

Thou Shalt is not You Will

Guido Governatori

Bologna, 8 January 2012



Australian Government
Department of Broadband,
Communications and the Digital Economy
Australian Research Council

NICTA Funding and Supporting Members and Partners



- Definition of (business process) compliance
- Process specifications
- Normative requirements
- Modelling Norms in (Linear) Temporal Logic

What is Compliance?



Ensuring that business operations, processes, and practices are in accordance with a given prescriptive (often legal) document

Regulatory

- Basel II
- Sarbanes-Oxley
- OFAC (USA Patriot Act)
- OSFI “blocked entity” lists
- HIPAA
- Graham-Leach-Bliley

Standards

- Best practice models
- SAP solution maps
- ISO 9000
- Medical guidelines

Contracts

- Service Agreement
- Customer Contract
- Warranty
- Insurance Policy
- Business Partnership

How to ensure compliance?



Compliance is a relationship between two sets of specifications

Alignment of formal specifications for business processes and formal specifications for prescriptive (legal) documents.

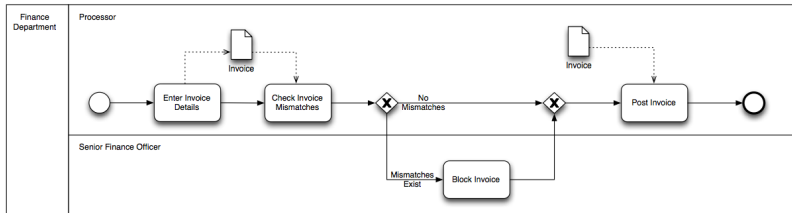
- Conceptually sound representation of processes
- Conceptually sound representation of and reasoning with norms

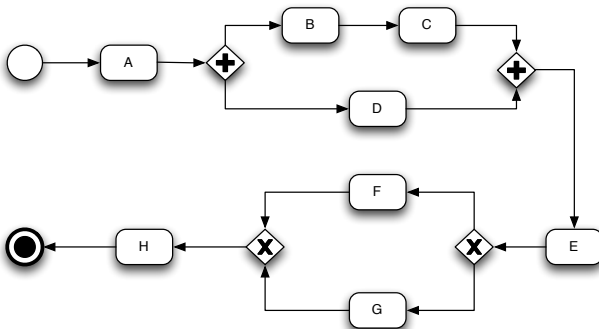
Part I

Business Process Models

Self-contained, temporal and logical order in which a set of activities are executed to achieve a business goal. It describes:

- What needs be done and when (control flows)
- What we need to work on (data)
- Who is doing the work (human and system resources)





$t_1: A, B, C, D, E, F, H$

$t_2: A, D, B, C, E, G, H$

$t_3: A, D, B, C, E, F, H$

...

Trace:

From sequence of tasks to sequence of states

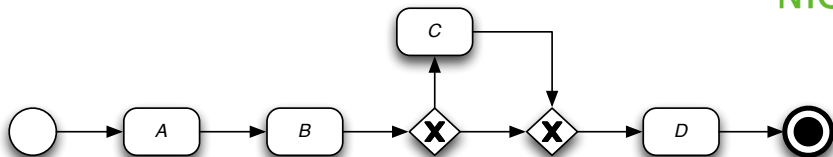


Let Lit be a set of literals, T be the set of traces of a process and $\mathbb{N}$ be the set of natural numbers

$$State: T \times \mathbb{N} \mapsto 2^{Lit}$$

The function *State* returns the set of literals describing “what’s going on in a trace t after the execution of the n -th task in the process”.

