Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS

Rüdiger Klein, Erich Rome, Césaire Beyel, Ralf Linnemann, Wolf Reinhardt

Fraunhofer IAIS, Schloß Birlinghoven, Sankt Augustin, Germany
{FirstName.LastName}@iais.fraunhofer.de

Abstract. Critical Infrastructures (CIs) and their protection play a very important role in modern societies. In the recent years, many studies and projects around this subject have investigated the growing (inter) dependencies and their mutual influence. In February 2006 the EU project IRRIIS [1] was started to increase the dependability, survivability and resilience of information-based critical infrastructures (CIs).
One of the main issues here is how to model information about critical infrastructures with special emphasis to their interdependencies. Many different aspects have to be taken into account for this purpose: systems with their components and their interactions, their behaviours, the services they provide, events and actions influencing them, risks to be considered, etc. Today, there are sophisticated information systems to manage CIs. They take special views on the respective CIs – but leave aside interdependencies to other systems. To some extend this is quite natural because interdependent systems can be quite different and need different kinds of information to be managed.
For interdependency analysis and management of critical infrastructures we need information focussing exactly on the interdependency aspects – in relation to all other relevant kinds of information. This is the aim of the IRRIIS information model. It is based on the assumption that there is a *generic approach* to CI interdependencies – regardless of the concrete CIs considered. They all need systems and behaviours, states and transitions, events and actions. In order to deal with these complex but interrelated kinds of information the IRRIIS Information Model is based on semantic information modelling techniques. They provide the necessary expressivity, clear structures, and the needed formalization.
This Generic Information Model allows us to integrate information from CIs – from real ones as in SCADA systems, or from simulations - in order to manage their interdependencies. In the simulation case, the behaviour of CIs will be simulated by their native simulation approaches. IRRIIS simulates interdependencies taking these native CI simulations into account – using simulation federation based on the IRRIIS Generic Information Model.
This paper gives an overview of the IRRIIS information model and the way it is used for the analysis of interdependent infrastructures.

Keywords: CI dependability, CI-interdependency, information modelling, federated simulation, simulation environment

1 Introduction

Critical infrastructure systems are getting more and more complex – and at the same time their interdependencies grow. Interactions through direct connectivity, through policies and procedures, or simply as the result of geographical neighbourhood often create complex relationships, dependencies, and interdependencies that cross infrastructure boundaries. In the years to come the number, diversity, and meaning of critical infrastructures and their interdependencies will still increase: advanced traffic management and control systems, mobile information services of any kind, ubiquitous computing, ambient intelligence – just to mention a few key words. Even classical domains like electric power networks will change their shape: more distributed generation facilities, intelligent consumers, smaller but interdependent distribution networks, etc. The good news is that more or less all of these critical infrastructures provide and use many kinds of information during operation. This allows us to use this information also for interdependency analysis and management.

The modelling and analysis of interdependencies between critical infrastructure elements is a relatively new and very important field of study. Much effort is currently being spent to develop models that accurately simulate critical infrastructure behaviour. The results of these simulations are used by private companies, government agencies, military, and communities to plan for expansion, reduce costs, enhance redundancy, improve traffic flow, and to prepare for and respond to emergencies [2].

Today, there exist already many experiences managing large and complex systems. The best examples are probably the large computer networks them selves – foremost the Internet. There are sophisticated approaches dealing with optimal operation, management of interoperation, safety and risk management issues, etc. Different modelling and problem solving approaches are considered including agent based modelling, game theory, mathematical models, Petri nets, statistical analysis, etc.

Though we all know how much is still to be done in these areas in order to improve interoperability and safety there is also a huge amount of experiences usable in critical infrastructure management.

One of the main challenges for managing CIs and their interdependencies comes from the *physical nature* of critical infrastructures. Electrical power networks, traffic systems, water and oil pipelines, logistics, or telecommunication systems have their information and communication systems needed for their control – but at the same time they exist in the physical world, they behave according to the laws of physics, and they interact with their physical environment. Whereas interdependency and safety analysis in computer networks can largely be done on the digital level the management of critical infrastructures has to take *both dimensions* and their mutual interactions into account: the physical and the information and communication aspect. To make things even more complicated the interdependent critical infrastructures can be quite different – needing different modelling, analysis, and simulation approaches. These are the main challenges of CI interdependency analysis.

For this purpose we need

- information models which are sufficiently expressive for CI interdependency modelling and analysis – for the physical as well as the information and control aspects and their relationships;

- simulation techniques which allow us to describe the physical behaviour of the different systems, their control, and the resulting interdependencies; and
- methods and tools supporting communication between CIs in order to manage interdependencies.

These are the main goals of the IRRIIS project. The modelling and simulation approach taken in this project to deal with CI interdependencies will be outlined in this paper.

The paper is organized as follows: we start with a brief overview of the IRRIIS project in Chapter 2. In Chapter 3 we motivate and describe our modelling approach to CI interdependencies. How to use the IRRIIS models for critical infrastructure simulation will be explained in more detail in Chapter 4. Chapter 5 outlines the usage of the IRRIIS Information Model for risk estimation and decision support. In Chapter 6 we summarize our results and give an outlook to future research.

2. IRRIIS Overview

The Integrated Project "Integrated Risk Reduction of Information-based Infrastructure Systems" (IRRIIS) is a European Project within the 6th Framework [1]. It started in February 2006 with a runtime of 3 years including 15 partners from nine European countries from industry, research organisations, and universities.

The IRRIIS project follows the aim to enhance substantially the dependability of large complex Critical Infrastructures (CIs) by introducing appropriate modelling and simulation techniques and to develop appropriate middleware based communication technologies (MIT) between CIs.

IRRIIS' main objectives are:

- to determine a sound set of public and private sector requirements based upon scenario and related data analysis;
- to design, develop, integrate and test communication components suitable for preventing and limiting cascading effects and supporting automated recovery and service continuity in critical situations;
- develop, integrate, and validate novel and advanced modelling and simulation tools integrated into a simulation environment for experiments and exercises; and to
- validate the functions of the middleware communication (MIT) components using the simulation environment and the results of the scenario and data analysis.

The electrical power infrastructure and its supporting telecommunication infrastructure are chosen as first priority example test case.

