PROTECT Guide
Version 2.0

PART I

PROTECT Message Scenario
GENERAL PART

Version: 2.0
Date: March 17, 2005

Author:
PROTECT Secretariat
Niek C. Waagmeester
tel: +31 6 2128 1702
email: WaagmeesterN@hetnet.nl

Document Version Control

Version	Date	Release note (and description of change)
0.5	October 1995	First formal release for implementation containing the messages IFTDGN and APERAK
1.0	January 1999	Updated release with extended functionality for the messages
2.0	June 17, 2004	New release for implementation, with extended functionality for IFTDGN and APERAK and with additional messages BERMAN and WASDIS, including service segment recommendations.
2.0	March 17, 2005	Editorial changes in Part I (cover page, page 18: inter-agent-use of IFTDGN) and Parts II, III, IV, V and VI.

The PROTECT Guide version 2.0 consists of the following 6 Parts:

- PART I PROTECT Message Scenario version 2.0 - General Part – March 17, 2005 *(this document)*

and the EDIFACT Message Implementation Guides:

- PART II Dangerous Goods Notification message - IFTDGN version 2.0 – March 17, 2005
- PART III Application error and acknowledgement message - APERAK version 2.0 – March 17, 2005
- PART IV Waste disposal information message - WASDIS version 2.0 – March 17, 2005
- PART V Berth services request message – BERMAN version 2.0 - March 17, 2005

and:

- PART VI EDIFACT Message envelope segment recommendations version 2.0 – March 17, 2005.

Table of content

1 FOREWORD

This document contains the specification of the PROTECT Message Scenario.

The message scenario covers all messages required for ship operators/agents and forwarders to support the information exchange with various authorities regarding the formal and legal notification requirements for vessels, as well as requesting services from the authorities and vessel handling companies when vessels berth and/or utilise the waters under the jurisdiction of these authorities.

In view of the recent developments resulting from new legislation from IMO and EU as regards ship and port security (SOLAS/ISPS) and from EU as regards Waste management and Vessel monitoring (repealing HAZMAT), the PROTECT Group recognised the need for harmonisation of the reporting requirements to minimise implementation differences for vessel operators/agents between the participating ports.

This new version of the PROTECT Guide aims to:

1. Support by means of EDI the *new legislation* from IMO and EU pertaining to *vessel security* when vessels berth or transit through a port and pertaining to reception of ship-generate *waste*, cargo residues and sewage.
   The Guide contains the new messages BERMAN and WASDIS.
2. Take into account the evolving business requirements since the previous version of this Guide, in the areas of vessel monitoring and port handling activities (especially for dangerous goods, including dangerous goods in limited quantities, polluting and noxious substances).
   The Guide contains an update of the IFTDGN message.
3. Support the possibilities for appropriate replies to these messages.
   The Guide contains an update of the APERAK message.
4. Present an up-to-date harmonised user guide for these messages based on the available international UN/EDIFACT standards for Directories and aligned with the General Recommendations and with the Principles and Rules for the implementation of the IFTDGN and APERAK, as published by ITIGG (International Transport Messages Implementation Guidelines Group) after consultation with PROTECT.
5. Fulfil the wish of IMO's Facilitation Committee to enable global use of these messages based on common implementation guides in line with IMO standards and agreements.

The PROTECT messages are specified in separate documents, PART II to PART IV.
Each document contains the specification of both:

- the functional data content of the specific message (*data attribute list*) and
- the equivalent of that content for electronic data interchange (EDI) in *EDIFACT message* format.

The development work for this PROTECT Message Scenario has been undertaken by the PROTECT Group, which consists of a number of co-operating Port Authorities in the major N.W. European ports: Antwerp, Bremen, Hamburg, Le Havre, Felixstowe and Rotterdam and the national competent authority of Spain, representing all Spanish ports.
The Port Authorities are supported by the Port Community Systems (EDI Service Providers) in their ports: for Antwerp: SEAGHA, Bremen: DBH, Hamburg: DAKOSY, Le Havre: SOGET, Felixstowe: MCP, Rotterdam: Port infolink, Southampton: CNS and for Spain: Portel.
In the development and harmonisation process, input has been taken into account from the authorities in Japan.

2 PROTECT Message Scenario

2.1 Scope

The aim of PROTECT is to improve safety in ports and waterways by facilitating the implementation of control and monitoring systems that relevant authorities exercise over movement of vessels and dangerous goods in areas under their jurisdiction.

