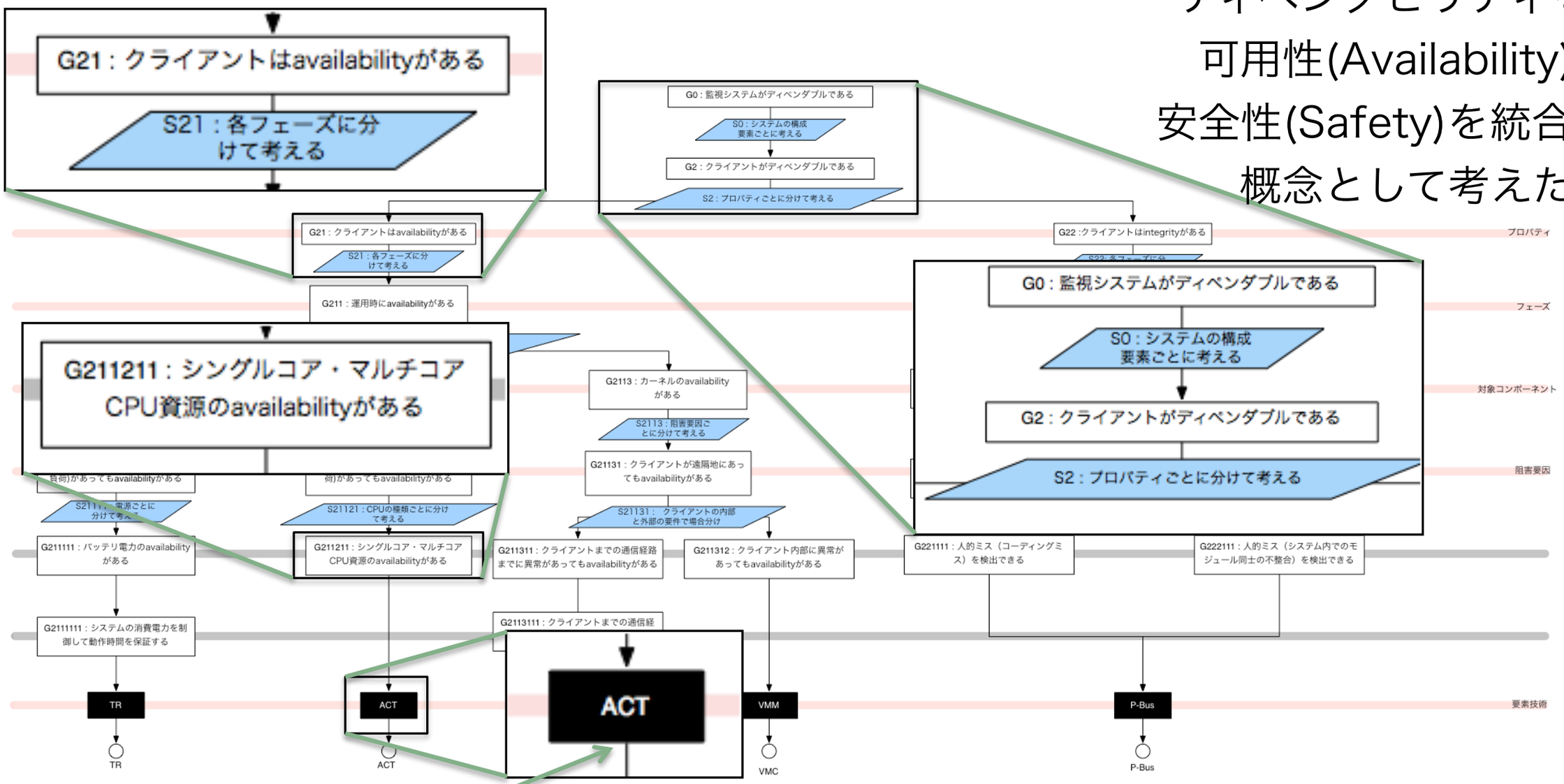
遠隔監視サーバデモシステムのD-Case



要素技術ノード
（いまはない）

遠隔監視サーバデモ
システムのD-Case

ディペンダビリティを、
可用性(Availability)や
安全性(Safety)を統合した
概念として考えた



要素技術ノード
（いまはない）

GSN(Goal Structuring Notation)
をもとに記述

議論、コメント

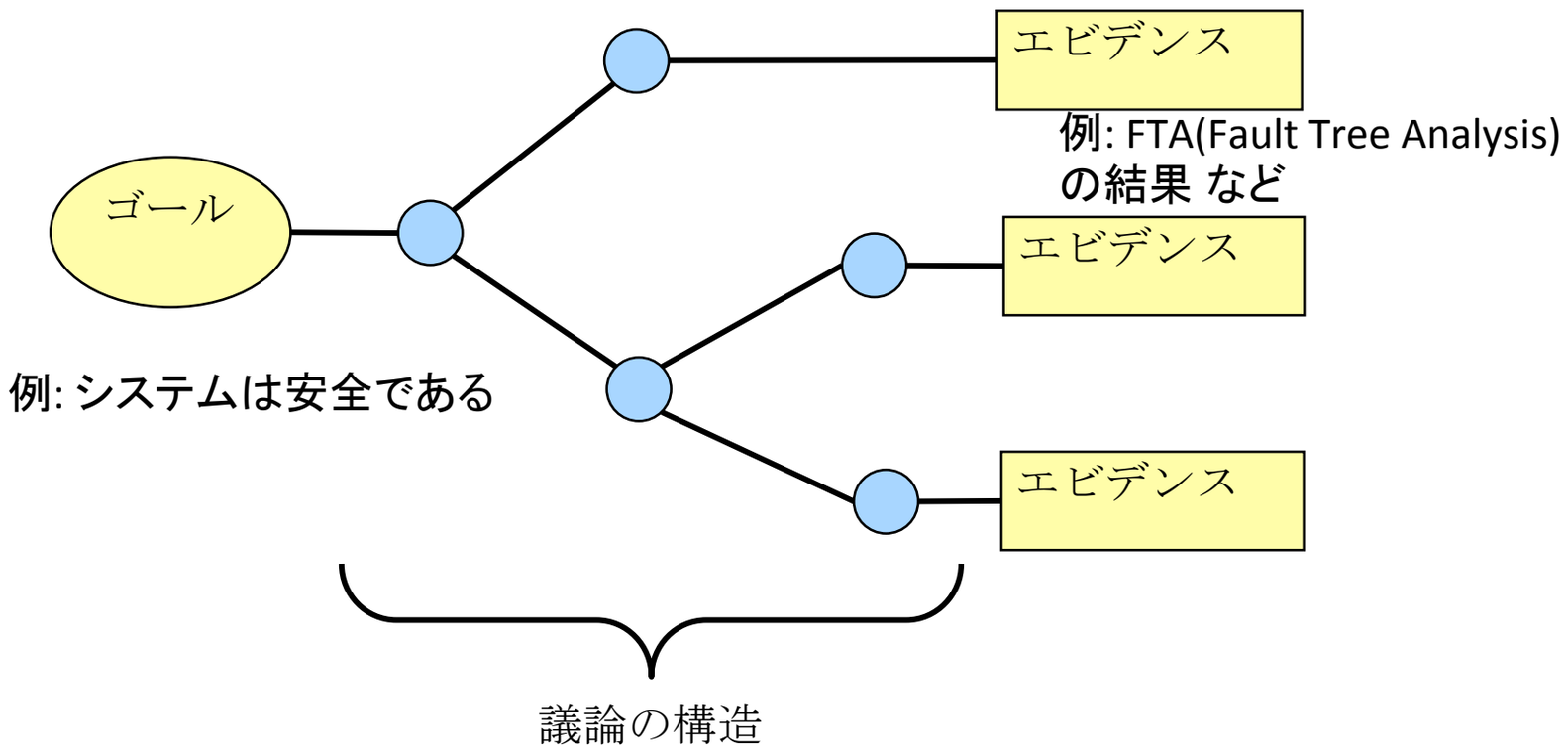
- 企業内、企業間で共通してディペンダビリティを議論、合意するための枠組みが望まれている
- ディペンダビリティは、障害対応機能を開発するだけでなく、どのようにディペンダブルであるか、利用者などに納得してもらうことも重要である

