Title: Defect Report concerning the Lotos description of OSI TP protocol
Source: AFNOR
Date: November 1995

1 Introduction

This defect report concerns the formal description in Lotos of the TP protocol. Such a formal description exists: it is published as annex H of the OSI TP Protocol ISO/IEC 10026-3:1992. This formal description is currently under revision.

This contribution is about the draft text of the LOTOS description for 10026-3 edition 2 (this edition included fixes from the first 86 defect reports). The source Lotos text we consider was electronically downloaded from the FTP server of the National Physical Laboratory (United Kingdom) on November 3, 1995 (version v4).

We report 11 defects in the Lotos description. These defects concern the data part of specification and the use of data in behaviour part. They have been discovered by applying the Caesar.adt compiler [Gar89, GT93, Mat93, Sig94, Sig95] to this Lotos description, and by attempting to translate the Lotos data-types defined in this description into E-Lotos data-types language, currently elaborated within E-Lotos design committee (ISO/IEC JTC1/SC21/WG7).

For each defect, we try to suggest an appropriate solution.

2 Defects found in the behaviour part

We describe in this sections the defects found in behaviour part of the OSI-TP description, due of incorrect or incomplete specification of sorts and operations.

D1: In processes `SACFRouter` (line 1672), `separator` (line 2911), and `separate` (line 2933), the constant operation `discard_PDUs` is used but not declared.

Proposed solution: A new constant operation should be defined in type `CoordinationKeys` (line 14842):

```
discard_PDUs : -> coord_key
```

Note: The `discard_PDUs` is used as value sent to the `sao` port. This port is used to synchronize the actions of SAO component process with SAO coordinating process in the body of an SAO process. The values sent at this port (without `discard_PDU's`) are all of sort `coord_key`.

D2: In process `SF_AFTokGiveInd` (line 2479), operation `IsLoser` used at lines 2530–2533:

```
return_token : bool = IsLoser(sp) and
  (IsFREE(info) or (not(valid) and (IsSTRAY(info) or IsBIDDING(info))))
```

the profile of which might be `ServicePrim` → `bool` was not declared.

Proposed solution: Substitute line:

```
return_token : bool = IsLoser(sp) and
```

by line:

```
    return_token : bool = IsLoser(info) and
```

Note: The operation `IsLoser` used is the one defined in type `SACF_info`, line 14158. It is always used with an argument of type `SACF_info` (in the process `SF_AFTokGiveInd`).

D3: In process `SACFRouter` (line 1672), the operation `get_aas` used in the two guards:

```
[(IsAAbortInd(sp) and (has_embedded_Abort(sp) or is_provider(get_aas(sp))))
      or
      IsAReleaseCnf(sp)]
```

and

```
    [IsAAbortInd(sp) and not(has_embedded_Abort(sp) and is_user(get_aas(sp)))]
```

the profile of which might be `ServicePrim` → `?` was not declared.

Proposed solution: In type `make_PDU_from_ServicePrim`, define the operation `get_aas` as follows:

```
get_aas : ServicePrim -> PDU
forall pq : PDUqueue,
  ofsort PDU
    not (IsEmpty (pq)) => get_aas (AAbortInd (pq)) = head (pq);
```

D4: In process `RespAssocEstab` (line 927) the operation `nrg` used in the guard:

```
[nrg (tp_aed)]
```

was not declared.

Proposed solution: In the type `TP_parameters`, declare the operation `nrg` as follows:

```
nrg : tp_assoc_estab_diagnostic_Opt -> bool
forall bs : bit_string
  ofsort bool
    nrg(tp_assoc_estab_diagnostic_Opt(bs)) = get_bit(4,bs);
```

3 Defects found in the data part of specification

D5: Operation `assigns_token_here` defined in type `P_ServicePrim`, has no related equations. This function is not used in the LOTOS description.

Proposed solution: Delete the declaration of this function.

D6: Operation `assigns_token_there`, defined in type `P_ServicePrim`, has no related equations. This function is not used in the LOTOS description.

Proposed solution: Delete the declaration of this function.

D7: Operation IsCAFDetachReq_clean_up, declared in type ServicePrim, line 12656, has no related equations. This function is not used in the Lotos description.

Proposed solution: Delete the declaration of this function.

D8: The operation allowed_CCR_concat declared in the type concatenation_sequences, line 14620, has no related equations, but is used later in the specification of allowed_concat function (line 14700):

```
not(IsEmpty(q)) =>
 allowed_concat(pdu . q) =
   can_begin(pdu) and allowed_tail(q) and allowed_CCR_concat(pdu . q);
```

Proposed solution: Add the missing equations for this function.

4 Defect regarding the future compatibility with the Extended-LOTOS

In this section, we highlight some characteristics of the Lotos description which, although they are not (strictly speaking) defects, do not follow the recommendation for separation of constructors and defined functions (i.e. non-constructors) formulated by the E-Lotos design committee. These characteristics may prevent the OSI-TP description from been simply translated into E-Lotos when the definition of E-Lotos will be finalized.

