

Permanent City Research Online URL: http://openaccess.city.ac.uk/2888/

Copyright & reuse
City University London has developed City Research Online so that its users may access the research outputs of City University London's staff. Copyright © and Moral Rights for this paper are retained by the individual author(s) and/ or other copyright holders. All material in City Research Online is checked for eligibility for copyright before being made available in the live archive. URLs from City Research Online may be freely distributed and linked to from other web pages.

Versions of research
The version in City Research Online may differ from the final published version. Users are advised to check the Permanent City Research Online URL above for the status of the paper.

Enquiries
If you have any enquiries about any aspect of City Research Online, or if you wish to make contact with the author(s) of this paper, please email the team at publications@city.ac.uk.
Better Abstractions for Reusable Components & Architectures

Christos Kloukinas
Department of Computing, City University London, Northampton Square, EC1V 0HB, U.K.

Abstract

Software architecture (SA) is a crucial component of Model Driven Engineering (MDE), since it eases the communication and reuse of designs and components. However, existing languages (e.g., UML, AADL, SysML) are lacking many needed features. In particular, they provide rudimentary support for connectors, a first-class element in the components and connectors (C&C) architectural view and one of the most reusable architectural elements. This is unfortunate, since the difficult properties that need to be guaranteed for complex systems are mainly the non-functional properties, like throughput, security and dependability, which are greatly influenced by the employed connectors.

This work reviews the basic abstractions of the C&C view of SA and examines extra architectural elements which can support the detailed, explicit and separate description of behaviour, interaction and control logic.

1. Introduction

Current standards for system architectures provide only rudimentary support for architectural connectors [1], thus impeding the description of the very basic C&C view [18, 8]. Since a UML 2.0 connector is just a UML association, architects must use modelling elements other than UML connectors to describe C&C connectors [11]. AADL [6] only supports certain specific, basic connector types and does not offer the possibility to define more complex connector types, while SysML [2] does not support connectors at all.

As such, designers either forgo describing connectors altogether or combine their description with the behavioural description of the components, thus producing unnecessarily complex models. Both these approaches obstruct architectural analysis and the early estimation of the non-functional properties of a system, such as throughput, security and dependability. Such properties are, however, crucial for a proper MDE-based architectural exploration and system development or for correctly supporting Service Level Agreements in the Service Oriented paradigm. One of the reasons for this situation is that CBSE has been advocated and used longer than SA and has a much better mapping to the constructs designers use routinely, e.g., modules, classes.

Indeed, connectors are always implemented through code which is either part of or a single component, e.g., pipes. For the formal analysis of SAs, connectors are also mapped to the same structures as components, e.g., automata, which doesn’t help distinguish them. Another possible reason could be the term connector itself; this aspect of SA might have been ignored less if the term used was interaction protocol. Finally, in certain cases we tend to use simple connectors [17, 10], e.g., procedure calls, to break down a more complex one. This hides the forest for its trees, making it difficult to see the usefulness of complex connectors and leading to system specifications which are at a very low level of abstraction, as is the case with AADL [4].

For these reasons we believe it is time to revisit the C&C view of SA and the support needed from modelling languages. Thus, we reexamine the basic elements of the C&C view and suggest ways to improve them, along with new architectural elements for easing high-level system specification. After a more or less standard treatise of components, we revisit connectors and some issues which are still problematic in them. Then, before concluding, we examine configurations and the new element of control strategies.

