Goal Modeling for FinTech Certification

Sepehr Sharifi[1], Patrick McLaughlin[2], Daniel Amyot[1], and John Mylopoulos[1]

[1] School of EECS, University of Ottawa, Ottawa, Canada
{sshar190, damyot, jmylopou}@uottawa.ca, patrick@brane.capital
[2] Brane Capital, Ottawa, Canada

Abstract. With an increasing investment in digital assets such as cryptocurrencies, many financial technology (FinTech) systems and custodians have become safety critical. Yet, current FinTech system development approaches often lack the rigorous safety practices found in other certified industries. This paper focuses on the development of goal models for analyzing a FinTech's system stakeholders, goals, and processes, as a first step towards system certification. A strategic dependency model is used to identify the interfaces of the system with its context, and is enriched with an operational/process view using Use Case Maps. This goal/process combination brought much in the identification of stakeholders, critical resources, priorities, and appropriate safety controls.

Keywords: Goal modeling · FinTech · Certification · Processes · GRL.

1 Background and Motivation

Systems developed in the FinTech industry are safety critical as they are more software-intensive and embedded in our lives than ever. This is especially prevalent when *digital assets* (DA), including cryptocurrencies such as Bitcoins, are involved as they are attracting increasing attention, both in investments and fraud. Rauchs et al. [8] state that, between 2011 and 2018, "exchange and storage service providers alone have accounted for the loss of more than $1.5 billion of cryptoasset funds", with 57% of that amount lost in 2018 alone. Furthermore, it can be argued that current financial systems have a high impact on people's lives and, with a rising number of security breaches and failures, the financial industry has a responsibility to move towards more stringent safety practices.

FinTech systems that involve custody or transfer of large amounts of DAs act as hubs in the highly-connected financial network, thus becoming a critical safety point that would have systemic effects when failing [4]. These systems should hence be treated as safety critical and designed with safety and security among their main objectives. Also, as the financial sector is highly regulated, financial institutions must assure regulators (policy makers, authorities, etc.) that their systems minimize the risk of losing investors' assets [7]. Such FinTech systems must also satisfy multi-faceted concerns (finance, business, software, cryptography, distributed ledgers) and convey compliance and risk assessment results in a clear and understandable manner to certification authorities.

This paper reports on an ongoing project that uses requirements modeling methodologies and standards that are foreign to the FinTech industry but common in other safety-critical engineering domains, in addition to current financial regulations, to rise up to the challenge of building a digital asset custody system that will keep institutional investors' assets safe (e.g., through a set of multi-signature smart contracts and wallets). Additionally, the results of safety-guided design and safety evaluations of the system should be communicated to the stakeholders in a clear and comprehensible manner to provide cost and schedule reductions in the certification process, and reduce dependencies on very expensive accounting firms (including the Big Four) that provide the certification services.

2 Goal Modeling for FinTech Certification

In North-America, the most notable certification applied to financial entities is the *System and Organization Controls* (SOC)(https://www.aicpa.org/soc). Different SOC reports approach system controls from different perspectives, namely compliance, operations, and financial reporting. The most relevant report on system-level and entity-level operational controls of a financial service organization is the SOC2 report, based on the guidelines provided by the American Institute of Chartered Professional Accountants (AICPA) and CPA Canada, known as Trust Services Principles and Criteria (TSC) for *Security*, *Availability*, *Processing Integrity* and *Confidentiality*(https://bit.ly/2ZnNhgB). A new standard has also been developed for financial service organizations that interact with digital assets: *Cryptocurrency Security Standard* (CCSS)(https://cryptoconsortium.github.io/CCSS/). CCSS certification is deemed by auditing firms as a major stepping stone towards establishing confidence in novel blockchain-based systems.

The above standards do not name *safety* explicitly as a criterion. They rather use the term *controls*, which are essentially the tools that are imposed on the system to ensure its safety. The development process of the system must employ an approach that addresses the controls of the system, while considering all other criteria requested by the standards, e.g., availability, security, and privacy.

