Systemic Risk analysis through SE methods and techniques

Andrea Tundis, Max Mühlhäuser
Telecooperation Lab, Department of Computer Science
Technische Universität Darmstadt
Darmstadt, Germany
{tundis, max}@tk.tu-darmstadt.de

Teresa Gallo, Alfredo Garro, Domenica Saccá
Department of Informatics, Modeling, Electronics and Systems Engineering (DIMES), University of Calabria
Via Ponte P. Bucci 41C, Rende (CS), 87036 Italy
{t.gallo, a.garro, sacca}@dimes.unical.it

Simona Citrigno, Sabrina Graziano
Centro di Competenza ICT-SUD
Piazza Vermicelli, 87036 Rende (CS), Italy
{simona.citrigno, sabrina.graziano}@cc-ict-sud.it

***Abstract*—The Systemic Risk is the risk that derives from the interdependence of the system under consideration, object of the analysis, and the services provided by other systems and, in general, by the interactions among them. The combination of the GOReM methodology and the RAMSoS method is proposed for Systemic Risk Assessment so as to provide the following benefits: (i) Effective modeling of SoSs structure and behavior; (ii) Explicit representation of dysfunctional behavior; (iii) Evaluation of different risk scenarios through agent-based simulation; (iv) Quantitative and qualitative risk assessment also in combination with classical analysis techniques (such as Bayesian Networks).**

Keywords—Cybersecurity, Modeling and Simulation, Requirement Engineering, Systemic Risk Analysis

I. Idea and Proposal

- Identify the main phases of the Systemic Risk (SR)
- Proposed a Modelling and Simulation based approach
- Defined a step by step methodology (not a software tool)
- Performing Static and Dynamic Systemic Risk Analysis

II. Systemic Risk Analisys Phases

The proposed process to support the analysis of the systemic risk can be organized in three macro-phases (see Figure 1): *System Analysis, System Design and Simulation Modeling and Results Assessment.*

A. System Analysis

System requirements and other aspects of interest are identified and described. The involved entities (such as stakeholders, services providers and so on) are identified along with their roles and related objectives. Goals to be achieved and their dependencies are highlighted. The rules and regulations that govern the context under analysis are identified.

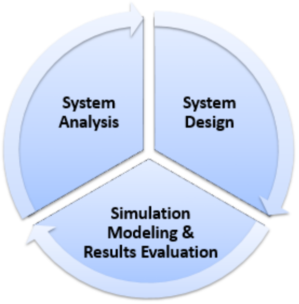


Fig. 1. Systemic Risk Analysis Phases

B. System Design

The target of the analysis as well as boundaries of the design, i.e. what needs to be represented and what can or should be neglected/omitted, are defined. Specific use cases are redefined in terms of scenarios of interest. Application scenarios are introduced to specify the functionalities that should be provided in each business scenario description of the system is delivered by providing from different points of view such as for structural, functional, and so on.

C. Simulation Modeling & Results Evaluation

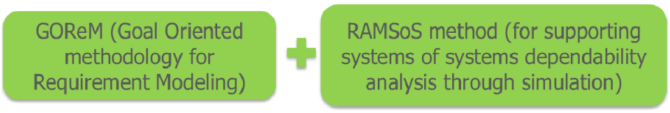
At this point, a subset of the models generated in the System Design macro-phase is selected and processed. According to the simulation-platform different Model-to-Model transformation rules are defined. Great attention is placed on the indices / objectives identified during the System Analysis. From these indices and the objectives to be pursued, the simulation platform, which is able to support the desired analysis, is selected. Based on the objectives to be verified, it is possible to choose the simulation environment that better fits the type of analysis to be carried out.

III. Deriving Bayesian Networks models for supporting Systemic Risk Analysis

A. A combined approach for modeling and assessing the Systemic Risk

Systems Engineering approach + Modeling and Simulation techniques

How and which entities of the overall system influence the operation of the entire system and the evaluation of the Systemic Risk.



GOReM (Goal Oriented methodology for Requirement Modeling) + RAMSoS method (for supporting systems of systems dependability analysis through simulation)

Modeling and evaluating Systemic Risk by exploiting (agent-based) simulation + Bayesian Network

B. RAMSoS and GOReM: Enabling Factors

- Common modeling notation: SysML/UML.
- Both RAMSoS and GOReM are defined in terms of phases and work-products
- GOReM is defined as a method to support the analysis of system requirements with particular emphasis on their elicitation and tracking; while RAMSoS is meant to be used mostly for supporting the validation and verification phases. Together they cover the entire Systemic Risk Analysis Phases
- Reuse of models.

