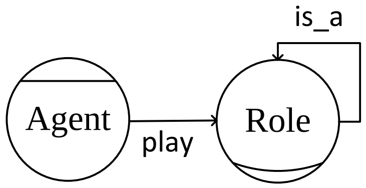
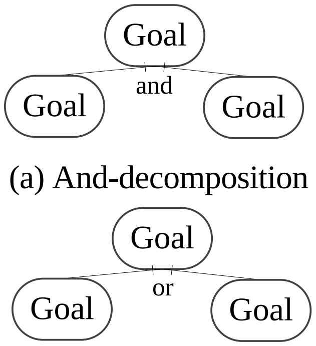
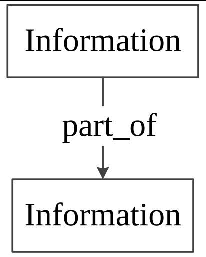
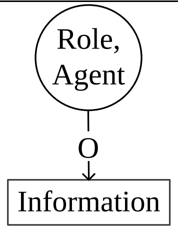
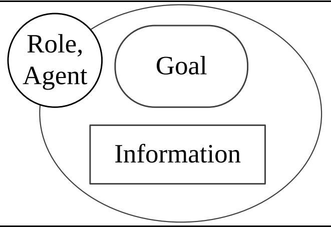
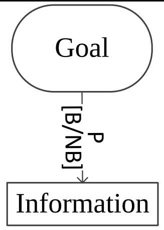
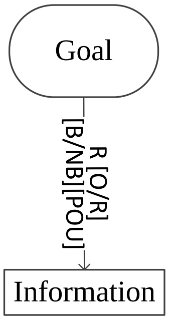
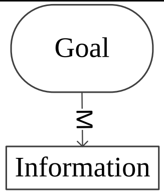
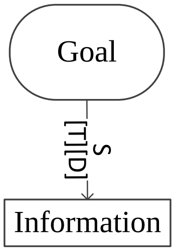
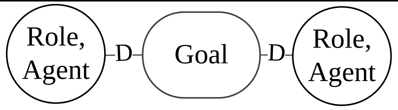
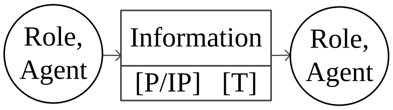
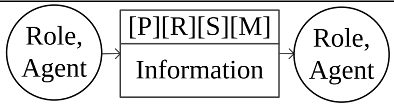
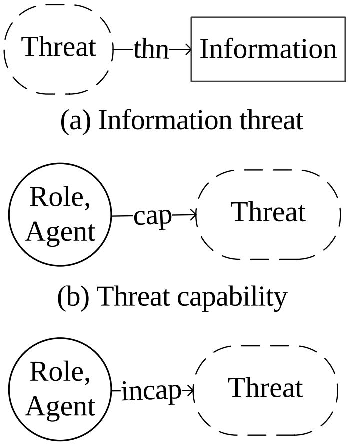
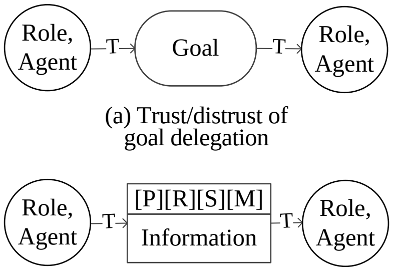
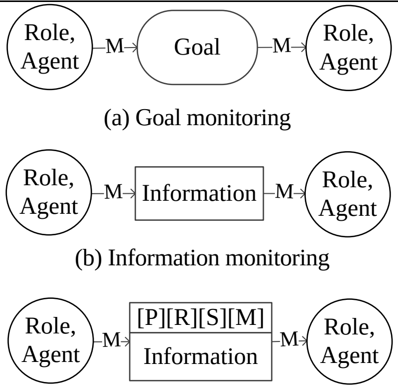
STS-IQ Modeling Language

STS-IQ modeling language adopts and extend concepts for modeling and analyzing IQ requirements from our previous work [1,2], which have been built based on Secure Tropos [3] and SI* [4] modeling languages. In the following table we list and discuss the key concepts of STS-IQ modeling language.

