INTERNATIONAL STANDARD

ISO/IEC 15909-1

First edition
2004-12-01

Software and system engineering — High-level Petri nets —

Part 1:
Concepts, definitions and graphical notation

Ingénierie du logiciel et du système — Toiles de Petri de haut niveau —

Partie 1: Concepts, définitions et notation graphique

Reference number
ISO/IEC 15909-1:2004(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15909-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and system engineering*.

ISO/IEC 15909 consists of the following parts, under the general title *Software and system engineering — High-level Petri nets*:

— *Part 1: Concepts, definitions and graphical notation*

Introduction

This International standard is Part 1 of a multi-part standard concerned with defining a modelling language and its transfer format, known as High-level Petri Nets. Part 1 defines a semi-graphical technique for the specification, design and analysis of discrete event systems.

The technique is mathematically defined and may thus be used to provide unambiguous specifications and descriptions of applications. It is also an executable technique, allowing specification prototypes to be developed to test ideas at the earliest and cheapest opportunity. Specifications written in the technique may be subjected to analysis methods to prove properties about the specifications, before implementation commences, thus saving on testing and maintenance time and providing a high level of quality assurance.

Petri nets have been used to describe a wide range of systems since their invention in 1962. A problem with Petri nets is the explosion of the number of elements of their graphical form when they are used to describe complex systems. High-level Petri Nets were developed to overcome this problem by introducing higher-level concepts, such as the use of complex structured data as tokens, and using algebraic expressions to annotate net elements. The use of 'high-level' to describe these Petri nets is analogous to the use of 'high-level' in high-level programming languages (as opposed to assembly languages), and is the usual term used in the Petri net community. Two of the early forms of high-level nets that this standard builds on are Predicate-Transition Nets and Coloured Petri Nets, first introduced in 1979 and developed during the 1980s. It also uses some of the notions developed for Algebraic Petri nets, first introduced in the mid 1980s. It is believed that this standard captures the spirit of these earlier developments (see bibliography).

The technique promises to have multiple uses. For example, it may be used directly to specify systems or to define the semantics of other less formal languages. It may also serve to integrate techniques currently used independently such as state transition diagrams and data flow diagrams. The technique is particularly suited to parallel and distributed systems development as it supports concurrency. The technique is able to specify systems at a level that is independent of the choice of implementation (i.e. by software, hardware (electronic and/or mechanical) or humans or a combination). This International Standard may be cited in contracts for the development of systems (particularly distributed systems), or used by application developers or Petri net tool vendors or users.

Part 1 of this International Standard provides an abstract mathematical syntax and a formal semantics for the technique. Conformance to the standard is possible at several levels. The level of conformance depends on the class of high-level net chosen and the degree to which the syntax is supported. The basic level of conformance is to the semantic model.

Clause 1 describes the scope, areas of application and the intended audience of Part 1 of this International Standard. Clause 2 provides a glossary of terms and defines abbreviations. The main mathematical apparatus required for defining the semantic model and its graphical form is developed in normative Annex A and referred to in clause 3. The basic semantic model for High-level Petri Nets is given in clause 4, while the main concepts behind the graphical form are in formally introduced in clause 5. Clause 6 defines the High-level Petri Net Graph, the form of the standard intended for industrial use. Components of the graph are annotated. The annotations are defined at a meta-level allowing many different concrete syntaxes to be used. Clause 7 describes several syntactical conventions. Clause 8 maps the graphical form to the basic semantic model. The conformance statement is given in clause 9. Normative Annex B defines Place/Transition nets (without capacities) as a restriction of the definition of Clause 6. Place/Transition nets is often what is meant when the term Petri nets is used. Three informative annexes are included: Annex C defines a High-level Petri Net Schema, which allows classes of systems to be described at a syntactic level; Annex D is a tutorial on the High-level Petri Net Graph; and Annex E provides pointers to analysis techniques for High-level Petri Nets. A bibliography concludes this International Standard.

Software and system engineering — High-level Petri nets —

Part 1: Concepts, definitions and graphical notation

1 Scope

1.1 Purpose

This International Standard defines a Petri net technique, called High-level Petri Nets, including its syntax and semantics. It provides a reference definition that can be used both within and between organisations, to ensure a common understanding of the technique and of the specifications written using the technique. This International Standard will also facilitate the development and interoperability of Petri net computer support tools.

Part 1 of this International Standard defines a mathematical semantic model, an abstract mathematical syntax for annotations and a graphical notation for High-level Petri Nets, known as the High-level Petri Net Graph. A mathematical mapping is provided that defines the graphical form in terms of the semantic model. A transfer format for the High-level Petri Net Graph is the subject of Part 2 of this International Standard, while Part 3 addresses techniques for modularity (such as hierarchies) and the augmentation of High-level Petri Nets with time.

