Integrity level の汎用規格

ISO/IEC15026-3:2011

2013.12.3 認証工学WG@SICE(東京)

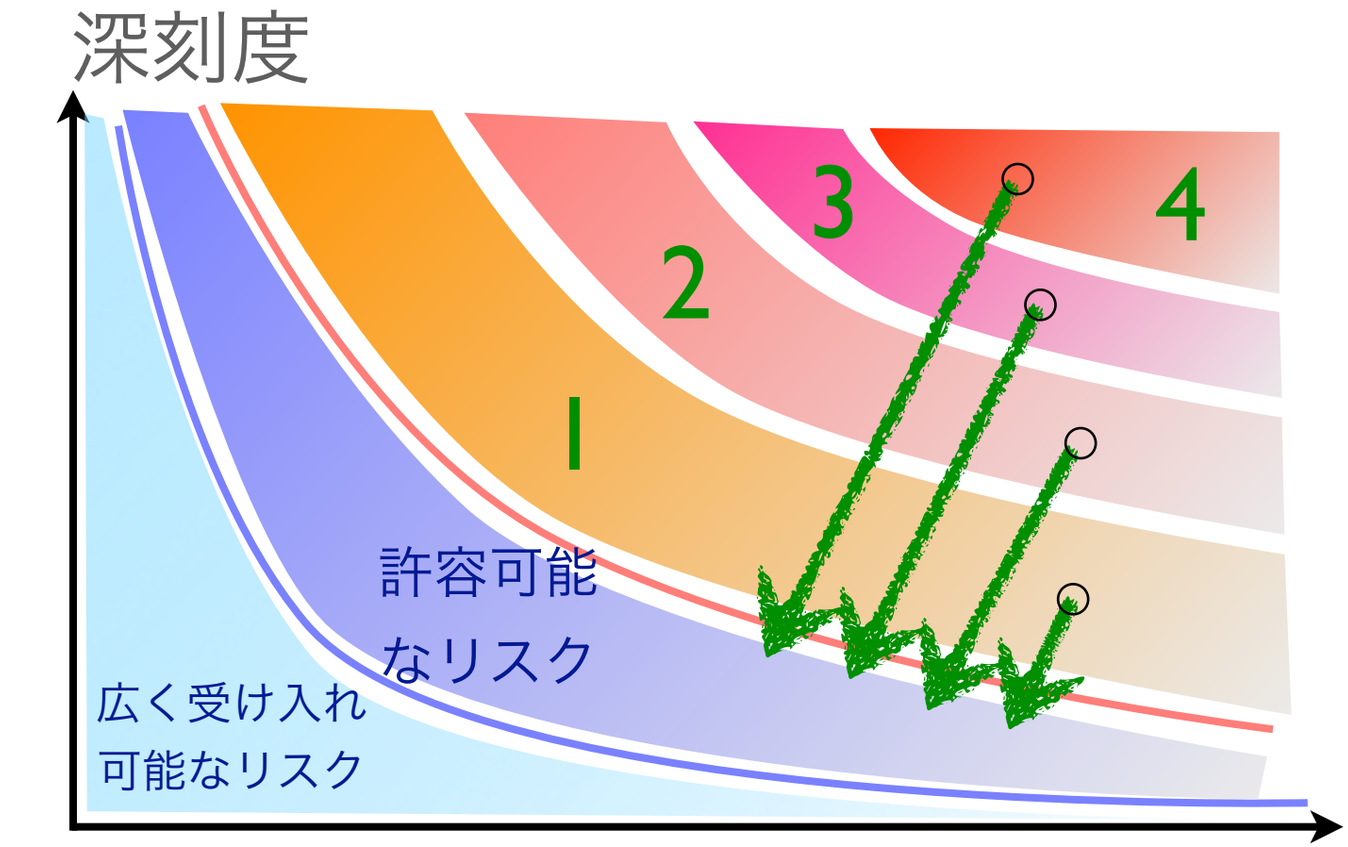
高井利憲

歴史

- ISO/IEC15026:1998 System and software integrity levels
  - IEC61508も1998年に初版発行
  - Integrity level一般に関する規格として位置づけ
    - 「共通技術としてソフトウェアを取り扱う必要性高まる」 (*)
    - 分野ごとのintegrity levelを策定するものが主な想定読者
      - safety, security, economics などリスクの属性に限定しない
  - JIS化済み: JIS X0134:1999 システム及びソフトウェアに課せられたリスク抑制の完全性水準
- ISO/IEC15026-3:2011 System integrity levels
  - 広くシステムアシュランス規格として改訂
- ISO/IEC15026-3:201x
  - 現在、ISO26262などとも整合性を保つために改訂中

(*) 松尾谷徹:“WG9 System and software Integrity level クリティカルソフトウェアの標準化”, 2001年.