Systems developed in the FinTech industry have major human and software elements, and are hence considered socio-technical systems. Goal modeling has shown its utility when it comes to capturing intentionality of stakeholders in such systems, while providing support for compliance, trade-off and decision-making [5]. The User Requirements Notation (URN)(https://www.itu.int/rec/T-REC-Z.151) integrates the *Goal-oriented Requirement Language* (GRL) with the *Use Case Maps* (UCM) process notation. URN provides a combined goal/process view used in requirements engineering activities, but also in regulatory compliance [1]. Though many work have been done on safety/security requirements, to our knowledge none of them have addressed certification [5].

For a FinTech system to be successful, important stakeholders such as regulators, banks, and insurers must be on-board and be assured that their concerns

are handled properly. Therefore, the results of the safety-guided design of a system to-be must be communicated to them as clearly, and yet as completely, as possible. Due to the novelty of FinTech systems being developed (e.g., involving advanced blockchain-based technologies), communication of proper artifacts, documents, and justifications to help regulators and other stakeholders decide on the acceptable safety of systems is crucial. Although many guidelines and standards exist for general financial systems (including SOC, TSC, and CCSS), process and product standards have not caught up to recent FinTech advancements and are not sufficient to address certification problems.

For the above reasons, and since goal-oriented approaches are useful for developing socio-technical systems, we propose to enhance traditional (prescriptive) approaches with a normative (goal-oriented) view [10]. This view has been utilized in various safety-critical domains (e.g., aerospace and nuclear industries) for certification [9]. Assurance cases are used to provide justified assurance in the qualities of the system. As stated in the systems engineering standard ISO/IEC/IEEE:15026-1:2019, a quality of the system is claimed, and then an argument based on evidence needs to justify that claim for the regulators.

3 Stakeholder and Operational Analysis

The first step in modeling the goals of a FinTech system is to gain a holistic understanding of all the stakeholders and their dependencies. They can often be categorized into four major expertise domains: *governance and policy*, *regulatory and compliance*, *business and operations*, and *technical (engineering)*.

The stakeholders, with varied expertise in the above domains, have unequal understanding of the core of the system. In an onion model, we find them in various layers from the core *operational* layer, to the *system* layer (containing the management and support elements), and then to the *environment* layer:
– **System Operations:** Normal Operators (Finance Manager and Technical Users), Maintenance Ops (Hardware, Software), Operational Support (Transaction Mining, Customer Support), Interfacing System (Cloud, Internal Network).
– **System:** Internal Consultants (Compliance Officer), Client (Investors, Management), Functional Beneficiary (Institutional Funds).
– **System Environment:** Customer (White-label Partners), Interfacing System (Crypto-exchanges, Blockchains Platforms, Insurers), Regulators (Securities, Judiciary, Tax and KYC/AML[3] Authorities, Non-statutory Regulators including standards, consortia, and Self-Regulatory Organizations), Negative Actors (Competitor, Hacker), External Consultants (Business Auditor, Security Specialist, Legal Counsel).

This view is employed in the early stages of the system development to draft the *Concept of Operations* (ConOps) of the system. Adding a development viewpoint to the ConOps view would require the list of stakeholders to be augmented with, e.g., project managers and system developers. The system development

[3] Know Your Client (KYC) and Anti-Money Laundering (AML) efforts are crucial in the financial industry.

team is present in all three layers of the system and has interactions with virtually all other stakeholders (except negative actors such as hackers).

Various sources of information such as handbooks, standards, and interviews with stakeholders and decision makers will uncover valuable dependencies. These dependencies will in turn become the basis for sketching a strategic dependency model of the system, which starts by outlining the actors and their directional dependencies, hence enabling the elicitation of the actors' goals. In GRL, the source and target of a dependency are intentional elements from different actors.