The IRRIIS approach is based on the analysis of vulnerabilities of large complex CIs and on the knowledge CI stakeholder have acquired about management and control of their systems (including the used information systems like SCADA).

It's the aim of the IRRIIS project to reduce present weaknesses and vulnerabilities by applying advanced ICT solutions between the basic software and the application layer of the ICT systems controlling complex infrastructures [3]. Novel types of ICT

systems will be tested and validated by applying the IRRIIS simulation environment for comprehensive experiments.

Many different kinds of information are relevant for CI interdependency analysis. Because interdependencies exist between quite different systems information exchange between them about critical situations, risks, vulnerabilities etc. is essential. Proprietary information approaches alone are not sufficient for this purpose. We need a generic information model as a lingua franca for communication between CIs. This reference model allows us to exchange information between different systems in a way that the meaning of this information is "understood" by all stakeholders and their ICT systems. Taking the many different kinds of relevant information in this domain into account we need an expressive information model. In order to process this information in different kinds of ICT systems we need clear semantics for our information to be achieved by using established well structured modelling techniques.

3. The IRRIIS Information Model

Today, the management and control of critical infrastructures depends to a large extend on information and communication technologies (ICT). They provide the "nerve systems" of these large infrastructures. There are highly sophisticated software systems allowing the stakeholders to manage, control, and analyse their systems under more or less every condition. What is frequently missing today is information related to interdependencies to other systems: geographic neighbourhood information, physical or information and control dependencies, etc.

The information systems used to model the critical infrastructures tend to be very different. There is no common modelling approach. They are quite different for different domains, but even within the same domain different information modelling and processing approaches are used. This is quite natural considering the many different kinds of information and the various approaches and algorithms taken for these purposes.

Critical infrastructures are *physical systems*. Electrical power networks, traffic systems, or telecommunication systems exist in the physical world, they behave according to the laws of physics, and they interact with their physical environment. They process information about their state, and they may also exchange information with other systems in order to manage their interdependencies. The interdependency analysis of critical infrastructures has to take both dimensions and their mutual interactions into account: the physical and the information and communication aspect.

Consequently, a key issue is to establish information models and simulation techniques which take exactly these issues into consideration: the components and systems, their behaviours, events, actions of control, risks, etc. This will help to manage critical infrastructures more effectively and efficiently, and it will improve information interchange between information systems dealing with different critical infrastructures.

The main point is to bring all *interdependency* related information together with *all other* kinds of information necessary to manage and control the various kinds of

critical infrastructures. We need an information model which is sufficiently *expressive* in order to represent the many different kinds of related information, and which is well defined and has a *clear semantics* in order to be manageable by the different kinds of information systems to work with them. On this basis a set of well defined inferential services can be defined showing in which way the Information Model will be *used* for CI interdependency analysis and management.

The IRRIIS Information Model (IM) has exactly these goals:

- to be as expressive as necessary for CI interdependency modelling and analysis, and
- to be semantically well defined.

Currently, it is based on standard object-oriented and constraint modelling techniques like UML class diagrams, UML state charts, and OCL constraints. This provides an acceptable trade-off between needed expressivity and formalization[1].

The IRRIIS modelling approach contains three levels of generalization:

1. the Generic Information Model (GIM): it is based on the assumption that there is a common core information model for critical infrastructures and their interdependencies. Whatever the CI to be modelled and its interdependencies are: for the purpose of CI interdependency analysis and management it will be described in terms of this IRRIIS Generic Information Model. This common model provides the basis for communication between different CIs as pre-condition to manage their interdependencies It captures the basic physical structure of the CI with its components and systems and their connections, their behaviours on an appropriate level of abstraction, the services they provide, and events, actions and associated risks. In this way it is sufficiently expressive to capture all interdependency related information.
2. The domain specific information models: they adapt, specialize and extend the Generic Information Model according to the special needs of the various domains (like electrical power networks, traffic systems, or telecommunication nets). They contain the specific types of components and their behaviours as specializations of the more general concepts introduced in the GIM.
3. The instance level models: this third layer describes the concrete critical infrastructures in terms of the respective domain specific information model as instantiations of the concepts and relations defined in this model.

These three modelling layers will be described now in more detail.

[1] This issue still needs more investigation in subsequent research. UML has mainly been used because it is a well established and widely used modeling approach. The IRRIIS UML models can easily be transformed into logically equivalent OWL models. There are other proposals for UML based models [5], [6] in the interdependency area which need comparison with the IRRIIS approach.

3.1. The IRRIIS Generic Information Model

The IRRIIS Generic Information Model (GIM) contains all types of information which are needed in order to describe critical infrastructures and their interdependencies in general – without any special reference to the concrete kind of systems to be modelled; this modelling approach assumes that critical infrastructures have sufficient commonalities – regardless of their specific kind.

The model presented here is just a first approach which may be modified or extended in subsequent versions. Though the content of the IRRIIS Generic Information Model is of course important it is more important to understand the *general role* of the GIM within the IRRIIS approach. Whatever the critical infrastructures and their interdependencies are – the GIM is the set of main concepts and relations in this domain to describe system behaviour and interdependencies independent from the concrete (type of) system to be considered. This enables us to analyse CI interdependencies in general and to develop methods and tools for their simulation and management independent from the concrete (type of) systems. We will clearly specify in which way these information models will be used within the IRRIIS approach, i.e., which information services

To some extent any IRRIIS model has to take into account modelling aspects which are more general than the IRRIS domain as such: system models, service models, agent models, etc. We could re-use existing models of such more generic domains as modules within the IRRIIS Generic Information Model – but by reasons of simplicity and practicality we will not formulate these issues as separate information modules. Instead, we will formulate a compact, coherent and comprehensive IRRIIS GIM comprising all relevant aspects.