2. Specifying Components

Components are the best supported abstraction of the C&C view. As such, the definition provided herein is largely similar to what one would expect to see in other formalisms. They contain a set of ports, \(P\), through which they are used, divided into sockets, \(P^s\), and plugs, \(P^p\). Plugs are the ports through which a component uses other components, while sockets are the ports through which it is used. Each port supports a specific interface of the computation/data related actions it can perform. Interfaces supported by plugs are the required interfaces, while those supported by sockets are the provided interfaces. Unlike UML, ports cannot both provide and require interfaces, since this complicates architectural descriptions unnecessarily. Note that the same interface may be both provided and required by a component, as for example is often the case with filters. Components also define cardinality constraints (\(Ca\)) on the number of ports which will be supporting each interface, \(Ca = I \rightarrow (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{\infty\})\). For example, a monitor has an explicit requirement to restrict the ports of the component to
3. Connectors - Interaction Protocols

As aforementioned, a connector represents an interaction protocol. As such, its foremost characteristic is a description of the different roles participating in the interaction. Roles are finite - in a protocol instantiation however there can be many, even infinite, instances of them. Each role defines the interaction primitives that components assuming that role are allowed to perform and their acceptable sequences. Roles, just like the behaviour of the components, can be modelled using different formalisms, depending on the particular interaction semantics one wishes to enforce and the analyses that need to be performed, e.g., CSP as in [1] or BIP [3]. In any case, structurally the (inter-)actions used in the definition of a role are parametric ones, e.g., send#asynch(server, id, f(arguments)), whose parameters are given specific values by the components that use them, e.g., send#asynch(server, ID1, add(1, 2, 3)). Role behavioural descriptions may also comprise private data, which effectively model the local knowledge of the roles concerning the global state of the protocol.

Another very important (and ignored) defining characteristic of a protocol is its goal, G, that it tries to achieve, which usually can be expressed in temporal logic. This goal, defines what should be achieved at the end of the protocol or the invariant of the protocol, if it is not to ever terminate. In complex protocols one may wish to describe a separate goal for each of the participating roles, G_i^R. For example, in a bus communication protocol, each sender role may have a goal to eventually transmit a message, which is different to saying that eventually a message will be transmitted, since the latter is not necessarily fair to all senders. In the request-response protocol, the goal is the reception of the response by the client, i.e., ⊤ ⊢ client:receive(response(id, r)), while the roles do not need to specify their own goals. Again, the choice of logic for describing the protocol and roles goals depends on the specific protocol; some may require support for metric time or probabilities in order to express their goal, such as “the message will be transmitted within x time units, with a probability higher than p.” Others may need epistemic operators to specify security properties as well. Explicit, formal goals can substantially help in the documentation, design and testing of roles, in the synthesis of control strategies or in run-time monitoring [16, 15, 19, 5].

Along with these two main characteristics of a protocol, i.e., its roles and goals, other useful structural characteristics can be defined as well. These have to do with extra constraints one may wish to impose upon the instances of the roles. So one can define compatibility constraints (Co) concerning which roles can be assumed by the same component, Co = R × R. For example, in order to disallow recursion, role client can be rendered incompatible with server. Or one can define cardinality constraints (Ca) on the number of role instances that can participate in the same instantiation of a protocol, e.g., #client = #server = 1, Ca = R → (N ∪ {0}) × (N ∪ {∞}). Finally, one can define constraints on the min/max number of instances of a role (IC) that a single component can assume, IC = R → (N ∪ {0}) × (N ∪ {∞}), e.g., to state that a replica must have a single vote. In other protocols, however, a single entity can assume many instances of the same role, e.g., in Blackjack, where players can split their hand and start playing as two players. It should be noted here that the aforementioned constraints are orthogonal to architectural style constraints, such as these of ACME [12]. The latter are global constraints enforcing a particular style, while the ones presented herein are local, part of the definition of a connector, required to define when a protocol is adhered to or not. So there can be cases where the connector constraints are respected but the style ones are not. An example of this is a pipe-and-filter style which requires linear sequences of pipes and filters - this cannot be described by the local connector constraints proposed herein, which can only constrain

\[
\begin{align*}
I & = \{i_1 = \{\text{long read()}, \text{void write(long)}\}, \\
P_i^* & = \{p_0^i\}, P^p = \emptyset, \\
D & = \{\text{long D}, B, \} \\
Pre & = \{(D = \_ ) \cup \text{write}(X)\}, \\
Inv & = \emptyset, \\
Post & = \{\text{read()} = D, \text{write}(X) \Rightarrow (D = \_ \cup \text{write}(X'))\}, \\
Ca & = \{(i_1, 1, 1), F = \{\text{implemented as = software}\} \}
\end{align*}
\]

where B is the following:

\[
\text{long read(void)} = \{\text{return } D; \}, \\
\text{void write(long } d) = \{D = d; \}
\]

