Security Requirements Document

Healthcare

STS-Tool team

Nov 10, 2014

This document has been generated by STS-Tool
http://www.sts-tool.eu

Table of Contents:

Introduction

This document describes the security requirements for the Healthcare project. It provides a detailed description of the socio-technical security requirements models from different views (*Social*, *Information*, *Authorization*) and then presents the list of *security requirements* derived from them.

The *Social view* represents stakeholders as intentional and social entities, representing their goals and important information in terms of documents, together with their interactions with other actors to achieve these goals and to exchange information. Stakeholders express constraints over their interactions in terms of *security needs.* The *Information view* represents the informational content of stakeholders' documents, showing how information and documents are interconnected, as well as how they are composed respectively. The *Authorization view* represents which stakeholders own what information, and captures the flow of permissions or prohibitions from one stakeholder to another. The modelling of authorizations expresses other *security needs* related to the way information is to be manipulated.

The document ends with the list of *security requirements* for the system to be expressed in terms of *social commitments*, namely promises with contractual validity stakeholders make to one another. The security requirements are derived automatically once the modelling is done and the designer has expressed the security needs. Whenever a security need is expressed over an interaction from one stakeholder to the other, a commitment on the opposite direction is expected from the second stakeholder to satisfy the security need.

Social View

The social view shows the involved stakeholders, which are represented as *roles* and *agents*. Agents refer to actual participants (stakeholders) known when modelling the Healthcare project, whereas roles are a generalisation (abstraction) of agents. To capture the connection between roles and agents, the *play* relation is used to express the fact that certain agents play certain roles.

Stakeholders have goals to achieve and they make use of different information to achieve these goals. They interact with one another mainly by *delegating goals* and *exchanging information*. Information is represented by means of documents, which actors manipulate to achieve their goals.

Social View Diagram

Figure 1 presents the graphical representation of the social view (a larger picture is shown in appendix A).

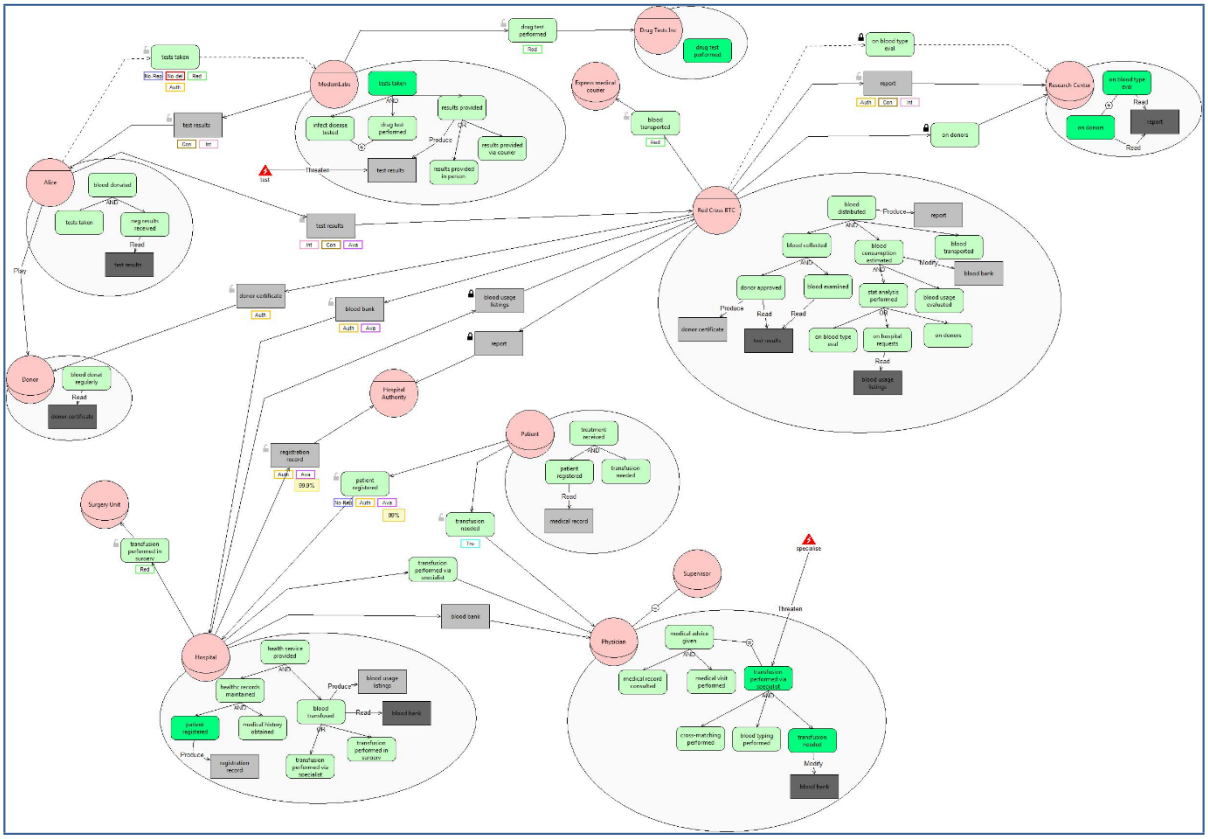

Figure 1 - Social View for the Healthcare project

Stakeholders

This section describes the stakeholders identified in the Healthcare project. Stakeholders are represented as roles or agents.

In particular, identified roles are: *Donor*, *Patient*, *Hospital*, *Physician*, *Supervisor*, *Surgery Unit*, *Express medical courier* and *Research Center* (Figure 1), while identified agents are: *Alice*, *ModernLabs*, *Red Cross BTC*, *Hospital Authority* and *Drug Tests Inc* (Figure 1). Table 1 and Table 2 summarise the stakeholders.

Role	Description	Mission	Purpose
Donor			
Patient			
Hospital			
Physician			
Supervisor			
Surgery Unit			
Express medical courier			
Research Center			

Table 1 - Roles in the Healthcare project.

Agent	Description	Abilities	Important Features	Certifications Accreditations	Type Of Organisation
Alice					
ModernLabs					
Red Cross BTC					
Hospital Authority					
Drug Tests Inc					

Table 2 - Agents in the Healthcare project

Agents and roles are related by means of *play* relations, as reported on Table 3

Agent	Role
Alice	Donor

Table 3 - Agent/Role relations in the Healthcare project

Stakeholders' documents

Stakeholders have documents they possess or exchange with others to achieve their goals. Documents are represented within the rationale of the role/agent (Figure 1).

In the Healthcare project (Figure 1) we have:

- **Alice** has document *test results* provided by *ModernLabs*.
- **Donor** has document *donor certificate* provided by *Red Cross BTC*.
- **ModernLabs** has document *test results* .
- **Patient** has document *medical record*.
- **Red Cross BTC** has documents *report*, *blood bank*, *donor certificate* and *health record*. Moreover it has document *test results* provided by *Alice* and document *blood usage listings* provided by *Hospital*.
- **Hospital** has documents *registration record* and *blood usage listings*. Moreover it has document *blood bank* provided by *Red Cross BTC*.
- **Physician** has document *blood bank* provided by *Hospital*.
- **Hospital Authority** has document *privacy regulation*. Moreover it has document *report* provided by *Red Cross BTC* and document *registration record* provided by *Hospital*.
- **Research Center** has document *report* provided by *Red Cross BTC*.

Table 4 summarises stakeholders' *documents* for the Healthcare project.

Agent/Role	Document	Description
Alice	test results	
Donor	donor certificate	
ModernLabs	test results	
Patient	medical record	
Red Cross BTC	report	
	blood bank	
	donor certificate	
	health record	
	test results	
	blood usage listings	
Hospital	registration record	
	blood bank	
	blood usage listings	
Physician	blood bank	
Hospital Authority	registration record	
	report	
	privacy regulation	
Research Center	report	

Table 4 - Stakeholders' documents in the Healthcare project

Stakeholders' documents and goals

Stakeholders' documents are linked to their goals: they read (make) documents to achieve their goals, they modify documents while achieving their goals, and they may produce documents from achieving their goals.

In the Healthcare project (Figure 1) stakeholders' documents and goals are related as follows:

- **Alice** *reads* document *test results* to achieve goal *neg results received*.
- **Donor** *reads* document *donor certificate* to achieve goal *blood donat regularly*.
- **ModernLabs** *produces* document *test results* to achieve goal *results provided*.
- **Patient** *reads* document *medical record* to achieve goal *patient registered*.
- **Red Cross BTC** *modifies* document *blood bank* to achieve goal *blood consumption estimated*, *produces* document *report* to achieve goal *blood distributed*, *reads* document *test results* and *produces* document *donor certificate* to achieve goal *donor approved*, *reads* document *test results* to achieve goal *blood examined* and *reads* document *blood usage listings* to achieve goal *on hospital requests*.
- **Hospital** *produces* document *registration record* to achieve goal *patient registered* and *reads* document *blood bank* and *produces* document *blood usage listings* to achieve goal *blood transfused*.
- **Physician** *modifies* document *blood bank* to achieve goal *transfusion needed*.
- **Hospital Authority** *reads* document *report* to achieve goal *verify donors' privacy*, *reads* document *registration record* to achieve goal *verify patients' privacy* and *reads* document *privacy regulation* to achieve goal *verify privacy ensured*.
- **Research Center** *reads* document *report* to achieve goal *on donors* and *reads* document *report* to achieve goal *on blood type eval*.

Table 5 summarises goal-document relations for all stakeholders in the Healthcare project.

Agent/Role	Goal	Document	Relation
Alice	neg results received	test results	read
Donor	blood donat regularly	donor certificate	read
ModernLabs	results provided	test results	Produce
Patient	patient registered	medical record	read
Red Cross BTC	blood consumption estimated	blood bank	Modify
	blood distributed	report	Produce
	donor approved	test results	read
		donor certificate	Produce
	blood examined	test results	read
	on hospital requests	blood usage listings	read
Hospital	patient registered	registration record	Produce
	blood transfused	blood bank	read

		blood usage listings	Produce
Physician	transfusion needed	blood bank	Modify
Hospital Authority	verify donors' privacy	report	read
	verify patients' privacy	registration record	read
	verify privacy ensured	privacy regulation	read
Research Center	on donors	report	read
	on blood type eval	report	read

Table 5 - Relation of stakeholders' documents to their goals

Goal Refinement

Stakeholders have goals to achieve. Goals are represented within the rationale (round compartment attached to the role/agent, see Figure 1) of the role/agent representing the stakeholder. They achieve their goals by further refining them into finer-grained goals (subgoals) by means of AND/OR-decompositions. AND-decompositions structurally refine a goal into multiple subgoals (all AND subgoals need to be achieved for the goal to be achieved), while OR-decompositions represent alternative ways for achieving a goal (at least one of the subgoals in the OR-decomposition needs to be achieved for the goal to be achieved).