A slice of the strategic dependency model is provided in Fig. 1, illustrating how three actors, namely the Underwriter, the Securities Regulator, and the Judiciary, depend on the system's goal Report to produce the Security Report and on the Auditor's ability to perform verification (Verify). Multiple dependency inbound and outbound links are a shorthand for a *distributive* dependency relationship, i.e. there are 6 dependency relationships that have Security Report as their dependum. Here, the Brane actor is the DA custodian and service provider.

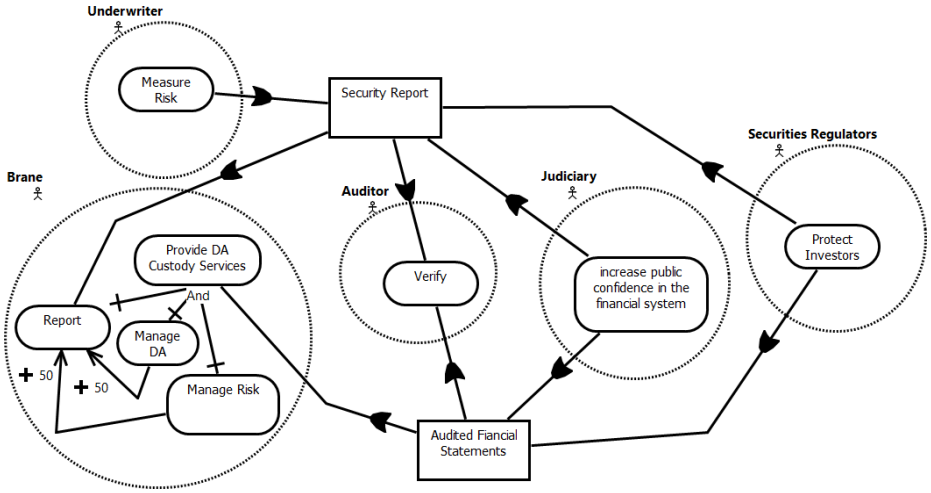

Fig. 1: A Slice of the FinTech system strategic dependency model during its operation, specified in GRL. Note that the multiple dependencies that depend on the same dependum, illustrates the criticality of the resource.

The creation of the GRL model has allowed the organization to discover critical resources, i.e., resources that have a high number of dependencies which, if not realized properly, would result in the simultaneous dissatisfaction of multiple stakeholders. Thus, the requirements elicitation, system development/testing, and certification efforts can be prioritized in accordance with the criticality of the *dependums* and the system goals that provide them.

As explained in Section 2, the main concern of financial regulators is the controls on systems operations. To analyze the operational aspect of the system, the GRL model is expanded by defining Use Case Map processes for functional

goals of the system. A process model of the Perform Due Diligence system goal is provided in Fig. 2. The UCM model allows for analysis of the business process. The operationalization of goal Perform Due Diligence starts by the activity Evaluate Jurisdiction, which is the responsibility of the service provider (Brane) and yield one of two possible outcomes (illustrated by an OR-fork), i.e., being of low or high risk (the latter leading to the rejection of the client).

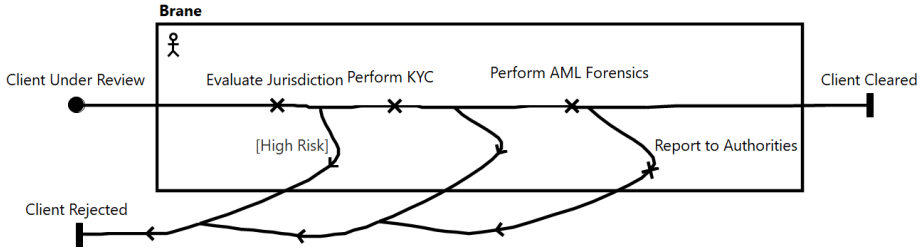

Fig. 2: Extract of the UCM model that describes the Perform Due Diligence goal

Performing the operational analysis, has allowed the organization to check the controls it has in place, assess alternative ones, provide a means to demonstrate compliance to the regulators, and have a basis for the analysis of systemic safety.