This chapter aims at highlighting the main functionalities addressed by the messages in the PROTECT Message Scenario.

The parties to the exchange of the messages are specified and the scenario of the messages is depicted.

2.2 Messages and parties

The messages in the scenario are exchanged between the following parties:

- the vessel operators, carriers, their agents and freight forwarders in the ports/places of call of a vessel (or barge, truck or train) and
- the competent authorities in those port/places of call, normally the Port Authority or Inland Waterway Authority.

The message scenario consists of the following messages:

1. **BERMAN message**
   Berth services request or transit request message, covering the requirements of announcing the vessel's call to the port or port area and requesting the services required for the vessel.
   The message supports the implementation by means of EDI of the notification requirements as laid down in:
   - the **IMO General Declaration, IMO FAL Form 1** (as also contained in the IMO Compendium on Facilitation and electronic business, document FAL.5/Circ.15, dated February 19, 2001 and also contained in the European Directive "on reporting formalities for ships arriving in and/or departing from ports of the Member States of the Community", Directive 2002/6/EC, dated 18 February 2002); and
   - the **International Ship and Port facility Security (ISPS) Code**, adopted by the Conference of Contracting Governments of the International Maritime Organisation (IMO) on 12 December 2002, in the amendments to the annex to the International Convention of Safety of Life at Sea (SOLAS), 1974 and as may be amended under agreed provisions and also contained in Regulation 725/2004 of the European Parliament and of the Council of 31 March 2004 "on enhancing ship and port facility security".
   - the European Directive on **'Vessel Monitoring'**, full name: European Directive establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (Directive 2002/59/EC of the European Parliament and Council, dated 27 June 2002), *as far as Annex I 'General information*' is concerned.

2. **WASDIS Message**
   Waste notification message (WASDIS message), covering the information on the ship-generated waste, cargo residues and sewage on board the vessel.
   The message supports the implementation by means of EDI of the notification requirements as laid down in:

   - the European Directive on Port Reception Facilities for ship-generated waste and cargo residues (Directive 2000/59/EC of the European Parliament and the Council, dated 27 November 2000).

3. **IFTDGN message**
   Dangerous Goods Notification message, covering the information on the dangerous and/or polluting goods carried by or to be carried by a vessel or other means of transport such as a train, truck or barge, as required by Port Authorities and Inland Water Authorities.
   The message supports the implementation by means of EDI of the notification requirements as laid down in:

   - the IMO Dangerous Goods Manifest - IMO FAL Form 7; and
   - the European Directive on 'Vessel Monitoring', full name: European Directive establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (Directive 2002/59/EC of the European Parliament and the Council, dated 27 June 2002), *as far as Annex I 'Cargo information*' is concerned.

