IRIS AperTO

UNIVERSITÀ DEGLI STUDI DI TORINO

AperTO - Archivio Istituzionale Open Access dell'Università di Torino

Supporting the Analysis of Risks of Violation in Business Protocols: the MiFID Case Study

This is the author's manuscript

Original Citation:

Availability:

This version is available http://hdl.handle.net/2318/117172 since 2016-06-27T23:36:08Z

Publisher:

Springer

Published version:

DOI:10.1007/978-3-7908-2789-7_59

Terms of use:

Open Access

Anyone can freely access the full text of works made available as "Open Access". Works made available under a Creative Commons license can be used according to the terms and conditions of said license. Use of all other works requires consent of the right holder (author or publisher) if not exempted from copyright protection by the applicable law.

(Article begins on next page)

12 October 2024

IRIS AperTO

UNIVERSITÀ DEGLI STUDI DI TORINO

This is the author's final version of the contribution published as:

Matteo Baldoni, Cristina Baroglio, Elisa Marengo, and Viviana Patti. Supporting the Analysis of Risks of Violation in Business Protocols: the MiFID Case Study. In M. De Marco, D. Te'eni, V. Albano, and S. Za, editors, Information Systems: Crossroads for Organization, Management, Accounting and Engineering, pages 545-553. Springer, 2012. ISBN: 978-3-7908-2788-0, DOI: 10.1007/978-3-7908-2789-7_59

The publisher's version is available at:
http://dx.doi.org/110.1007/978-3-7908-2789-7_59

When citing, please refer to the published version.

Link to this full text:
http://hdl.handle.net/2318/117172

This full text was downloaded from iris-AperTO: https://iris.unito.it/

iris-AperTO

University of Turin's Institutional Research Information System and Open Access Institutional Repository

Supporting the analysis of risks of violation in business protocols: the MiFID case study

Matteo Baldoni, Cristina Baroglio, Elisa Marengo, and Viviana Patti

Abstract – Enterprises and especially banks are subject to a number of regulations, with multilevel nature which continuously change. They must not only to adapt their business processes to the regulations and their changes but also to evaluate the risks of violation of the new rules and to account for responsibilities. This work proposes a formal framework for modeling business interactions ruled by protocols that, being based on the notions of commitment and responsibility, supports the analysis of risks of violation when a new regulation is issued. We provide a software tool for the visualization of the "risk space" and apply the approach to a real-work case study in the banking sector.

1 Introduction

Business processes involve autonomous partners with heterogeneous software designs and implementations. In many practical settings, the reality in which business processes operate is characterized by a high degree of regulation. This is, for instance, the case of banking and of trading services. The single organization needs to actively determine its processes on a permanent basis, to understand how regulations impact on the internal organization, to reason about possible *risks of violation*, and to ensure *compliance* to directives and laws. In such cases, the specification of the business interaction acquires a normative value and is commonly referred to as *business protocol*. Traditionally, business protocols are tackled by means of BPMS adopting standardized notations. Unfortunately these approaches are characterized by high rigidity; they do not account for the decisional processes nor for responsibilities. Instead, business protocols should enable a *flexible enactment*, to allow the interacting parties, who are heterogeneous, autonomous, and basically

Matteo Baldoni, Cristina Baroglio, Elisa Marengo, and Viviana Patti
Dipartimento di Informatica, Università degli Studi di Torino e-mail: {baldoni, baroglio, emarengo, patti}@di.unito.it

self-interested entities, to find the way of interacting that better suits their characteristics and requirements, and to profit of opportunities. Moreover, business protocols must be *modular* in a way that simplifies keeping them compliant to regulations, which often change along time. Let us consider the case of directives issued by supranational authorities and institutions, these *graft* onto protocols, by adding new activities which are interleaved with those of the previous protocols. Traditional approaches make protocols not suitable to easily take in new regulations because the composition techniques, that can be applied, easily impose unnecessary orderings of the interactions, by and large, require to rewrite the protocols from scratch.