In the Healthcare project (Figure 1) we have:

- **Alice** has to achieve goal *blood donated*. To achieve *blood donated*, Alice should achieve goal *tests taken* and goal *neg results received*
- **Donor** has to achieve goal *blood donat regularly*.
- **ModernLabs** has to achieve goal *tests taken*. To achieve *tests taken*, ModernLabs should achieve goal *infect disease tested*, goal *results provided* and goal *drug test performed* To achieve *results provided*, ModernLabs should achieve either goal *results provided in person* or goal *results provided via courier*
- **Patient** has to achieve goal *treatment received*. To achieve *treatment received*, Patient should achieve goal *patient registered* and goal *transfusion needed*
- **Red Cross BTC** has to achieve goal *blood distributed*. To achieve *blood distributed*, Red Cross BTC should achieve goal *blood collected*, goal *blood consumption estimated* and goal *blood transported* To achieve *blood collected*, Red Cross BTC should achieve goal *donor approved* and goal *blood examined* To achieve *stat analysis performed*, Red Cross BTC should achieve either goal *on blood type eval*, goal *on hospital requests* or goal *on donors* To achieve *blood consumption estimated*, Red Cross BTC should achieve goal *stat analysis performed* and goal *blood usage evaluated*
- **Hospital** has to achieve goal *health service provided*. To achieve *health service provided*, Hospital should achieve goal *healthc records maintained* and goal *blood transfused* To achieve *healthc records maintained*, Hospital should achieve goal *patient registered* and goal *medical history obtained* To achieve *blood transfused*, Hospital should achieve either goal *transfusion performed via specialist* or goal *transfusion performed in surgery*
- **Physician** has to achieve goal *medical advice given* and goal *transfusion performed via specialist*. To achieve *medical advice given*, Physician should achieve goal *medical record consulted* and goal

medical visit performed To achieve *transfusion performed via specialist*, Physician should achieve goal *transfusion needed*, goal *blood typing performed* and goal *cross-matching performed*

- **Hospital Authority** has to achieve goal *verify privacy ensured*. To achieve *verify privacy ensured*, Hospital Authority should achieve goal *verify donors' privacy* and goal *verify patients' privacy*
- **Drug Tests Inc** has to achieve goal *drug test performed*.
- **Surgery Unit** has to achieve goal *transfusion performed in surgery*.
- **Express medical courier** has to achieve goal *blood transported*.
- **Research Center** has to achieve goal *on donors* and goal *on blood type eval*.

Table 6 summarises the goals of each agent/role in the Healthcare project and how they are decomposed, when applicable.

Agent/Role	Goal	Dec. Type	Subgoals
Alice	blood donated	AND	tests taken
			neg results received
Donor	blood donat regularly	-	
ModernLabs	tests taken	AND	infect disease tested
			results provided
			drug test performed
Patient	treatment received	AND	patient registered
			transfusion needed
Red Cross BTC	blood distributed	AND	blood collected
			blood consumption estimated
			blood transported
Hospital	health service provided	AND	healthc records maintained
			blood transfused
Physician	medical advice given	AND	medical record consulted
			medical visit performed
	transfusion performed via specialist	AND	transfusion needed
			blood typing performed
			cross-matching performed
Hospital Authority	verify privacy ensured	AND	verify donors' privacy
			verify patients' privacy
Drug Tests Inc	drug test performed	-	
Surgery Unit	transfusion performed in surgery	-	
Express medical courier	blood transported	-	
Research Center	on donors	-	

on blood type eval	-

Table 6 - Goal Decompositions

Goal Contributions

Goals can contribute one to another. A contribution identifies the impact the fulfilment of one goal has on the fulfilment of another goal. This impact can be either positive or negative, and is represented with "++" and "--" respectively. Positive contribution means that the achievement of a goal also achieves the other goal. Negative contribution means that the achievement of a goal inhibits the achievement of another goal.

In the Healthcare project there are no contribution relations taking place for the given agents/roles.

Stakeholders Interactions

This section describes stakeholders' interactions, providing insights on whom they interact with to fulfil their desired objectives, as well as which are the stakeholders that rely on them to fulfil their respective goals. This kind of interaction is carried out by means of *goal delegations*.

To achieve their goals stakeholders might need specific information. If they do not possess this information, they may ask other stakeholders to provide them documents. *Document transmission* is used to capture this interaction.

Goal Delegations

Stakeholders interact with others to achieve some of their goals by means of goal delegations. Goal delegations are graphically represented as a relation that starts from a delegator actor to a delegatee actor (following the direction of the arrow), having a rounded corner rectangle representing the goal being delegated. Security needs are graphically specified as labels that appear below the delegated goal (Figure 1).

The following description enlists all the delegations from one role/agent to the others. When applicable, security needs expressed over the delegations are enumerated.

In the Healthcare project (Figure 1), we have the following goal delegations:

- **Alice** delegates goal *tests taken* to **ModernLabs**.

  The following security needs apply to this delegation:

  Non Repudiation: delegation, No-Delegation, Redundancy: true-single-actor and Authentication: delegator.

- **ModernLabs** delegates goal *drug test performed* to **Drug Tests Inc**.

  The following security needs apply to this delegation:

  Redundancy: true-multi-actor.

- **Patient** delegates goal *patient registered* to **Hospital**.

  The following security needs apply to this delegation:

  Non Repudiation: acceptance, Authentication: delegatee and Availability: 99.

- **Patient** delegates goal *transfusion needed* to **Physician**.

  The following security needs apply to this delegation:

  Trustworthiness.

- **Red Cross BTC** delegates goal *blood transported* to **Express medical courier**.

  The following security needs apply to this delegation:

  Redundancy: fallback-single-actor.

- **Red Cross BTC** delegates goal *on donors* to **Research Center**.

  The following security needs apply to this delegation:

  Non Repudiation: acceptance.

- **Red Cross BTC** delegates goal *on blood type eval* to **Research Center**.

  The following security needs apply to this delegation:

  No-Delegation.

- **Hospital** delegates goal *transfusion performed in surgery* to **Surgery Unit**.

  The following security needs apply to this delegation:

  Redundancy: fallback-multi-actor.

- **Hospital** delegates goal *transfusion performed via specialist* to **Physician**.

Table 7 summarises *goal delegations*, together with the eventual *security needs* when applicable, and eventual description respectively.

Delegator	Goal	Delegatee	Security Needs	Delegation Description
Alice	tests taken	ModernLabs	**Non Repudiation**: *delegation* **No-Delegation** **Redundancy**: *true-single-actor* **Authentication**: *delegator*	
ModernLabs	drug test performed	Drug Tests Inc	**Redundancy**: *true-multi-actor*	
Patient	patient registered	Hospital	**Non Repudiation**: *acceptance* **Authentication**: *delegatee* **Availability**: *99*	
	transfusion needed	Physician	**Trustworthiness**	
Red Cross BTC	blood transported	Express medical courier	**Redundancy**: *fallback-single-actor*	
	on donors	Research Center	**Non Repudiation**: *acceptance*	
	on blood type eval	Research Center	**No-Delegation**	
Hospital	transfusion performed in	Surgery Unit	**Redundancy**: *fallback-multi-actor*	

	surgery	
	transfusion performed via specialist	Physician

Table 7 - Goal Delegations and Security Needs

Document Transmission

Stakeholders exchange information by means of documents with other stakeholders. The following description enlists all the transmission from one role/agent representing the stakeholder, to other roles/agents. *Document transmission* is represented as an arrow from the transmitter to the receiver, with a rectangle representing the document. The security needs expressed over the transmission are described, if applicable. Security needs are specified with the help of labels that appear below the document being transmitted.

In the Healthcare project (Figure 1), we have the following *document transmissions*:

- **Alice** transmit document *test results* to **Red Cross BTC**.

  The following security needs apply to this transmission:

  Integrity: receiver, Confidentiality: receiver and Availability: 95.

- **ModernLabs** transmit document *test results* to **Alice**.

  The following security needs apply to this transmission:

  Confidentiality: sender and Integrity: sender.

- **Red Cross BTC** transmit document *blood bank* to **Hospital**.

  The following security needs apply to this transmission:

  Authentication: receiver and Availability: 99.

- **Red Cross BTC** transmit document *donor certificate* to **Donor**.

  The following security needs apply to this transmission:

  Authentication: receiver.

- **Red Cross BTC** transmit document *report* to **Research Center**.

  The following security needs apply to this transmission:

  Authentication: receiver, Confidentiality: sender and Integrity: receiver.

- **Red Cross BTC** transmit document *report* to **Hospital Authority**.

  The following security needs apply to this transmission:

  Authentication: receiver and Confidentiality: sender.

- **Hospital** transmit document *registration record* to **Hospital Authority**.

  The following security needs apply to this transmission:

  Authentication: sender and Availability: 99.

- **Hospital** transmit document *blood bank* to **Physician**.

- **Hospital** transmit document *blood usage listings* to **Red Cross BTC**.

  The following security needs apply to this transmission:

  Integrity: receiver and Availability: 90.

Table 8 summarises the *document transmissions* for the Healthcare project.

Transmitter	Document	Recivier	Security Needs	Transmission Descr.
Alice	test results	Red Cross BTC	**Integrity**: *receiver* **Confidentiality**: *receiver* **Availability**: *95*	
ModernLabs	test results	Alice	**Confidentiality**: *sender* **Integrity**: *sender*	
Red Cross BTC	blood bank	Hospital	**Authentication**: *receiver* **Availability**: *99*	
	donor certificate	Donor	**Authentication**: *receiver*	
	report	Research Center	**Authentication**: *receiver* **Confidentiality**: *sender* **Integrity**: *receiver*	
	report	Hospital Authority	**Authentication**: *receiver* **Confidentiality**: *sender*	
Hospital	registration record	Hospital Authority	**Authentication**: *sender* **Availability**: *99*	
	blood bank	Physician		
	blood usage listings	Red Cross BTC	**Integrity**: *receiver* **Availability**: *90*	

Table 8 - Document Transmissions and Security Needs

Organisational Constraints

Apart from the security needs actors specify over their interactions, there are others, which are dictated either by the organisation, business rules and regulations, or law. In this section we enlist these constraints, together with the security requirements derived from them. Currently, the language supports these organisational constraints: *Separation of Duties (SoD)* and *Binding of Duties (BoD)*. Graphically we represent these constraints using a similar notation to that used in workflows, as a circle with the *unequal* sign within and as a circle with the *equals* sign within, respectively. The relations are symmetric, and as such they do not have any arrows pointed to the concepts they relate (being these roles or goals).