Figure 1: A component for a simple monitor exactly one, so as to enforce serial, mutual-exclusive access. The lower bound can be zero to disallow certain actions, e.g., in an element of a product family. Along with the component’s behaviour, B and a set of private data variables, D, for specifying the preconditions (Pre), invariants (Inv) and postconditions (Post), a minimal description of a component type is \(I, P_i^*, P^p, D, B, Pre, Inv, Post, Ca, F\), where F is a list of additional features (e.g., whether it should be a hardware or software component). Figure 1 shows a simple monitor component. This example shows a basic problem with components - they almost always assume a particular interaction protocol with their environment [7]. Indeed, the interface of this component declares two procedures, which assume a request-response interaction protocol. As a consequence of this, each interface must offer actions of only a single type, i.e., either procedures or notifications, and each port must support interfaces of a similar type only.

Apart from the cardinality constraints and the requirement that all procedures of an interface should be of the same type, the definition of components herein is more or less standard and well supported by the various specification languages and tools. Indeed, it is the connector element which is not supported so well.

Another very important (and ignored) defining characteristic of a protocol is its goal, G, that it tries to achieve, which usually can be expressed in temporal logic. This goal, defines what should be achieved at the end of the protocol or the invariant of the protocol, if it is not to ever terminate. In complex protocols one may wish to describe a separate goal for each of the participating roles, $G_i^R$. For example, in a bus communication protocol, each sender role may have a goal to eventually transmit a message, which is different to saying that eventually a message will be transmitted, since the latter is not necessarily fair to all senders. In the request-response protocol, the goal is the reception of the response by the client, i.e., $\Box \Diamond$ client:receive(response(id, r)), while the roles do not need to specify their own goals. Again, the choice of logic for describing the protocol and roles goals depends on the specific protocol; some may require support for metric time or probabilities in order to express their goal, such as “the message will be transmitted within x time units, with a probability higher than p.” Others may need epistemic operators to specify security properties as well. Explicit, formal goals can substantially help in the documentation, design and testing of roles, in the synthesis of control strategies or in run-time monitoring [16, 15, 19, 5].

Along with these two main characteristics of a protocol, i.e., its roles and goals, other useful structural characteristics can be defined as well. These have to do with extra constraints one may wish to impose upon the instances of the roles. So one can define compatibility constraints (Co) concerning which roles can be assumed by the same component, $Co = R \times R$. For example, in order to disallow recursion, role client can be rendered incompatible with server. Or one can define cardinality constraints (Ca) on the number of role instances that can participate in the same instantiation of a protocol, e.g., $#client = #server = 1$, $Ca = R \rightarrow (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{\infty\})$. Finally, one can define constraints on the min/max number of instances of a role (IC) that a single component can assume, $IC = R \rightarrow (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{\infty\})$, e.g., to state that a replica must have a single vote. In other protocols, however, a single entity can assume many instances of the same role, e.g., in Blackjack, where players can split their hand and start playing as two players. It should be noted here that the aforementioned constraints are orthogonal to architectural style constraints, such as these of ACME [12]. The latter are global constraints enforcing a particular style, while the ones presented herein are local, part of the definition of a connector, required to define when a protocol is adhered to or not. So there can be cases where the connector constraints are respected but the style ones are not. An example of this is a pipe-and-filter style which requires linear sequences of pipes and filters - this cannot be described by the local connector constraints proposed herein, which can only constrain