内容

- D-Caseのきっかけ
- アシュアランスケースについて
- これまでと現在
- これから
- まとめ

アシュアランスケースとは

- システム・プロセスの安全性、ディペンダビリティなどをエビデンスを元に展開するドキュメント



背景

- 1988年の北海油田事故(167名死亡)などを契機に、欧米で規格認証の際に提出が義務付けられるまでに普及
  - 手順のみでなく、なぜ安全性が保たれるのか、明示された議論で、エビデンスをもとに保証する
  - ISO 26262 (TC22/SC3, 自動車の機能安全規格)の要求項目の一つ

アシュアランスケース、ディペンダビリティケース、セーフティケース、…

- 日本語だと、保証ケース
  - Case: all the reasons that one side in a legal argument can give against the other side (Longman)
  - Assurance Caseは、安全性を議論する場合は Safety Case, ディペンダビリティを議論する場合は Dependability Caseと呼ばれる
  - 歴史的には、最初にSafety Caseという言葉が使われ、それを一般化したものとしてAssurance Caseという言葉ができた

アシュアランスケースの表記法

- Assurance Caseは通常、自然言語で書く
- 主要なグラフィカルな表記法
  - GSN (Goal Structuring Notation)
    - イギリスUniversity of York
  - CAE (Claim, Argument, Evidence)
    - イギリスAdelard社、City University London

ここでは、GSNを説明する

GSNの主要なノード

ゴール

保証したいこと、命題
例:
システムは安全である

ストラテジ

ゴールをサブゴールに分けるときの考え方:
個別の障害ごとに議論する

エビデンス
(ソリューション)