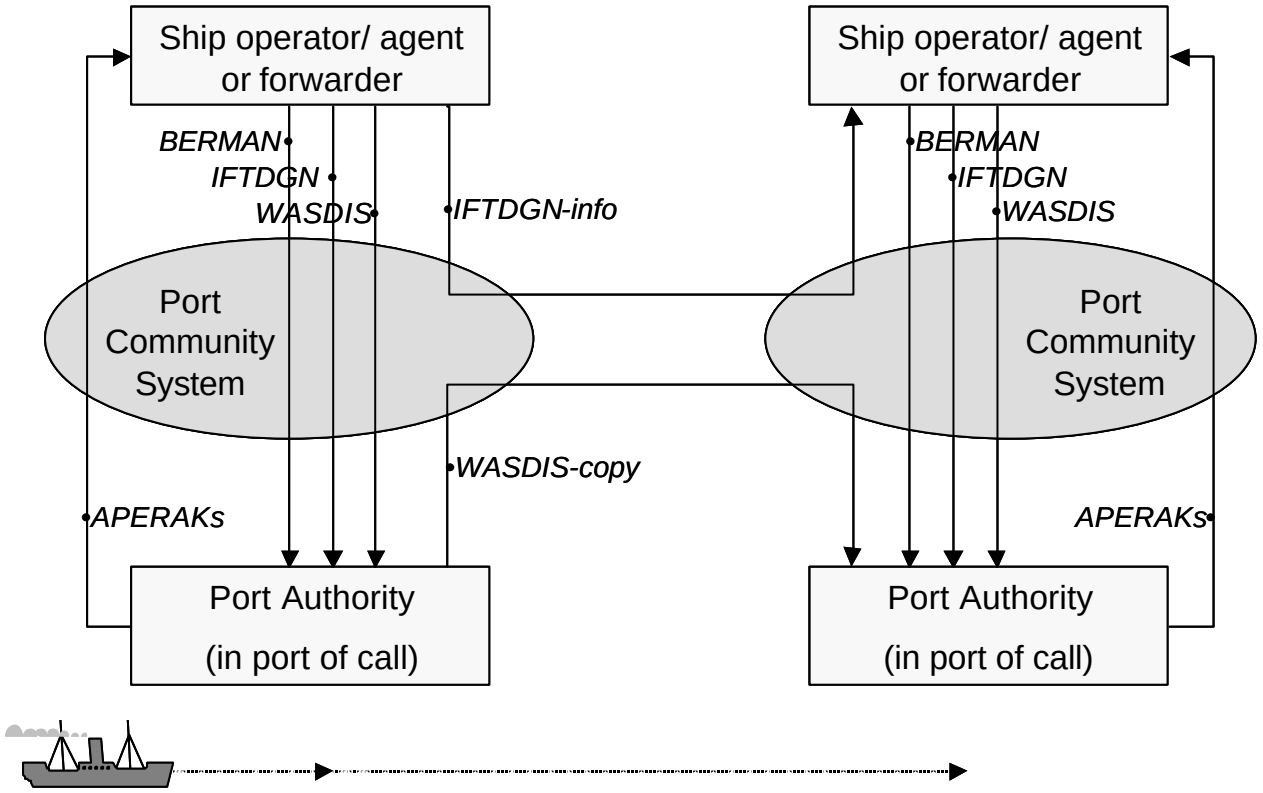
   The IFTDGN message can also be used as 'Dangerous Cargo list' exchanged between the agent in the port of call and the agent in next port(s) of call of the vessel (i.e. inter-agent use of the IFTDGN message).

4. **APERAK message**
   Application Error and Acknowledgement message, containing a reply from the authority pertaining to the processing of the received messages (IFTDGN, WASDIS and BERMAN).
   The reply can be that the received message is accepted, pending or rejected. The cause of rejection may be specified in the reply.

2.3 Scenario of messages

The scenario of the messages is depicted, showing the typical situation in which parties to the process are interconnected through the services of a Port Community System.

The following figure depicts the information flows between the parties in the scenario (using the sea mode terms for these parties):



Legend:

- BERMAN - Berth services request or transit services request message, including vessel security details as required;
- IFTDGN – Dangerous Goods Notification message;
- WASDIS – Waste Disposal message;
- IFTDGN-info – IFTDGN message that is used as 'Dangerous Cargo list' and exchanged between the agent in the port of call and the agent in next port(s) of call of the vessel (i.e. inter-agent use of the IFTDGN message);
- WASDIS-copy – WASDIS message used to inform the (competent) authority in the next port of call of the vessel in case there is clear evidence that the ship has proceeded to sea without having complied with the rules to dispose of her waste in the port of call;
- APERAK – Application Error and Acknowledgement message; each BERMAN, IFTDGN and WASDIS message will normally be replied to with an APERAK.

2.4 Maintenance role of PROTECT

The PROTECT Group will continue to act as the maintenance body for the messages (BERMAN, IFTDGN, WASDIS and APERAK).

Having established a sound platform for consultation between the Port Authorities (and their Port Community Systems/ Port EDI Service Providers), shipping lines and ITIGG, the PROTECT Group will continue to maintain and promote the implementation of PROTECT EDIFACT messages for the exchange of vessel and dangerous goods related information at an international level.

The group will maintain the messages to incorporate requirements of new or changing legislation. In addition, modifications may be introduced for practical reasons resulting from on-going consultation among Port Authorities, shipping lines and agents.

The PROTECT Group welcomes ideas and recommendations for further improvement in data interchange. Requests, questions and remarks should be directed to the PROTECT Group secretariat (see address details on the cover page of this document).

2.5 References

The UN/EDIFACT Draft Directories and Syntax Rules are published by the UN/CEFACT organisation. The UN/CEFACT organisation is the United Nations Centre for Trade Facilitation and Electronic Business.