Concept	Graphical representation
A role can be defined as an abstract characterization of system actor in terms of a set of behaviors and functionalities within some specialized context [4] [5]. **An agent** can be defined as an autonomous entity that has a specific manifestation in the system [5]. **Roles** can be a ***specialized*** from one another, where such relation can be used to model roles hierarchies based on the concept of *specialization* represented as (**is\_a**) [4]. While an **agent** can ***play*** a role or more within the system [5].	
A goal can be defined as a state of affairs that an actor (role or an agent) intends to achieved, and it is used to represent actors' strategic interests [3] [5]. When a goal is too coarse to be achieved, it can be refined through and/or-decompositions of a root goal into finer sub-goals [3] [5]. Refining a root-goal into finer sub-goals through and-decomposition implies that the achievement of the root-goal requires the achievement of all its sub-goals. While or-decomposition is used to provide different alternatives to achieve the root goal, since or-decomposition allows for different alternatives for achieving the root-goal, i.e., achieving any of the sub-goals allows for achieving the root-goal.	 (a) And-decomposition (b) Or-decomposition
Information represents any informational entity without intentionality[1]. In [1] we extended ***information*** construct with a ***(V)olatility*** attribute to represent the change rate of information value [6], which enables to analyze information timeliness (validity). Information can be composed of several sub items (composite information item), we rely on ``***part of***'' concept to model the relation between a composite information item and its sub-items [1].	
Ownership: an actor may **own** an information item, which indicates that such actor is the legitimate owner of an information item [3], where information owner has full control over the use of information it owns, i.e., it has the authority to control the delegated permissions over information it owns.	

[1] In [5] [3] [4], they use the term resource to refer to both physical and informational entities.

Scope is represented as an oval and it is used to model the goals that an actor aims to achieve, and information (resources) that an actor have [3].	
Produce: indicates that an information item can be created by achieving the goal that is responsible of its creation process [1,2]. Produce relation is represented as an edge between the goal and information labeled with P, and it is enriched with a believability attribute **[B/NB]** that can help in analyzing the believability of the produced information, where **[B]** means that such produce relation apply a believability check, while **[NB]** means it does not.	
Read: indicates that a goal consumes an information item, and it can be strictly classified under: • ***Optional.*** indicates that information is not required for the goal achievement; • ***Required.*** indicates that information is required for the goal achievement. Read relation is represented as an edge between the goal and information labeled with **R** that can be **R[R]** (**read required**) or **R[O]** (**read optional**). Read relation is enriched with a believability attribute [B/NB], and **Purpose Of Use [POU]** attribute that captures the intended purpose of information usage that helps in analyzing information consistency.	
Modify: indicates that the goal achievement depends on modifying a particular information item [2] [7]. Modify relation is represented as an edge between the goal and information labeled with **M.**	
Send: indicates that the goal achievement depends on transferring a particular information item to a specific destination under predefined criteria [1,2]. Send relation is represented as an edge between the goal and information labeled with **S**. Send relation has two attributes that help in analyzing information timeliness (validity) for information to be sent: • ***Send (t)ime*** that represents the allowed amount of time for information to reach its final destination; • ***(D)estination*** that represents the intended send destination of information.	
Goal delegation: is a ternary relation between two actors concerning the delegatum (e.g., a goal), where the source of delegation called the delegator and the destination is called delegatee [3].	
Information provision: actors may depend on one another for information to be provided, where information provision has a time attributes that represent the transmission (provision) time **[T]**, and it has a provision type that can be either: (1) Integrity Preserving **[IP]** provision that preserves the	

