ON COMMUNICATION PROTOCOL
MODELLING AND DESIGN

G. JUANOLE, B. ALGAYRES, J. DUFAY
Laboratoire d'Automatique
et d'Analyse des Systèmes du C.N.R.S.
7, avenue du Colonel Roche
31077 TOULOUSE CEDEX - France

ABSTRACT
The design of a protocol in a distributed computing system requires two successive modellings: the first one concerns the distributed system architecture modelling which must make clear what are the inputs and outputs of the remote communicating entities; the second one concerns the formal modelling of the communication in the aim of a protocol verification.

The aim of this paper is to analyse the different architecture models which have been used in the different studies on protocols, to show their interest and their deficiency and finally to reach the one which allows to take into account all the environment of a protocol entity (we call, this model, the three level model). Petri nets are the formal tool which is used.

KEY-WORDS
Distributed systems ; system architecture ; modelling methodology ; protocol ; service ; Petri nets.

I. INTRODUCTION
The correct design of a protocol between distant entities in a distributed computing system requires two kinds of modelling:
- the first one concerns the modelling of the distributed system architecture: this modelling must make clear what are the inputs and outputs of each entity,
- the second one concerns the formal modelling of the protocol: this modelling must allow the protocol verification.

About the architecture model, we can, at first, refer to the ISO model i.e. a hierarchy of levels where a level (N) offers a service ((N) Service) to the level (N+1) by using the service of the level (N-1) i.e. the (N-1) Service. More precisely, in order to provide a (N) Service, two level (N) peer Entities (that we note (N)E) have a protocol to manage their cooperation ((N) protocol): the (N) protocol is achieved by using the (N-1) service. When talking about a level (N), two kinds of exchanges have to be considered:
- the exchanges of Protocol Data Units (PDU) in the level (N): that is a virtual communication,
- the exchanges of Service Primitives (Requests and Indications) with the adjacent levels (N+1) and (N-1): these ones are real exchanges.

When we want to focus on the study of a (N) protocol, it is essential to take into account, as architecture model, the simplest one to apply a formal modelling. Obviously, in the context of a (N) protocol analysis, it is impossible to take into account, for complexity reasons, the six other levels of ISO model.

The object of this paper is to describe the different architecture models which have been used along the different studies on the protocol...
cols, to show their capabilities as well as their limits and deficiencies and, from there, to reach the simplest model which must allow to perform a complete study.

We use, as formal modelling tool, the labelled Petri nets /KELL 76 - DIAZ 82/. The formal modelling is performed in two steps: first, we define the local model of an entity; second, we interconnect the local models of the two entities (global model).

We will focus our analysis on the connection establishment (ce) phase and the connection termination (ct) phase in a level (N) /BREM 78 - SUNS 78 - ALGA 82 - JUAN 83/.

II. DIFFERENT ARCHITECTURE MODELS

II.1. One level model

This model only considers the virtual communication in a level (N). It is represented on Figure 1: (N)EP is a (N)E which manages the PDU exchanges; the virtual transmission medium which connects the two (N)EP's represents the virtual link in the level (N) where the PDU's are exchanged. The virtual transmission medium can be perfect or imperfect (i.e. we can have lost PDU, abnormally delayed PDU, duplicated PDU). This model has been used by /MERL 76/ for the alternating bit protocol modelling.

The use of this model has interest in order to design a protocol with what we call good intrinsic properties.

Definition: Protocol with good intrinsic properties.

1. Accounting for a perfect medium: it is a protocol such that the PDU exchange between the two peer entities lead them in coherent states (goal of the protocol). Furthermore the goal must be reached without pollution of the medium:

   .by coherent states, in the ce phase, we want to say that each entity go in a state called "connected state" in such a way that the data transfer can normally begin i.e. if data is sent from any entity, in the "connected state", this data will normally arrive in the remote entity itself in the "connected state".

   .by coherent states, in the ct phase, we want to say that each entity go in a state called "disconnected state" only when it knows that it cannot receive more data from the remote entity.

   .we call pollution of the medium the following fact: a PDU can indefinitely stay in the medium because it is not necessary to the evolution of an entity: then in order to not have medium pollution, each PDU must have an indispensable function.

2. Accounting for an imperfect medium: in addition to the properties expressed with a perfect medium, the protocol must have the recoverability property.

However, the one level model masks the relations between the (N) protocol and the (N) service (service obtained from level (N) by level (N+1)): the different phases of a (N) protocol (connection establishment, connection termination, data transfer) are synchronised from level (N+1) which must then be necessary taken into account in order to effectuate a more complete analysis. Then we have to consider what we call a two level model (Figure 2).

II.2. Two level model

This model, used by /BOCH 78 - DANT 80 - JUAN 82/, is obtained from