ゴールが成り立つことを最終的に保証するもの
例:テスト結果、運用事例など

コンテキスト

システムの状態、環境など、ゴールを議論するときの前提など
例:リスク分析の結果得られたハザードのリスト

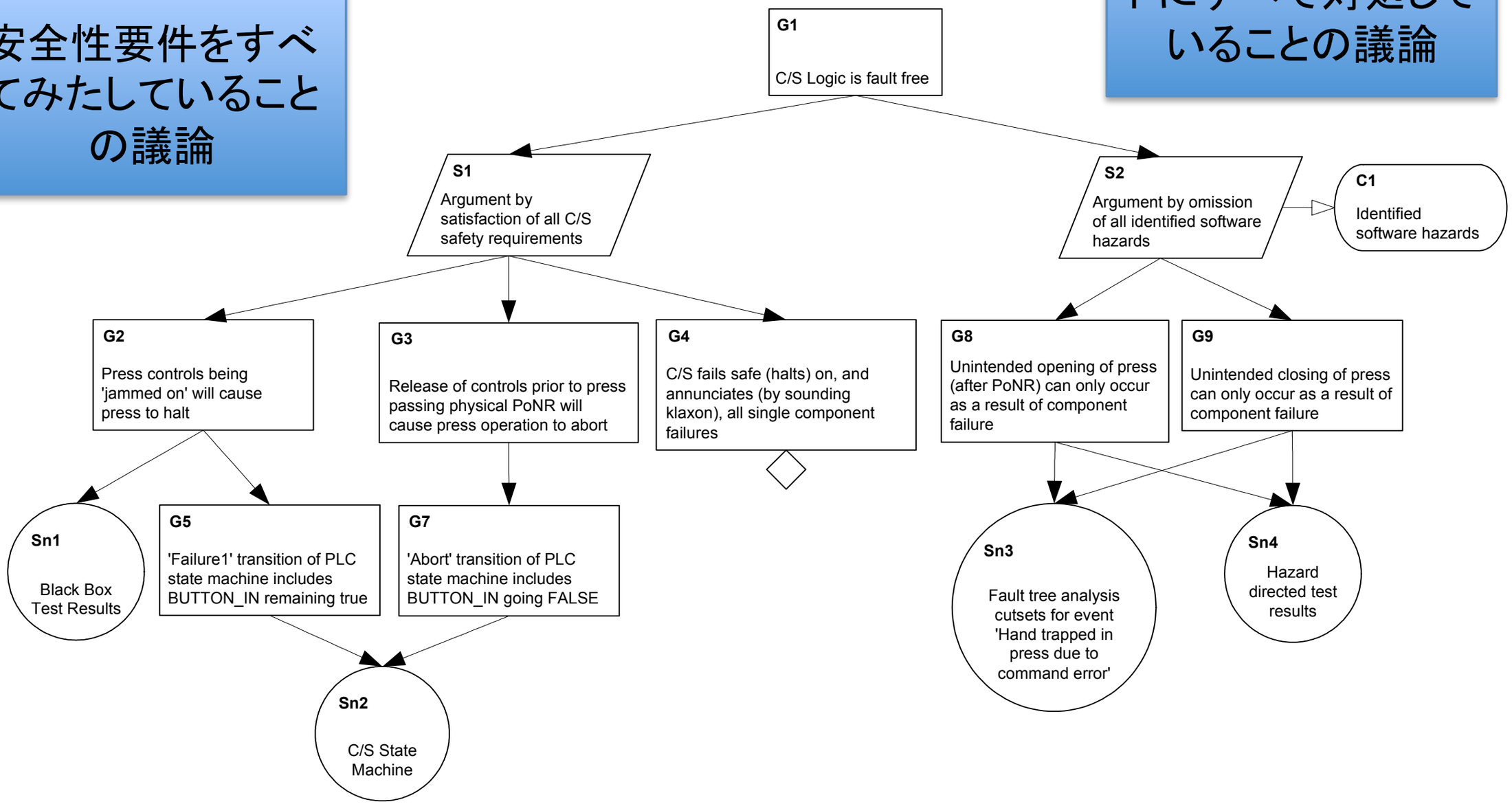
Undeveloped

ゴールをサポートする議論、エビデンスがまだないことをあらわす

GSNの例 1

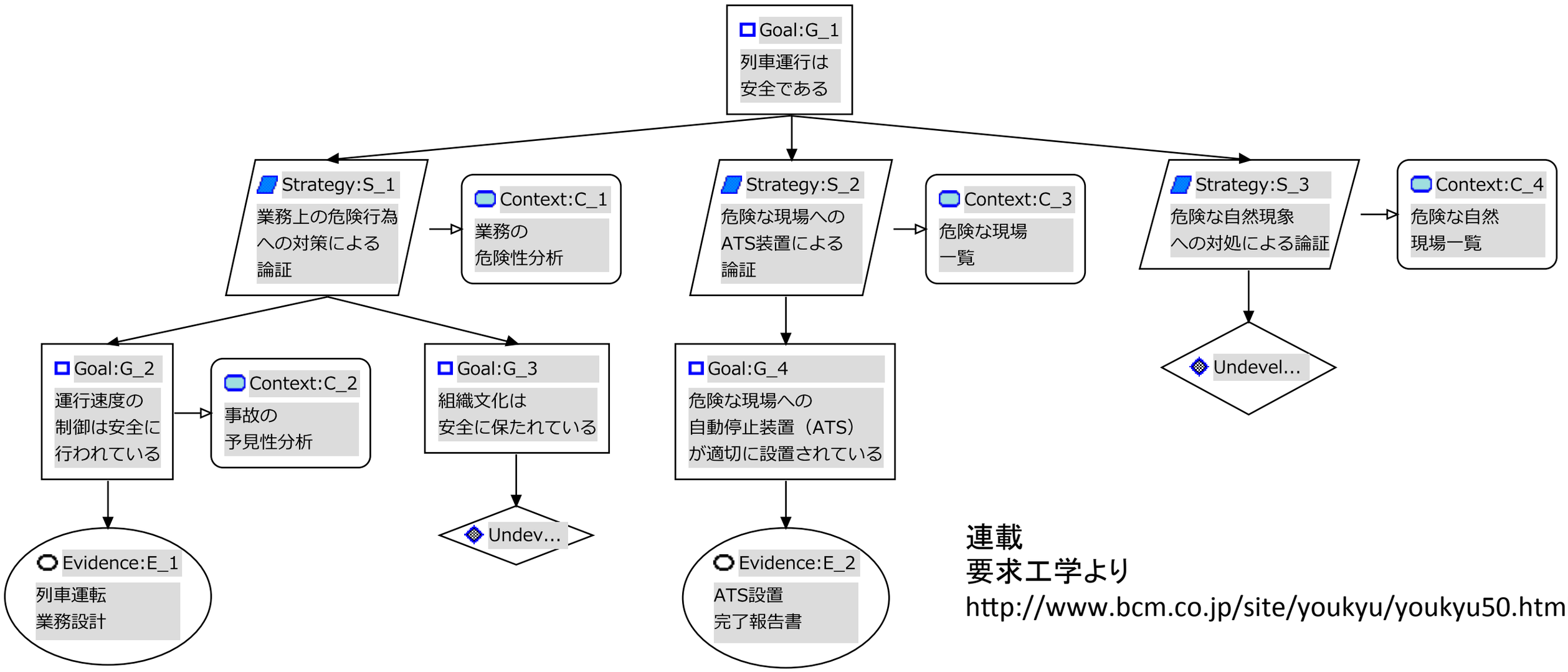
安全性要件をすべてみたしていることの議論

識別されたハザードにすべて対処していることの議論



T.Kelly, R. Weaver, Goal Structuring Notation: A Safety Argument Notation , In Proc. Workshop on Assurance Cases, DSN 2004

GSNの例2



連載
要求工学より
http://www.bcm.co.jp/site/youkyu/youkyu50.html

アシュアランスケースの現況

- イギリスにおいては、高安全、軍事システムなどの調達に必須
  - システム供給者、防衛省、第３者コンサルティング会社間になどにおけるリスクコミュニケーションに使われる
  - MoD Defence Standard 00-56
- US. Food and Drug Administration (FDA)
  - Infusion Pump
    - “… and for making an argument as to why the evidence, your data and analyses, supports the claim”
  - “A safety case is the best way to both document and review a submittal based on a risk management approach because the argument shows the proportionality of the mitigation”

アシュアランスケースの現況

- 2006年9月2日、アフガニスタンで作戦飛行中のMR.2 XV230が、空中給油を受けた直後に火災が発生して墜落する事故が発生した。2007年12月4日、イギリス国防省は調査報告を発表し、墜落した機体は、給油後タンクから燃料漏れが生じており、高温空気パイプの熱によって発火、拡大して墜落に至った、と分析した

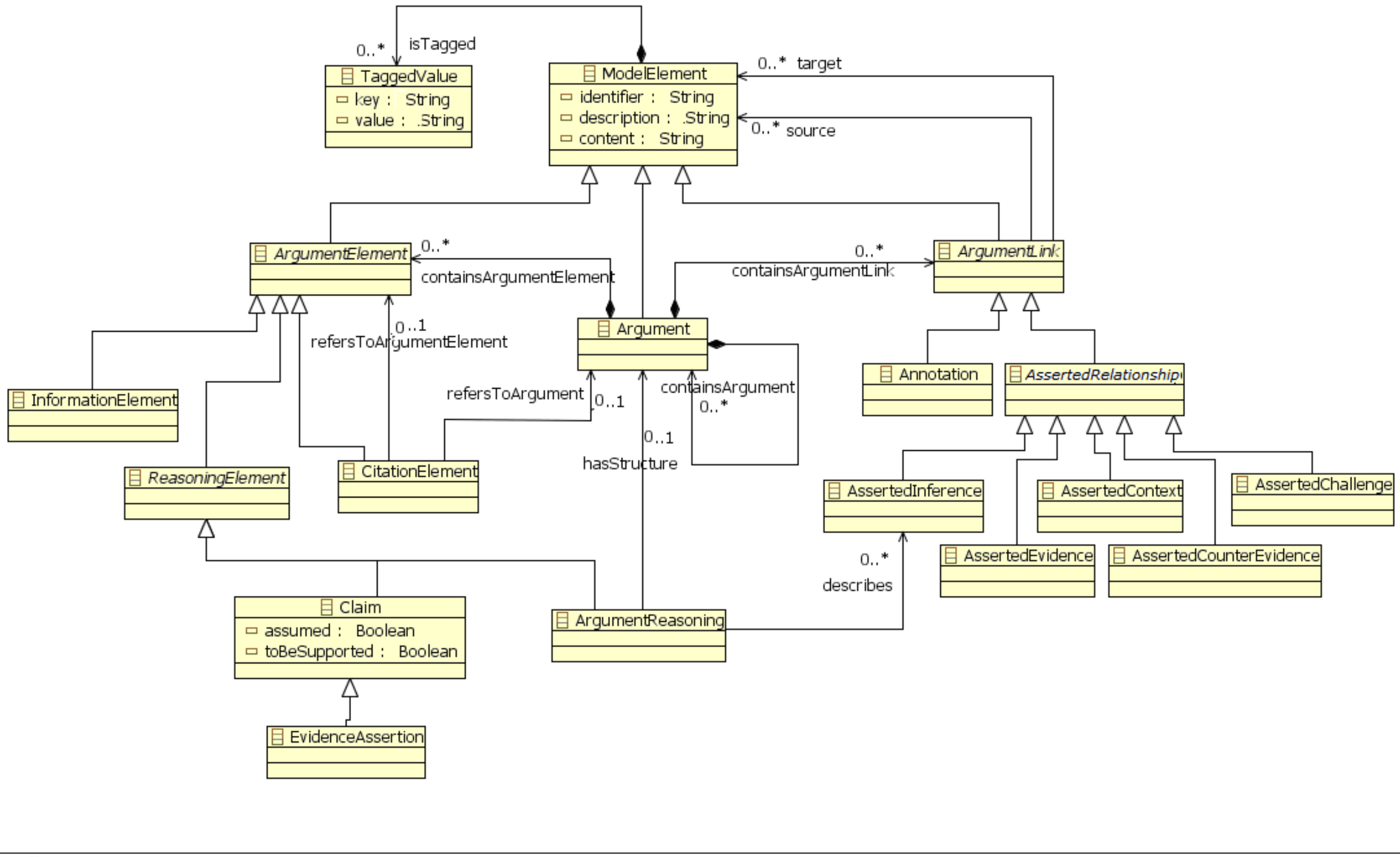
- Safety Caseがいい加減であったことがわかった。きちんと書かれていれば、欠陥を発見できたであろうと報告された