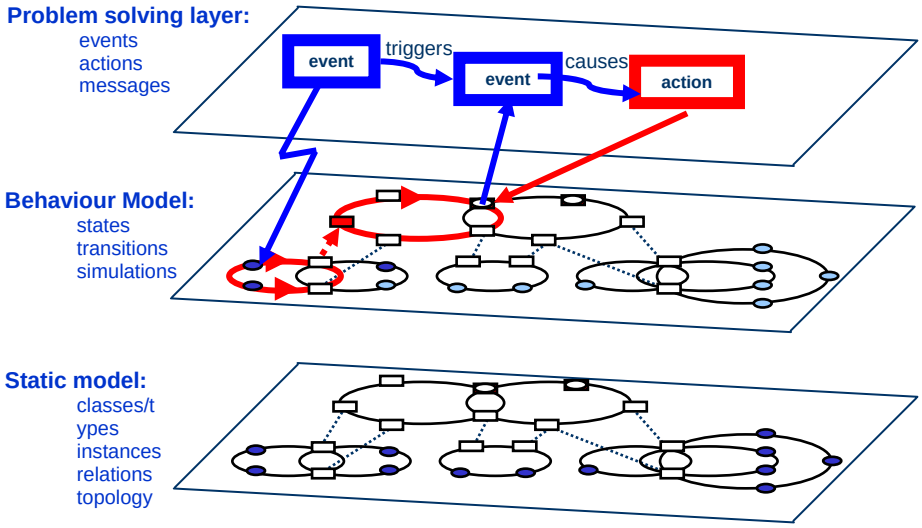

Fig. 1: an overview of the three layers IRRIIS Generic Information Model: the static model, the behaviour model, and the problem solving layer

We will develop the IRRIIS GIM in three steps (see fig. 1):

- the *static model* allowing us to describe a system, its services, dependencies, etc. at a given point in time ("snapshot");
- the next step is to add *behaviour* to this static model: to model state transitions, the conditions under which they occur, how they propagate, etc.
- and finally we consider how events, scenarios, actions, agents, etc. can be integrated into the IRRIIS Generic Information Model.

3.1.1. The Static Information Model

In the tradition of semantic information models [4] the Static Model contains all main categories of our domains, their relations and attributes (see fig. 2):

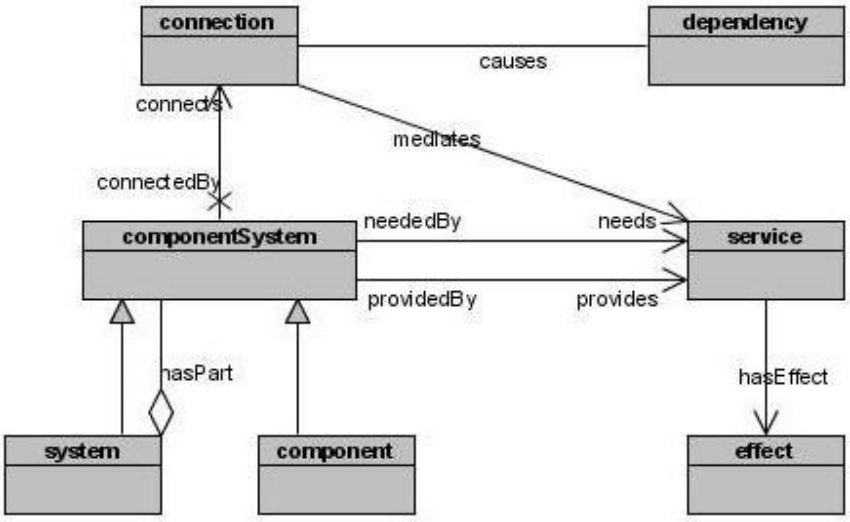

Fig. 2a: the core of the IRRIIS Static Model: components, systems, services and connections

- Components and systems describe the structure and topology of a CI. Components and systems can be described by a set of relevant attributes (not shown here). In the domain model more specific sub-classes of systems, components and attributes may be introduced.
- Systems can have parts – described by the has_part relation. This relation forms a directed acyclic graph allowing us to describe hierarchical structures. Its terminal elements are components. In the behaviour model we will describe how behaviour within hierarchical structures can be modelled. The attributes of the higher layers can depend on the attributes of its components or sub-systems in various ways (summation for el-power, weight, etc.; equality for voltage);
- Systems and components may be connected to other systems and components. (Because connections form a central element in typical IRRIIS models they are

described by classes with attributes etc. – not just as relations). We may have different types of connections in the domain models (see below).

- Systems and components may provide services to other systems/components, and systems and components need services in order to work correctly. This is an attractive abstraction providing a lot of flexibility for modelling.
  In parts of the model or in the whole model we may use services as the basic level of description – omitting the component layer.
- A connection may be used to mediate some services – that's a way how interactions of systems and components can be described in IRRIIS;
- A connection causes a dependency. Due to the different types of connections there may be different types of dependency. Dependencies may be characterized in more detail by various attributes;
- Components/systems, services, and connections can have states. An entity is in a certain state either if explicitly given (like 'broken' or 'switched-off') or if the criteria defining this state are fulfilled by this entity (see below). These criteria are typically formulated as a set of conditions – frequently as constraints on attribute values of the involved entities. A system/component can have more then one state – characterizing different "dimensions" of its overall state. The states are defined according to the respective entity type, i.e., components of a certain type may have different states then other type or as services. Which states are defined depends on the application – the IRRIIS model does deliberately not provide any restrictions here. All what is necessary is a finite state machine.
- Services may have effects. An effect is described as resulting in certain values for attributes of involved components or services (heating, cooling, …).
- States (as discrete entities) are related to each other via transitions – i.e., both together form finite state machines for the entities they apply to. The transitions do not have to be deterministic – i.e., we may have probabilistic state machines. We may also assign temporal aspects to such transitions (duration, delay, etc.).
- Transitions are triggered either by external or internal events, or by actions performed by a certain agent.
- An event is something triggering a state transition at a system/component, at a connection, or at a service (if the implementation layer is omitted).
- A state transition may act as an event (triggering other transitions) – depending on dependency relations the respective entity has to other entities. Not every state transition is an event. Events may trigger state transitions in other systems/CIs.
- A scenario is a sequence of events and actions. They are ordered by time, and they may have causal relations to each other. They may also be independent from each other (just happening by accident) – thus allowing us to model a large variety of different types of scenarios and of analyzing in which way they affect the interdependent critical infrastructures.
- Scenarios may contain events coming from outside, and events resulting from the evolution of the system. Actions (see below) are similar to events – with the exception that they are executed deliberately as reaction to a certain state, pursuing a certain goal (a state to be reached) and following a certain strategy or policy.