In the Healthcare project (Figure 1) the following organisational constraints have been specified:

- **Physician** should be combined with **Supervisor**, since *BoD* constraints are specified between these roles.
- **Supervisor** should be combined with **Physician**, since *BoD* constraints are specified between these roles.
- **drug test performed** is incompatible with **infect disease tested**, given that *SoD* constraint is specified between these goals.
- **on donors** is incompatible with **on blood type eval**, given that *SoD* constraint is specified between these goals.
- **on blood type eval** is incompatible with **on donors**, given that *SoD* constraint is specified between these goals.
- **infect disease tested** is incompatible with **drug test performed**, given that *SoD* constraint is specified between these goals.
- **transfusion performed via specialist** should be combined with **medical advice given**, given that *BoD* constraint is specified between these goals.
- **medical advice given** should be combined with **transfusion performed via specialist**, given that *BoD* constraint is specified between these goals.

Table 9 summarises the organisational constraints for the Healthcare project.

Organisational Constraint	Role/Goal	Role/Goal	Description
BoD (Role - Role)	Physician	Supervisor	
	Supervisor	Physician	
SoD (Goal - Goal)	drug test performed	infect disease tested	
	on donors	on blood type eval	
	on blood type eval	on donors	
	infect disease tested	drug test performed	
BoD (Goal - Goal)	transfusion performed via specialist	medical advice given	
	medical advice given	transfusion performed via specialist	

Table 9 - Organisational Constraints

Events

Table 10 represents all the events modeled in the project Healthcare together with the set of elements each event threatens. Additionally, for each reported event a textual description is provided.

Event name	Threatened elements	Description
specialised physician sick	GoalReference: transfusion performed via specialist	
test results lost	Document: test results	

Table 10 - Events

Information View

The information view gives a structured representation of the information and documents in the Healthcare project. It shows what is the informational content of the documents represented in the social view. Information is represented by one or more documents (*tangible by*), and the same document can make tangible multiple information entities. Moreover, the information view considers composite documents (information) capturing these by means of *part of* relations.

Information View Diagram

Figure 2 presents the graphical representation of the information view (a larger picture is shown in appendix A).

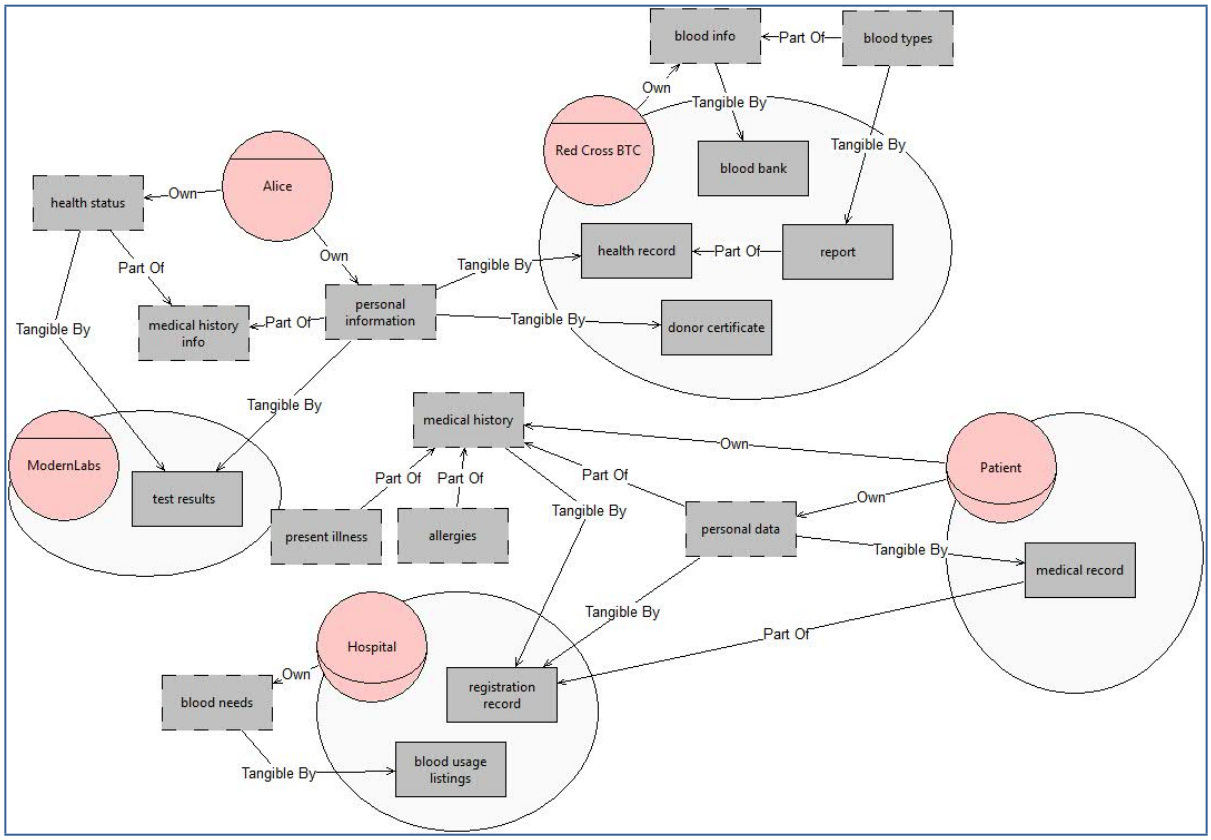

Figure 2 - Information View for the Healthcare project

Modelling Ownership

The information view represents also who are the *owners* of the information that is being manipulated through the documents that represent them in the social view.

The owners for the different information in the Healthcare project are summarised in Table 11.

Agent/Role	Information	Description
Alice	health status	
	personal information	
Patient	personal data	
	medical history	
Red Cross BTC	blood info	
Hospital	blood needs	

Table 11 - Information owners

Representation of Information

Information is represented (*made tangible by*) by documents, which stakeholders have and exchange.

The documents stakeholders in the Healthcare project (Figure 2) have and exchange with one another contain the information as summarised in Table 12:

Information	Document	Description
blood needs	blood usage listings	
health status	test results	
medical history	registration record	
blood info	blood bank	
personal information	test results	
	donor certificate	
	health record	
personal data	medical record	
	registration record	

Table 12 - Representation of Information through Documents

Structure of Information and Documents

Documents (information) are composed of other documents (information). Composition of documents (information) is captured through *part of* relations. This gives us an idea of how information and/or documents in the Healthcare project are structured.

Table 13 and Table 14 summarises the information and documents in the Healthcare project (Figure 2), showing how they are composed and describing the composition.

Information	Composition	Description
medical history	personal data	
	allergies	
	present illness	
blood info	blood types	
medical history info	personal information	
	health status	

Table 13 - Information composition

Document	Composition	Description
health record	report	
registration record	medical record	

Table 14 - Documents composition

Authorization View

The authorization view shows the permissions or prohibitions flow from a stakeholder to another, that is, the authorizations stakeholders grant or deny to others about information, specifying the operations the others can and must perform over the information. Apart from granting authority on performing operations, a higher authority can be granted, that of further authorising other actors (i.e. authorization transferability)

Authorizations start from the information owner. Therefore, in the authorization view, ownership is preserved and inherited from the information view.

Authorization View Diagram

Figure 3 presents the graphical representation of the Authorization view (a larger picture is rappresented in appendix A).

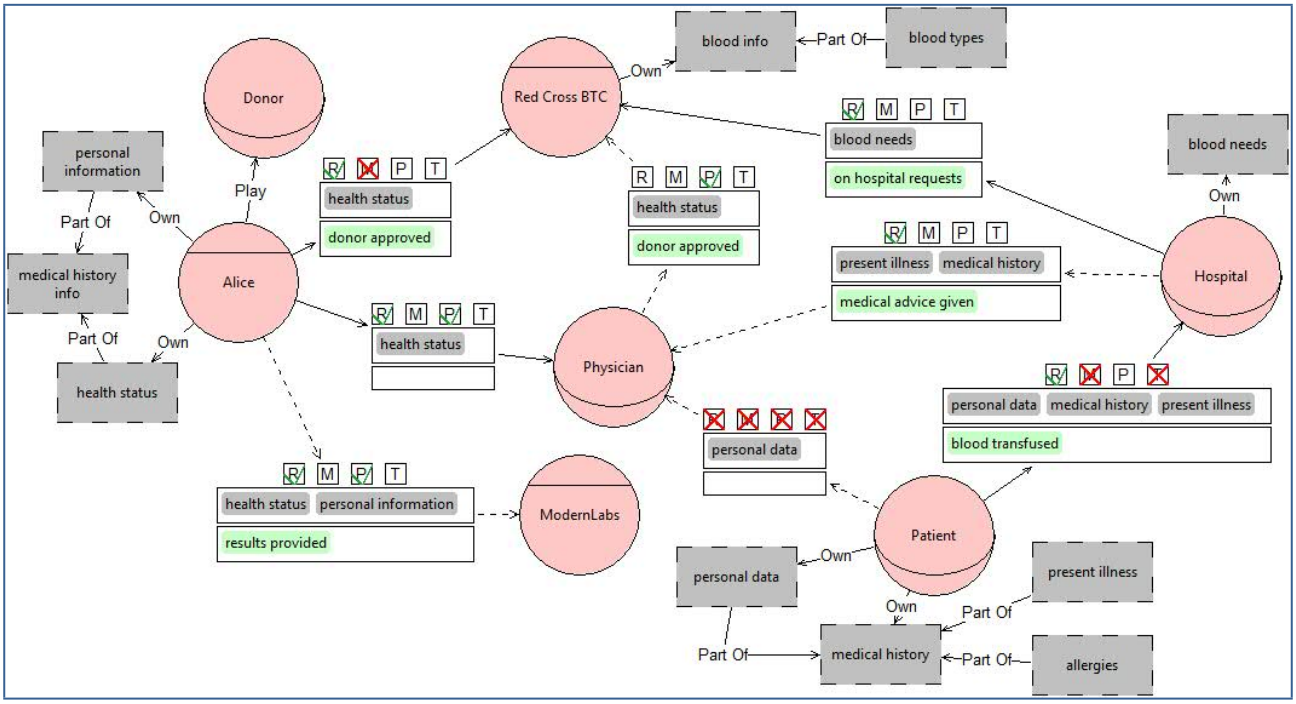

Figure 3 - Authorization View for the Healthcare project

Authorization Flow

In this section are described for each role/agent, the authorizations it passes to others and what authorizations it receives from other roles/agents.In the Healthcare project (Figure 3) the authorizations for each role/agent are:

- *Agent* **Alice**:
  - **Alice** authorises *Red Cross BTC* to *read* and prohibits to *modify* information *health status*, in the scope of goal *donor approved*, *passing* the right to further authorising other actors, and authorises *ModernLabs* to *read* and *produce* information *health status* and *personal information*, in the scope of goal *results provided*, *passing* the right to further authorising other actors, and authorises *Physician* to *read* and *produce* information *health status*, *passing* the right to further authorising other actors.
- *Agent* **ModernLabs**:
  - **ModernLabs** is authorised by *ModernLabs* to *read* and *produce* information *health status* and *personal information*, in the scope of goal *results provided*, *having* the right to further authorising other actors.
- *Role* **Patient**:
  - **Patient** authorises *Hospital* to *read* and prohibits to *modify* and *transmit* information *personal data*, *medical history* and *present illness*, in the scope of goal *blood transfused*, *passing* the right to further authorising other actors, and prohibits *Physician* to *read*, *modify*, *produce* and *transmit* information *personal data*, *passing* the right to further authorising other actors.
- *Agent* **Red Cross BTC**:
  - **Red Cross BTC** is authorised by *Red Cross BTC* to *read* and prohibited to *modify* information *health status*, in the scope of goal *donor approved*, *having* the right to further authorising other actors, and is authorised by *Red Cross BTC* to *produce* information *health status*, in the scope of goal *donor approved*, *having* the right to further authorising other actors, and is authorised by *Red Cross BTC* to *read* information *blood needs*, in the scope of goal *on hospital requests*, *having* the right to further authorising other actors.
- *Role* **Hospital**:
  - **Hospital** authorises *Physician* to *read* information *present illness* and *medical history*, in the scope of goal *medical advice given*, *passing* the right to further authorising other actors, and authorises *Red Cross BTC* to *read* information *blood needs*, in the scope of goal *on hospital requests*, *passing* the right to further authorising other actors.
  - **Hospital** is authorised by *Hospital* to *read* and prohibited to *modify* and *transmit* information *personal data*, *medical history* and *present illness*, in the scope of goal *blood transfused*, *having* the right to further authorising other actors.
- *Role* **Physician**:
  - **Physician** authorises *Red Cross BTC* to *produce* information *health status*, in the scope of goal *donor approved*, *passing* the right to further authorising other actors.

- **Physician** is authorised by *Physician* to *read* and *produce* information *health status*, *having* the right to further authorising other actors, and is prohibited by *Physician* to *read*, *modify*, *produce* and *transmit* information *personal data*, *having* the right to further authorising other actors, and is authorised by *Physician* to *read* information *present illness* and *medical history*, in the scope of goal *medical advice given*, *having* the right to further authorising other actors.

Security Requirements

This section provides the list of security requirements derived for the Healthcare project.

The list of security requirements shows the roles/agents that are *responsible* to satisfy them, so that stakeholders know what they have to bring about in order to satisfy the corresponding security needs. Security requirements also include the authorizations granted by stakeholders to other stakeholders.

Security needs are expressed mainly over goal delegations, document provisions and authorizations. Therefore, the list of security requirements is derived from every type of security need. Moreover, the organisational constraints specify further *needs* over roles and goal, leading to the generation of other security requirements.

Finally, the *requester* actors are represented to capture the actors requiring certain security needs to be brought about.

The security requirements for the Healthcare project (Table 15) are:

- **Alice** requires *ModernLabs single-actor-true-redundancy* (true_rs) and *no-delegation* on goal *tests taken*, when delegating *tests taken* to *ModernLabs*; while it is required by *ModernLabs non-repudiation-of-delegation* of the delegation of goal *tests taken* and *delegator-authentcation* when delegating *tests taken* to *ModernLabs*.
- **Alice** requires *Red Cross BTC* an *availability* level of 95%, a *receiver-integrity* and a *receiver-confidentiality* , when transmitting *test results* to *Red Cross BTC*.
- **Alice** requires *Red Cross BTC* the *non-modification* of information *health status*, and *need-to-know* of these pieces of information for the goal *donor approved*, when authorising *Red Cross BTC* to *read health status* in the scope of goal *donor approved*.
- **ModernLabs** requires *Drug Tests Inc multi-actor-true-redundancy* (true_rm), when delegating *drug test performed* to *Drug Tests Inc*.
- **ModernLabs** is required by *Alice* a *sender-integrity* and a *sender-confidentiality* when transmitting *test results* to *Alice*.
- **Patient** requires *Hospital non-repudiation-of-acceptance* of the delegation of goal *patient registered*, an *availability* level of 99% and *delegatee-authentcation* , when delegating *patient registered* to *Hospital*; while it requires *Physician trustworthiness*, when delegating *transfusion needed* to *Physician*.
- **Patient** requires *Hospital* the *non-modification* and *non-disclosure* of information *personal data*, *medical history* and *present illness*, and *need-to-know* of these pieces of informations for the goal *blood transfused*, when authorising *Hospital* to *read personal data*, *medical history* and *present illness* in the scope of goal *blood transfused*; while it requires *Physician* the *non-reading*, *non-modification*, *non-production* and *non-disclosure* of information *personal data*, not-reauthorised is required since the authorization is non-transferable.
- **Red Cross BTC** requires *Express medical courier single-actor-fallback-redundancy* (multi_rs), when delegating *blood transported* to *Express medical courier*; while it requires *Research Center non-repudiation-of-acceptance* of the delegation of goal *on donors*, when delegating *on donors* to *Research Center*; while it requires *Research Center no-delegation* on goal *on blood type eval*, when delegating *on blood type eval* to *Research Center*.

- **Red Cross BTC** requires *Hospital* an *availability* level of 99% and a *receiver-authentcation* , when transmitting *blood bank* to *Hospital*requires *Donor* a *receiver-authentcation* , when transmitting *donor certificate* to *Donor*requires *Research Center* a *receiver-authentcation* and a *receiver-integrity* , when transmitting *report* to *Research Center*; while it is required by *Research Center* a *sender-confidentiality* when transmitting *report* to *Research Center*requires *Hospital Authority* a *receiver-authentcation* , when transmitting *report* to *Hospital Authority*; while it is required by *Hospital Authority* a *sender-confidentiality* when transmitting *report* to *Hospital Authority*.
- **Hospital** requires *Surgery Unit multi-actor-fallback-redundancy* (multi_rm), when delegating *transfusion performed in surgery* to *Surgery Unit*.
- **Hospital** requires *Hospital Authority* an *availability* level of 99%, when transmitting *registration record* to *Hospital Authority*; while it is required by *Hospital Authority* a *sender-authentcation* when transmitting *registration record* to *Hospital Authority*requires *Red Cross BTC* an *availability* level of 90% and a *receiver-integrity* , when transmitting *blood usage listings* to *Red Cross BTC*.
- *Any agent* playing *Physician* is required to play *Supervisor*, and any agent playing *Supervisor* is required to play *Physician*, given that an CoD constraint is specified between *Physician* and *Supervisor*.
- *Any agent* achieving *infect disease tested* is required not to achieve *drug test performed*, and any agent achieving *drug test performed* is required not to achieve *infect disease tested*, when specifying a SoD constraint between these goals.
- *Any agent* achieving *on donors* is required not to achieve *on blood type eval*, and any agent achieving *on blood type eval* is required not to achieve *on donors*, when specifying a SoD constraint between these goals.
- *Any agent* achieving *medical advice given* is required to achieve *transfusion performed via specialist*, and any agent achieving *transfusion performed via specialist* is required not to achieve *medical advice given*, when specifying a CoD constraint between these goals.

Responsible	Security Requirement	Requester	Description
Alice	non-repudiation-of-delegation (delegated(Alice,Modern Labs,tests taken))	ModernLabs	ModernLabs require non-repudiation-of-delegation for goal tests taken,when delegated tests taken by Alice.
	delegator-authentication (delegated(ModernLabs, Alice,tests taken))	Alice	ModernLabs require Alice to be authenticated in order to delegate the goal tests taken.
Donor	receiver-authentication (transmitted(Donor,Red Cross BTC,donor certificate))	Red Cross BTC	Red Cross BTC require Donor to authenticate in order to receive document donor certificate.
ModernLabs	single-actor-true-redundancy (tests taken)	Alice	ModernLabs requires single-actor-true-redundancy for goal tests taken,when delegating tests taken to ModernLabs.

	no-delegation (tests taken)	Alice	ModernLabs requires no-delegation for goal tests taken,when delegating tests taken to ModernLabs.
	sender-integrity (transmitted(Alice,ModernLabs,test results))	Alice	ModernLabs shall ensure the integrity of transmission of the document test results while being transmitted.
	sender-confidentiality (transmitted(ModernLabs,Alice,test results))	Alice	ModernLabs shall ensure the confidentiality of transmission of the document test results while being transmitted.
	need-to-know (health status,personal information) (results provided)	Alice	Alice requires ModernLabs need-to-know of Information health status and personal information, in the scope of goal results provided.
	not-reauthorized ({health status,personal information},{results provided},{R})	Alice	Alice wants ModernLabs not to redistribute permissions on information {health status,personal information} to other actors.
	not-reauthorized ({health status,personal information},{results provided},{P})	Alice	Alice wants ModernLabs not to redistribute permissions on information {health status,personal information} to other actors.
Patient	trustworthiness (Physician, delegated(Patient,Physician,transfusion needed))	Patient	Physician shall provide proof of trustworthiness for Patient to delegate him goal transfusion needed.
Red Cross BTC	availability (test results ,95%)	Alice	Alice require Red Cross BTC to assure an availability level of 95% for document test results .
	recivier-confidentiality (transmitted(Alice,Red Cross BTC,test results))	Alice	Red Cross BTC shall ensure the confidentiality of transmission of the document test results being transmitted.
	receiver-integrity (transmitted(Alice,Red Cross BTC,test results))	Alice	Red Cross BTC shall ensure the integrity of transmission of the document test results being transmitted.
	availability (blood usage listings,90%)	Hospital	Hospital require Red Cross BTC to assure an availability level of 90% for document blood usage listings.
	receiver-integrity (transmitted(Hospital,Red Cross BTC,blood usage listings))	Hospital	Red Cross BTC shall ensure the integrity of transmission of the document blood usage listings being transmitted.
	sender-confidentiality	Research Center	Red Cross BTC shall ensure