integrity of the transmitted information; (2) Normal Provision **[P]** that does not guarantee the integrity of the transferred information [8].	
Permission delegation: permissions can be delegated among actors, where permissions delegation indicates that an actor delegates to another actor **[P]**roduce, **[R]**ead, **[M]**odify, and/or **[S]**end permissions over a specific information item [7].	
Threat & threaten concepts are used to analyze the trustworthiness of information source by identifying and modeling the different ***intentional threats*** [9] that might ***threaten*** the trustworthiness of information it produces. Threat and threaten graphical representations are shown in **Fig** (a). In particular, actors (information sources) are intentional entities and some of the threats might be within their objectives, which ***threatens*** the trustworthiness of information they produce. However, not all actors have the capability to achieve the defined threat(s).Thus, We classify actors' capabilities toward achieving a threat under: (1) ***Capable:*** when the actor has the competency of achieving the threat (**Fig** (b)); (2) ***Incapable:*** when the actor does not have the competency of achieving the threat (**Fig** (c)).	 Threat thn Information Role, Agent cap Threat Role, Agent incap Threat (a) Information threat (b) Threat capability (c) Threat incapability
Social trust: STS-IQ language adopts the notion of trust and distrust to capture the actors' expectations in one another concerning their entitlements and authorities [3]. In our work, trust/distrust mainly focuses on delegated goals and permissions, and they can be defined as follows: - ***Trust[T]:*** indicates the expectation of trustor that the trustee will behave as expected considering the trustum (e.g., trustee will achieve the delegated goal, or it will not misuse the delegated permission); - ***Distrust [DT]:*** indicates the expectation of trustor that the trustee will not behave as expected considering the trustum (e.g., trustee will not achieve the delegated goal, or it will misuse the delegated permission).	 Role, Agent T Goal T Role, Agent Role, Agent T [P][R][S][M] Information T Role, Agent (a) Trust/distrust of goal delegation (b) Trust/distrust of permission delegation
Monitoring: Monitoring can be defined as the process of observing and analyzing the performance of an actor in order to detect any undesirable performance [10]. Following [11] [4], the lack of trust or distrust can be compensated by monitoring. Thus, we rely on monitoring to compensate the lack of trust or distrust in goal delegation **Fig** (a), information producing **Fig** (b), and permission delegation **Fig** (c).	 Role, Agent M Goal M Role, Agent Role, Agent M Information M Role, Agent Role, Agent M [P][R][S][M] Information M Role, Agent (a) Goal monitoring (b) Information monitoring (c) Permission delegation monitoring

Bibliography

[1] Mohamad Gharib and Paolo Giorgini, "A Framework for Information Quality Requirements Engineering," in *Joint Proceedings of*

[2] Mohamad Gharib and Paolo Giorgini, "Dealing with Information Quality Requirements," in *Enterprise, Business-Process and Information Systems Modeling*.: Springer, 2015, pp. 379-394.

[3] H. Mouratidis and P. Giorgini, "Secure : A security-oriented extension of the methodology," *International Journal of Software Engineering and Knowledge Engineering*, vol. 17, no. 2, pp. 285-309, 2007.

[4] N. Zannone, "A requirements engineering methodology for trust, security, and privacy," PhD thesis, University of Trento, Ph.D. dissertation 2006.

[5] Eric Siu-Kwong Yu, "Modelling strategic relationships for process reengineering," University of Toronto, Ph.D. dissertation 1995.

[6] R.Y. Wang and D.M. Strong, "Beyond accuracy: What data quality means to data consumers," *Journal of management information systems*, pp. 5-33, 1996.

[7] Mohamad Gharib and Paolo Giorgini, "A Goal-based Approach for Automated Specification of Information Quality Policies," in *Research Challenges in Information Science (RCIS), 2015 IEEE Ninth International Conference, to appear*, 2015.

[8] Mohamad Gharib and Paolo Giorgini, "Modeling and Analyzing Information Integrity in Safety Critical Systems," in *Advanced Information Systems Engineering Workshops*, 2013, pp. 524-529.

[9] Axel Van Lamsweerde, "Elaborating security requirements by construction of intentional anti-models," in *Proceedings of the 26th International Conference on Software Engineering*, 2004, pp. 148-157.

[10] Zahia Guessoum, Mikal Ziane, and Nora Faci, "Monitoring and organizational-level adaptation of multi-agent systems," in *Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems-Volume 2*, 2004, pp. 514-521.

[11] G. Gans, M. Jarke, S. Kethers, and G. Lakemeyer, "Modeling the impact of trust and distrust in agent networks," in *Proc. of AOIS'01*, 2001, pp. 45-58.