Our complete URN model of the FinTech's digital asset management system, developed with the jUCMNav tool, is composed of 15 actors, 100 intentional elements, and 96 intentional links for the GRL view, and of 5 components, 84 responsibilities, and 22 interconnected process maps with up to 7 levels of nesting through stubs for the UCM view.

4 Conclusions and Future Work

With the emergence of Distributed Ledger Technologies, the new FinTech certification landscape has become hard to navigate, both for service providers and regulators. A service provider not only bears the responsibility of developing an efficient system addressing many stakeholders concerns, but also of conveying its design rationale and safety analysis to regulators that provides justified assurance. Assurance cases can easily be misused if their authors do not focus on discovering the system risks or form arguments that enforce *confirmation bias*.

The first step towards a goal-based approach in acquiring certification for FinTech systems starts with the analysis of stakeholders, their interfaces, and the system-level operations of the system. The stakeholders were identified based on an onion model, while their interfaces with the service provider were studied via the creation of a strategic dependency goal model. This has aided the service provider in discovering critical resources, the system goals providing them, and the stakeholders' goals depending on them. This also enabled a better prioritization of development efforts while increasing system effectiveness. The system goals were expanded with a UCM process view, enabling the analysis of the current controls and acting as a stepping stone towards systemic safety analysis.

The development process of FinTech systems should be improved by implementing systemic safety analysis approaches such as STPA [6], which ensures that controls (in the form of safety requirements/constraints) on the system operations are introduced as early as possible during the development process.

The results of the a safety-based design should then be clearly communicated to the regulators. Assurance cases describe the argumentation on system properties in a structured manner. Although many notations and tools have been provided in order to create structured assurance arguments [9], Feodoroff has proposed that GRL goal models can document argumentations and justifications (of safety and other qualities) as part of design rationales rather than in other formats, which lack the ontological richness of URN, while also preventing assurance case development activities that may be redundant [2,3]. As previous experience with the application of URN in a regulatory compliance context has shown [1], providing regulators with (objective) evidence and their links to qualities in terms of URN models would help attain a clearer picture of the system and decide on its acceptability of safety risks.

References

1. Akhigbe, O., Amyot, D., Richards, G.: A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance. Requirements Engineering **24**(4), 459–481 (2019). https://doi.org/10.1007/s00766-018-0294-1
2. Feodoroff, R.: Intentional enterprise architecture. In: 2016 Annual IEEE Systems Conference (SysCon). pp. 1–8. IEEE (2016)
3. Feodoroff, R.: URN in place of GSN - Design Rationale versus Assurance Argument (2016). https://doi.org/10.13140/RG.2.1.1378.6480
4. Haentjens, M., de Graaf, T., Kokorin, I.: The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them. Singapore Journal of Legal Studies (2020). https://doi.org/10.2139/ssrn.3589381
5. Horkoff, J., et al.: Goal-oriented requirements engineering: an extended systematic mapping study. Requirements Engineering **24**(2), 133–160 (2019). https://doi.org/10.1007/s00766-017-0280-z
6. Leveson, N.G.: Engineering a safer world: Systems thinking applied to safety. The MIT Press (2016)
7. Office of the Comptroller of the Currency: Custody services – comptroller's handbook (2002)
8. Rauchs, M., Blandin, A., Klein, K., Pieters, G.C., Recanatini, M., Zhang, B.Z.: 2nd global cryptoasset benchmarking study. Cambridge Centre for Alternative Finance (CCAF) (2018). https://doi.org/10.2139/ssrn.3306125
9. Rinehart, D.J., Knight, J.C., Rowanhill, J.: Current practices in constructing and evaluating assurance cases with applications to aviation. Tech. Rep. CR2015-218678, NASA (2015), https://ntrs.nasa.gov/search.jsp?R=20150002819
10. Stensrud, E., et al.: Towards goal-based software safety certification based on prescriptive standards. In: 2011 First International Workshop on Software Certification. pp. 13–18. IEEE CS (2011). https://doi.org/10.1109/WoSoCER.2011.7