	(transmitted(Red Cross BTC,Research Center,report))		the confidentiality of transmission of the document report while being transmitted.
	sender-confidentiality (transmitted(Red Cross BTC,Hospital Authority,report))	Hospital Authority	Red Cross BTC shall ensure the confidentiality of transmission of the document report while being transmitted.
	non-modification (health status)	Alice	Alice requires Red Cross BTC non-modification of Information health status.
	need-to-know (health status) (donor approved)	Alice	Alice requires Red Cross BTC need-to-know of Information health status, in the scope of goal donor approved.
	need-to-know (health status) (donor approved)	Physician	Physician requires Red Cross BTC need-to-know of Information health status, in the scope of goal donor approved.
	not-reauthorized ({health status},{donor approved},{P})	Physician	Physician wants Red Cross BTC not to redistribute permissions on information {health status} to other actors.
	need-to-know (blood needs) (on hospital requests)	Hospital	Hospital requires Red Cross BTC need-to-know of Information blood needs, in the scope of goal on hospital requests.
Hospital	non-repudiation-of-acceptance (delegated(Patient,Hospital,patient registered))	Patient	Patient require non-repudiation-of-acceptance for goal patient registered,when delegating patient registered to Hospital.
	availability (patient registered,99%)	Patient	Patient require Hospital to assure an availability level of 99% for goal patient registered.
	delegatee-authentication (delegated(Patient,Hospital,patient registered))	Patient	Patient require Hospital to authenticate in order to achieve goal patient registered.
	availability (blood bank,99%)	Red Cross BTC	Red Cross BTC require Hospital to assure an availability level of 99% for document blood bank.
	receiver-authentication (transmitted(Hospital,Red Cross BTC,blood bank))	Red Cross BTC	Red Cross BTC require Hospital to authenticate in order to receive document blood bank.
	sender-authentication (transmitted(Hospital,Hospital Authority,registration	Hospital Authority	Hospital Authority requires Hospital to be authenticated in order to transmit the document registration

	record))		record.
	non-modification (personal data,medical history,present illness)	Patient	Patient requires Hospital non-modification of Information personal data, medical history and present illness.
	non-disclosure (personal data,medical history,present illness)	Patient	Patient requires Hospital non-disclosure of Information personal data, medical history and present illness.
	need-to-know (personal data,medical history,present illness) (blood transfused)	Patient	Patient requires Hospital need-to-know of Information personal data, medical history and present illness, in the scope of goal blood transfused.
Physician	non-reading (personal data)	Patient	Patient requires Physician non-reading of Information personal data.
	non-modification (personal data)	Patient	Patient requires Physician non-modification of Information personal data.
	non-production (personal data)	Patient	Patient requires Physician non-production of Information personal data.
	non-disclosure (personal data)	Patient	Patient requires Physician non-disclosure of Information personal data.
	need-to-know (present illness,medical history) (medical advice given)	Hospital	Hospital requires Physician need-to-know of Information present illness and medical history, in the scope of goal medical advice given.
	not-reauthorized ({present illness,medical history},{medical advice given},{R})	Hospital	Hospital wants Physician not to redistribute permissions on information {present illness,medical history} to other actors.
Hospital Authority	availability (registration record,99%)	Hospital	Hospital require Hospital Authority to assure an availability level of 99% for document registration record.
	receiver-authentication (transmitted(Hospital Authority,Red Cross BTC,report))	Red Cross BTC	Red Cross BTC require Hospital Authority to authenticate in order to receive document report.
Drug Tests Inc	multi-actor-true-redundancy (drug test performed)	ModernLabs	Drug Tests Inc requires multi-actor-true-redundancy for goal drug test performed,when delegating drug test performed to Drug Tests Inc.
Surgery Unit	single-actor-fallback-	Hospital	Surgery Unit requires

	redundancy (transfusion performed in surgery)		single-actor-fallback-redundancy for goal transfusion performed in surgery,when delegating transfusion performed in surgery to Surgery Unit.
Express medical courier	single-actor-fallback-redundancy (blood transported)	Red Cross BTC	Express medical courier requires single-actor-fallback-redundancy for goal blood transported,when delegating blood transported to Express medical courier.
Research Center	non-repudiation-of-acceptance (delegated(Red Cross BTC,Research Center,on donors))	Red Cross BTC	Red Cross BTC require non-repudiation-of-acceptance for goal on donors,when delegating on donors to Research Center.
	no-delegation (on blood type eval)	Red Cross BTC	Research Center requires no-delegation for goal on blood type eval,when delegating on blood type eval to Research Center.
	receiver-authentication (transmitted(Research Center,Red Cross BTC,report))	Red Cross BTC	Red Cross BTC require Research Center to authenticate in order to receive document report.
	receiver-integrity (transmitted(Red Cross BTC,Research Center,report))	Red Cross BTC	Research Center shall ensure the integrity of transmission of the document report being transmitted.
"Any agents"	not-achieve-both (infect disease tested,infect disease tested)	-	Any agent that achieves infect disease tested or infect disease tested, is required not to achieve the other goal too.
	play-both (Physician,Supervisor)	-	Any agent that play Physician or Physician, is required not play the other role too.
	achieve-in-combination (medical advice given,medical advice given)	-	Any agent that achieves one of medical advice given or medical advice given, is required to achieve the other goal too.
	not-achieve-both (on donors,on donors)	-	Any agent that achieves on donors or on donors, is required not to achieve the other goal too.

Table 15 - Security Requirements for the Healthcare Project

Table 16 summarises the authorizations actors in the Healthcare project grant to one another.

Authorisor	Information	Goal	Allowed Operations	Denyed Operations	Authorisee	Description
Alice	health status	donor approved	R	M	Red Cross BTC	Transferable authority
	health status personal information	results provided	R, P		ModernLabs	Non-transferable authority
	health status		R, P		Physician	Transferable authority
Patient	personal data medical history present illness	blood transfused	R	M, T	Hospital	Transferable authority
Hospital	present illness medical history	medical advice given	R		Physician	Non-transferable authority
	blood needs	on hospital requests	R		Red Cross BTC	Transferable authority
Physician	health status	donor approved	P		Red Cross BTC	Non-transferable authority

Table 16 - Authorizations in the Healthcare project

Well-formedness Analysis

The purpose of well-formedness analysis is to verify whether the diagram for the project Healthcare is consistent and valid. A diagram is considered to be consistent if its constituent elements (concepts and relationships) are drawn and interconnected following the semantics of the modelling language (STS-ml in our case). Thus, well-formedness analysis performs post checks to verify compliance with STS-ml semantics for all checks that cannot be performed live over the models.

More details about the performed checks and their purpose can be found in Appendix B.

The Well-formedness Analysis analysis for the Healthcare has identified the problems summarised in Table 17.

Type	Category	Text	Description
WARN.	Information No Ownership	Information "medical history info" has no owner	There is no ownership relationship specified towards information "medical history info" from any actor

Table 17 - Well-formedness Analysis Analysis Results

Security Analysis

The purpose of security analysis is to verify whether the diagram for the project Healthcare allows the satisfaction of the specified security needs or not. As a result, for all security needs expressed by stakeholders, it checks in the model whether there is any possibility for the security need to be violated. This analysis takes into account the semantics of STS-ml, defining the behaviour of the different elements represented in the models. The elements' behaviour is defined by propagation rules that consider what concepts and what relationships the specification of a given security need affects. Datalog is used to define the semantics of STS-ml to express facts (things always hold) and rules.

You can find more details about the performed checks in Appendix C.

The Security Analysis analysis for the Healthcare has identified the problems summarised in Table 18.

Type	Category	Text	Description
ERROR	No_Delegation Violation check	"ModernLabs" makes an unauthorised redelegation of goal "drug test performed"	"Alice" has expressed a no_delegation security need over the delegation of the goal "tests taken" to "ModernLabs", and yet "ModernLabs" is re-delegating goal "drug test performed" to "Drug Tests Inc"
ERROR	Redundancy Violation check	ModernLabs is violating the multi actor redundancy requirement expressed by Drug Tests Inc on drug test performed	ModernLabs is violating the multi actor redundancy requirement specified by Drug Tests Inc on the fulfilment of drug test performed
ERROR	Redundancy Violation check	Alice is violating the redundancy requirement expressed by ModernLabs on tests taken	Alice has not employed more strategies for the fulfilment of tests taken, violating the redundancy requirement specified by ModernLabs on the fulfilment of tests taken
ERROR	Redundancy Violation check	Hospital is violating the multi actor redundancy requirement expressed by Surgery Unit on transfusion performed in surgery	Hospital is violating the multi actor redundancy requirement specified by Surgery Unit on the fulfilment of transfusion performed in surgery
ERROR	Redundancy Violation check	Alice is violating the single actor redundancy requirement expressed by ModernLabs on tests taken	Alice is violating the single actor redundancy requirement specified by ModernLabs on the fulfilment of tests taken
ERROR	Authorization Conflict check	There is a conflict of authorizations related to the reading of information personal data for actor Physician	There is a conflict of authorizations on reading of information personal data for Physician, since there are two incoming authorizations to Physician, one from Hospital allowing Physician and the other one