The Nimrod Review
http://www.official-documents.gov.uk/document/hc0809/hc10/1025/1025.pdf

アシュアランスケースに関する国際規格

- ISO/IEC
  - 15026 System and Software Assurance
    - Assurance Caseの基本構造、用語の定義
    - JST CREST DEOS(Dependable Embedded Operating System)プロジェクトメンバーが編集に参加している
- OMG
  - ARM (ARgument Metamodel), SAEM(Software Assurance Evidence Metamodel)
  - 統合されてSACM(Structured Assurance Case Metamodel)となった(2012年6月)
- Open Group
  - DEOSプロジェクトから、TOGAFに取り入れることを提案中

ARM

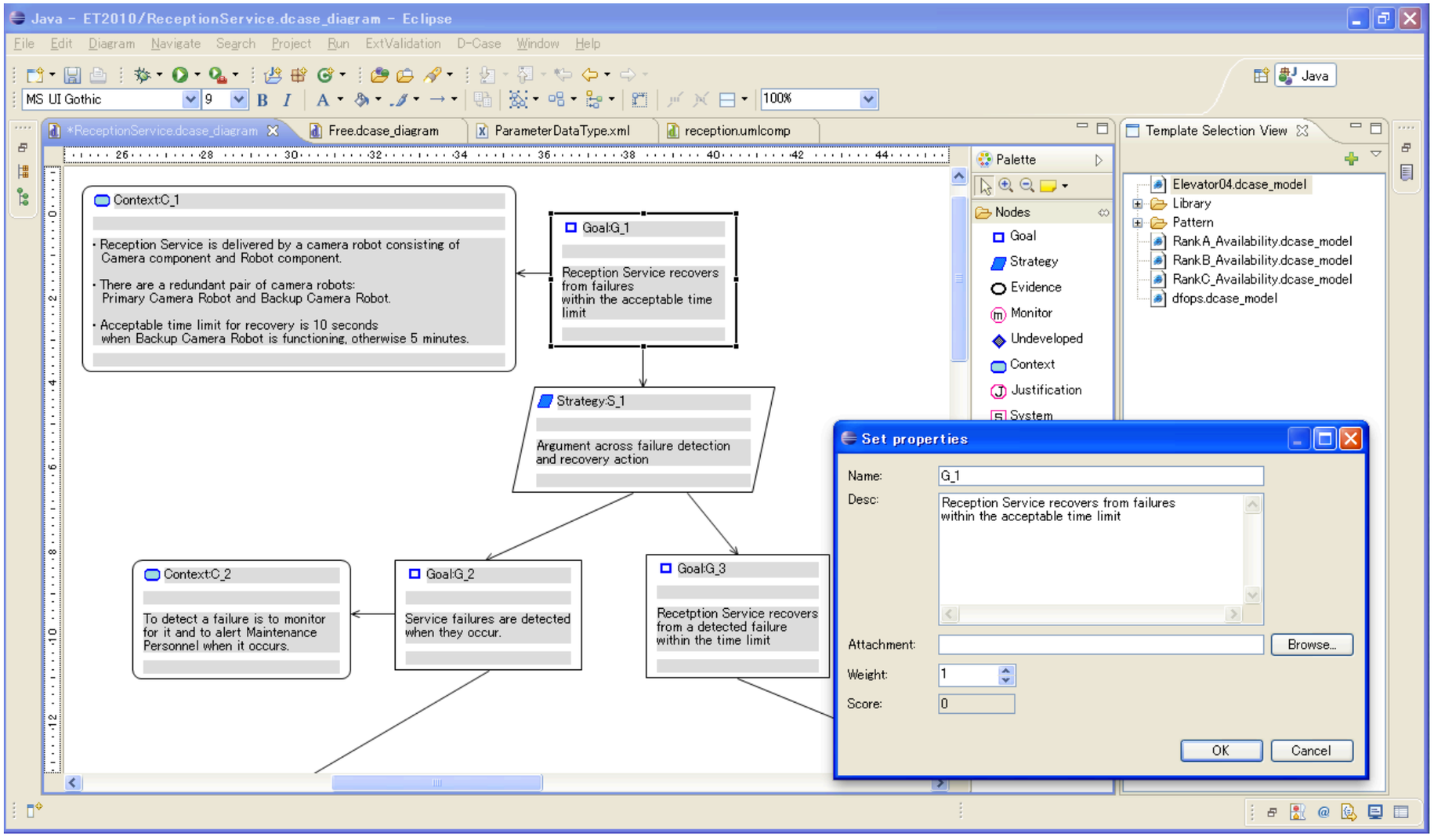

0..*
isTagged
TaggedValue
key : String
value : .String
ModelElement
identifier : String
description : .String
content : String
0..* target
0..* source
ArgumentElement
0..*
containsArgumentElement
0..*
containsArgumentLink
ArgumentLink
0..1
refersToArgumentElement
Argument
InformationElement
refersToArgument
0..1
containsArgument
0..*
0..1
hasStructure
Annotation
AssertedRelationship
ReasoningElement
CitationElement
AssertedInference
AssertedContext
AssertedChallenge
0..*
describes
AssertedEvidence
AssertedCounterEvidence
Claim
assumed : Boolean
toBeSupported : Boolean
ArgumentReasoning
EvidenceAssertion

ツール

- ASCE Tool (イギリスAderald)
  - CAE, GSNなどを編集できるツール
    - 軍事関係だけでなく、医療機器の安全性記述などにも近年用いられている
- Certware(http://nasa.github.com/CertWare/)
  - NASAが開発したオープンソースのツール
  - 既存のARMなどの規格に多く準拠

D-Case Editor

(後述)



http://www.dependable-os.net/tech/D-CaseEditor/

内容

- D-Caseのきっかけ
- アシュアランスケースについて
- これまでと現在
- これから
- まとめ

これまで

- D-Caseチーム(2010.4-)
  - リーダー:松野, スーパーバイザー:山本 (2011.6-)
    - 東大、産総研、富士ゼロックス、慶大、横国大、名古屋大、…
- DEOS推進委員、他の企業・研究機関との議論・共同研究開発

研究開発内容

- オープンシステムのディペンダビリティ
  - D-Case記述ステップ開発
    - 企業や研究機関とのD-Case記述実験
  - D-Caseツール、ツールチェーンの開発