The EDIFACT Message implementation guides, as contained in the other Parts to the PROTECT Guide, are based on the *UN/EDIFACT Draft Directory D.2003A* as published in the *United Nations Trade Data Interchange Directory* (UNTDID).

- The following interdependent documents, which are included in the *UN/EDIFACT Draft directory*, are required in order to interpret, understand and use EDIFACT messages:

    1. *UN/EDIFACT Syntax Rules* (ISO 9735), which define in concise form the standard for formatting data elements and segments into messages (Part 4, section 2.2 of UNTDID).
    2. *UN/EDIFACT Syntax Implementation Guidelines*, which expand on some of the details of the syntax rules (Part 4, section 2.3 of UNTDID).
    3. *UN/ECE UNSM (United Nations Standard Message)- General Introduction to UNSM descriptions Section 2*, which explains terms and gives definitions used in the EDIFACT standard (Part 4, section 2.6 of UNTDID).

These documents can be downloaded from the web site of the United Nations:

http://www.unece.org/trade/untdid/texts/unredi.htm

- The message specifications are also based on the Principles & Rules for the Implementation of Transport EDI messages for IFTDGN and APERAK, and on the General Recommendations, published by ITIGG in 1998-2000. At the time of publication A reference to a website for these documents did not exist at the time of this publication.
- This document including the EDIFACT Message Implementation Guides as contained in the other Parts to the PROTECT Guide can be downloaded from the PROTECT section on the web site of SMDG, the user group for shipping lines and container terminals:
  http://www.smdg.org/Protect

3 Background and context

3.1 PROTECT Policy statement

The PROTECT Group maintains ongoing studies of new business requirements in the area of vessel reporting arising from consultations with the ports.

PROTECT Group works to produce harmonised reporting requirements.

The PROTECT Group aims at minimising implementation differences for vessel operators/agents between the participating ports and providing the benefits to vessel operators/agents of making available one harmonised worldwide standard implementation guide for vessel reporting in relation to port and inland water authorities.

3.2 Recent developments

Recent developments in the area of waste management, vessel monitoring and vessel and port security induced the PROTECT group to work on harmonisation of the resulting reporting requirements.

3.2.1 Waste Directive

In the year 2000 new European legislation was adopted aiming at reducing illegal discharges of waste at sea by improving the availability and use of port reception facilities and thereby enhancing the protection of the environment.

The European Directive on Port Reception Facilities for ship-generated waste and cargo residues (Directive 2000/59/EC) was adopted on 27 November 2000 and introduced a requirement for masters of a vessel bound for European ports to notify prior to arrival a set of details of the waste being carried or generated by the vessel, such as volumes of waste oils (sludge, bilge) and garbage (food and plastics) and cargo residues, according to MARPOL Annexes, to be carried on board or discharged

MARPOL Annexes are part of Convention, officially known as the 'International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto' and known as "MARPOL 73/78".

Since the adoption of the Directive IMO approved an Annex to the MARPOL on the 'Prevention of pollution by sewage from ships'.

The PROTECT Group, with the appearance of the Directive and the MARPOL Annexes, has taken the initiative to produce an electronic message format enabling the maritime transport operator to present this information in an electronic format to the authorities in the port of call of the vessel.

The reporting requirements of the Waste Directive, presented in the text, were translated into information data attributes. The data was mapped to the WASDIS message. In view of the desired implementation of the Waste Directive, some additional data items were identified and added in the message.

In presenting this message, the PROTECT Group aims at providing the benefits to carriers of making available one worldwide standard implementation guide for waste reporting.

3.2.2 Vessel Monitoring Directive

In the aftermath of the sinking of the tanker “Erika”, the European Commission undertook several actions to improve vessel safety and the prevention and detection of pollution by ships.

A new Directive was adopted to establish a Community vessel traffic monitoring and information system (Directive 2002/59/EC, dated 27 June 2002).

This Directive repealed the so-called HAZMAT Directive (the Directive 93/75/EEC, of 13 September 1993 concerning minimum requirements for vessels bound for or leaving Community ports and carrying dangerous or polluting goods).

The new Directive significantly extends the requirements of the old HAZMAT Directive.

The Directive stipulates the reporting requirements of ships bound for or leaving a Community port with respect to carrying dangerous or polluting goods, and regarding incidents at sea, for which ship operators have the duty to make the report.