Figure 2 shows the integration approach based on Work-Products

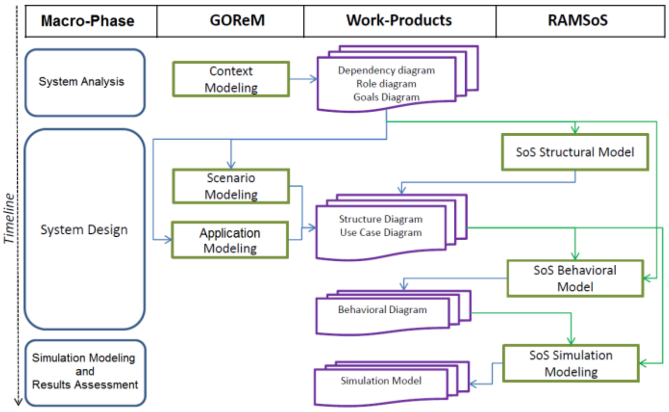


Fig. 2. Combining GOReM and the RAMSoS method

IV. Risk Analysis applied to a Service of Electronic Online Payment of Poste Italiane

The risk of success or failure of the PEO service relies on two complementary services:

- SMS Notifications service (Mobile Service Provider)
- Payments and Transactions service (Web Service Provider, Energy Provider, IT infrastructure)

1. A statistics based approach using a tool for a static analysis is applied: GeNIe (Graphical Network Interface) a development environment for the creation of decision models based on Bayesian Network (BN)
2. An agent-based approach using a dynamic tool is adopted: ReActor an object oriented framework based on discrete-events simulation

For each actor the following risk ranges (or QoS) have been identified:

- SMS Notification: Good, Low;
- Payments and Transactions: LowRisk, HighRisk;
- IT Internal Infrastructure: Good, Standard, Poor;
- WebServiceProvider: High, Medium, Low;
- Energy Provider: High, Standard;
- MobileServiceProvider: HighLevelOfService, StandardLevelOfService;

Once the model and relationships among actors and their goals are well described and defined, it is possible to use simulation to provide an assessment about what can happen into an application scenario according to specific inputs to the system. Figure 3 shows Architectural Modeling for risk analysis applied to a service of Electronic Online Payment of Poste Italiane.

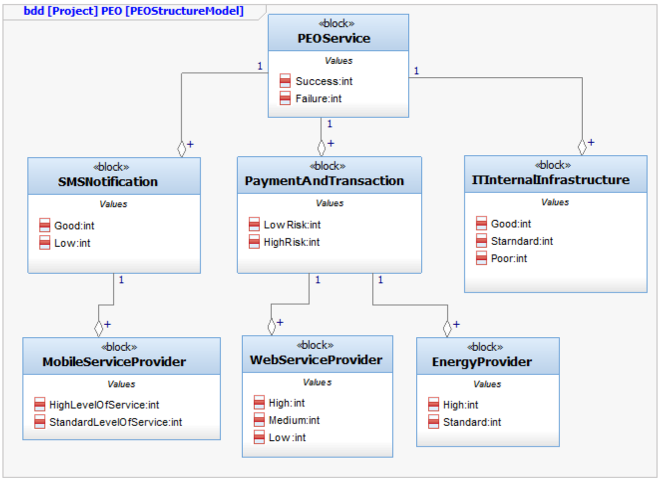


Fig. 3. RAMSoS – System Design

Figure 4 and Figure 5 represent, respectively, examples of GOReM Application and Behavioural Model.

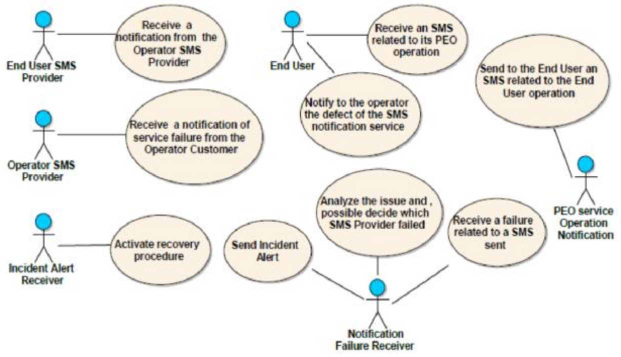

End User SMS Provider
Receive a notification from the Operator SMS Provider
End User
Receive an SMS related to its PEO operation
Send to the End User an SMS related to the End User operation
Notify to the operator the defect of the SMS notification service
Operator SMS Provider
Receive a notification of service failure from the Operator Customer
Analyze the issue and , possible decide which SMS Provider failed
PEO service Operation Notification
Receive a failure related to a SMS sent
Incident Alert Receiver
Activate recovery procedure
Send Incident Alert
Notification Failure Receiver