- A scenario has a certain risk if as a consequence of one of the events or actions in it a component/system or a service reaches a state which is classified as risky (domain dependent).
- Components and systems may be described by their location as well as events which may happen at a certain place (with effects = state transitions on those components and systems located there).
- Events are also described by their moment of incidence which is a point in time, and maybe by their duration (a temporal attribute). As usual consistency conditions apply to temporal and causal relations between events and actions.

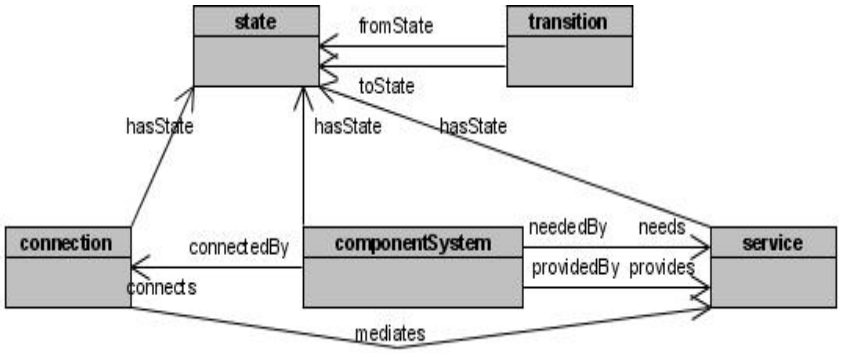

Fig. 2b: the IRRIIS static information model with states and transitions

States and Attributes

States are a key element in IRRIIS information models. Components, systems, services, and connections may have states.

These states can be related to physical attributes: in order to be in normal operational state a system has to fulfil some constraints on its attributes (fig. 3). In this way states can be classified according to attribute values using classification constraints. These constraints are part of the domain model and are applied to each instance.

System simulations tell us what the attribute values in a system model are. As a consequence, we may classify the states of the components and connections in the system model. Some of these states may be "critical" – thus triggering events to be managed by one of the simulators or any of the other IRRIIS tools.

States may also be changed directly – without explicit reference to involved attributes. For instance, a system's state may change when the state of one of its components changes – without taking explicit reference to system attributes. Or we simply say that a component is broken without saying why and in which way.

The definition of states is a key issue in an IRRIIS model. It may be adequate for an IRRIIS application just to discriminate between two states like "working" and "out of work". In other cases we may need much more fine-grained states (and transitions between them). For instance, a system may still provide the services it is responsible for but with the restriction that some of its sub-systems do not work at the moment

and that the built-in redundancy or emergency systems already took over responsibility for the services (thus with a higher risk of failure).

Some of these state definitions may be part of the Generic Information Model (thus being part of the general IRRIIS modelling methodology), and some others may be contained in the domain specific extensions of the generic model. Most classification constraints will be "local", i.e., the state of an entity only depends on attribute values of that entity or of directly related ones. But there may be also more complex "non-local" constraints where a state depends on a whole bunch of other entities. In these cases the expressive IRRIIS Information Model with its systems, connections, services etc. provides the basis for an adequate representation of such constraints.

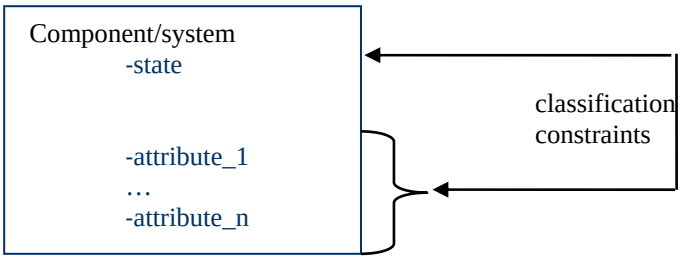

Fig. 3: States and attributes can be related through classification constraints

Systems and services

Every service is provided by a system/component. In the same way a system/component may need some services in order to work correctly (see fig. 4).

A service oriented modelling may be an adequate abstraction in those cases where a system or CI may provide this service in different ways to other systems/CIs. Then it is of minor importance in which way this is done – just the service as such counts. On the other hand, just to know that a service is provided may not tell us all we have to know about a system's state. If one way to provide this service already failed the risk to loose the service completely may be increased. Consequently, service oriented modelling may be a comfortable and adequate abstraction in some cases – in others a more detailed system and behaviour oriented model is necessary.

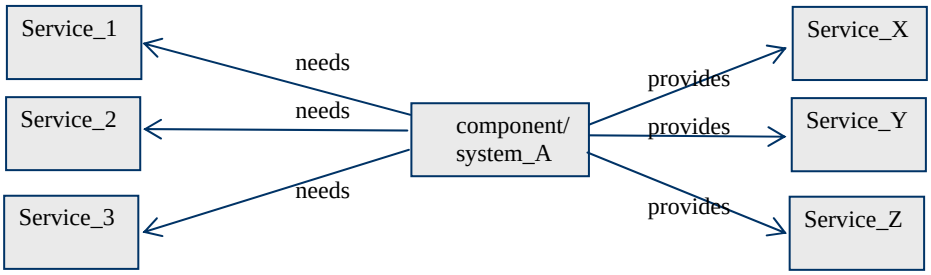

Fig. 4: systems and services are connected through needs and provides relations

System Theory

The systems, components, their connections, the services they provide and the dependencies resulting there from form the basic ingredients of the IRRIIS system models. Especially important is the classification of connections, services and dependencies because they allow us to describe the interdependent systems and components in a well defined way.