In this work we propose to use *commitment-based protocols* that include temporal regulations [3]. These are fundamental in highly regulated contexts because they allow the specification of those behavioral constraints that are foreseen by norms. For this framework we developed a tool (available at http://www.di.unito.it/˜alice/2CL) for allowing the business analyst to visualize and study all the possible enactments of a protocol, in order to detecting the possible violations. The interaction of a set of parties complies to a business protocol (i.e. it causes no violation) if, in the end, all the commitments they have taken were fulfilled and no temporal regulation was broken. The analysis of possible violations amounts to the identification of the risks the interaction could encounter. The evaluation of such risks will allow the definition of operational strategies, that will affect the business process, by, alternatively, preventing the occurrence of violations (*regimentation*) or implementing alerting mechanisms (*enforcement*) [8]. The tool was applied to the MiFID case study, which is one of the benchmark case studies of the ICT4LAW project (http://www.ict4law.org). MiFID stands for the Markets in Financial Instruments Directive, directive number 2004/39/EC [1], issued by the European Commission within the Financial Services Action Plan, which represents a fundamental step in the creation of an integrated and harmonized financial market within EU.

The paper is organized as follows. Section 2 introduces MiFID, models a sales protocol pre-existing MiFID, and then grafts MiFID into this protocol. Section 3 shows the outcome of the tool we developed and the kinds of reasoning that this supports. Conclusions and related works end the paper.

2 Modeling MiFID

In this work we adopt the approach to the representation of the *business protocol* that is discussed in [2, 3], and which is based on *commitments*. Commitments are directed from a debtor to a creditor. The notation $C(x,y,r,p)$ denotes that agent x commits to an agent y to bring about consequent condition p when the antecedent condition r holds. When r equals $true$, we use the short notation $C(x,y,p)$. The business partners share a social state that contains commitments and other literals that are relevant to their interaction. Every partner can affect the social state by executing actions, whose definition is given in terms of operations onto the social state, see [13]. The partners' behavior is affected by commitments, which have a *regu-*

lative nature, in that debtors should act in accordance with the commitments they have taken. Moreover, the proposal is characterized by a regulative specification that explicitly foresees the representation of temporal constraints among commitments/facts. Such temporal regulations represent, as we will see, those "grafting points" that allow the accommodation of a new regulation inside a business protocol.

Definition 1 (Business protocol). A business protocol P is a tuple $\langle Ro, F, A, C \rangle$, where Ro is a set of roles, identifying the interacting parties, F is a set of literals (including commitments) that can occur in the social state, A is a set of actions, and C is a set of constraints.

The set of social actions A, defined on F and on Ro, forms the *constitutive specification* of the protocol, while the set of constraints C, defined on F and on Ro too, forms the *regulative specification* of the protocol. We assume that facts persist in the social state, they denote observations about events that occurred.

2.1 Pre-MiFID sale business protocol.

Let us begin by presenting a sales business protocol, that was legal before the introduction of MiFID. The actions involve three parties: an investor (*inv*), an intermediary (the financial promoter fp), and a bank (*bank*). This protocol foresees an initial state containing a commitment, $\mathsf{C}(fp, inv, invested)$, from the intermediary to the investor to find a good investment. By the action *propose_solution*, the intermediary presents a selected financial product to the investor. The proposal is characterized by a risk level, and can be rejected (*reject_proposal*) or accepted (*sign_order*). In the first case, the commitment of the intermediary is released. When the order is signed, the investor commits to the bank to respect the purchase contract ($\mathsf{C}(inv, bank, contract_ended)$). The bank is expected to countersign the contract (it does it by the action *countersign_contract*, which creates a commitment $\mathsf{C}(bank, inv, executed_order)$ from the bank to the investor to actually execute the order), and send a copy of it to the investor (*send_contract*). When the bank countersigns the contract, the initial commitment of the intermediary is discharged. Moreover, the bank is also expected to $notify$ the intermediary the contract was countersigned. The notification guarantees to the intermediary that everything was fine and he/she will get his/her commission. This should be done after the contract was sent but before the natural end of the contract. The natural end of the contract is captured by the action *end* which causes the discharge of the pending commitments of the investor and of the bank.

