

CLAIMS

1. A method for securing a first program with a second program, a third program and a fourth program, each program comprising constitutive elements, said constitutive elements comprising a finite number of program points and evolution rules associated with the program points and defining the passage from one program point to another program point, and each program comprising a definition of a set of properties each property being associated with one or more of the constitutive elements of the program, said method comprising:

constructing the fourth program by defining at least one relation between at least one constitutive element of the second program and at least one constitutive element of the third program, said relation being named a correspondence relation;

exploiting the correspondence relation for establishing a relation between one property of the first program and at least one property of the third or fourth program, said relation being named a "sufficiency relation" and being such that it creates an oriented relationship between one local property of a program, and one or more local properties of the same or another program such that the proof of the latter properties proves the first local property, or propagate the proof of said property to at least one property of the first program.

2. The method according to claim 1, wherein the first program is the second program or the fourth program.

3. The method according to claim 1 or 2, wherein the fourth program is the second program or the third program.

4. The method according to claim 1, 2 or 3, wherein the fourth program is constructed automatically by applying synchronization rules between the second program and the third program

5. A computer software product comprising software instructions to implement the method according to any one of claims 1 to 4 when said computer software product is executed on a computer.

6. A system for securing a first program with a second program, a third program and a fourth program, each program comprising constitutive elements, said constitutive elements comprising a finite number of program points and evolution rules associated with the program points and defining the passage from one program point to another program point, and each program comprising a definition of a set of properties each property being associated with one or more of the constitutive elements of the program, said system comprising:

a program builder for constructing the fourth program by defining at least one relation between at least one constitutive element of the second program and at least one constitutive element of the third program, said relation being named a correspondence relation;

a prover exploiting the correspondence relation for establishing a relation between one property of the first program and said at least one property of the third or fourth program, said relation being named a "sufficiency relation" and being such that it creates an oriented relationship between one local property of a program, and one or more local properties of the same or another program such that the proof of the latter properties proves the first local property, or for propagating the proof of said property to at least one property of the first program.

CLAIMS

1. A method for securing a first program, referenced hereinafter as a target program, with a second program, a third program and a fourth program, hereafter referenced as a correspondence program, each program comprising constitutive elements, said constitutive elements comprising a finite number of program points and evolution rules associated with the program points and defining the passage from one program point to another program point, and each program comprising a definition of a set of properties each property being associated with one or more of the constitutive elements of the program, said method comprising:

constructing the correspondence program by defining at least one relation between at least one constitutive element of the second program and at least one constitutive element of the third program, said relation being named a correspondence relation;

exploiting the correspondence relation for establishing a relation between one property of the target program and at least one property of the third or correspondence program, said relation being named a "sufficiency relation" and being such that it creates an oriented relationship between one local property of a program, and one or more local properties of the same or another program such that the proof of the latter properties proves the first local property, or propagate the proof of said property to at least one property of the target program.

2. The method according to claim 1, wherein the target program is the second program or the correspondence program.

3.The method according to claim 1 or 2, wherein the correspondence program is the second program or the third program.

4.The method according to claim 1, 2 or 3, wherein the correspondence program is constructed automatically by applying synchronization rules between the second program and the third program

5. A computer software product comprising software instructions to implement the method according to any one of claims 1 to 4 when said computer software product is executed on a computer.

6. A system for securing a first program, referenced hereinafter as a target program, with a second program, a third program and a fourth program, hereafter referenced as a correspondence program, each program comprising constitutive elements, said constitutive elements comprising a finite number of program points and evolution rules associated with the program points and defining the passage from one program point to another program point, and each program comprising a definition of a set of properties each property being associated with one or more of the constitutive elements of the program, said system comprising:

a program builder for constructing the correspondence program by defining at least one relation between at least one constitutive element of the second program and at least one constitutive element of the third program, said relation being named a correspondence relation;

a prover exploiting the correspondence relation for establishing a relation between one property of the first program and said at least one property of the third or correspondence program, said relation being named a

"sufficiency relation" and being such that it creates an oriented relationship between one local property of a program, and one or more local properties of the same or another program such that the proof of the latter properties proves the first local property, or for propagating the proof of said property to at least one property of the target program.