D9: On the left of the following equation (line 14718):

```
not(all_TPpdus(q)) =>
  key(presentation_embedding(q)) = PWithEmbeddedAPDU_ReqRsp;
```

the arguments of non-constructor key contain the non-constructor operation presentation_embedding. Should presentation_embedding be declared as a constructor, there would be the following (forbidden) equations between constructors:

```
Istp_token_give_ri(pdu) =>
  presentation_embedding(pdu . emptyPDU) = PTokenGiveReq(pdu);
not(Istp_token_give_ri(head(q))) and all_TPpdus(q) =>
  presentation_embedding(q) = PDataReq(q);
```

because both PTokenGiveReq and PDataReq are constructors.

Proposed solution: Split operation presentation_embedding into a constructor presentation_embedding0 and a non-constructor presentation_embedding as explained in [Gar89]:

```
presentation_embedding0 : PDUqueue -> ServicePrim
forall q : PDUqueue, pdu : PDU
  ofsort ServicePrimkey
    not(all_TPpdus(q)) =>
       key(presentation_embedding0(q)) = PWithEmbeddedAPDU_ReqRsp;
  ofsort ServicePrim
    presentation_embedding(q) = presentation_embedding0(q);
    Istp_token_give_ri(pdu) =>
```

```
      presentation_embedding(pdu . emptyPDU) = PTokenGiveReq(pdu);
    not(Istp_token_give_ri(head(q))) and all_TPpdus(q) =>
      presentation_embedding(q) = PDataReq(q);
```

D10: In the type `ServicePrim`, on the left of the equations:

```
CBeginReq_CRecoverRspUnknown(CBegin_req, aaid, brid) =
  CBeginReq(aaid, brid);
CBeginReq_CRecoverRspUnknown(CRecover_rsp, aaid, brid) =
  CRecoverRsp(unknown, aaid, brid);
```

the arguments of non-constructor `CBeginReq_CRecoverRspUnknown` contain the non-constructors `CBegin_req` and `CRecover_rsp`, whereas they should only contains constructors and variables.

Proposed solution: Avoid this problem by rewriting these equations as follows:

```
spk eq CBegin_req =>
  CBeginReq_CRecoverRspUnknown(spk, aaid, brid) = CBeginReq(aaid, brid);
spk eq CRecover_rsp =>
  CBeginReq_CRecoverRspUnknown(spk, aaid, brid) = CRecoverRsp(unknown,
  aaid, brid);
```

D11: In the type `make_mapping_parameter_from_ServicePrimKey`, the left part of the followings equations:

```
make_map(AAbort_ind) = abortRI;
make_map(CCommit_ind) = commitRI;
make_map(CCommit_cnf) = commitRC;
make_map(CRollback_ind) = rollbackRI;
make_map(CRollback_cnf) = rollbackRC;
make_map(CRecover_cnf) = recover_doneRC;
```

contains non-constructors (`AAbort_ind`, `CCommit_ind`, etc.), whereas they should contain only constructors and variables.

Proposed solution: Avoid this problem by rewriting these equations as follows:

```
spk eq AAbort_ind => make_map(spk) = abortRI;
spk eq CCommit_ind => make_map(spk) = commitRI;
spk eq CCommit_cnf => make_map(spk) = commitRC;
spk eq CRollback_ind => make_map(spk) = rollbackRI;
spk eq CRollback_cnf => make_map(spk) = rollbackRC;
spk eq CRecover_cnf => make_map(spk) = recover_doneRC;
```

References

[Gar89] Hubert Garavel. Compilation of LOTOS Abstract Data Types. In Son T. Vuong, editor, *Proceedings of the 2nd International Conference on Formal Description Techniques FORTE'89 (Vancouver B.C., Canada)*, pages 147–162, Amsterdam, December 1989. North-Holland.

[GT93] Hubert Garavel and Philippe Turlier. CÆSAR.ADT : un compilateur pour les types abstraits algébriques du langage LOTOS. In Rachida Dssouli and Gregor v. Bochmann, editors, *Actes du Colloque Francophone pour l'Ingénierie des Protocoles CFIP'93 (Montréal, Canada)*, 1993.

[Mat93] Radu Mateescu. Optimisation de la compilation des types abstraits algébriques du langage LOTOS. Mémoire d'ingénieur de l'Institut Polytechnique de Bucarest, VERIMAG, Grenoble, September 1993.

[Sig94] Mihaela Sighireanu. Implémentation optimisée des types abstraits algébriques du langage LOTOS. Mémoire d'ingénieur de l'Institut Polytechnique de Bucarest, VERIMAG, Grenoble, September 1994.

[Sig95] Mihaela Sighireanu. *Méthodes de représentation des types abstraits algébriques en vue de la vérification de protocoles.* DEA, UniversiteĴoseph Fourier (Grenoble), June 1995.