CLAIMS

[Claim 1]

A validation processing device comprising:

a processing unit that performs model checking on a model to be checked that indicates a relay circuit of a security system; and

a selection unit that selects, on the basis of a result of the model checking, one element among elements of the relay circuit that have undergone a state change in a process leading to an unsafe event,

wherein the processing unit further performs model re-checking on a model to be checked which is obtained by excluding the one element.

[Claim 2]

The validation processing device according to claim 1, wherein in a case where the model to be checked has not led to the unsafe event in the model re-checking, the processing unit returns the one element to the model to be checked, and performs model re-checking on a model to be checked which is obtained by excluding an element, which is different from the one element, from the model to be checked.

[Claim 3]

The validation processing device according to claim 2, wherein in a case where the model to be checked has led to the unsafe event in the model re-checking, the processing unit does not return the one element to the model to be checked, and performs model re-checking on a model to be checked which is obtained by excluding an element, which is different from the one element, from the model to be checked.

[Claim 4]

The validation processing device according to any one of claims 1 to 3,

wherein the processing unit performs the model re-checking within a range equal to or less than the number of transition steps leading up to the unsafe event specified in a first model checking for the model to be checked.

[Claim 5]

The validation processing device according to any one of claims 1 to 4, further comprising a specification unit that specifies a shortest path from an element extracted on the basis of a result of the model re-checking to an element included in a definition of the unsafe event.

[Claim 6]

The validation processing device according to any one of claims 1 to 5, further comprising a calculation unit that calculates a probability of leading the model to be checked to the unsafe event from an initial state, on the basis of a trouble occurrence probability defined for each element.

[Claim 7]

The validation processing device according to claim 6, wherein in a case where the probability is lower than a predetermined determination threshold value, the selection unit omits processing of selecting the one element on the basis of a result of the model checking.

[Claim 8]

A validation processing method executed by a computer, comprising:

a step of performing model checking on a model to be checked that indicates a relay circuit of a security system;

a step of selecting, on the basis of a result of the model checking, one element among elements of the relay circuit that have undergone a state change in a process leading to an unsafe event; and

a step of performing model re-checking on a model to be checked which is obtained by excluding the one element.

[Claim 9]

A program causing a computer of a validation processing device to execute:

a step of performing model checking on a model to be checked that indicates a relay circuit of a security system;

a step of selecting, on the basis of a result of the model checking, one element among elements of the relay circuit that have undergone a state change in a process leading to an unsafe event; and

a step of performing model re-checking on a model to be checked which is obtained by excluding the one element.