オープンシステム

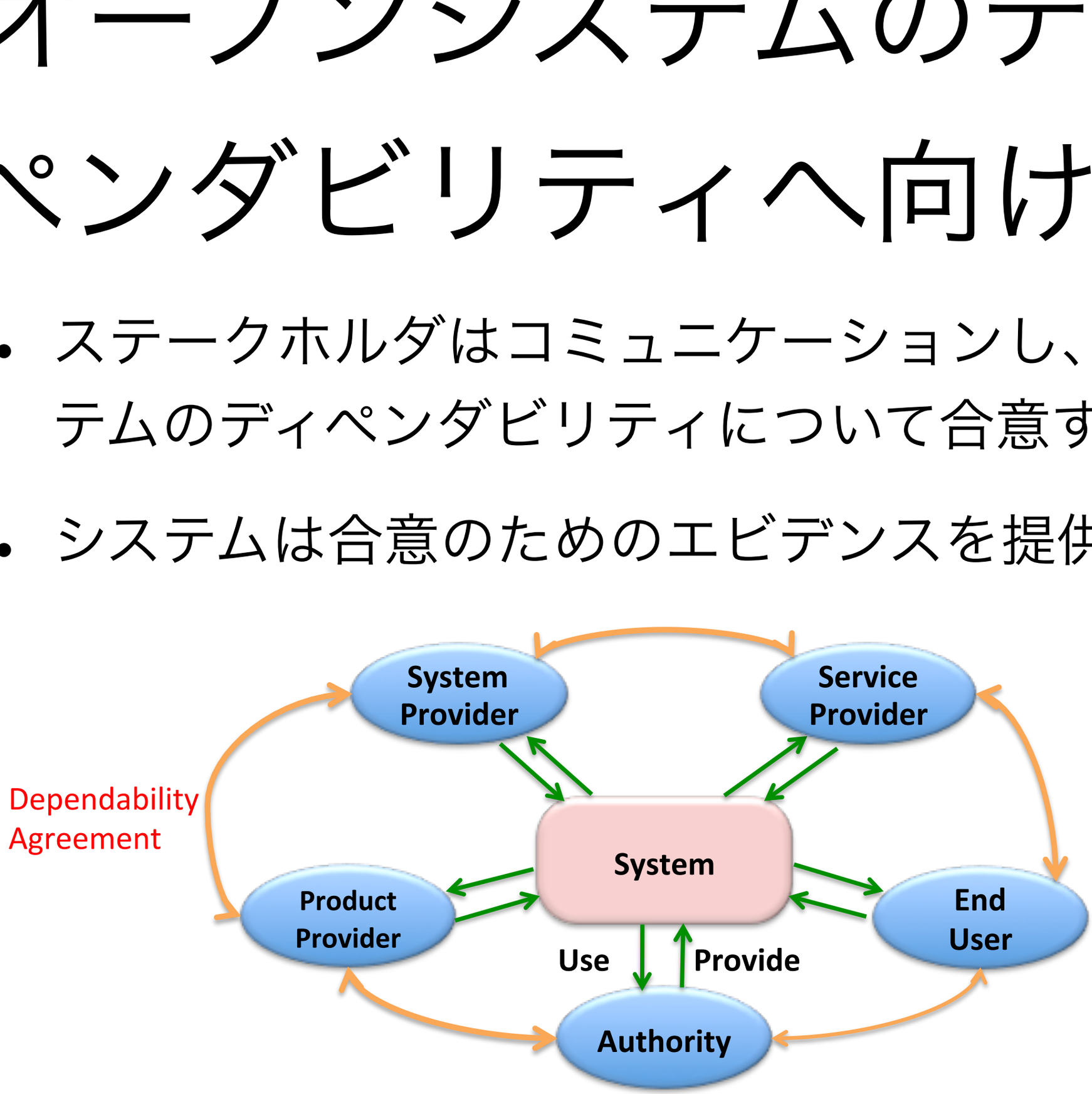
- A system whose boundary, function, structure, and interfaces change over time
- 最近のシステムはほとんどオープンシステム

オープンシステムのディペンダビリティへ向けて

- これまでの手法
  - テスト、形式手法、…
- プラス
  - エビデンスをもとに専門家を交えながら、ステークホルダがディペンダビリティを合意する

オープンシステムのディペンダビリティへ向けて

- ステークホルダはコミュニケーションし、システムのディペンダビリティについて合意する
- システムは合意のためのエビデンスを提供する



アプローチ

- アシュアランスケースをオープンシステムに対応させるため、拡張する

アシュアランスケースの現状

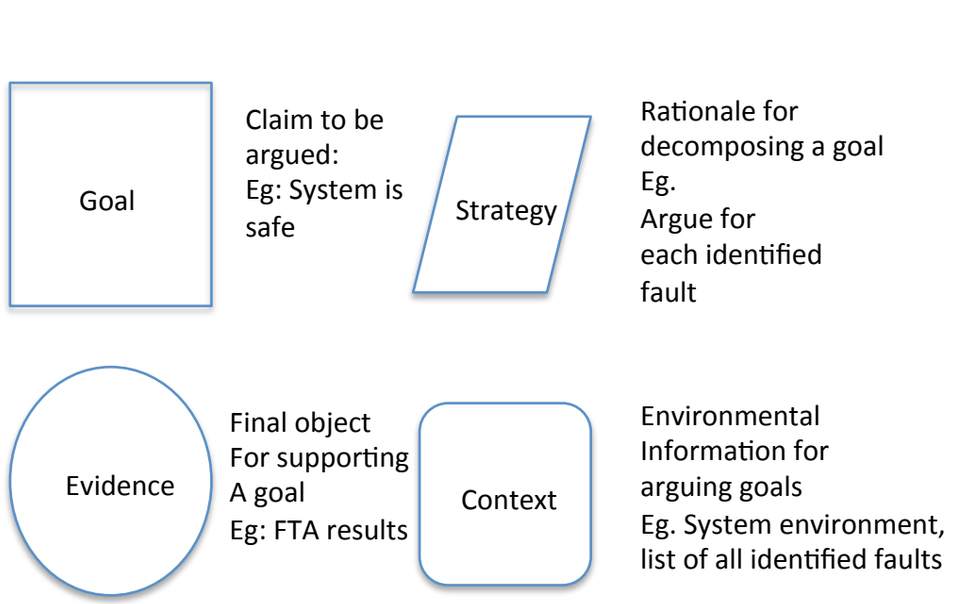
- 安全性、数理論理学など高度な知識を持つコンサルタント等によって記述されてきた
  - cf. google “safety case engineer”
    - 対象は原発や油田など、高安全システム
- 主に開発プロセスで使われている
  - システムの運用時の挙動を、特に障害発生時に、想定通り保証することは難しい