1.2 Field of Application

This International Standard is applicable to a wide variety of concurrent discrete event systems and in particular distributed systems. Generic fields of application include:

- requirements analysis;
- development of specifications, designs and test suites;
- descriptions of existing systems prior to re-engineering;
- modelling business and software processes;
- providing the semantics for concurrent languages;
- simulation of systems to increase confidence;
- formal analysis of the behaviour of systems; and
- development of Petri net support tools.

This International Standard may be applied to the design of a broad range of systems and processes, including aerospace, air traffic control, avionics, banking, biological and chemical processes, business processes, communication protocols, computer hardware architectures, control systems, databases, defence command and control, distributed computing, electronic commerce, fault-tolerant systems, hospital procedures, information systems, Internet protocols and applications, legal processes, logistics, manufacturing systems, metabolic processes, music, nuclear power systems, operating systems, transport systems (including railway control), security systems, telecommunications and workflow.

1.3 Audience

Part 1 of this International Standard is written as a reference for systems analysts, designers, developers, maintainers and procurers, and for Petri net tool designers and standards developers.

2 Terms, Definitions, Abbreviations and Symbols

For the purpose of this International Standard, the following definitions, abbreviations and symbols apply. Any ambiguity in the definitions is resolved by the mathematically precise definitions in the body of Part 1 of this International Standard.

2.1 Glossary

2.1.1 Arc: A directed edge of a net which may connect a place to a transition or a transition to a place, normally represented by an arrow.

2.1.1.1 Input Arc (of a transition): An arc directed from a place to the transition.

2.1.1.2 Output Arc (of a transition): An arc directed from the transition to a place.

2.1.1.3 Arc Annotation: An expression that may involve constants, variables and operators used to annotate an arc of a net. The expression must evaluate to a multiset over the type of the arc's associated place.

2.1.2 Arity: The input sorts and output sort for an operator.

2.1.3 Assignment: For a set of variables, the association of a value (of correct type) to each variable.

2.1.4 Basis Set: The set of objects used to create a multiset.

2.1.5 Binding: See Assignment.

2.1.6 Carrier: A set of a many-sorted algebra.

2.1.7 Concurrency: The property of a system in which events may occur independently of each other, and hence are not ordered (see also Step and Concurrent Enabling).

2.1.8 Declaration: A set of statements which define the sets, constants, parameter values, typed variables and functions required for defining the annotations on a High-level Petri Net Graph.

2.1.9 Enabling (a transition): A transition is enabled in a particular mode and net marking, when the following conditions are met:

The marking of each input place of the transition satisfies the demand imposed on it by its arc annotation evaluated for the particular transition mode. The demand is satisfied when the place's marking contains (at least) the multiset of tokens indicated by the evaluated arc annotation.

NOTE: The determination of transition modes guarantees that the Transition Condition is satisfied (see Transition Mode).

2.1.10 Concurrent Enabling (of transition modes): A multiset of transition modes is concurrently enabled if all the involved input places contain enough tokens to satisfy the sum of all of the demands imposed on them by each input arc annotation evaluated for each transition mode in the multiset.

2.1.11 High-level Net (High-level Petri Net): An algebraic structure comprising: a set of places; a set of transitions; a set of types; a function associating a type to each place, and a set of modes (a type) to each transition; *Pre* function imposing token demands (multisets of tokens) on places for each transition mode; *Post* function determining output tokens (multisets of tokens) for places for each transition mode; and an initial marking.

2.1.12 High-level Petri Net Graph: A net graph and its associated annotations comprising Place Types, Arc Annotations and Transition Conditions, and their corresponding definitions in a set of Declarations, and an Initial Marking of the net.

2.1.13 Many-sorted Algebra: A mathematical structure comprising a set of sets and a set of functions taking these sets as domains and co-domains.

2.1.14 Marking (of a net): The set of the place markings for all places of the net.

2.1.14.1 Initial Marking (of the net): The set of initial place markings given with the high-level net definition.

2.1.14.2 Initial Marking of a place: A special marking of a place, defined with the high-level net.

2.1.14.3 Marking of a place: A multiset of tokens associated with ('residing in') the place.

2.1.14.4 Reachable Marking: Any marking of the net that can be reached from the initial marking by the occurrence of transitions.

2.1.14.5 Reachability Set: The set of reachable markings of the net, including the initial marking.

2.1.15 Multiset: A collection of items where repetition of items is allowed.

2.1.15.1 Multiplicity: A natural number (i.e., non-negative integer) which describes the number of repetitions of an item in a multiset.

2.1.15.2 Multiset Cardinality (cardinality of a multiset): The sum of the multiplicities of each of the members of the multiset.

2.1.16 Net: A general term used to describe all classes of Petri nets.

2.1.16.1 Net Graph: A directed graph comprising a set of nodes of two different kinds, called places and transitions, and their interconnection by directed edges, called arcs, such that only places can be connected to transitions, and transitions to places, but never transitions to transitions, nor places to places.