Example



Tasks

- A: “turn the light on”
- B: “check if glass is empty”
- C: “fill glass with water”
- D: “turn glass upside-down”

Propositions

- p : “the light is on”
- q : “the glass is full”

Trace 1: $\langle A, B, D \rangle$

Trace 2: $\langle A, B, C, D \rangle$

- $State(i, 1) = \{p\}, i \in \{1, 2\}$
- $State(1, 2) = \{p, q\}$
- $State(2, 2) = \{p, \neg q\}$
- $State(2, 3) = \{p, q\}$
- $State(1, 3) = \{p, \neg q\}$
- $State(2, 4) = \{p, \neg q\}$

Part II

Modelling Norms

Norms are modelled as **if ... then** rules

$$A_1, \dots, A_n \Rightarrow C$$

- norms are defeasible (handling exceptions)
- two types of norms
 - constitutive rules: defining terms used in a legal context
 - prescriptive rules: defining “normative effects” (i.e., obligations, permissions, prohibitions ...)

Defeasibility: Reasonable results with minimum effort



TELECOMMUNICATIONS CONSUMER PROTECTIONS CODE (C628:2012)

Section 2.1. Definitions

Complaint means an expression of dissatisfaction made to a Supplier in relation to its Telecommunications Products or the complaints handling process itself, where a response or Resolution is explicitly or implicitly expected by the Consumer.

An initial call to a provider to request a service or information or to request support is not necessarily a Complaint. An initial call to report a fault or service difficulty is not a Complaint. However, if a Customer advises that they want this initial call treated as a Complaint, the Supplier will also treat this initial call as a Complaint.

If a Supplier is uncertain, a Supplier must ask a Customer if they wish to make a Complaint and must rely on the Customer's response.

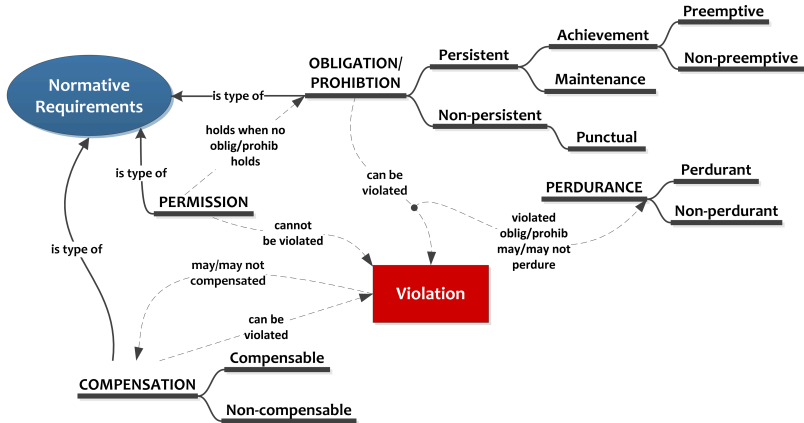
NATIONAL CONSUMER CREDIT PROTECTION ACT 2009 (Act No. 134 of 2009) Section 29

- (1) A person must not engage in a credit activity if the person does not hold a licence authorising the person to engage in the credit activity.
- (3) For the purposes of subsections (1) and (2), it is a defence if:
 - (a) the person engages in the credit activity on behalf of another person (the principal); and
 - (b) the person is:
 - (i) an employee or director of the principal or of a related body corporate of the principal; or
 - (ii) a credit representative of the principal; and . . .

Obligation A situation, an act, or a course of action to which a bearer is legally bound, and if it is not achieved or performed results in a violation.

Prohibition A situation, an act, or a course of action which a bearer should avoid, and if it is achieved results in a violation.

Permission Something is permitted if the obligation or the prohibition to the contrary does not hold.



Let Lit be a set of literals, T be the set of traces of a process and $\mathbb{N}$ be the set of natural numbers

$$Force: T \times \mathbb{N} \mapsto 2^{Lit}$$

The function *Force* returns the set of literals describing what is obligatory for a particular task.

- An **immediate** (or punctual or non-persistent) obligation must be satisfied in the task where it occurs.
'complaints in person or by phone must be acknowledged immediately'
- A **persistent** obligation is activated and it remain in force in the future after it has been activated.
'A service provider must not disclose personal information without the written consent of the customer'

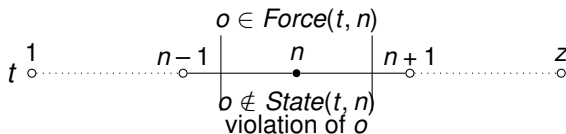
Definition (Punctual Obligation)

An obligation o is a **punctual obligation** in t if and only if

$$\exists n \in \mathbb{N} : o \notin \text{Force}(t, n-1), o \notin \text{Force}(t, n+1), o \in \text{Force}(t, n).$$

A punctual obligation o is **violated** in t if and only if $o \notin \text{State}(t, n)$.