\[
\begin{align*}
I & = \{i_1 = \{\text{long read()}, \text{void write(long)}\}, \\
P_i^* & = \{p_0^i\}, P^p = \emptyset, \\
D & = \{\text{long D}, B, \} \\
Pre & = \{(D = \_ ) \cup \text{write}(X)\}, \\
Inv & = \emptyset, \\
Post & = \{\text{read()} = D, \text{write}(X) \Rightarrow (D = \_ \cup \text{write}(X'))\}, \\
Ca & = \{(i_1, 1, 1), F = \{\text{implemented as = software}\} \}
\end{align*}
\]
protocol strategies employed by components will be trivial
the ID of the current port/component instance. Some of the
they may need information from the specific mapping, e.g.,
pings since they must be local (to be implementable) and
goals. These strategies are associated with the port-role map-
ing in the particular protocol, to achieve the role/protocol
the strategy that a component will follow when participat-
septuple defining a protocol, where

\[
\begin{align*}
G & = \{ \text{client} = \text{server} \} \\
R & = \{ \text{client} = \text{server} \} \\
C & = \{ \text{client} \} \\
C & = \{ \text{server} \} \\
IC & = \{ \text{client} \} \\
IC & = \{ \text{server} \}
\end{align*}
\]

> Where \( D \) is the following:

\[
\begin{align*}
\text{client} & = \{ \text{id} = \text{new nonce} \\
& ; \text{send\#asynch(server, id, f(args))} \\
& ; \text{receive(server, id, RESULT) ; client } \\
\text{server} & = \{ \text{receive(client, ID, F(ARGs))} \\
& ; r = F(ARGS) \\
& ; \text{send\#asynch(client, ID, r) ; server } \}
\end{align*}
\]

Figure 2: A simple request-response protocol
the system so that no local feedback loops exist (from a filter
back to itself).

More formally, \(< R, G, G^R, D, Ca, Co, IC >\) is the
sepulte defining a protocol, where \( G \) is the goal of the pro-
tocol, \( R \) the set of role names, \( G^R \) are the different role
goals, \( D \) the set of role descriptions and \( Ca, Co, IC \) the
sets of the cardinality, compatibility and instance constraints
respectively. Figure 2 shows a simple request-response con-
ector, where messages cannot be lost and therefore ac-
knowledgements or replays of messages are not required.

Connector Glue is Dangerous. Unlike [1], here a “glue”
does not link actions of different roles. This can be achieved
with other, simpler means, such as action renaming or the
use of send/receive primitives on channels, etc. In fact, glu-
es are dangerous, since they can introduce errors in the protocol
description by ignoring the distributed nature of the protocol
and requiring unimplementable behaviours [14]. This occurs
when the glue requires roles to perform an action when the
roles are unsure about the real global protocol state, i.e., the
glue’s state, due to their partial knowledge of its global state.
However, unimplementable protocols are impossible to spec-
ify when composing role descriptions directly without using a
glue, since the role actions in this case will depend neces-
sarily only upon their local knowledge.