The PROTECT Group has taken on board the development work to check the new Directive for any new requirements with respect to messages, be it a new message or a message already under maintenance. There was a need to amend the existing IFTDGN and it was felt that some new data items would best fit in the functionality covered by the BERMAN message.

3.2.3 SafeSeaNet

SafeSeaNet is a project of the European Commission and several EU Member States providing a communication infrastructure between the maritime (competent) Authorities in (the ports of) the Member States for the exchange of information between these authorities in (different) Member States regarding e.g. vessel monitoring, dangerous and polluting goods (HAZMAT information) and waste delivery.

The system uses the Trans-European Networks for electronic interchange of data between administrations (IDA) and is based on XML/Internet technologies. The system has a central registry that is updated each time on arrival and departure of the vessel in a port. The registry does not hold the information on the vessel or the cargo, but only holds the pointer information as to which (port) authority holds the information on the vessel. Authorities can consult the registry and may obtain the information from the referred (Port) Authority.

SafeSeaNet does not regulate how the (Port) Authorities obtain the information to be exchanged between Authorities.

It is recognised that the PROTECT messages form the main source for the Port Authorities to be able to create the required information in XML formats to be exchanged between Authorities in Member States.

It is obvious that SafeSeaNet underpins the PROTECT policy for harmonised and standardised messages at the source of the information chain, being the vessel operators/agents. It is obvious that information exchange through the whole chain is handled electronically, be it by means of EDI (PROTECT) or by means of XML (SafeSeaNet).

It is foreseen that in the near future the SafeSeaNet system will also be used to exchange the vessel security information.

3.2.4 SOLAS/ISPS Code

Following the tragic events of 11th September 2001, the USA initiated new developments to introduce protection measures against terrorist acts. In the field of international shipping and maritime transport the prevention and countering of unlawful acts call for the implementation of new security measures.

In December 2002 IMO adopted comprehensive maritime security measures in the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (SOLAS), 1974. The Conference adopted a number of amendments to SOLAS to enter into force in July 2004.

A brand-new Chapter XI-2 "Special measures to enhance maritime security" is added containing the new International Ship and Port Facility Security Code (ISPS Code). The Code contains detailed security-related requirements for Governments, port authorities and shipping companies in a mandatory section (Part A), together with a series of guidelines about how to meet these requirements in a second, non-mandatory section (Part B).

The implementation of the ISPS Code (International Ship and Port Security Code) requires ship operators or their agents to provide certain security information to 'officers duly authorised by the Contracting Government' (i.e. the Competent Authority) prior to a call of their vessel in a port.

In the European Union the issue of maritime security was already a policy matter. The European Commission therefore supported the initiative of the IMO. The Commission recognised the need to provide a basis for harmonised interpretation and implementation of the amendments within the EU Member States, to be able to monitor implementation at Community level and to extend some of the provisions to domestic maritime transport.

Therefore, the European Commission has included the SOLAS Amendments and the ISPS Code in their proposal for a regulation of the European Parliament and the Council on "enhancing ship and port facility security". This proposal has been adopted as Regulation 725/2004 on 31 March 2004.

The PROTECT Group, with the appearance of the ISPS Code, has taken the initiative to enable the maritime transport operator to present the required security information in an electronic format to the authorities in the port of call of the vessel.
The reporting requirements of the ISPS Code, presented in the text, were translated into information data attributes. Together with other data required for a vessel when calling at a port the security information becomes an integral part of the BERMAN message. In view of the desired implementation of the ISPS Code, some additional data items for vessel security were identified and added in the message.

In presenting this message, the PROTECT Group aims at providing the benefits to carriers of making available one worldwide standard implementation guide for vessel reporting.

3.2.5 International Recognition Status

PROTECT will, as in the past, work towards recognition of the PROTECT Guide version 2.0 by IMO and ITIGG, both for the existing messages and for the new ones.

1. For existing messages (IFTDGN and APERAK)
    - IMO has recognised the IFTDGN version 1.0 as the EDI equivalent of the IMO FAL Form 7 (Dangerous Goods Declaration). This may need to be re-confirmed for the new version. PROTECT will propose to the respective IMO working groups that the new version be granted the same status.

- ITIGG and TBG3 (Transport) of UN/CEFACT may consider the messages as new input for their work on implementation guidelines. Is noted that ITIGG has not worked on new implementation guidelines since the previous versions of the messages.
- The relation with the EU for the vessel monitoring requirements incorporated in IFTDGN may need to be established.