				from Patient requiring non-read of information personal data.
	ERROR	Non_Reading Violation	"Hospital Authority" makes an unauthorised read of information "blood types"	There is no authorization relationship towards "Hospital Authority" for information "blood types", but "Hospital Authority" can read "blood types" since there is a read relationship from its goal "verify donors' privacy" towards document "report" representing "blood types"
	ERROR	Non_Reading Violation	"Donor" makes an unauthorised read of information "health status"	There is no authorization relationship towards "Donor" for information "health status", but "Donor" can read "health status" since there is a read relationship from its goal "blood donat regularly" towards document "" representing "health status"
	ERROR	Non_Reading Violation	"Hospital Authority" makes an unauthorised read of information "personal data"	There is no authorization relationship towards "Hospital Authority" for information "personal data", but "Hospital Authority" can read "personal data" since there is a read relationship from its goal "verify patients' privacy" towards document "registration record" representing "personal data"
	ERROR	Non_Reading Violation	"Hospital Authority" makes an unauthorised read of information "medical history"	There is no authorization relationship towards "Hospital Authority" for information "medical history", but "Hospital Authority" can read "medical history" since there is a read relationship from its goal "verify patients' privacy" towards document "registration record" representing "medical history"
	ERROR	Non_Reading Violation	"Red Cross BTC" makes an unauthorised read of information "health status"	There is no authorization relationship towards "Red Cross BTC" for information "health status", but "Red Cross BTC" can read "health status" since there is a read relationship from its goal "blood examined" towards document "test results " representing "health status"
	ERROR	Non_Reading Violation	"Hospital" makes an unauthorised read of information "blood	There is no authorization relationship towards "Hospital" for information

			types"	"blood types", but "Hospital" can read "blood types" since there is a read relationship from its goal "blood transfused" towards document "" representing "blood types"
	ERROR	Non_Reading Violation	"Donor" makes an unauthorised read of information "personal information"	There is no authorization relationship towards "Donor" for information "personal information", but "Donor" can read "personal information" since there is a read relationship from its goal "blood donat regularly" towards document "donor certificate" representing "personal information"
	ERROR	Non_Reading Violation	"Hospital Authority" makes an unauthorised read of information "present illness"	There is no authorization relationship towards "Hospital Authority" for information "present illness", but "Hospital Authority" can read "present illness" since there is a read relationship from its goal "verify patients' privacy" towards document "" representing "present illness"
	ERROR	Non_Reading Violation	"Red Cross BTC" makes an unauthorised read of information "personal information"	There is no authorization relationship towards "Red Cross BTC" for information "personal information", but "Red Cross BTC" can read "personal information" since there is a read relationship from its goal "donor approved" towards document "test results " representing "personal information"
	ERROR	Non_Reading Violation	"Donor" makes an unauthorised read of information "medical history info"	There is no authorization relationship towards "Donor" for information "medical history info", but "Donor" can read "medical history info" since there is a read relationship from its goal "blood donat regularly" towards document "" representing "medical history info"
	ERROR	Non_Reading Violation	"Red Cross BTC" makes an unauthorised read of information "personal information"	There is no authorization relationship towards "Red Cross BTC" for information "personal information", but "Red Cross BTC" can read "personal information" since there is a read relationship from its goal "blood examined" towards

				document "test results " representing "personal information"
	ERROR	Non_Reading Violation	"Hospital Authority" makes an unauthorised read of information "blood info"	There is no authorization relationship towards "Hospital Authority" for information "blood info", but "Hospital Authority" can read "blood info" since there is a read relationship from its goal "verify donors' privacy" towards document "" representing "blood info"
	ERROR	Non_Reading Violation	"Research Center" makes an unauthorised read of information "blood types"	There is no authorization relationship towards "Research Center" for information "blood types", but "Research Center" can read "blood types" since there is a read relationship from its goal "on blood type eval" towards document "report" representing "blood types"
	ERROR	Non_Reading Violation	"Research Center" makes an unauthorised read of information "blood types"	There is no authorization relationship towards "Research Center" for information "blood types", but "Research Center" can read "blood types" since there is a read relationship from its goal "on donors" towards document "report" representing "blood types"
	ERROR	Non_Reading Violation	"Red Cross BTC" makes an unauthorised read of information "health status"	There is no authorization relationship towards "Red Cross BTC" for information "health status", but "Red Cross BTC" can read "health status" since there is a read relationship from its goal "donor approved" towards document "test results " representing "health status"
	ERROR	Non_Reading Violation	"Red Cross BTC" makes an unauthorised read of information "medical history info"	There is no authorization relationship towards "Red Cross BTC" for information "medical history info", but "Red Cross BTC" can read "medical history info" since there is a read relationship from its goal "donor approved" towards document "" representing "medical history info"
	ERROR	Non_Reading Violation	"Red Cross BTC" makes an unauthorised read of information "medical history info"	There is no authorization relationship towards "Red Cross BTC" for information "medical history info", but "Red Cross BTC" can read "medical history info" since there is a read relationship

				from its goal "blood examined" towards document "" representing "medical history info"
	ERROR	Non_Reading Violation	"Hospital" makes an unauthorised read of information "blood info"	There is no authorization relationship towards "Hospital" for information "blood info", but "Hospital" can read "blood info" since there is a read relationship from its goal "blood transfused" towards document "blood bank" representing "blood info"
	ERROR	Non_Reading Violation	"Hospital Authority" makes an unauthorised read of information "allergies"	There is no authorization relationship towards "Hospital Authority" for information "allergies", but "Hospital Authority" can read "allergies" since there is a read relationship from its goal "verify patients' privacy" towards document "" representing "allergies"
	ERROR	Non_Reading Violation	"Research Center" makes an unauthorised read of information "blood info"	There is no authorization relationship towards "Research Center" for information "blood info", but "Research Center" can read "blood info" since there is a read relationship from its goal "on blood type eval" towards document "" representing "blood info"
	ERROR	Non_Reading Violation	"Research Center" makes an unauthorised read of information "blood info"	There is no authorization relationship towards "Research Center" for information "blood info", but "Research Center" can read "blood info" since there is a read relationship from its goal "on donors" towards document "" representing "blood info"
	ERROR	Non_Modification Violation	"Physician" makes an unauthorised modification of information "blood info"	There is no authorization relationship towards "Physician" for information "blood info", but "Physician" can modify "blood info" since there is a modify relationship from its goal "transfusion needed" towards document "blood bank" representing "blood info"
	ERROR	Non_Modification Violation	"Physician" makes an unauthorised modification of information "blood types"	There is no authorization relationship towards "Physician" for information "blood types", but "Physician" can modify "blood types" since there is a modify relationship from

				its goal "transfusion needed" towards document "" representing "blood types"
	ERROR	Non_Production Violation	"Hospital" makes an unauthorised production of information "personal data"	There is no authorization relationship towards "Hospital" for information "personal data", but "Hospital" can produce "personal data" since there is a produce relationship from its goal "patient registered" towards document "registration record" representing "personal data"
	ERROR	Non_Production Violation	"Red Cross BTC" makes an unauthorised production of information "health status"	There is no authorization relationship towards "Red Cross BTC" for information "health status", but "Red Cross BTC" can produce "health status" since there is a produce relationship from its goal "donor approved" towards document "" representing "health status"
	ERROR	Non_Production Violation	"Hospital" makes an unauthorised production of information "allergies"	There is no authorization relationship towards "Hospital" for information "allergies", but "Hospital" can produce "allergies" since there is a produce relationship from its goal "patient registered" towards document "" representing "allergies"
	ERROR	Non_Production Violation	"Red Cross BTC" makes an unauthorised production of information "personal information"	There is no authorization relationship towards "Red Cross BTC" for information "personal information", but "Red Cross BTC" can produce "personal information" since there is a produce relationship from its goal "donor approved" towards document "donor certificate" representing "personal information"
	ERROR	Non_Production Violation	"Red Cross BTC" makes an unauthorised production of information "medical history info"	There is no authorization relationship towards "Red Cross BTC" for information "medical history info", but "Red Cross BTC" can produce "medical history info" since there is a produce relationship from its goal "donor approved" towards document "" representing "medical history info"
	ERROR	Non_Production Violation	"Hospital" makes an unauthorised production	There is no authorization relationship towards

			of information "medical history"	"Hospital" for information "medical history", but "Hospital" can produce "medical history" since there is a produce relationship from its goal "patient registered" towards document "registration record" representing "medical history"
	ERROR	Non_Production Violation	"Hospital" makes an unauthorised production of information "present illness"	There is no authorization relationship towards "Hospital" for information "present illness", but "Hospital" can produce "present illness" since there is a produce relationship from its goal "patient registered" towards document "" representing "present illness"
	ERROR	Non_Disclosure Violation	"Hospital" makes an unauthorised distribution of information "blood types"	There is no authorization relationship towards "Hospital", but "Hospital" is distributing "blood types" to "Physician" by providing document "blood bank" to "Physician"
	ERROR	Non_Disclosure Violation	"ModernLabs" makes an unauthorised distribution of information "health status"	There is no authorization relationship towards "ModernLabs", but "ModernLabs" is distributing "health status" to "Alice" by providing document "test results " to "Alice"
	ERROR	Non_Disclosure Violation	"Hospital" makes an unauthorised distribution of information "present illness"	"Patient" has required "Hospital" non_disclosure of information "present illness", but "Hospital" is distributing "present illness" to "Hospital Authority" by providing document "registration record"
	ERROR	Non_Disclosure Violation	"Hospital" makes an unauthorised distribution of information "medical history"	"Patient" has required "Hospital" non_disclosure of information "medical history", but "Hospital" is distributing "medical history" to "Hospital Authority" by providing document "registration record"
	ERROR	Non_Disclosure Violation	"ModernLabs" makes an unauthorised distribution of information "personal information"	There is no authorization relationship towards "ModernLabs", but "ModernLabs" is distributing "personal information" to "Alice" by providing document "test results " to "Alice"