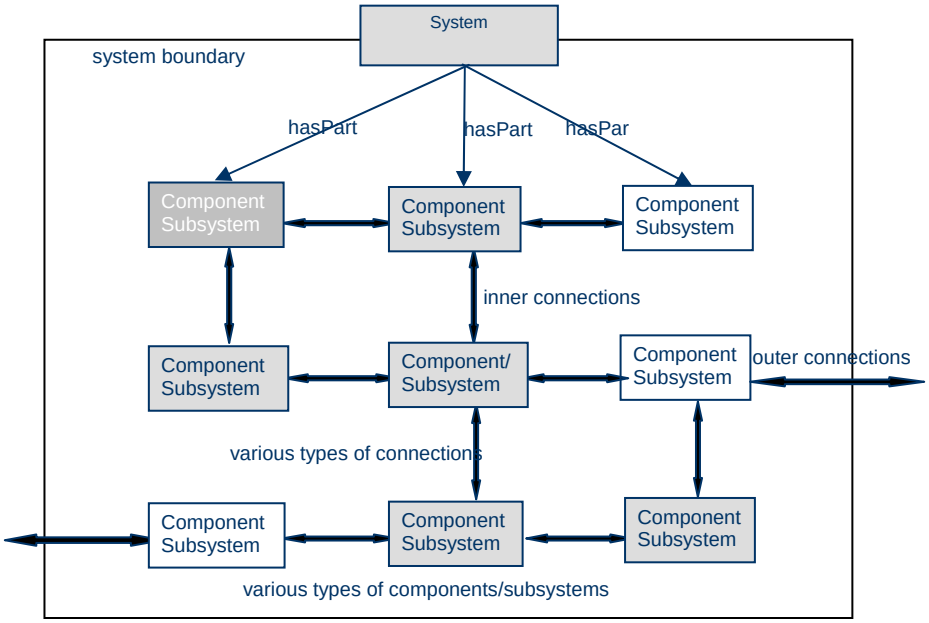

Fig. 5: a system, its components and subsystems with their inner and outer connections

A more detailed description includes explicitly the various part-of levels and their interactions.
Following general system theory we can say that

- a system is the set of its parts, and of their internal and external connections (fig. 5);
- inner parts of a given system are those which do not have a connection to any other system or component outside the given system
- boundary parts have a connection to any system or component not belonging to the given system;
- a system has at least two parts;
- every external connection of a system means that there is a boundary part of this system with the same connection;

- for services this means that every service needed by a system is also needed by its boundary parts, and every service delivered to the outside is delivered from one of its parts.
- Components are “atomic” and do not have parts (on the given level of granularity).
- In our system theory the environment is just a special system interacting with the technical systems. It may also be considered simply as a “component” in the sense that no internal structure of this environment is modelled.

The relation between a system and its parts may be modelled at a finer granularity. We may describe not just its parts as such but the roles they play within the system. This may be achieved by introducing special part relations (like controls, main_cabinet, etc.). Associated with such fine-grained part relations we can specify how attributes or states on the system level and on the part level depend on each other (the state of the control unit is equal to the control state of the system; the power consumption of a system is the sum of the power consumption of all its power consuming parts).

3.1.2. The IRRIIS Behaviour Model

The static model provides the basis to describe behaviour in the IRRIIS Generic Information Model.

The key elements in the IRRIIS behaviour model are *states* and their *transitions*. With them we have all the means needed for a comprehensive behaviour model:

- we can describe what the state of a single “entity” (component, system, connection, service) in a model is: it may be specified from “outside” (for instance to declare a component to be broken), or it may result from attribute value classifications;
- in a next step states and transitions can be propagated through a model using the connections and dependencies explicitly given in the model.

The main point for the IRRIIS behaviour model is its relation to the physical behaviour model of the systems and components in a critical infrastructure. The IRRIIS behaviour model is focused onto states and transitions – not on physical attribute values. Whatever the electrical power flowing through a transformer is – in IRRIIS this value has to be interpreted in terms of states like ‘normal’, ‘high’, ‘critical’, etc. This interpretation needs, of course, knowledge from the domain. An attribute change can result in a state transition. That’s the point where IRRIIS’ behaviour model comes into play: this state transition of a certain component or system in a CI will be interpreted in terms of dependencies within the CI and to other CIs and, if necessary, propagated to them.

The rules of propagation are part of the IRRIIS behaviour model. They are formulated as state transition rules. They allow us to represent the logical relations ruling the states of a system as result of the states of its connected systems or its part systems (see fig. 6).

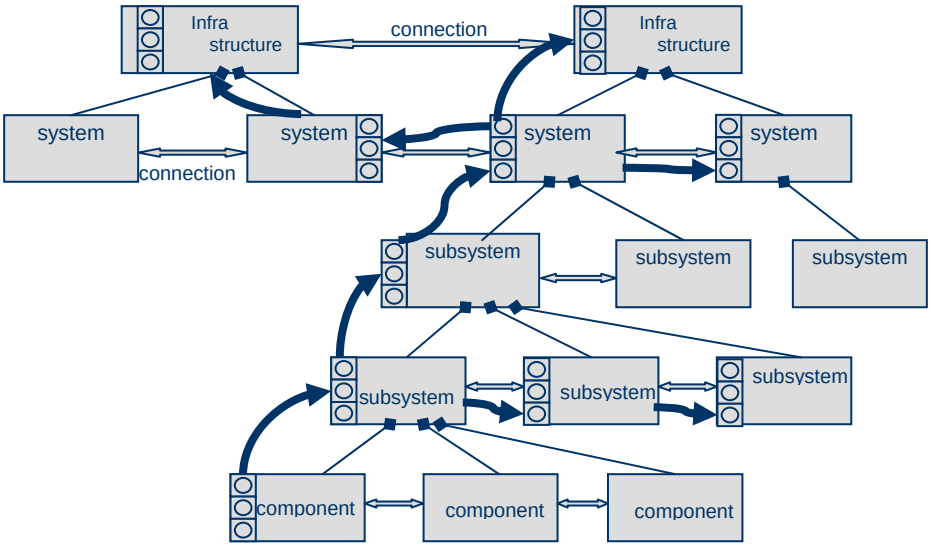

Fig. 6: The IRRIIS behaviour model: states and transitions and their propagation along connections and part relations

3.1.3. The IRRIIS Problem Solving Model: Scenarios, Events, Actions, etc.

The IRRIS Generic Information Models contains the types needed to describe scenarios, events, actions, etc. - and how these types are related to the other main information categories (see fig. 7).

Events are directly related to state transitions of systems, components, connections, or services. They may come from outside (the special system “environment”), or from other related systems.