2. For the newly developed messages (BERMAN and WASDIS)
   The BERMAN incorporates the vessel reporting requirements as laid down in the SOLAS/ISPS-Code, and the WASDIS incorporates the reporting requirements as laid down in the EU Directive on Port Reception Facilities.

   - The PROTECT Group will propose that the functionality for these messages be accepted as new IMO FAL legislation, falling under the Convention on Facilitation of International Maritime Traffic (FAL), 1965 and its amendments.
     It is noted that the IMO Facilitation Committee has already acknowledged the need for the development of a BERMAN message (28th session October-November 2000).
     With the appearance of the ISPS Code in December 2002, and the obligations to implement the ISPS Code, PROTECT has taken the initiative to incorporate the vessel security reporting requirement of the ISPS Code as an integral part of the BERMAN message.
   - The PROTECT Group will propose that new IMO FAL Forms be designed for the new message functionalities and that the BERMAN and WASDIS messages are recognised as EDI equivalents of those new IMO FAL Forms (e.g. FAL Forms 8 and 9?). It could be investigated whether FAL Form 1/CUSREP could be replaced or extended with the BERMAN functionality).

3.3 History of PROTECT

This paragraph places the recent developments as presented in previous paragraphs in a historical perspective.

3.3.1 The start of PROTECT

From the year 1988 PROTECT has been the banner under which the ports of Antwerp, Bremen, Felixstowe, Hamburg, Le Havre and Rotterdam have combined their efforts to develop a method for data exchange for vessels visiting these ports. The data contains details of dangerous goods aboard the vessels, as well as other port related information.

Concentrating on a standardised format for dangerous goods notification, the PROTECT group first developed a message framework for dangerous goods notification from the shipping lines (or their agents and forwarders) to the Port Authorities, the IFTDGN message.

To support the notification from liner agent to Port Authorities a second message was developed for the exchange of dangerous goods data between agents, the IFTIAG message. The majority of the data for both messages is essentially the same; therefore, in practice the IFTDGN can also be used for the inter-port data exchange between agents. An agent receiving the IFTDGN from an agent in another port can redirect the data selectively to notify his own port authority. He has only to merge the data he receives with data relating to the identity of the dangerous goods under his responsibility to create his notification.

The messages developed were submitted for standardisation to UN/EDIFACT through the Western European UN/EDIFACT Board, Message Development group 2 for Transport (WEEB/MD2, later called EEG2, European Experts Group 2 for Transport) and were accepted world-wide by the other regions of the EDIFACT Board in the UN/ECE/TRADE/ Working Party 4.

In mid 1994 the Port Authorities in the PROTECT ports formed the PROTECT Group supported by their Port Community Systems (EDI Service Providers) and organised through EurotransPortnet. It was realised that standardising the format for the dangerous goods notification (IFTDGN) alone was not enough to create a totally standardised notification procedure.

It was accepted that differences existed in national, local, and Port Authority legislation. These differences could not be eliminated (at least in the short term) so the objective was to harmonise the use of the IFTDGN message whilst taking account of them. This resulted in October 1995 in the version 0.5 of the PROTECT Message scenario.

An important reason for the formation of this group, apart from technical message development, was to ensure close co-operation with the container lines. The container lines are, generally speaking, highly automated; so all the necessary information is held, usually centrally, in their computer systems. As these lines use most of the PROTECT ports they would prefer to have one notification procedure for dangerous goods, common to all ports. They would then need to develop only one application in their central computer system.

Again, it became obvious that a purely local approach by each port would not lead to the main objective of a common system of electronic dangerous goods notification.

3.3.2 IMO and European Union legislation

The PROTECT Group developed the IFTDGN framework to ensure that the data requirements of each port were met in terms of national and international legislation, which

are mainly IMO-based legislation (such as IMDG, ICG and IBC Codes) as well as local port legislation.

Soon after the start of the work, it became apparent that the requirements of the so-called HAZMAT Directive of the European Union (EU Council Directive 93/75/EEC of 13 September 1993) were closely aligned to the data contained in the IFTDGN. The group then worked to determine whether the IFTDGN could also satisfy HAZMAT requirements.