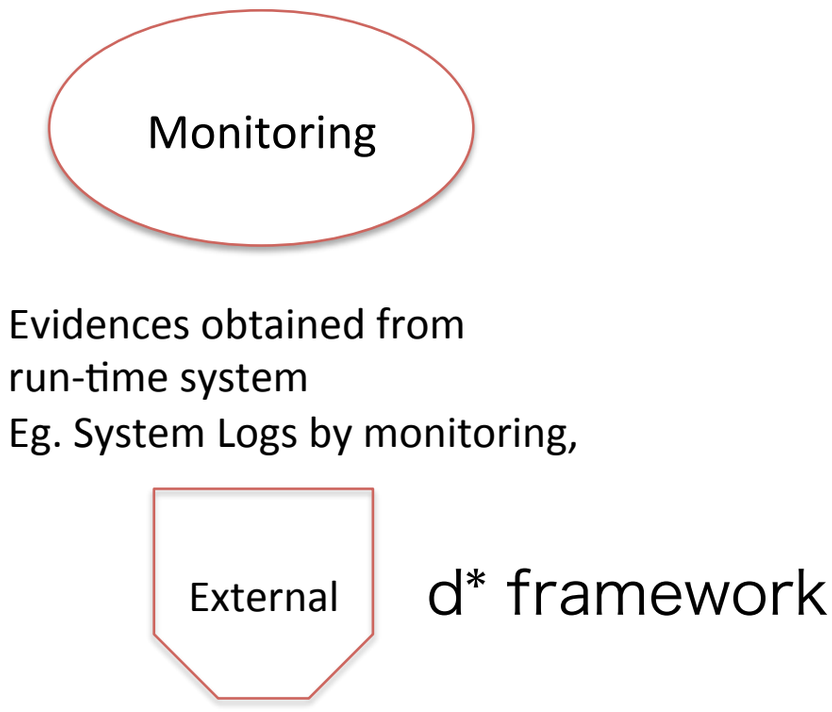
アイデア

- 一般の企業の方が容易に使える記述方法を開発する
- 開発と運用両方で使う
  - 開発時には、運用時におけるリスクをできるだけ想定する
  - 運用時には、常に合意されたディペンダビリティが満たされているかモニタリングする

D-Case

- 運用時のモニタリングを表すモニタリングノード
- (他のシステムのD-Caseへのリンクを表すエクスターナルノード)





d* framework

D-Case記述ステップ

- 目標は、一般の方が、できるだけ容易に開発する様々なシステムを対象に使えることである
- 多くの記述実験を通して検討を行った

D-Case記述実験

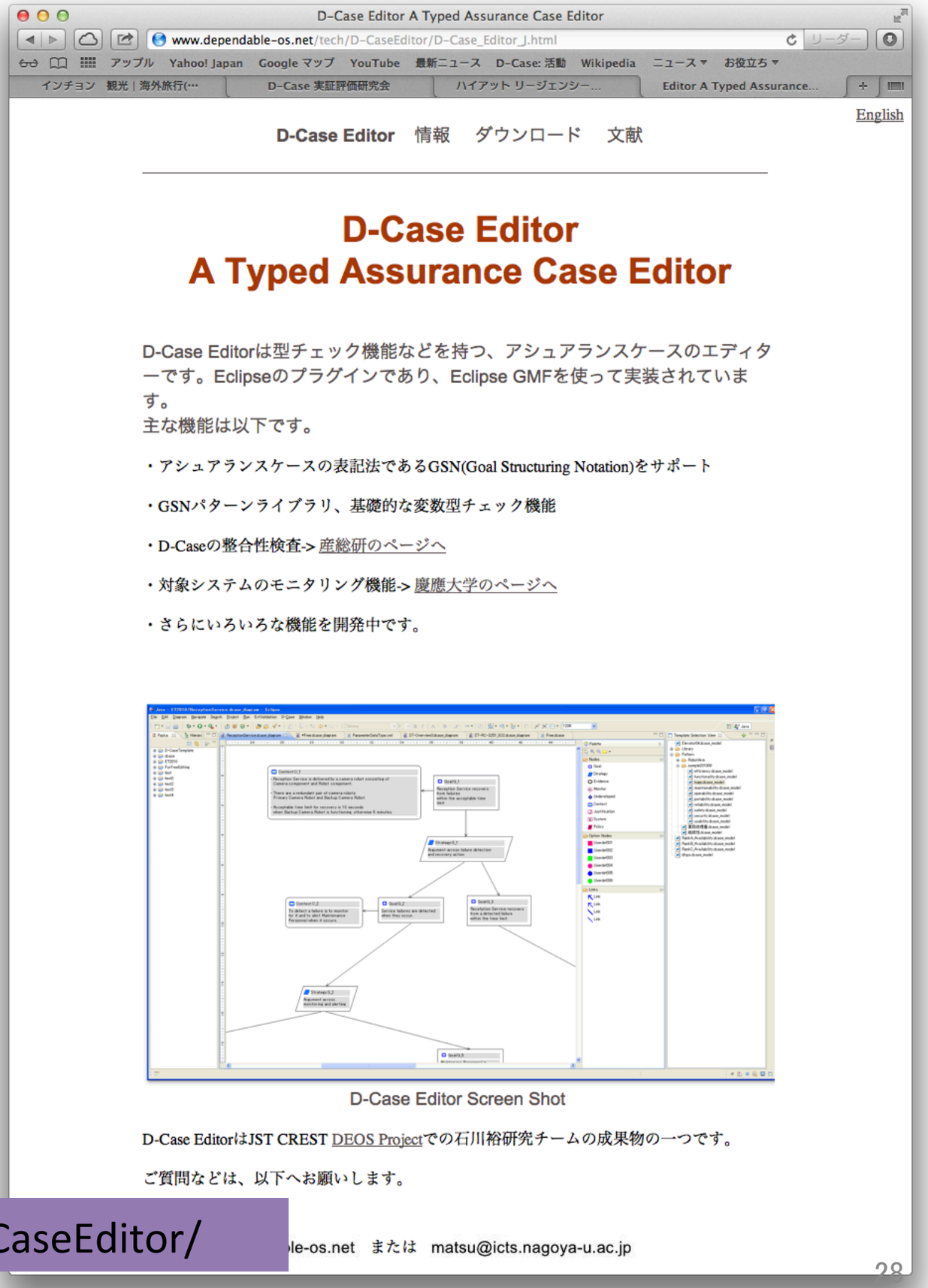
- デモシステム(D-Case, D-REチーム)
- エレベータ (富士ゼロックス恩田グループ)
- センサネットワークシステム(慶応大徳田チーム)
- マインドストームロボットコンテスト(富士ゼロックス恩田グループ)
- バージョンコントロールシステム(産総研木下チーム)
- 受付ロボット(産総研加賀美チーム)
- スーパーコンピュータの運用マニュアル(名古屋大山本グループ)
- TOGAF(The Open Group Architecture Framework)(名古屋大山本グループ)
- 自動車のエンスト問題(トヨタ石崎さん)
- 超小型人工衛星(慶応大田中さん、白坂先生)

D-Case入門
初版
出版

D-Caseツール

D-Case Editor

Eclipse Plugin
Pattern Library
Simple Type Checking
Monitoring Function
などの機能をもつ



http://www.dependable-os.net/tech/D-CaseEditor/

D-Case/Agda Download Page

agda.cvs.gr.jp/agda/D-Case-Agda/

EdWikiPage アップル Yahoo! Japan Google マップ YouTube 最新ニュース D-Case: 活動 Wikipedia ニュース お役立ち

D-Case/Agda Download Page | D-Case 実証評価研究会 | 第1回 DCER研究会 参加申し込み | (D-Case 実証評価研究会) | yutaka matsuno - Google 検索

"D-Case in Agda" Verification Tool (D-Case/Agda) Pre-release download page for testing

D-Case整合性検査ツール
(産総研木下チーム)

"D-Case in Agda" Verification Tool (D-Case/Agda) is a system for construction and verification of arguments in D-Cases. D-Cases are a kind of assurance cases for dependability of "open" systems, whose concept is being developed in the project DEOS[1]. D-Case/Agda provides a two-way translation between Agda[2], an interactive proof-assistant, and D-Case Editor[3], a graphical editor for D-Case structured arguments. A user can switch back and forth between the two for construction / checking based on formal meaning of a D-Casse and its visual manipulation.