2.1.16.2 Node (of a net): A vertex of a net graph (i.e., a place or a transition).

2.1.16.3 Petri Net: An algebraic structure with two sets, one called places and the other called transitions, together with their associated relations and functions, and named after their inventor, Carl Adam Petri.

2.1.16.4 Place/Transition Net: A Petri net comprising a net graph with positive integers associated with arcs and an initial marking function which associates a natural number of simple tokens ('black dots') with places.

2.1.17 Operator: A symbol representing the name of a function.

2.1.18 Parameter: A symbol that can take a range of values defined by a set. It is defined as a constant in the signature.

2.1.19 Parameterized High-level Net Graph: A high-level net graph that contains parameters in its definition.

2.1.20 Place: A node of a net, taken from the place kind, normally represented by an ellipse in the net graph. A place is typed.

2.1.20.1 Input Place (of a transition): A place connected to the transition by an input arc.

2.1.20.2 Output Place (of a transition): A place connected to the transition by an output arc.

2.1.20.3 Place Type: A non-empty set of data items associated with a place. (This set can describe an arbitrarily complex data structure.)

2.1.21 Reachability Graph: A directed graph of nodes and edges, where the nodes correspond to reachable markings, and the edges correspond to transition occurrences.

2.1.22 Signature/Many-sorted signature: A mathematical structure comprising a set of sorts and a set of operators.

2.1.22.1 Boolean signature: A signature where one of the sorts is $Bool$, corresponding to the carrier Boolean in any associated algebra, and one of the constants is $true_{Bool}$ corresponding to the value true in the algebra.

2.1.23 Sort: A symbol representing the name of a set.

2.1.23.1 Argument Sort: The sort of an argument of an operator.

2.1.23.2 Input Sort: The same as an argument sort.

2.1.23.3 Output Sort: The sort of an output of an operator.

2.1.23.4 Range Sort: The same as an output sort.

2.1.24 Term: An expression comprising constants, variables and operators built from a signature and a set of sorted variables.

2.1.24.1 Closed Term: A term comprising constants and operators but no variables. Also known as a **Ground Term**.

2.1.24.2 Term Evaluation: The result obtained after the binding of variables in the term, the computation of the results of the associated functions, and any simplifications performed (such as gathering like terms to obtain the symbolic sum representation of a multiset).

2.1.25 Token: A data item associated with a place and chosen from the place's type.

2.1.25.1 Enabling Tokens: The multiset of values obtained when an input arc annotation is evaluated for a particular binding to variables.

2.1.25.2 Simple Token: A valueless token, normally represented by a black dot, and used in Place/Transition nets (as opposed to high-level nets).

2.1.26 Transition: A node of a net, taken from the transition kind, and represented by a rectangle in the net graph.

2.1.26.1 Transition Condition: A boolean expression (one that evaluates to true or false) associated with a transition.

2.1.26.2 Transition Mode: A pair comprising the transition and a mode.

2.1.26.2.1 Mode: A value taken from the transition's type. When considering a High-level Petri Net Graph, a mode may be derived from an assignment of values to the transition's variables that satisfies the transition condition.

2.1.26.3 Transition Occurrence (Transition Rule): If a transition is enabled in a mode, it may occur in that mode. On the occurrence of the transition, the following actions occur indivisibly:

1. For each input place of the transition: the enabling tokens of the input arc with respect to that mode are subtracted from the input place's marking, and

2. For each output place of the transition: the multiset of tokens of the evaluated output arc expression is added to the marking of the output place.

NOTE: A place may be both an input place and an output place of the same transition.

2.1.26.4 Step: The simultaneous occurrence of a finite multiset of transition modes that are concurrently enabled in a marking.

2.1.26.5 Transition Variables: All the variables that occur in the expressions associated with the transition. These are the transition condition, and the annotations of arcs surrounding the transition.

2.1.27 Type: A set.

2.2 Abbreviations

2.2.1 HLPN: High-level Petri Net
2.2.2 HLPNG: High-level Petri Net Graph
2.2.3 HLPNS: High-level Petri Net Schema
2.2.4 *iff*: if and only if
2.2.5 PN: Petri Net
2.2.6 PTNG: Place/Transition Net Graph.

3 Conventions and Notation

This International Standard uses the notation for sets, multisets and universal algebra defined in Annex A. Annex A also defines the concept of multiset addition, (using the '$+$' symbol), which should not be confused with arithmetic addition. The notion of multisets is required for clauses 4, 5, 6, 7 and 8. An understanding of many-sorted signatures, sorted variables and many-sorted algebras provided in Annex A is required for clauses 6 and 8 and Annexes B and C.

Wherever possible standard mathematical notation has been used. An instance of notation specific to Petri nets is when a marking of the net is transformed to a new marking.

$M[T_\mu\rangle M'$ is used to denote that a new marking, M', is created on the occurrence of a multiset of transition modes, T_μ, when in the marking M.