The Directive demands that all ships entering European waters, bound for a European port, notify all dangerous goods on board to the National Competent Authorities (NCA) for that port. Again, on leaving a European port all dangerous goods on board have to be notified to the NCA of the port of departure.

The aim of the Directive is to facilitate search and rescue operations for ships in distress in European waters, and to assist in the limitation of environmental damage. Each European member state has to designate a National Competent Authority to which all data has to be notified.

The IFTDGN version 1.0, published in January 1999, contains changes in the message that result from a further harmonisation of the requirements to notify dangerous cargo by means of EDI in the participating PROTECT ports, and from the need to accommodate the requirements to implement the so-called HAZMAT Directive.

As a rule dangerous goods data is currently sent to the Port Authority 24 hours prior to the arrival of a ship in port. The Port Authority or Harbour Master needs this information to satisfy local or national legislation. If the Harbour Master could act as the (Local) Competent Authority, the same data can be sent either directly or on request to the National Competent Authority. In this way a double or parallel notification can be avoided.

For the IFTDGN framework to solve this problem it supports sufficient dangerous goods data to function at three legal levels:

a) Local/port bylaw legislation
b) National/international transport legislation (IMO)
c) EU-HAZMAT Directive requirements

3.3.3 Recognition from IMO and ITIGG

3.3.3.1 IMO

Co-operation between the N.W. European ports was established through the PROTECT Group. The PROTECT ports, with the further co-operation of ICHCA and IAPH, presented the PROTECT initiative to IMO (the FAL and SPI Committees) in order to make the principles of the PROTECT standardised notification available to other ports worldwide. The shipping lines require this.

As a result, in July 1997 the IMO FAL Committee *"agreed to recommend in principle the use of the IFTDGN Implementation Guide issued by PROTECT as the EDI equivalent of the IMO FAL Form 7 (Dangerous Goods Declaration)."* IMO FAL observed the proximity between the PROTECT Implementation Guide and agreed international standards: "It is recognised that the PROTECT guide may need slight modifications and enhancements, which take into account the harmonisation recommendations being developed by ITIGG."

In September 1998 the PROTECT approach for a new version *was accepted by IMO without restrictions and IMO agreed to issue an IMO Circular to distribute this Guide* as soon as it is available. This version came available as version 1.0 in January 1999.

3.3.3.2 UN/EDIFACT, ITIGG

PROTECT is permanently represented in ITIGG (International Transport Implementation Guidelines Group, a subgroup of the EDIFACT Working Group, Message Design group D4 for Transport) where decisions are made to implement harmonised international EDI messages.

PROTECT has forwarded comments to ITIGG for alignment of the PROTECT IFTDGN Implementation Guide against the ITIGG Principles and Rules (high level) documentation standard. As a result, ITIGG recommendations for the handling of dangerous goods information for other messages are now fully in line with this version of the PROTECT messages.

In the consultation process with ITIGG, specific comments from Japan and Australia were also taken into account.

Also the PROTECT Guide has been enhanced to align with ITIGG General Recommendations and accommodates new business requirements in the area of special dangerous substances such as noxious substances, radioactive materials and explosives.

The result of this consultation is that the PROTECT Guide version 1.0 is fully 'ITIGG compliant'. The PROTECT Guide has been endorsed by ITIGG.

The PROTECT Group is recognised by ITIGG as the maintenance group for dangerous goods message issues generally, as well as the PROTECT IFTDGN message.

4 ANNEX - Explanations of notations in PARTS II to VI

In other parts of this document instructions for use are given for each PROTECT message.

This annex explains the notation used in the EDIFACT Message Implementation Guides for both the functional data content of the messages (data attribute list) and the EDIFACT message format.

4.1 Legend to Data attribute list

The columns in the data attribute list have the following meanings:

- All data attributes have a unique **Name** that in short identifies the meaning according to a naming convention and which is preceded by a unique number.
- All data attributes have in principle a **Definition**, but where there is no ambiguity the definition may be omitted.
- An indication is added for the occurrence (**r/o/d**) of the data attribute in the message:
  r = Required – attribute should be present in message
  o = Optional – attribute may be present in message
  d = Dependant – a condition is applicable to the occurrence of the attribute.
  For a dependant data attribute the **Condition** is specified.

Further the **Mapping** of the data attribute to the EDIFACT segment is specified in a string, e.g. NAD(MS).3035. The string contains the segment tag, fixed qualifier values between brackets and the data element tag in which the value for the data attribute is contained.