- D-Case/Agda Installer for Windows XP or 7
  - This installation may fail under Java 7 with the massage 'Installation of GMF liblary failed.' If this is the case, please: (1) uninstall Java 7; (2) install Java 6 (32bit); (3) run the D-Case/Agda installer; (4) uninstall Java 6; (5) reinstall Java 7.
  - This installs specific versions of Haskell Platform, Emacs, and Agda. Preexisting installations are not overwritten, but may be overridden (Details).
  - This installs D-Case Editor (Eclipse), too, but this does not affect existing installations.

- A Brief Introduction to D-Case/Agda

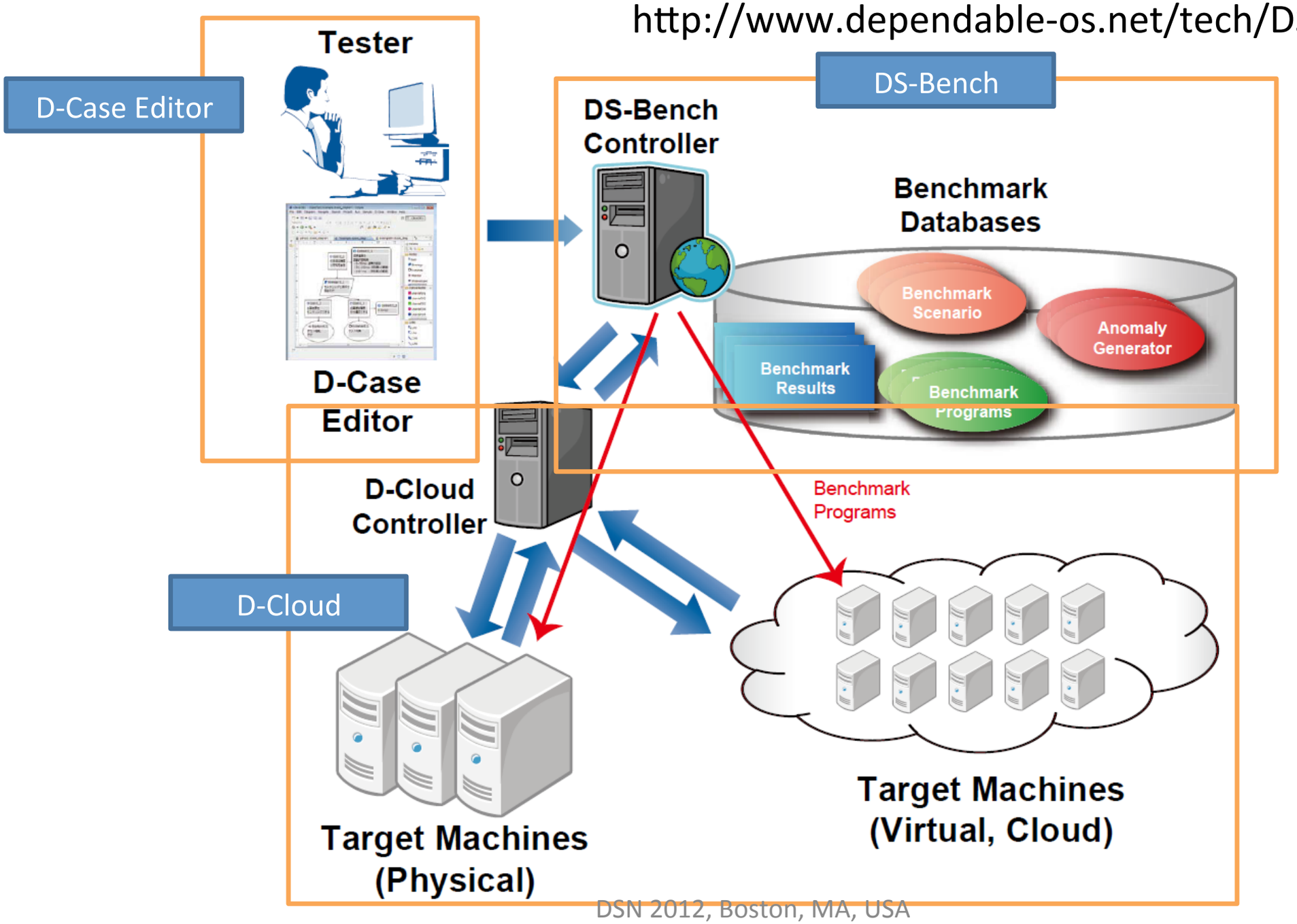
1. The research is funded by Dependable Embedded Operating Systems for practical use (DEOS) research area in Core Research for Evolutional Science and Technology (CREST) programme of Japan Science and Techonology Agency (JST). 2. Agda is developed at Chalmers University of Technology; homepage: http://wiki.portal.chalmers.se/agda/ 3. D-Case Editor is developed in the project DEOS; see http://www.il.is.s.u-tokyo.ac.jp/deos/dcase/Download.html

