トップエスイー修了制作

形式手法を用いた 高可用性クラスタ･システムのモデル化と検証

日本ユニシスグループ　ユニアデックス株式会社　今泉 正雄　Masao.Imaizumi@uniadex.co.jp

システム設計における問題点

HAシステムの設計には，クラスタ･ソフトウェアの仕様や管理する各種リソースに対する，多くの知識･スキルを要する．またシステムが大規模化，複雑化すると，構築後の網羅的なテストも現実的でない上，それを補うべきモデル検証も人手だけでは困難である．

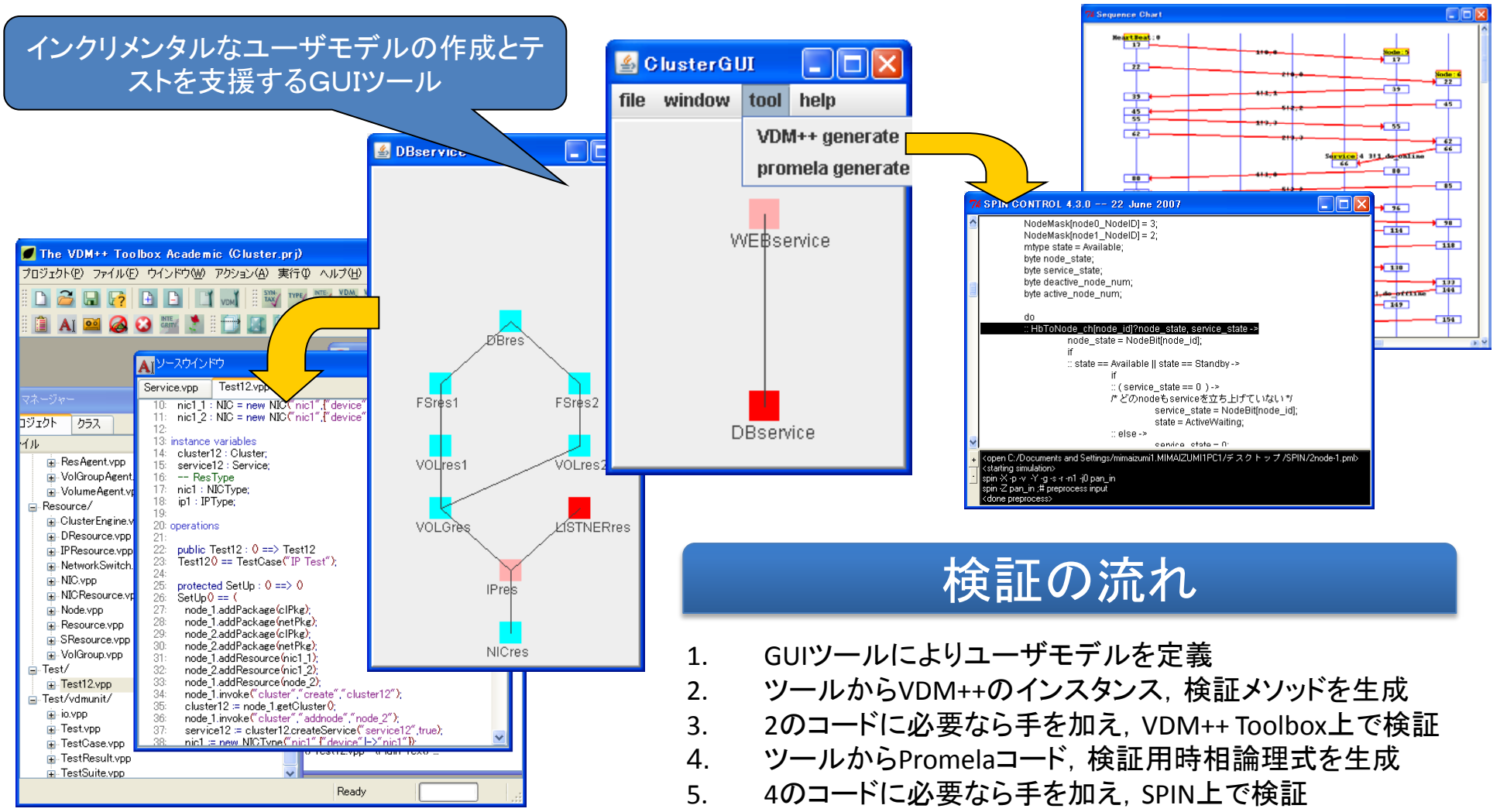
形式手法の適用による解決

クラスタ･ソフトウェアの仕様をVDM++により記述した．これにより，個々のユーザモデルが仕様において正しいことを，半自動で検査可能となった．また同じユーザモデルからPromelaモデルを生成することで，ハードウェア障害時の動作についてもシミュレート可能となった．

VDM++によるHAクラスタソフトウェアの仕様記述

- クラスタソフトウェアの仕様を，ユーザモデルの定義部，サービス起動等の動作部，ノードや各種リソース等の環境部に分割定義　⇒　ポータビリティの確保
- 定義部は，クラスタ，サービス，リソースタイプなどのクラス（ユーザモデルのメタクラス）として記述
- モデルの正しさは，不変条件やメソッドの事前条件，事後条件として記述
- ユーザモデルは，各クラスのインスタンスとして生成
- ユーザモデルを複雑化させながら，仕様の正しさを確認，修正　⇒　制約を利用したテスト駆動開発
- 出来上がった仕様に基づき，本来のユーザモデルを検証　⇒　動的な検証はSPINを援用

インクリメンタルなユーザモデルの作成とテストを支援するGUIツール



検証の流れ

1. GUIツールによりユーザモデルを定義
2. ツールからVDM++のインスタンス，検証メソッドを生成
3. 2のコードに必要なら手を加え，VDM++ Toolbox上で検証
4. ツールからPromelaコード，検証用時相論理式を生成
5. 4のコードに必要なら手を加え，SPIN上で検証