Actions are quite similar to events in their effects on systems – but with the important difference that they follow some rationale, i.e., a strategy of the agent responsible to manage a system. Also planned maintenance operations or similar changes of the CI can be represented as actions.

As described in the definition of the event category not every state transition triggers an event. In the domain model it must be defined which state transitions result in events. Events are defined as having meaning for the system as a whole and for related (connected, depending) other systems.

A scenario is defined as a sequence of actions and events taking place on a CI or interdependent CIs (see also fig. 8).

Internal transitions result in component states within a system which are not considered as events. Events are defined as having meaning for the system as a whole and for related (connected, depending) other systems.

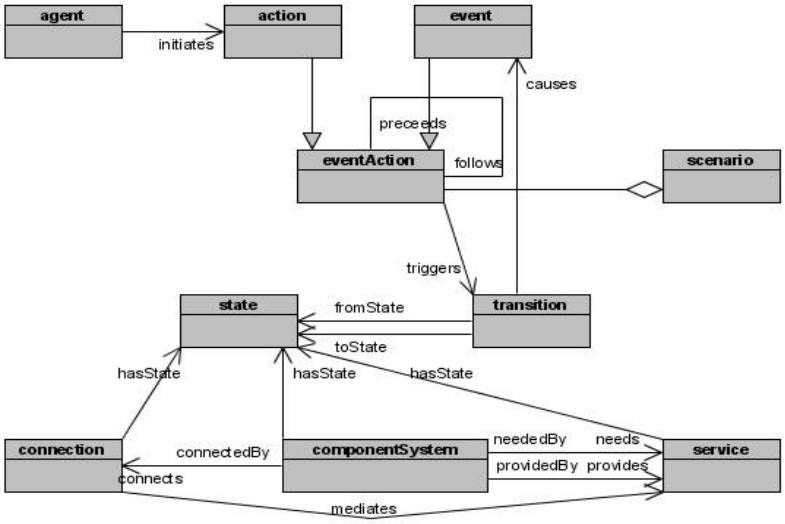

Fig. 7: The IRRIIS Problem Solving Model: events, actions, scenarios

3.2. The IRRIIS Domain Models

The IRRIIS Generic Information Model contains the main information categories for modelling large critical infrastructures and their interdependencies. It provides the basis for the concrete domain models which contain those concepts and relations needed to model domains like electrical power grids or telecommunication networks. These concrete domain concepts and their relations are *specializations* of the generic concepts defined in the GIM. For instance, in the electrical power grid domain we may have concepts like power station, transformer, and consumer as special categories under the general concept "component/system", or we may have special relations like 'controls' as specialization of the general connection concept in the GIM[2].

The IRRIIS domain models will be instantiated in order to model concrete systems like the ACEA electrical power network Rome or the TI communication network in central Italy. It will not necessarily contain all information used by the external systems but those parts of the information (maybe abstracted) which are necessary for the management of interdependencies between systems. On the other hand, the IRRIIS instance model will augment the information provided by the external systems

[2] There are some efforts to define such domain specific models as part of standardization activities (like, for instance, CIM…). Some of the concepts defined there (or their equivalents) belong to the IRRIIS Generic Information Model, others to the domain models. This needs further discussions.

by those kinds of information which are currently not managed by the external systems (like interdependency related information, geographic information, etc.).

In this way the IRRIIS GIM and the domain models provide an expressive and comprehensive modelling framework for critical infrastructures and their interdependencies.

The data from the real infrastructures or from the simulation systems used to simulate their behaviour have to be mapped to the IRRIIS instance level. This mapping has to be adapted by each external system in such a way that the meaning of its native data is equivalently represented in the IRRIIS information model. This will typically include name space adaptations, abstractions and generalizations.

3.3. The IRRIIS Instance Model

The IRRIIS Generic Information Model and the domain specific models provide the necessary general information about CIs to be modelled. A concrete critical infrastructure will be modelled as set of instances of concepts and relations between them defined in the generic and the domain specific information models.

The meaning of these instance level terms is precisely defined in the generic and domain models. This guarantees that all information used to model each concrete infrastructure system will be related to information from other depending systems in a well defined way (though this depending system and the model used to describe it might by quite different).

3.4. Information Models of CIs

IRRIIS aims at two different but related areas: the *simulation* of CI interdependencies and the support of real CI interdependency management. In both cases information from the involved CIs has to be used: in the first case from simulation tools of the respective CI, and in the second case from the real systems (their SCADA or network management systems).

These CIs (if simulated or in reality) come with there own “native” information models. They may contain much more information then needed for interdependency analysis or management. The native information needed in IRRIIS has uniquely to be mapped to the corresponding semantically equaivalent IRRIIS model elements (if generic or concrete). The resulting semantic information integration will be described in more detail in Chapter 4.2.

4. Critical Infrastructure Interdependency Analysis

In the previous chapter we outlined the IRRIIS Information Model. Now we will explain in which way these models will be *used*.

There are mainly two ways to deal with CI interdependency:

- the management of *real* critical infrastructures extending current management and control functionalities by taking the various CI interdependencies explicitly into account; and
- the *simulation* of such CIs and their interdependencies for various purposes like
  - design optimization and validation;
  - policy and strategy formulation for control of such systems;
  - method and tool validation for system control; and
  - training.

The simulation approach will need a simulation environment which allows us to simulate the behaviour of the systems to the necessary granularity and precision. Such models will typically also be useful (or even necessary) for the management of *real* systems because this more or less always includes system simulations for forecast.

4.1. Simulation Federation

Obviously, critical infrastructures can be quite different and behave in quite different ways. There is a whole bunch of highly sophisticated techniques used to simulate such diverse systems – depending on the type of the systems, their behaviours, and the purposes the simulation is aiming at. Typically these simulations do not consider interdependencies between systems. That's exactly the place where the IRRIIS Information Model and its usage come into play. The IRRIIS approach can be characterized as a federated simulation approach: IRRIIS takes the simulations of each critical infrastructure and integrates them – taking in this way the interdependencies between them into account.

The IRRIIS Information Model provides the information "glue" for this federated simulation. It allows us to relate the results from simulation of one CI in a *standardized* way to the simulation results of another, depending CI. It is expressive enough from an application (modelling) viewpoint and formally well defined from a computation (federated simulation) perspective.