ERROR	Non_Disclosure Violation	"Hospital" makes an unauthorised distribution of information "personal data"	"Patient" has required "Hospital" non_disclosure of information "personal data", but "Hospital" is distributing "personal data" to "Hospital Authority" by providing document "registration record"
ERROR	Non_Disclosure Violation	"Red Cross BTC" makes an unauthorised distribution of information "medical history info"	There is no authorization relationship towards "Red Cross BTC", but "Red Cross BTC" is distributing "medical history info" to "Donor" by providing document "donor certificate" to "Donor"
ERROR	Non_Disclosure Violation	"Hospital" makes an unauthorised distribution of information "blood info"	There is no authorization relationship towards "Hospital", but "Hospital" is distributing "blood info" to "Physician" by providing document "blood bank" to "Physician"
ERROR	Non_Disclosure Violation	"Hospital" makes an unauthorised distribution of information "allergies"	There is no authorization relationship towards "Hospital", but "Hospital" is distributing "allergies" to "Hospital Authority" by providing document "registration record" to "Hospital Authority"
ERROR	Non_Disclosure Violation	"Red Cross BTC" makes an unauthorised distribution of information "personal information"	There is no authorization relationship towards "Red Cross BTC", but "Red Cross BTC" is distributing "personal information" to "Donor" by providing document "donor certificate" to "Donor"
ERROR	Non_Disclosure Violation	"ModernLabs" makes an unauthorised distribution of information "medical history info"	There is no authorization relationship towards "ModernLabs", but "ModernLabs" is distributing "medical history info" to "Alice" by providing document "test results " to "Alice"
ERROR	Non_Disclosure Violation	"Red Cross BTC" makes an unauthorised distribution of information "health status"	There is no authorization relationship towards "Red Cross BTC", but "Red Cross BTC" is distributing "health status" to "Donor" by providing document "donor certificate" to "Donor"
ERROR	Sod Goal Violation	There is a separation of duty violation with respect to the goals "on donors" and "on blood type eval"	Goal "on donors" and goal "on blood type eval" should not be achieved by the same actor, since a separation of duty is expressed between these two goals, but "Research Center" wants to

			achieve them both
ERROR	Sod Goal Violation	There is a separation of duty violation with respect to the goals "on donors" and "on blood type eval"	Goal "on donors" and goal "on blood type eval" should not be achieved by the same actor, since a separation of duty is expressed between these two goals, but "Red Cross BTC" wants to achieve them both
ERROR	Sod Goal Violation	There is a separation of duty violation with respect to the goals "infect disease tested" and "drug test performed"	Goal "infect disease tested" and goal "drug test performed" should not be achieved by the same actor, since a separation of duty is expressed between these two goals, but "ModernLabs" wants to achieve them both
ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "medical advice given" and goal "transfusion performed via specialist" should be achieved by the same actor, since a binding of duty is expressed between these goals, but there is no actor to achieve them both
ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "medical advice given" and goal "transfusion performed via specialist" should be achieved by the same actor, since a binding of duty is expressed between these goals, but there is no actor to achieve them both