The *constitutive specification* of actions is given by defining their meaning in terms of how they affect the social state. The *means* construct amounts to a *counts-as* relation [10]:

(a) *propose_solution* **means** *proposed_RiskL* **if** $\neg$*proposed_RiskL* $\wedge$ $\neg$*rejected_proposal*.
(b) *reject_proposal* **means** *rejected_proposal*, RELEASE(C(*fp*, *inv*, *invested*))

if $\neg$*accepted_proposal* $\wedge$ *proposed_RiskL* $\wedge$ $\neg$*rejected_proposal*.
(c) *sign_order* **means** CREATE(C(*inv*, *bank*, *contract_ended*)), *accepted_proposal*, *order_signed* **if** $\neg$*order_signed* $\wedge$ *proposed_RiskL* $\wedge$ $\neg$*rejected_proposal*.
(d) *countersign_contract* **means** *contract_countersigned*, CREATE(C(*bank*, *inv*, *executed_order*)), *invested* **if** *order_signed* $\wedge$ *proposed_RiskL* $\wedge$ $\neg$*contract_countersigned*.
(e) *send_contract* **means** *contract_sent* **if** $\neg$*contract_sent* $\wedge$ *contract_countersigned*.
(f) *notify* **means** *notified* **if** *contract_countersigned* $\wedge$ $\neg$*notified* $\wedge$ $\neg$*contract_ended* $\wedge$ $\neg$*contract_abort*.
(g) *end* **means** *executed_order*, *contract_ended* **if** *contract_sent* $\wedge$ $\neg$*contract_ended* $\wedge$ $\neg$*contract_abort*.

The protocol also includes some temporal constraints:

(c1) $notified \rightarrow\!\bullet\ contract_ended$ (i.e. $notified$ before $contract_ended$)
(c2) $contract_sent \bullet\!\rightarrow notified$ (i.e. $notified$ in response to $contract_sent$)

These constraints give the bank the freedom to choose whether notifying the intermediary before sending the investor copy of the contract, or the other way around. In the latter case, (c2) imposes that after the contract was sent, the bank must perform the pending notification.

2.2 Grafting of MiFID.

One of the main advantages of our proposal is that it supports a *modular composition* of the protocols, which is obtained by performing a simple union of the components of the protocols (after a renaming aimed at avoiding name clashes). Intuitively, this composition amounts to the *grafting* of a new regulation inside a protocol. Let us, therefore, consider the "Markets in Financial Instruments Directive" (MiFID) [1], issued by the European Commission, and, specifically, the regulation that applies to the offer of investment services off-site. This is the case when a bank promotes and sells financial products with the help of external collaborators (called "tied agents" or intermediaries). MiFID grafts onto the previously existing financial product *sales protocols*. In other words, it affects a previously existing reality and must be accommodated with activities, that are normed by already existing regulations. It requires the enrichment of the business protocol with new, specific actions aimed at:

- identifying the investor and supplying the foreseen documentation (*interview*),
- profiling the investor (*profile*). In the profiling process, the intermediary commits to evaluate, with the help of a simulation, financial products in order to identify one that suits the client ($\mathsf{C}(fp, inv, evaluation)$), and assigns the investor a risk category (*investor_classified*).
- classifying the financial products according to the possible risk levels ($classify$).
- evaluating the proposed financial product through a simulation (*fi_evaluation*). This action commits the intermediary to propose a product with a risk level that is adequate to the investor's profile ($\mathsf{C}(fp, inv, proposed_RiskL)$).
- discarding solutions that are not adequate to the profile (*fi_discard*). In this case the intermediary's commitments will be canceled.

- verifying that the documentation, sent to the investment trust, does not contain errors or missing data (*order_verification*). If everything is right, this action commits the bank to the investor to execute.
- withdrawing a contract (*withdraw*). This action concludes a contract by aborting it and by releasing the commitment from the bank to execute the order.

The selection and evaluation of a new proposal are modeled as a new interaction.

(h) *interview* **means** *investor_identified*, *document_supplied*
if $\neg$*investor_identified* $\wedge$ $\neg$*contract_abort* $\wedge$ $\neg$*contract_ended* $\wedge$ $\neg$*rejected_proposal* $\wedge$ $\neg$*fi_discarded*.