The starting point for using the IRRIIS Information Model are events and actions forming scenarios (event action chains). An event may be an external event (something just happening from outside including incidents, hostile attacks, or events from other depending CIs), internal events (a state change within a CI resulting from system behaviour), or actions purposefully changing the state in a CI by control measures). An event is characterized by a *state change*. States have been defined as abstractions which allow us to classify a component, system, connection, or service according to its properties. It depends on the system and its interdependencies to be considered what will be defined as a state (and how).

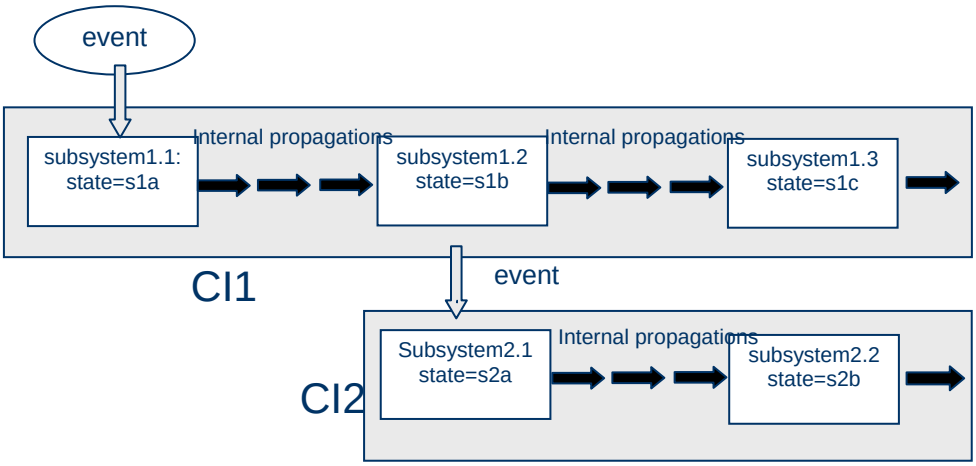

Fig. 8: Federated system simulation

The main idea behind IRRIIS' federated system simulation approach is outlined in fig. 8:

At the beginning an external event triggers a state transition in a subsystem (or component) of a critical infrastructure (here named CI1). This event can, for instance, mean that a service is lost which is needed by this subsystem to work properly. Consequently, its state is changed (to 'failed' or 'reduced' or whatever an appropriate characterization of this new state is). The resulting changes are propagated through CI1 using CI1's native behaviour simulation. There may be a whole sequence of such changes in other subsystems or components of CI1 which are not considered as state changes. They just change physical parameter values. Others may result in state changes of other subsystems of CI1.

If any of these subsystems is connected through a dependency to a system or component in another critical infrastructure this state change will be propagated as an event to this other CI (in our example CI2). Now at CI2 the same process starts as for CI1 – but taking *CI2's native* behaviour (and simulation) into account.

Though the critical infrastructures may be different they "communicate" through the exchange of state transitions and events with each other. The simulation of the system behaviour of the involved critical infrastructures is combined (or federated) to an overall simulation of interdependent critical infrastructures by using the native simulations of each CI and the state transition and event chain mechanism of the IRRIIS simulation approach.

Two points should be highlighted here:

1. The expressive information model of IRRIIS allows us to represent all relevant information (systems, components, their part structure and dependencies, their behaviours, etc.) in an adequate and transparent way.
2. The classification of behaviour results from each CI simulation in terms of states, state transitions, and events is the main "interface" between native CI simulations and IRRIIS' interdependency simulation.

4.2. Information Integration

The IRRIIS Information Model was created in order to provide an expressive and well defined framework for the many different kinds of information relevant for CI interdependency analysis and management. Especially, it allows us to represent the various kinds of dependencies between systems and components within a CI and between different CIs and all information related to these dependencies.

On the other side, IRRIIS is not the "universal simulation approach" allowing us to simulate all kinds of behaviours within a single simulation. This is not feasible. IRRIIS is based on federated simulation. Therefore we have to solve two problems on the information level [8]:

- the *information integration* problem between the respective native information models of the involved CIs and the IRRIIS Information Model;
- additionally, we have to provide those kinds of information not taken into account in the native CI information models at all (like, for instance, geographic neighbourhood information or information about direct dependencies from one CI to another one). Interdependency analysis and management should be able to integrate information from many different sources like traffic messages, weather reports, geographic information. This information may come in very different shapes.

The IRRIIS Information Model uses semantic modelling. For information integration semantic mapping will be used providing the necessary expressivity and semantic precision [8]. For each kind of information needed in IRRIIS we need a mapping from a semantically equivalent expression in the respective CI information model to the respective IRRIIS information.

There are two main aspects to be considered in information integration: mapping the generic or schema information between the IRRIIS model and the native CI models, and mapping the entities ("instances").

The classes and relations or the database schema in a native CI information model tend to be quite stable. Consequently, the mappings from these CI models to the IRRIIS Information Model can be formulated by those experts responsible for the respective native information model. In this way, the IRRIIS Information Model acts as a standard reference for CI interdependency modelling.

The other key issue in information integration is entity disambiguation. One way is to disambiguate entities explicitly through mapping tables or formalized descriptions of naming conventions used. In those cases where this is not feasible heuristic approaches taking additional information (for instance about geographic position) and related heuristics into account.

The same approach can be applied for additional information needed to describe interdependencies between CIs. It can be provided as databases or in similar form and be integrated into the IRRIIS Information Model.

4.3. Inferential Services

One of the main issues of the IRRIIS Information Model is its semantic foundation. This allows us to manage the many different but related kinds of information needed to analyse and manage CI interdependencies in a clear, transparent and concise way.

If we want, for instance, to formulate a general rule for risk estimation we can do this by saying that a CI is at a certain risk if any of its subsystems of a certain type is at this risk. This risk may be characterized as a certain risky state this subsystem may achieve at taking the current state of the all related components and subsystems into account. Recursive part relations, type taxonomies, recursive dependency relations, and sequences of states are the "ingredients" needed to formulate such a rule. These elements are part of the IRRIIS Information Model. Due to the semantics of this model the risk estimation rule can be formulated in a clear and transparent manner.