4. Architectural Configuration

In most approaches on software architectures, the configu-
ration is more or less an assignment of component ports
to protocol roles. However, we believe that the architec-
tural configuration needs to specify a lot more than sim-
ple port-role mappings. Indeed, for each port-role mapping
there needs to be defined a control strategy for it. This is
the strategy that a component will follow when participat-
ing in the particular protocol, to achieve the role/protocol
goals. These strategies are associated with the port-role map-
pings since they must be local (to be implementable) and
they may need information from the specific mapping, e.g.,
the ID of the current port/component instance. Some of the
protocol strategies employed by components will be trivial
ones, when a protocol has no choices, like the server of the
request-response connector of Figure 2. In other cases these
strategies can be quite complicated, e.g., in real-time sys-
tems [16, 13]. There a connector describes the protocol used
by components to request resources with specific deadlines
from the platform and synchronise with each other. There-
fore, the employed strategy will be crucial in achieving the
system goals - meeting deadlines, minimising jitter, etc. In
cases where it is difficult to express the component strategies
in this distributed fashion, it may well be necessary to
redesign the connector in question with an explicit role of a
centralised controller. Then, an extra component needs to be
used which will assume the role of the controller and imple-
ment a centralised strategy for all the protocol participants.
However, it should be noted that this is not always possible
- if the components are distributed then the control aspect
itself may need to be distributed. In certain cases, both dis-
tributed and centralised control will be needed, sometimes
for better structuring the system design. For example, the
distributed strategies may define local goals of the particu-
lar components, while the central one defines the overall, sys-
tem goals. In either case, we consider the explicit descrip-
tion of component strategies to be crucial in order to accu-
rately specify highly complex systems in a well structured
manner and be able to evaluate their correctness. Indeed,
through their use we may hope to disentangle the current
spaghetti-like combination of function, interaction and con-
trol behaviour within components, leading to a more struc-
tured approach, where the functional component behaviour
is separated from the behaviour describing their interaction
with and control of their environment.

Component strategies themselves may be structured [9],
e.g., as a stack, in order to specify generic strategies first and
then specialised ones. Thus, a designer can define a strategy
to guard against deadlocks, another one for deadlines and so
on, as in [16, 13]. This will make the strategies easier to un-
derstand/optimise/validate and also make the system easier
to analyse and more robust. For example it will remove ob-
scure dependencies of different system properties with each
other, such as deadlocks being hidden by temporal relations
which can easily change during implementation.

Control Strategies Increase Reuse. Figure 3a shows a
typical model for the philosopher component of the classic
dining philosophers problem. A problem with this model

(a) Dining Philosopher

(b) Reusable Dining Philosopher

(c) A control strategy for (b)

Figure 3: Two versions of the Dining Philosopher
is that the component has considered a specific interaction strategy with its environment, specifying the order in which it obtains and releases fork resources. By using control strategies this can be delayed, as in Figure 3b, where the specific order is to be specified by the port-role strategies. This is what will allow to model a deadlock-free system by setting the strategy of even philosophers to obtain the right fork first while odd philosophers obtain the left fork first, as in Figure 3c. This solution is not applicable on the first model, which combines its behavior with the control strategy for its communication. It should be noted that this way of specifying the components does not change their functional behavior. It simply identifies their interaction needs and specifies them in a general manner, without superfluous constraints. This increases the re-usability of the component and decreases the adaptation cost of the component in a new environment. More general strategies, applied at the role level, would usually need to work at a grosser grain than the ones applied at the configuration level chosen here. Thus they would unnecessarily over-constrain the system, with negative effects on other non-functional properties. However, when applying control strategies at the configuration level one can take advantage of the extra knowledge. For example, if there were fewer instances of philosophers than forks then a safe control strategy against deadlocks could very well be the empty, i.e., non-deterministic, one.

5. Conclusions

While Software Architecture is crucial for an MDE approach to the development of high quality complex systems, current modeling languages do not provide adequate support for it. The situation is particularly bad for connectors, thus one cannot easily describe and reason about interaction protocols. Yet these are crucial for analysing and meeting system-wide, non-functional properties and for disentangling the spaghetti-like component descriptions of today. This lack of support makes it even more difficult to develop secure and dependable systems. It also hinders the analysis of these systems, which is needed to support Service Level Agreements in the Service Oriented paradigm.

This work revisits the basic notions of Software Architectures (components, connectors and configuration) and discusses how these can be better supported. It introduces constraint relations upon both the component ports and the connector roles, assigns goals to roles and requires that port-role configuration bindings have associated control strategies, which describe how the port will behave when assuming that role. The constraints help with better describing the structural properties of an element, while the strategies help in separating the interaction and control logic from the computation one, thus leading to designs which are easier to understand and analyse. Future work includes the provision of tool support and the consideration of dynamic architectures.