(i) *profile* **means** CREATE(C(*fp*, *inv*, *evaluation*)), *investor_classified*
if $\neg$*investor_classified* $\wedge$ *investor_identified* $\wedge$ $\neg$*contract_ended* $\wedge$ $\neg$*contract_abort* $\wedge$ $\neg$*rejected_proposal* $\wedge$ $\neg$*fi_discarded*.

(j) *classify* **means** *classified*
if $\neg$*classified* $\wedge$ $\neg$*contract_abort* $\wedge$ $\neg$*contract_ended* $\wedge$ $\neg$*rejected_proposal* $\wedge$ $\neg$*fi_discarded* $\wedge$ $\neg$*proposed_RiskL*.

(k) *fi_evaluation* **means** CREATE(C(*fp*, *inv*, *proposed_RiskL*)), *evaluation*
if *classified* $\wedge$ *investor_identified* $\wedge$ $\neg$*evaluation* $\wedge$ $\neg$*contract_abort* $\wedge$ $\neg$*contract_ended* $\wedge$ $\neg$*rejected_proposal* $\wedge$ $\neg$*fi_discarded*.

(l) *fi_discard* **means** *fi_discarded*, CANCEL(C(*fp*, *inv*, *invested*)), CANCEL(C(*fp*, *inv*, *proposed_RiskL*)) **if** *evaluation* $\wedge$ $\neg$*proposed_RiskL* $\wedge$ $\neg$*contract_abort* $\wedge$ $\neg$*contract_ended* $\wedge$ $\neg$*fi_discarded*.

(m) *order_verification* **means** *order_verified*, CREATE(C(*bank*, *inv*, *executed_order*))
if $\neg$*order_verified* $\wedge$ *order_signed*.

(n) *withdraw* **means** *contract_abort*, RELEASE(C(*bank*, *inv*, *executed_order*)), CANCEL(C(*inv*, *bank*, *contract_ended*))
if *contract_sent* $\wedge$ $\neg$*contract_ended* $\wedge$ $\neg$*contract_abort*.

Actions *(h–l)* should be executed before the actual sale occurs, while *(m–n)* complete the sales process but MiFID does not have the power to modify the actions which implement a sale. The integration of the new directive with the previous regulation is, therefore, done by means of a set of 2CL constraints relating facts and commitments: in particular, those pertaining MiFID and those pertaining sales:

(c3) $\mathsf{C}(fp, inv, invested) \bullet\!\!\rightarrow investor_identified \wedge document_supplied$
(c4) $investor_classified \rightarrow\!\!\bullet\ \mathsf{C}(fp, inv, propose_riskL)$
(c5) $evaluation \wedge \neg fi_discarded \rightarrow\!\!\bullet\ proposed_RiskL$
(c6) $order_verified \rightarrow\!\!\bullet\ contract_countersigned$

(c3) states that once the intermediary took the commitment to serve the investor, he/she must have the investor identified and must supply the necessary documentation to him/her. (c4) expresses the fact that before committing to propose a solution with a certain degree of risk, the investor must have been classified. (c5) states that before proposing a financial product it is necessary to have it positively evaluated by the simulation. Finally, before the contract is countersigned by the bank, the data of the order must have been verified. The grafting of MiFID inside the sales protocol is given by the union of the respective components, in particular: actions (a) – (g) with (h) – (n); constraints (c1) – (c2) with (c3) – (c6).