Graphical Illustration of a Punctual Obligation



Persistent Obligations: Achievement vs Maintenance



- For an **achievement obligation**, a certain condition must occur at least once before the deadline
'Customers must pay before the delivery of the good, after receiving the invoice'
- For **maintenance obligations**, a certain condition must obtain during all instants before the deadline:
'After opening a bank account, customers must keep a positive balance until bank charges are taken out'

Definition (Maintenance Obligation)

An obligation o is a **maintenance obligation** in t if and only if

$$\begin{aligned} \exists n, m \in \mathbb{N} : n < m, \\ o \notin \text{Force}(t, n-1), \\ o \notin \text{Force}(t, m+1), \\ \forall k : n \leq k \leq m, o \in \text{Force}(t, k) \end{aligned}$$

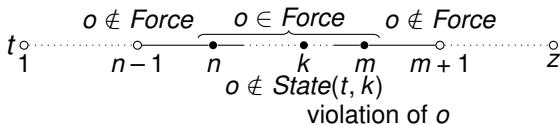
A maintenance obligation o is **violated** in t if and only if

$$\exists k : n \leq k \leq m, o \notin \text{State}(t, k).$$

It is possible to relax/strengthen the condition by dropping the conditions on m .

Maintenance obligations can be used to model prohibitions.

Graphical Illustration of a Maintenance Obligation



Achievement Obligations:

Preemptive vs Non-preemptive



- **preemptive obligations:** the fulfillment of an obligation can happen before the obligation has been triggered.
 - (1) A report under section 53 must be given:
 - (a) if the movement of the physical currency is to be effected by a person bringing the physical currency into Australia with the person—at the time worked out under subsection (2); or
 - [...]
 - (d) in any other case—at any time before the movement of the physical currency takes place.'
- **non preemptive obligations:** the fulfillment of an obligation can happen only after the obligation has been triggered.

'Executors and administrators of a decedent's estate will be required to give notice to each beneficiary named in the Will within 60 days after the date when an order admitting a will to probate has been signed.'

Definition (Achievement Obligation)

An obligation o is an **achievement obligation** in t if and only if

$$\begin{aligned} \exists n, m \in \mathbb{N} : n < m, \\ o \notin \text{Force}(t, n-1), \\ o \notin \text{Force}(t, m+1), \\ \forall k : n \leq k \leq m, o \in \text{Force}(t, k) \end{aligned}$$

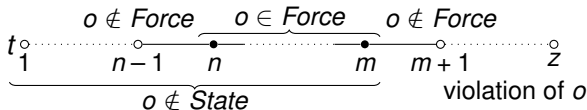
An achievement obligation o is **violated** in t if and only if

- o is preemptive and $\forall k : k \leq m, o \notin \text{State}(t, k)$;
- o is non-preemptive and $\forall k : n \leq k \leq m, o \notin \text{State}(t, k)$.

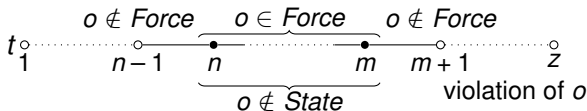
Graphical Illustration of Achievement Obligations



Achievement preemptive



Achievement non-preemptive



- **perdurant obligation:** the violation of the obligation does not extinguish the obligation itself.
'A billing error must be fixed in the next billing cycle'
- **non-perdurant obligation:** the violation of the obligation terminates the obligation.
'The assignment must be submitted by the due date'

Definition (Perdurant Obligation)