Acknowledgements. This work has been funded by the European Commission Information Society Technologies Programme, as part of the projects SERENITY (contract FP6-27587) and SLA@SOI (contract FP7-216556).

References

Current modelling languages for MDE, e.g., UML, AADL, SysML, have been developed with the CBSE paradigm in mind. As such they offer very little support for connectors. This is unfortunate, given how reusable connectors are and how important they are for deriving the non-functional, system properties that are of most interest at the architectural level - a level where components are usually barely defined at any detail.

This work attempts to review the situation and hopefully help refocus the architectural design support towards the use of connectors.

1 Introduction

Current CBSE languages do not support the definition of complex connectors and focus instead on specifying as many component characteristics as possible; given two resistors they will attempt to describe their impedance, weight, size, . . . However, the overall impedance is a property of how these two resistors are connected and how they communicate, i.e., a property of the connector used.

Let us use connectors to approach the architectural level - a level where components are defined as boxes. This work aims at reviewing the situation and hopefully help refocus the architectural design support towards the use of connectors.

2 XBSE - Changing the Paradigm

| Algorithms + Data Structures = Programs | Connectors + Components = Architectures |

CBSE is designed for lower-level designs and development, but at higher levels it is the connectors that matter most - so we need to develop a soft architecture approach (Connector-Based . . .) to designing system architectures. XBSE essentially follows Wirth’s statement (1), turning it into (2) with connectors standing for algorithms and components for data structures.

In both levels, there are two forms of design: top-down and bottom-up. In the former, the system is divided into smaller subsystems, each of which is then further divided into smaller parts. In the latter, the system is built up from existing components.

The distinction between these two approaches is not always clear-cut, but it is important to keep in mind that they can be used together.

3 More Support for XBSE’s Connectors

Connectors for XBSE need better support. They need at least:

- **Roles**
  - Who participates in the connector’s protocol?
  - How should they interact?

- **Goals**
  - What is the overall goal of the connector?
  - What is the local goal of each role?

- **Structural constraints**
  - Who can assume which/how many role(s)?

4 XBSE’s Configuration & Control Strategies

Architectural configuration should go beyond simple port-role mappings; it needs to add support for the control strategies to be used by components in order to meet the goals of the roles they have assumed.

5 Control Strategies & Reusability - An Example

| \(\text{CS}(N)\) = ( when \(N/2=0\) \(\text{f}[N+1].\text{take} \); \(\text{f}[N].\text{take} \) \\
| \(\text{c} \) A control strategy for (b) |

Combining control with behavior as in (a) leads to problems and reduces reuse, while separating them as in (b) & (c) solves the problem and allows the component to be used in more contexts, e.g., without a butler component.

6 How Can All These Help?

- Better separate: Increase component reuse.
- Behaviour (components), from - Reduce over-specification.
- Interaction (connectors), and - Ease the system’s control.
- Control (strategies). - Better connector description.
- Re-balance the architectural description of systems:
  - Ease communication - no more a million “wires” but a small set of well understood communication protocols.
  - Analysis depends on connectors - components sometimes abstracted to a small set of numbers, e.g., period, computation time, mean time between failure, etc.

7 Future Work - What’s Missing?

Almost everything . . . Some points in particular are:

- Should **channels** and **connectivity patterns** (star, bus, hypercube, etc.) be included? Seems so - but how best to do it?
- **Provide a link with CBSE at the level below.**
- **Explore the connections with Aspect-Oriented - cross-cutting system properties, interaction patterns** (might provide the link to CBSE).
- Model real systems - what are their connectors? Not the wires or basic communication technology like blackboard/bus but the real protocols, like Model-View-Controller (i.e., feedback control), Master-Slave, . . .
- **Good tool support** (for more than just drawing boxes).

Acknowledgments

This work has been funded by the European Commission Information Society Technologies Programme, as part of the projects:

- SERENITY (contract FP6-27587); and
- SLA@SOI (contract FP7-216556).

The author would also like to thank the anonymous reviewers for their very helpful feedback.