The information services needed for this purpose can be described as follows:

Semantic information retrieval: this allows us to use type taxonomy, recursive relations, and other elements in the Information Model in a kind of deductive database retrieval. As described in the previous sub-chapter the information integration between the IRRIIS Information Model and the native information model of the involved critical infrastructures is done at the semantic level. In this way the semantic information retrieval can be done not just within the IRRIIS Information Model but through it to all the other integrated information.

The other main inferential service of IRRIIS' semantic Information Model is consistency preservation. The Generic Information Model allows us to constrain the domain models in such a way that they are consistent with general IRRIIS approach – a main pre-condition for exchange of meaningful information between CIs. The same is true for the information to be exchanged with the native information systems of the involved CIs.

5. Critical Infrastructure Interdependency Simulation in IRRIIS

The IRRIIS Information Model, the federated simulation, and the information integration it is based on provide the framework for interdependency simulation of critical infrastructures.

In the IRRIIS simulator different event and action chains can be defined and simulated. They allow us to detect critical situations caused in one CI from an interdependent CI.

The IRRIIS approach to critical infrastructure simulation provides the basis for a comprehensive and systematic interdependency analysis. This allows us to develop methods and tools dedicated to increase the dependability, survivability and resilience of Critical information-based Infrastructures.

- Information interchange: MIT middleware technology

  A number of recent studies and reports point out the necessity of information sharing to reduce the risk critical infrastructures are exposed to. Depending on the critical infrastructures there are many different kinds of information that could be

shared: ranging from information about current attacks or disturbances (e.g. viruses in computer networks, disconnected power lines) to information about scheduled maintenance. This information interchange shall be accomplished by provision of a suitable middleware. The Middleware Improved Technology (MIT) under development within the IRRIIS project supports communication between critical infrastructures in order to increase overall situational awareness. It is based on the IRRIIS information model and allows information in this model to be shared between different CIs.

- Risk estimation and decision support:
  an essential aspect of the IRRIIS project is to develop methods and tools for risk estimation in critical infrastructures. Currently, there are sophisticated methods and tools for risk estimation within a single critical infrastructure – maybe with some reference to neighbouring CIs (as in electrical power networks). But in general interdependencies from and to other CIs can not be taken into account – neither from decisions within the own system to other, depending CIs nor vice versa. IRRIIS will develop such extended risk estimation methods. Simulations as well as expert knowledge will be used for this purpose. The expressive IRRIIS Information Model provides the basis to formulate the simulation results as well as the expert knowledge with the necessary reference to systems and components, their dependencies within a CI, their behaviours, etc.

6. Summary and Outlook

The IRRIIS Information Model introduced here provides the basis for information modelling for CI interdependency analysis and management. It supports IRRIIS' federated simulation approach by providing an expressive and well defined framework for the different kinds of information needed here. It has been introduced as an expressive and semantically well founded basis to capture the many different kinds of relevant information in an adequate and transparent way. As a lingua franca of interdependencies it provides the communicational platform for exchanging interdependency related information between critical infrastructures.

The model introduced here is a first approach which will be further elaborated. Especially, more experiences are needed about the necessary expressivity of the IRRIIS Information Model and the granularity of the domain models (which states, which dependencies, how to model risks, etc.).

The IRRIIS Information Model provides a powerful basis for simulations of CI interdependencies and for their analysis and control in risk estimation and decision support.

The simulation approach taken in IRRIIS is simulation federation. The different types of CIs to be considered are simulated in quite different ways. Their interdependencies are simulated in IRRIIS through simulation federation on the basis of the IRRIIS Information Model – especially of states, transitions and events in the IRRIIS' behaviour model.

Currently, various scenarios are elaborated within the IRRIIS project based on real incidents in critical infrastructures. Their simulation and analysis will allow us to

further elaborate our methodology. The SimCIP simulator has been developed for these purposes within the IRRIIS project and is now under completion and extension.

At the moment, event and action chains are specified by hand by domain experts. A logical next step would be to generate such event action chains automatically in a systematic way. This will allow us to analyse interdependencies more thoroughly. A systematic survey of real incidents undertaken in the project together with estimates about their probabilities will help to develop a sound methodology of interdependency and risk analysis.

An important issue which needs further investigation is the formulation of policies and decision criteria for incidence management. The simulation of external events allows us to analyse interdependencies – but not how to treat them adequately. Actions to be undertaken in reaction to events is an important aspect of CI interdependencies. The IRRIS Information Model provides an expressive basis for policy and strategy formulation – which will be extended in order to allow the representation of decision criteria, of decision rationale, etc.

Experiences from other domains will be incorporated into our approach: from risk analysis and management in complex technical systems (like power stations or chemical plants) or from social organizations. A more sophisticated risk model will be elaborated and integrated into the IRRIIS Information Model.

References

[1] The IRRIIS European Integrated Project: www.irriis.org

[2] P. Pederson et al.: Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Technical Report, Idaho National Lab, August 2006.

[3] U. Beyer, F. Flentge: Towards a Holistic Metamodel for Systems of Critical Infrastructures, in: ECN CIIP NEWSLETTER OCT/NOV 2006.

[4] Steffen Staab, Rudi Studer (Eds.): Handbook on Ontologies. International Handbooks on Information Systems Springer 2004.

[5] Simona Bernardi and Jose Merseguer: A UML Profile for Dependability Analysis of RealTime Embedded Systems, in Proc. WOSP'07, February 5–8, 2007, Buenos Aires, Argentina

[6]Alessandro Annoni: Orchestra: Developing a Unified Open Architecture for Risk Management Applications, in: Peter van Oosterom et al. (eds.): Geo-information for Disaster Management, Springer, 2005.

[7] Walter Schmitz et al.: "Interdependency Taxonomy and Interdependency Approaches", The IRRIIS Consortium, Deliverable D.2.2.1., June 2007.

[8] Vladimir Alexiev et al: Information Integration with Ontologies, Wiley, Sussex, 2005.

Acknowledgement

The research described in this paper was partly funded by the EU commission within the 6th IST Framework in the IRRIIS Integrated Project under contract N° 027568. The authors thank all project partners for many interesting discussions which greatly helped to formulate the approach described here.