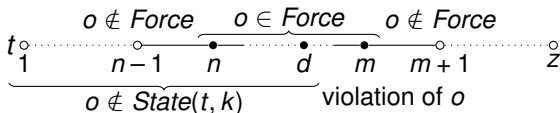
An obligation o is a **perdurant obligation** in t if and only if

$$\begin{aligned} \exists n, m \in \mathbb{N} : n < m, \\ o \notin \text{Force}(t, n-1), \\ o \notin \text{Force}(t, m+1), \\ \forall k : n \leq k \leq m, o \in \text{Force}(t, k) \end{aligned}$$

A perdurant obligation o is **violated** in t if and only if

$$\exists k : n < k < m, \forall j, j \leq k, o \notin \text{State}(t, j)$$

Graphical Illustration of Perdurant Obligations



- **compensable obligations:** fulfilling the penalty related to the violation of the obligation makes the process compliant.
'Each complaint must be either resolved or escalated and reported to the Telecommunication Ombudsmen'
- **non-compensable obligations:** violating the obligation makes the process non-compliant.
'To pass the course a student has to pass the final exam'

TCPC 2012, Section 8.1.1

...implement, operate and comply with a Complaint handling process that:

(vii) requires all Complaints to be:

- A. Resolved in an objective, efficient and fair manner; and
- B. escalated and managed under the Supplier's internal escalation process if requested by the Consumer or a former Customer.

YAWL Deed of Assignment, Clause 5.2.

Each Contributor indemnifies and will defend the Foundation against any claim, liability, loss, damages, cost and expenses suffered or incurred by the Foundation as a result of any breach of the warranties given by the Contributor under **clause 5.1**.

Definition (Compensation)

A **compensation** is a function $Comp: Lit \mapsto 2^{Lit}$.

Definition (Compensable Obligation)

An obligation o is **compensable** in t if and only if $Comp(o) \neq \emptyset$ and $\forall o' \in Comp(o), \exists n \in \mathbb{N} : o' \in Force(t, n)$.

Definition (Compensated Obligation)

An obligation o is compensated in t if and only if it is violated and for every $o' \in Comp(o)$ either:

- 1 o' is not violated in t , or
- 2 o' is compensated in t .

Is the Proposed Compliance Semantics Appropriate?



- Mathematically the proposed classification is complete (exhaustive)
- It is supported by current legal theory
- Evaluated empirically with real life (industry scale) case study
 - formalised Chapter 8 (Complaints) of TCPC 2012
 - Modelled the compliant handling/management processes of an Australian telco

Managing Complaints Process

41 tasks, 12 decision points (xor), 2 loops
shortest trace: 6 traces longest trace (loop): 33 tasks
longest trace (no loop): 22 tasks
over 1000 traces, over 25000 states

Evaluation (2)



TCPC 2012 Chapter 8. Contains over 100 commas, plus 120 terms (in Terms and Definition Section).

Required 223 propositions, 176 rules.

Punctual Obligation	5	(5)
Achievement Obligation	90	(110)
Preemptive	41	(46)
Non preemptive	49	(64)
Non perdurant	5	(7)
Maintenance Obligation	11	(13)
Prohibition	7	(9)
Non perdurant	1	(4)
Permission	9	(16)
Compensation	2	(2)

Part III

Modelling Compliance

Given a business process and a regulation:

- How do we populate the *State*, *Force* and *Comp* functions.

Can we model the normative statements in (Linear) Temporal Logic

- $X\phi$: at the next time ϕ holds;
- $F\phi$: eventually ϕ holds (sometimes in the future ϕ); and
- $G\phi$: globally ϕ holds (always in the future ϕ).

In addition we have three binary operators:

- $\phi \text{ U } \psi$ (until): ϕ holds until ψ holds;
- $\phi \text{ W } \psi$ (weak until): ϕ holds until ψ holds and ψ might not hold.