Table 18 - Security Analysis Analysis Results

Appendix A

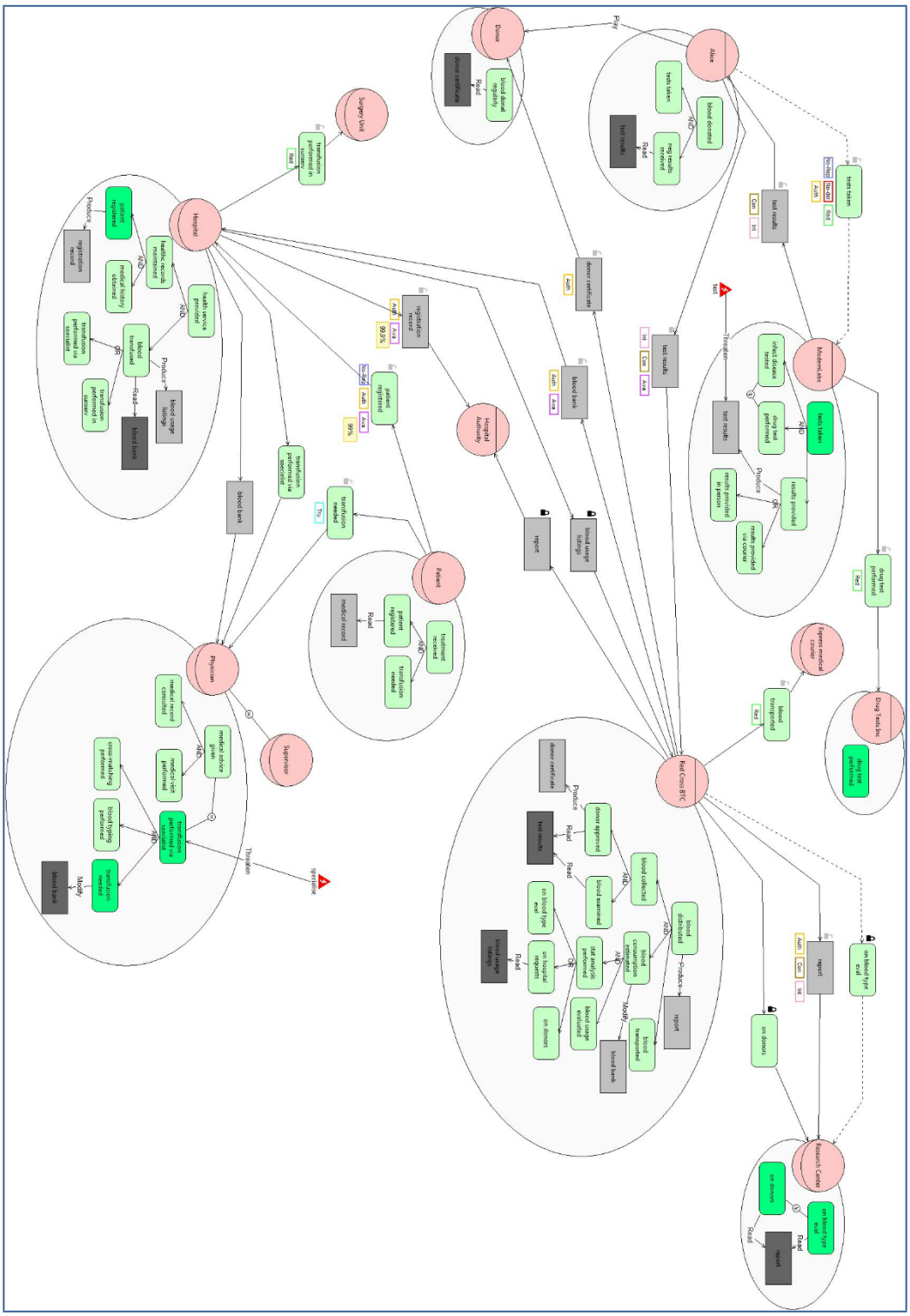

Figure 1 - Social View for the Healthcare project

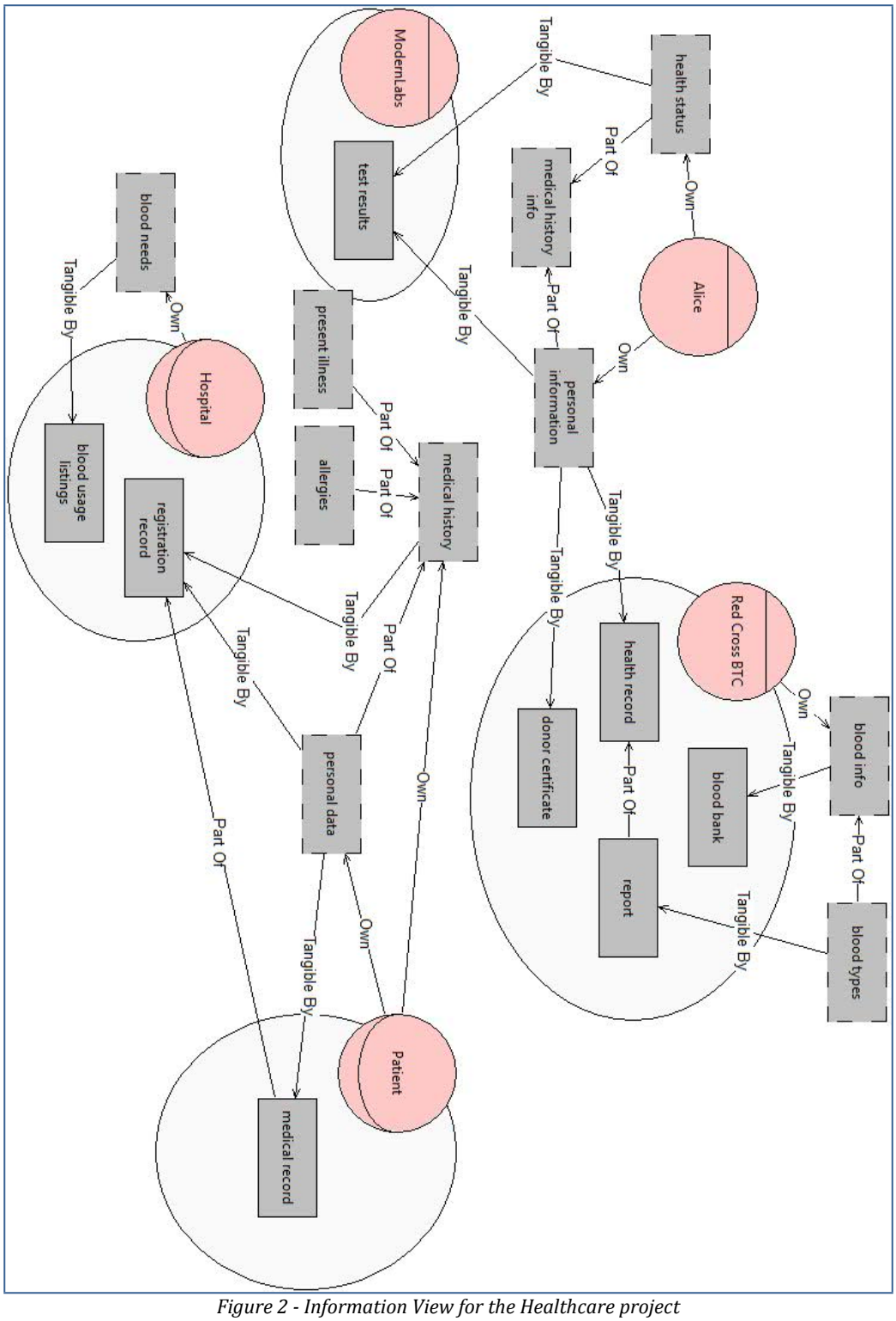

Figure 2 - Information View for the Healthcare project

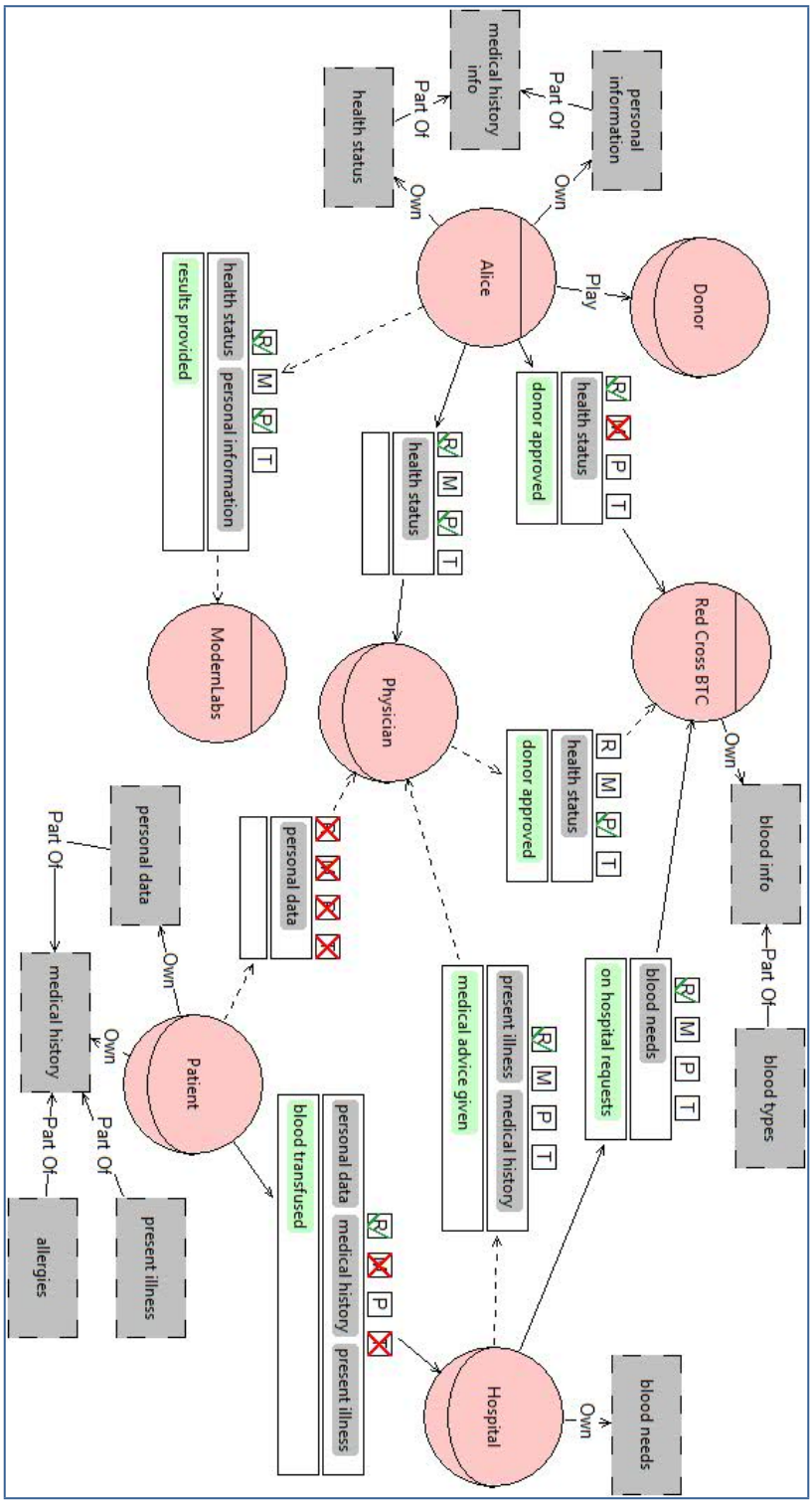

Figure 3 - Authorization View for the Healthcare project

Appendix B

Details of Well-formedness analysis:

- **Empty Diagram**

This check verifies whether the given diagram is empty or not. If that is the case, then no other well-formedness checks are performed. If the diagram is not empty, the well-formedness analysis returns: "No errors found" and continues performing the rest of the well-formedness checks.

- **Goal Single Decomposition**

This check verifies the consistency of goal decompositions. Following the semantics of STS-ml a given goal is decomposed in two or more subgoals. As a result, the decomposition should specify at least two subgoals. Therefore, goal single decomposition verifies whether there are cases of decompositions to a single subgoal.

- **Delegation Child Cycle**

This check verifies the consistency of goal delegations, so that no cycles or loops are identified as a result of the delegatee decomposing the delegatum (delegated goal) and re-delegating back one of the subgoals. Delegation child cycle verifies exactly this and gives a warning in case of inconsistency.

- **Delegated Goal Part Of a Decomposition**

This check verifies that all goals (in the delegatee's scope) that have been delegated are not child (subgoals) in the decomposition.

- **Inconsistent Contribution Cycle**

This check verifies whether there are loops of positive or negative contribution relationships, and whether this loop contains contradictory relationships. If such a loop is identified, the well-formedness analysis returns a warning.

- **Negative Contributions Between AND Subgoals**

This check verifies that there are no negative contribution relationships between and-subgoals of a given goal (within an actor's scope). It returns a warning if such a case is identified.

- **Documents PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

- **Informations PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

- **Information No Ownership**

This check verifies that all information have an owner. If there are cases of information without any ownership relationships from any actor in the diagram, the well-formedness analysis returns a warning.

- **Authorizations Validity**

This check verifies that all authorization relationship between two given actors are valid. An authorization relationship specifies authorizations or permissions an actor grants to another on some information, to perform some allowed operations. The authorizations could be limited to a goal scope and they can be re-delegated or not. However, the first two attributes should be specified for an authorization relationship to be valid. If there are no information specified, the well-formedness analysis returns an error. The same applies to the cases, in which no allowed operations are specified.

- **Duplicate Authorizations**

This check verifies that there are no duplicate authorization relationships, that could be merged. There are several cases that are addressed by this check: (i) we encounter two identical authorization, i.e., between the same roles, in the same direction, for the same set of information, allowed operations and goals, and having the same value of transferability; (ii) identify authorization relationships between the same roles, in the same direction, in which one grants permissions that are subset of the other authorization's relationship.

Appendix C

Details of security analysis:

- **No_Delegation Violation check**

This violation is verified whenever a delegatee actor further delegates a goal, over the delegation of which a no-delegation security need is specified from the delegator actor. No-delegation is specified over a goal delegation by the delegator, who requires the delegatee not to further delegate the delegated goal. Therefore, to check for any violations of no-delegation, the analysis searches for redelegations of the delegatum (delegated goal) or any of its subgoals.

- **Redundancy Violation check**

This check verifies if redundancy is satisfied by controlling that single actor redundancy or multi actor redundancy are not violated. At design time we cannot make the distinction between fallback and true redundancy, so they cannot be verified at this stage.Therefore, both fallback redundancy single and true redundancy single are mapped to single actor redundancy. Similarly for multi actor redundancy. The analysis verifies a redundancy violation if one of the following occurs: (1) actor does not decompose the delegated goal in any or-subgoals, for which both types of redundancy are violated (2) actor decomposes the goal into or-subgoals and delegates one to another actor when single actor redundancy has been specified, for which this type of redundancy is violated (3) actor decomposes the goal into or-subgoals, but does not delegate any of the subgoals to another actor when multi actor redundancy has been specified, for which this type of redundancy is violated.

- **Authorization Conflict check**

This task identifies a conflict of authorization whenever at least two authorization relationships for the same information are drawn towards the same actor from two illegible actors (being the owner of information or another authorised actor) such that: (1) one limits the authorization to a goal scope (requiring a need-to-know security need) and the other does not (authorising the actor without any limitations) (2) for the same goals or intersecting goal scopes, different permissions are granted in terms of operations or authority to transfer authoristaion. That is, one passes the actor the authority to perform operations (use, modify, produce, distribute) on a given information, and the other does not (requiring non-usage, non-modification, non-production, non-disclosure); one passes the actor the authority to further transfer authorizations and the other requires no further authorizations take place.

- **Non_Reading Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

- **Non_Modification Violation**

This violation is detected whenever an actor modifies information without having the right to modify it. Non-modification expresses the need that information should not be changed (modified), i.e. authority to modify the information is not granted. To verify if there could be any violations of non-modification, the analysis looks if the authorisee (or an actor that is not authorised by authorised party) modifies the given information. For this, it searches for modify relationships from any goal of this actor to any document representing the given information.

- **Non_Production Violation**

This violation is detected whenever an actor produces information without having the right to produce it. Non-production expresses the need that information should not be produced in any form, i.e. authority to produce the information is not granted. To verify if there could be any violations of non-production, the analysis checks whether if the authorisee (or an actor that is not authorised by authorised party) produces the given information. For this, it searches for produce relationships from any goal of this actor to any document representing the given information.

- **Non_Disclosure Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

- **NTK Violation**

This violation is detected whenever an actor uses, modifies or produces information for other purposes (goal achievement) than the ones for which it is authorized. Need-to-know requires that the information is used, modified, or produced in the scope of the goals specified in the authorization. This security need concerns confidential information, which should not be utilised for any other purposes other than the intended ones. To verify if there could be any violations of need-to-know, security analysis checks if the authorisee (or an actor that is not authorised by any authorised party) uses, modifies or produces the given information while achieving some goal different from the one it is authorised for. In a nutshell, it searches for need, modify, or produce relationships starting from goals different from the specified ones towards documents representing the given information.

- **Explicit non-reauthorization**

Verifies whether a given actor transfer rights to others even when it does not have the authority to further delegate rights.

- **Non-reauthorization Violation: read**

Verifies whether a given actors transfer to other actors the right to use a given information, without having itself the right to do so.

- **Non-reauthorization Violation: modify**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

- **Non-reauthorization Violation: produce**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

- **Non-reauthorization Violation: transmit**

Verifies whether a given actors transfer to other actors the right to distribute a given information, without having itself the right to do so.

- **Sod Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

- **Bod Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

- **Agent Play Sod**

This check verifies the consistency of the Separation of Duty (SoD) constraint between roles. This constraint requires that two roles are not played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case an error is identified, otherwise the check finds no errors.

- **Agent Not Play Bod**

This check verifies the consistency of the Binding of Duty (BoD) constraint between roles. This constraint requires that two roles are played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case the check finds no errors, otherwise an error is identified.

- **Organizational Constraint Consistency**

This check verifies that no conflicting organisational constraints (SoD or BoD) between goals are specified.