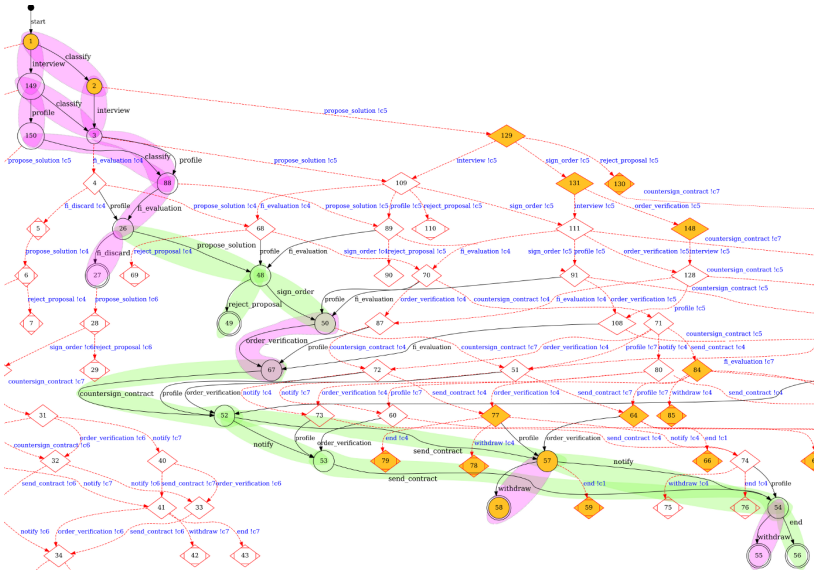

Fig. 1 Excerpt of MiFID risk space. High resolution images at http://www.di.unito.it/~alice/2CL.

3 Detecting Risks of violation

The developed model allows reasoning about the risks of violation that are introduced by the introduction of new regulations. So, for instance, what happens if an intermediary buys a financial product for a client, violating some of the constraints imposed by MiFID? The *sale is valid*, the client results to be the owner of the product. This happens because MiFID does not define *sales* (sales are defined by a different regulation) but dictates how the interaction with the client should be carried on. So, the violation does not affect the sale directly but creates both a *risk of sanction* and an *risk of exposure* for the intermediary. This is witnessed by a sentence by the Italian Supreme Court (*Cassazione civile a sezioni unite*, num. 26724 and 26725 [6]) which decided that in case of violations, like the above, if the client was economically damaged he/she can ask for a compensation and, in the most serious cases, for the cancellation of the contract between the client and the intermediary.

Basically, in our model we identify two kinds of violation: a commitment is not satisfied, a constraint is not respected. The tool that we developed allows exploring all the possible executions of a business protocol, showing both kinds of violations. Technically, it is an extension of Winikoff et al.'s enhanced commitment machine [12], implementated in *tuProlog*, which can interpret 2CL business protocols by means of a parser written in Java. The tool produces a graph that shows all the possible executions visualizing the "risk space". Figure 1 reports part of the graph obtained in the case of MiFID. Each state represents a possible configuration of

the interaction. Arrows correspond to actions and are directed. The source is a state where the "if" condition of the action labelling the arc holds. The target is, instead, the state obtained by applying the meaning of the executed action to the source state. Basically, black arrows denote legal moves. States that are drawn as diamonds with an incoming red arrow (e.g. states 129 and 77) represent the fact that a *before* constraint, or a *cause* constraint or their negation has been violated. Some states are yellow (e.g. 129 and 57), the meaning (independently from the shape) is that some *response* constraints or a *cause* constraint are not fulfilled yet. Yellow states with a single outline (e.g. 1 and 149), independently from the shape, mean that there are some active commitments (not discharged, released or cancelled). States with a double outline (independently from the shape) do not contain any active commitment (e.g. 27, 58, 79). Final acceptable states are, therefore, white and are denoted by double circles to express that there is no active commitment and all constraints are satisfied (e.g. 55, 56). A legal path connects the initial state with one of the final states and is made by all black arrows.

The legal executions are highlighted in green and pink. Notice how the actions of MiFID (highlighted in green) are immersed in the original sales protocol (highlighted in pink). As the figure shows, *classify* and *profile* must be executed before proposing a product but since there is no relation between them, they can be executed in any order. The protocol, however, does not need to specify explicitly each of the interleavings. Moreover, state 58 is not final: its color tells us that some commitment is not satisfied yet but since no action is executable, this state is a *cul-de-sac* to be avoided. Instead, proposing a solution when being in state 3 (right after interview and classification) violates constraint (c4) imposed by MiFID.

By analyzing the graph, the designer can identify the points where it could be helpful to intervene to reduce the possible violations, for instance, by applying enforcement policies or by regimenting some steps. For example, one action on which it would make sense to intervene is *propose_solution*. The reason is that most of illegal paths start from a bad use of this action. Of course, this choice depends on many factors (e.g. the cost of implementing the prospected solution, the time needed to update the software) that are out of the scope of the directive.