Fig. 4. GOReM - Application Modeling

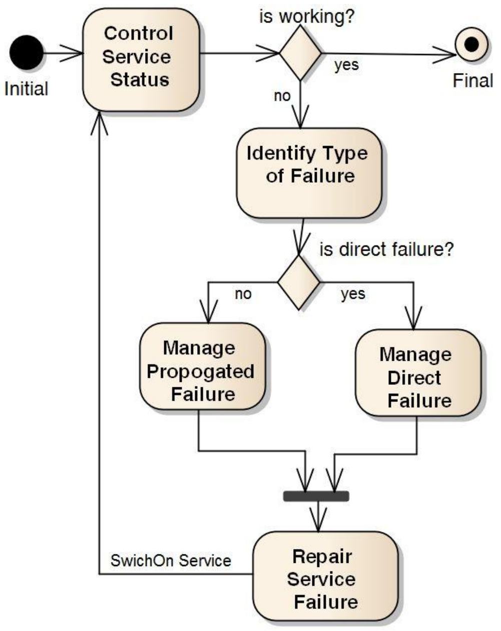


Fig. 5. GOReM - Behavioural Model

A. *PEO Service Result Analysis*

Considering a combination of services based on high level quality percentage, the probability of PEO success is 99%, which means a LowRisk.

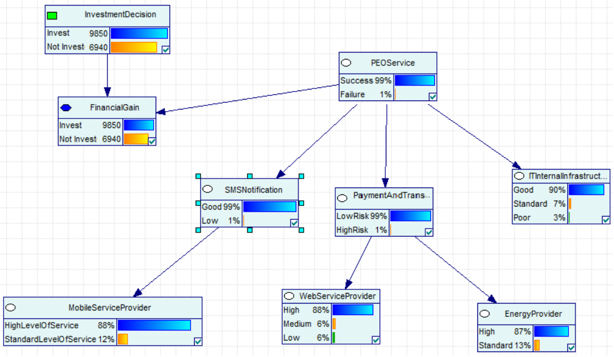


Fig. 6. Exploitation of Bayesian Network

Figure 7 and Figure 8 show further quantitative and qualitative information gathered by exploiting agent-based simulation such as:

(i) the availability (working) or unavailability (not working) of a service

(ii) the time when the failure of a service happened (timestamps)

(iii) the cause of the failure, if it is due to internal or external factors.

This allows to assess the main system (PEO Service) and its interdependencies with the involved services, by considering events of faults and failures and their propagation in the network, from a dynamic point of view by including temporal constrains.

Service Name	Timestamp	Service status	External causes of failure	Impact (€) per Hour
WebService Provider	44	Not Working	no	3
Payment & Transaction	44	Not Working	yes	2
PEO	47	Not Working	yes	5
WebService Provider	56	Working	-	3
Payment & Transaction	58	Working	-	2
PEO	64	Working	-	5
...	...	...	...	...

Fig. 7. Simulation Results related to the PEO Service

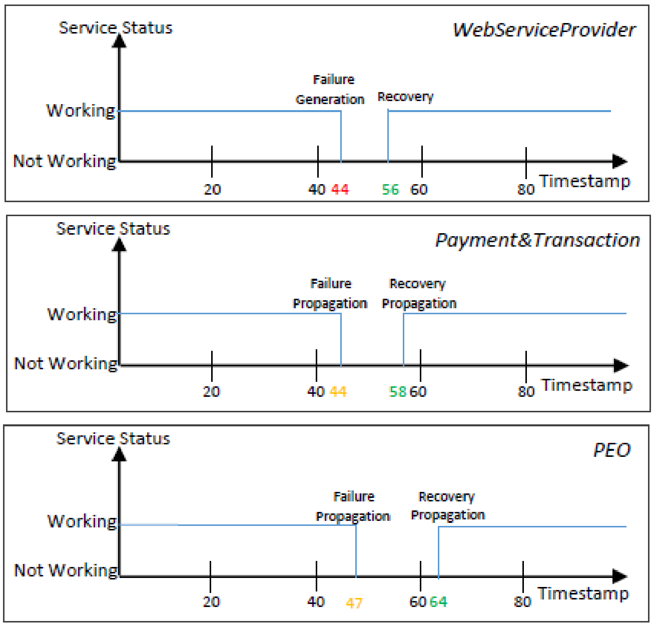


Fig. 8. Simulation Implementation related to the PEO Service

REFERENCES

[1] A. Tundis, A. Garro, T. Gallo, D. Saccá, S. Citrigno, S. Graziano, and M. Mühlhäuser. 2017. Systemic Risk Modeling and Evaluation through Simulation and Bayesian Networks. Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES 2017), Reggio Calabria (Italy), 29 August - 1 September 2017.