4.2 Legend to EDIFACT Technical specification

The following clarifications will help the reader in understanding the documentation.

The EDIFACT technical specification for a message consists of:

1. **Branching diagram** - showing the message structure with occurrence of segments and segment groups in the message.
   This is presented in two layouts: in a text table and schematically in boxes for the segments.
2. **Segment specifications** - showing the occurrence of (composite) data elements in the segments, and if applicable also the code value(s) for data elements and business rules.
3. **Segment group specifications** - if applicable – showing the occurrence of segments in a segment group.

Ad 1 The branching diagram contains the segments and segment group in the sequence and hierarchy as defined in the UNSM. In the text table also the position numbers as defined in the UNSM are specified:

- **Base status** indicates the occurrence as per UN Directory for the segment,
- **User status** indicates the use of the segment in the message according to the subset as defined for the PROTECT use of the message
- **Max use** (and Group repeat) indicates the number of occurrences of the segment (and segment group) as defined in the subset.

Ad 2 The segment specification contains in the heading the details from the branching diagram (e.g. Usage indicates e.g. 'Conditional (Required)', meaning respectively: 'Base status (User status)'.
Below the sub-heading 'data element summary', the specification of the segment as per UN Directory (with data element number, name, definition and representation) is presented.
Further, there are two additional columns:

- **Base attributes** for (composite) data elements in the segment
  This term refers to the occurrence as per UN Directory for the segment or data elements in segments:
  M = Mandatory - segment/data element should occur.
  C = Conditional - segment/data element may occur, may be omitted or could conditionally be present in the message. This is further defined in the Message Implementation Guide, using the User attributes.
- **User attributes** for (composite) data elements in the segment
  This term refers to the use of the elements in the message according to the subset defined for the PROTECT use of the message. It is the result of translating (mapping) the occurrence of the data attribute - as specified in the data attribute list in the previous chapter - to the data elements in segments (and in segments groups):
  M = Mandatory (as per UN Directory)
  R = Required – segment/data element should occur in the message
  O = Optional – segment/data element may be present in the message
  X = Not used – segment/data element should not be present in the message
  D = Dependant – segment/data element is conditionally present in the message

For data elements that are conditionally present, a **Business rule** is created. The other data element to which the data element in question is dependant is assigned a **variable name**.

E.g.: For the APERAK message: the value for the code of data attribute Message response accepted Yes/No (in BGM.4343) implies whether the Message acceptance reason NO code should occur or not (in ERC.9321).
The data element BGM.4343 is assigned the variable name: MessageAcceptanceCode.
For data element ERC.9321 a business rule is created, reading e.g.:
If MessageAcceptance Code EQ (= equals) 'AP' (AP code for accepted), then ERC.9321 should Not be used. This means that in all other cases this data element may be used (and a code for Message acceptance reason NO may be specified).
NE = Not equals
EQ = Equals

The name of the **Data attribute** is referred to below the data element to which that data attribute is mapped.
Code values together with their names and definitions are presented in *italics* below the data element.

Ad 3 The segment group specification indicates the single segments or the nested segment groups that occur in the segment group, together with their status and maximum use count (number of occurrences).

- **Reading help – for hierarchy in data levels**

Please note that there is a hierarchy in the levels of the information in the segments and their groups, and data elements and their composites.
This hierarchy is important in identifying from the EDIFACT message specification whether a certain data element on which a certain data attribute is mapped is to occur in that place in the message or not.

The hierarchy of the data levels in the message is top down, as follows:
- 1st R/M/O/D indication for the **segment group** - as per user status in branching diagram
- 2nd R/M/O/D indication for the **segment** - as per user status in branching diagram
- 3rd R/M/O/D indication for the **composite data element** in the segment - as indicated in the segment specification;
- 4th R/M/O/D indication for the **data element** - as indicated in the segment specification;

The rule is as follows: If all data levels are required or if conditions for their occurrence are met, the data element and the higher levels occur in the message. If one of the levels is indicated as optional or as conditional and the condition for its occurrence is not met, then the data element should not occur in the message.

Example 1: If a required data element occurs in a composite that is optional in a segment that is mandatory in a segment group that is optional, that data element does not occur in the message.

It is noted that the first mentioned segment in the group (the trigger segment) is always mandatory; that means that when the segment group occurs that segment should always be present.

***