D-Case/Agda License

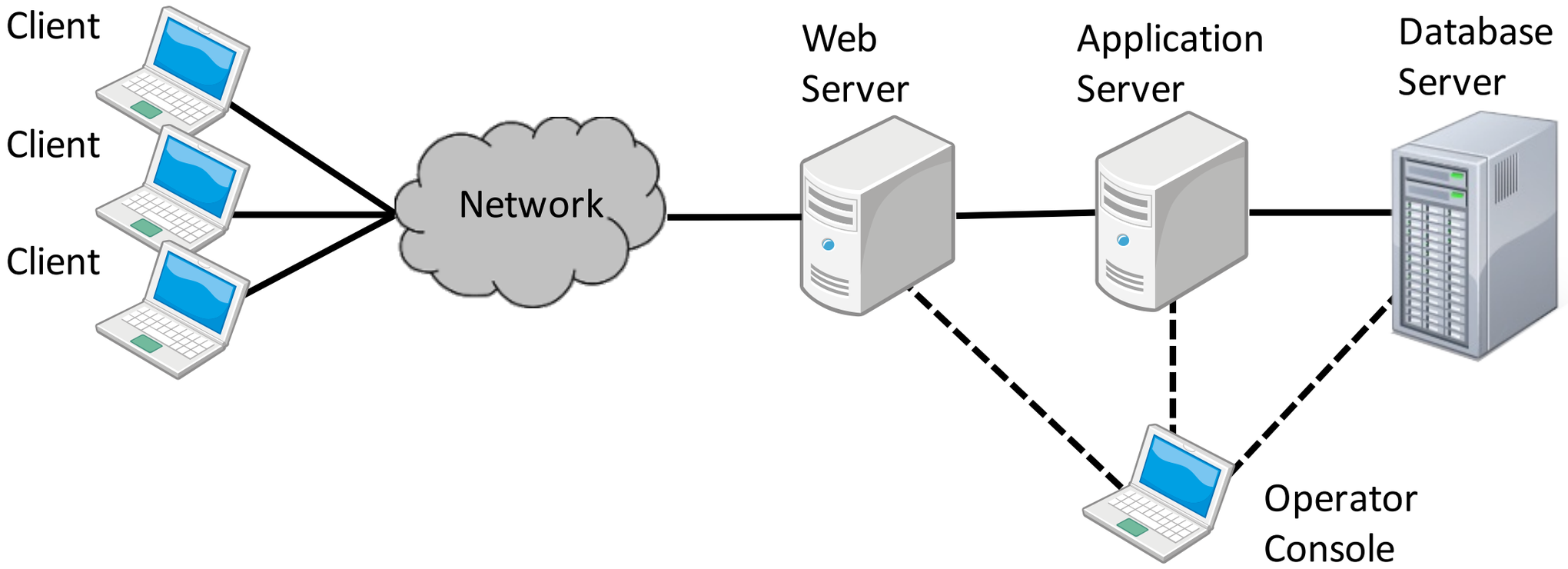
http://agda.cvs.gr.jp/agda/D-Case-Agda/

DS-Bench Toolset

DEOSセンターで公開
http://www.dependable-os.net/tech/DSBenchDCloud/



Web Serve Demo
(DEOSセンター開発)



Requirement
- Maximum Access Number: 2500 times/minute
- Response Time is within 3 seconds
- Recovery for one failure is within 5 minutes

....

Risk Analysis Result
- Too Many Access from Users
- Response Time Delay
- Memory Leak, …

内容

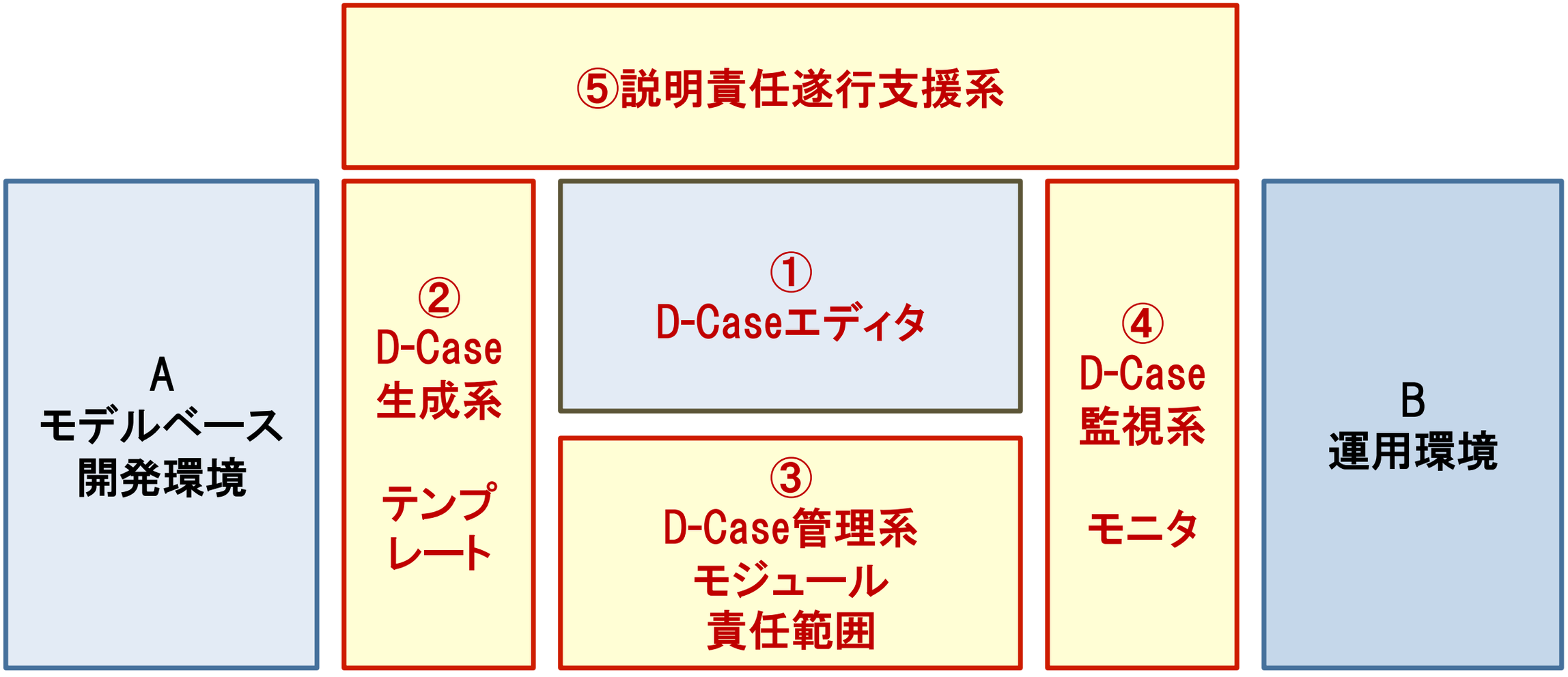
- D-Caseのきっかけ
- アシュアランスケースについて
- これまでと現在
- これから
- まとめ

これから

- D-Caseツールの拡充
- D-Case実証評価研究会
- D-Case入門、講習の開発
- TOGAF Next編集などへの参加

D-Caseツールの拡充

本開発
- ① D-Caseを対話的に編集
- ②モデル構成に基づきD-Caseの部分木(テンプレート)を生成
- ③ D-Caseモジュールと対象責任者の範囲を管理
- ④システムの運用状況を提示するモニタインタフェースを提供
- ⑤問題状況に対するD-Caseの責任範囲を提示



注)A,Bについては，既存の標準的環境を想定

D-Case実証評価研究会

- ディペンダビリティ、アシュアランスなどの、企業、研究機関の交流の場としていきたい
- さらに多くの実証実験を行なって行きたい

D-Case半日コース案

時限	時間	内容
1	13:00-14:00	アシュアランスケース入門
2	14:05-15:05	D-Case作成法
3	15:10-16:10	D-Caseエディタ
4	16:15-17:15	D-Case 演習
5	17:20-18:00	質疑応答

D-Case研修コース案

時間	1日目 (基礎)	2日目 (リスク分析)	3日目 (D-Case)
1	オープンシステム ディペンダビリティ	システム安全性分析-1	アシュアランス ケースとGSN
2	DEOS プロセス	システム安全性分析-2	D-Case
3	要求プロセスISO/IEC/IEEE 29148:2011	要求リスク分析	D-Case Case Study 1
4	要求工学概論	アーキテクチャ リスク分析	D-Case Case Study 2
5	運用プロセス概念	運用プロセスリスク分析	演習
6	ディペンダビリティ 標準規格	リスク分析事例	DEOS Case Study 1
7	演習	演習	DEOS Case Study 2

講義(18時間) +演習(3時間) = 21時間

TOGAF Next編集
などへの参加

- TOGAF(The Open Group Architecture Framework)
  - 代表的なエンタープライズアーキテクチャの一つ

TOGAF Next (2013~)

- Part 1 Concept←Open Systems Dependability
- Part 2 How to←DEOSプロセス, D-Caseプロセステンプレート
- Part 3 Tools← D-Case/D-Script/...

まとめ

- D-Caseのこれまで、現在、これからを説明した
- 今後もよろしくお願いします