Interdefinability

- $F\phi \equiv \phi \text{ U } \top$,
- $G\phi \equiv \neg F\neg\phi$,
- $\phi \text{ W } \psi \equiv (\phi \text{ U } \psi) \vee G\psi$

Transition system

$$TS = (S, R, v)$$

- S set of states
- $R \subseteq S \times S$ such that

$$\forall s \in S \exists t \in S: (s, t) \in R$$

- v valuation function

Fullpath (trace or run)

$$s_0, s_1, s_2 \dots \quad \text{such that } (s_i, s_{i+1}) \in R$$

$\sigma = s_0, s_1, \dots, \sigma_i$ subsequence of σ starting from the i -th element, $\sigma[i]$
 i -th element of σ

- $TS, \sigma \models p$ ($p \in Prop$) iff $p \in v(\sigma[0])$;
- $TS, \sigma \models \neg\phi$ iff $TS, \sigma \not\models \phi$;
- $TS, \sigma \models \phi \wedge \psi$ iff $TS, \sigma \models \phi$ and $TS, \sigma \models \psi$;
- $TS, \sigma \models X\phi$ iff $TS, \sigma_1 \models \phi$;
- $TS, \sigma \models \phi \cup \psi$ iff $\exists k: k \geq 0$, $TS, \sigma_k \models \psi$ and $\forall j: 0 \leq j < k$ $TS, \sigma_j \models \phi$;
- $TS, \sigma \models G\phi$ iff $\forall k \geq 0$, $TS, \sigma_k \models \phi$;
- $TS, \sigma \models F\phi$ iff $\exists k \geq 0$, $TS, \sigma_k \models \phi$;

A formula ϕ is true in a fullpath σ iff it is true at the first element of the fullpath.

A formula is true in a state S

$$TS, s \models \phi \text{ iff } \forall \sigma: \sigma[0] = s, TS, \sigma \models \phi.$$

- Temporal logic and model checking have been used to verification of software and hardware systems
- Mature technology
- Structural Compliance
- Does not distinguish normative positions
- Standard Deontic Logic can be simulated in Temporal Logic
- Permissions must always be instantiated

How do we model obligations in LTL?

- Achievement obligations: F (sometimes in the future)
- Maintenance obligations: G (always in the future)

$$Fp \equiv \neg G\neg p$$

In deontic logic the dual of obligation is permission.

$$Pp \equiv \neg O\neg p$$

Obligation implies permission

$$Op \rightarrow Pp$$

How do we model permission in LTL?

- tautologies are not obligatory (i.e., $\neg O\top$)
- obligations, prohibitions and permissions cannot be obtained from a model, but are given by bodies with the power to issue them.
In every factual model, in every path and every state in the path we have 'if planet Earth exists the Sun rises in the East'.

$$O(\textit{Earth} \rightarrow \textit{SunriseEast})$$

Who do we sue if one morning the Sun does not rise in the East?

- aggregation and distribution are problematic

$$\begin{aligned} O^a p \wedge O^a q &\not\models O^a(p \wedge q) \\ O(p \wedge q) &\not\models O p \wedge O q \end{aligned}$$

Section 1: (Prohibition to collect personal medical information)

Offence: It is an offence to collect personal medical information.

Defence: It is a defence to the prohibition of collecting personal medical information, if an entity immediately destroys the illegally collected personal medical information before making any use of the personal medical information

Section 2: An entity is permitted to collect personal medical information if the entity acts under a Court Order authorising the collection of personal medical information.

Section 3: (Prohibition to collect personal information) It is forbidden to collect personal information unless an entity is permitted to collect personal medical information.

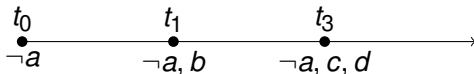
Offence: an entity collected personal information

Defence: an entity being permitted to collect personal medical information.

Definitely running out of time



- 'b' is forbidden, its violation is compensated by 'c': $O\neg b \otimes c$
- if 'a' is the case then 'b' is permitted: $a \rightarrow Pb$
- 'd' is forbidden: $O\neg d$
- if 'b' is permitted, so is 'd': $Pb \rightarrow Pd$



the trace is (weakly) compliant in LTL, but the prohibition of 'd' is violated.