4 Conclusion and Related Works

We have proposed a declarative approach to business protocol specification that extends [11] by explicitly including 2CL temporal regulations. We implemented a tuProlog extended commitment machine, which was applied to the MiFID case study, whose output allows the analysis of the business protocol and of possible violations. Indeed, in these contexts it is important to define mechanisms for detecting possible violations and decide about possible regimentations/enforcements. One of the main advantages of the declarative approach, that we have proposed for the representation of business protocols, is that it supports a modular composition of such protocols, as hoped for in [9]. Another advancement w.r.t. the literature is that

we developed an analysis tool, which supports the business analyst in performing task like: understanding the impact of new regulations on the business protocol or deciding about enforcement policies or regimentation.

Telang and Singh [11] proposed a commitment-based approach to representing business protocols and identified a set of common patterns of interaction, that can be used by the business analyst. Along this line, also [4] proposes commitment patterns that capture common business patterns, showing which robustness requirements are met by each of them. These requirements are supposed to guide the protocol designer in the selection and composition process. Concerning composition, [14] proposes temporal operators to compose the data flow in a commitment-based approach. The use of expressive temporal constraints allows going one step beyond the ones above thanks to a finer-grained representation of the regulations. This is an added value in the modeling of business interactions because it enables the embedding of regulations that stratify along time.

Recently, many works, like [5, 7], focused on the problem of verifying the compliance of a business process to a body of norms. This issue is different in that the business process is rigidly modeled as a (YAWL or BPM) workflow, and the verification aims at checking if this process strictly respects the norms, providing, in some cases, a yes or no answer and, in some others, a degree of compliance.

References

1. Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments. *Official Journal of the European Union*, L145:1–44.
2. M. Baldoni, C. Baroglio, and E. Marengo. Behavior-Oriented Commitment-based Protocols. In *Proc. of ECAI*, pages 137–142. IOS Press, 2010.
3. M. Baldoni, C. Baroglio, E. Marengo, and V. . Patti. Constitutive and Regulative Specifications of Commitment Protocols: a Decoupled Approach. *ACM Trans. on Int. Sys. and Tech.*, 2011.
4. A. K. Chopra and M. P. Singh. Specifying and applying commitment-based business patterns. In *Proc. of AAMAS*. IFAAMAS, 2011.
5. D. D'Aprile, L. Giordano, V. Gliozzi, *et al.* Verifying business process compliance by reasoning about actions. In *Proc. of CLIMA*, pages 99–116. Springer, 2010.
6. G. Gibilaro. Cassazione Civile Sentenza, Sez. SS.UU., 19/12/2007, n. 26724 e 26725. Intermediazione finanziaria, nullità del contratto e risarcimento del danno, 2007.
7. G. Governatori. Law, Logic and Business Processes. In *Proc. of Requirements Engineering and Law, RELAW 2010*, pages 1–10. IEEE, 2010.
8. A. J. I. Jones and M. Sergot. *On the characterization of law and computer systems: the normative systems perspective*, pages 275–307. John Wiley & Sons, Inc., 1994.
9. T. Miller and J. McGinnis. Amongst first-class protocols. In *Proc. of Eng. Societies in the Agents World VIII*, volume 4995 of *LNCS*, pages 208–223. Springer, 2008.
10. J. Searle. *The construction of social reality*. Free Press, New York, 1995.
11. P. R. Telang and M. P. Singh. Abstracting Business Modeling Patterns from RosettaNet. In *Service-Oriented Computing: Agents, Semantics, and Engineering*, 2010.
12. M. Winikoff, W. Liu, and J. Harland. Enhancing Commitment Machines. In *In Proc. of DALT 2004*, volume 3476 of *LNCS*, pages 198–220. Springer, 2004.
13. P. Yolum and M. P. Singh. Commitment Machines. In *Intelligent Agents VIII, Proc. of ATAL*, volume 2333 of *LNCS*, pages 235–247. Springer, 2001.

14. N. V. Desai, A. K. Chopra, M. Arrott, B. Specht, and M. P. Singh. Engineering Foreign Exchange Processes via Commitment Protocols. In *SCC 2007*, pages 514–521.