Integrity levelとは？



	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Separation of E/E/PE system safety functions from non-safety functions	B.1.3	HR low	HR low	HR medium	HR high
	Structured specification	B.2.1	HR low	HR low	HR medium	HR high
	Inspection of the specification	B.2.6	– low	HR low	HR medium	HR high
	Semi-formal methods	B.2.3, see also Table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	R low	R low	R medium	R high
	Computer aided specification tools	B.2.4	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high

View1：リスククラス

View2：許容可能なリスクレベルを実現するために必要な
リスク抑制の幅

View3：上記リスク抑制を達成するために必要な
安全機能の故障率

View4: 上記リスク抑制を達成するために必要な
開発プロセスに関する要求事項

さらに・・・

View a: 要求の水準

View b: 実績の水準

View5: どれだけコストをかけられるか

61508および26262での定義

- 61508
  - Safety integrity level: discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest
  - Safety integrity: probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time
- 26262
  - ASIL: one of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable residual risk , with D representing the most stringent and A the least stringent level

15026での定義

リスククラス

リスク抑制の幅

安全機能の故障率

規格の準拠に必要な
要求事項のレベル

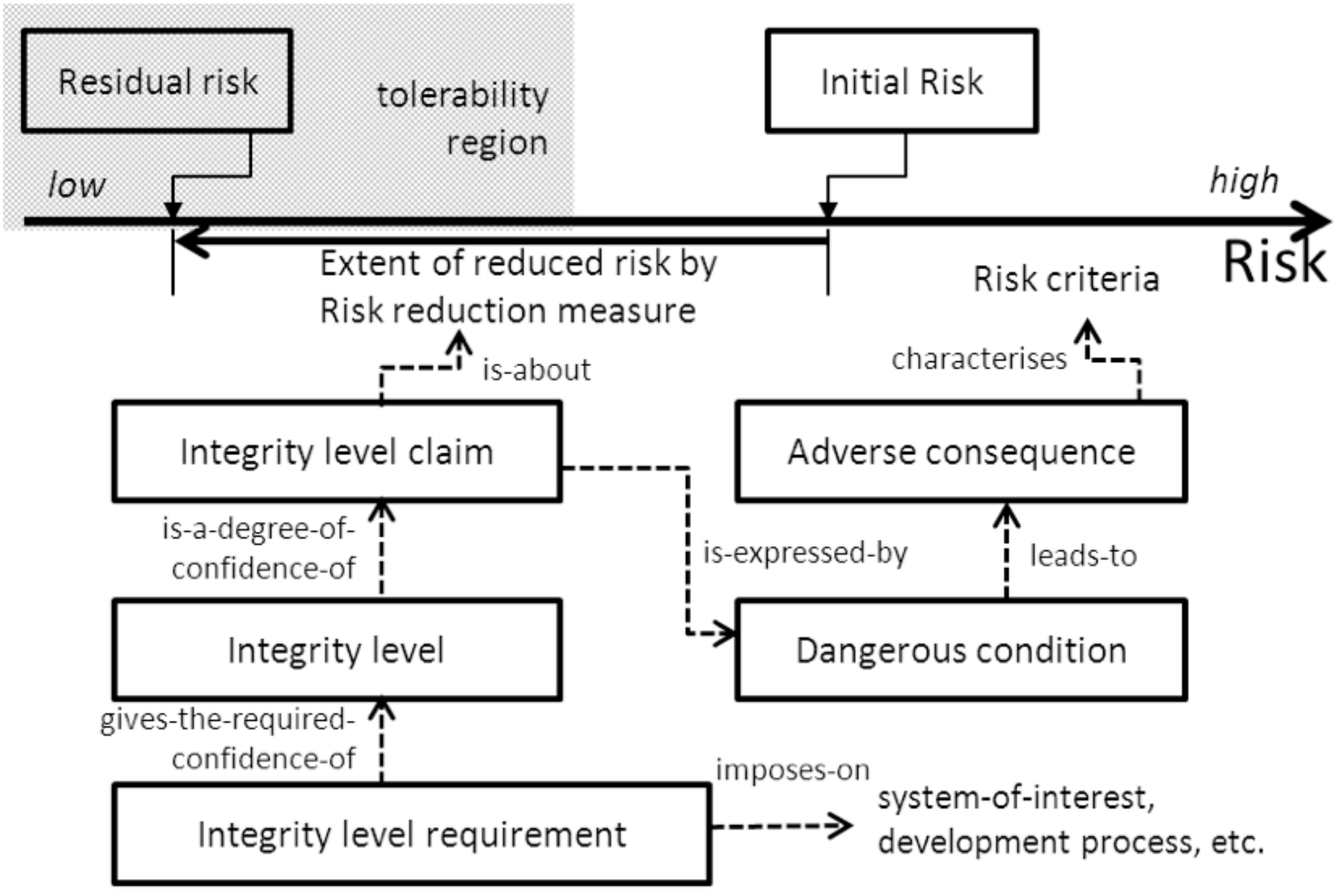
信用の程度

* degree of confidence that the system-of-interest meets the associated integrity level claim

Integrity level claim

- 15026
  - a proposition representing a requirement on a risk reduction measure identified in the risk treatment process of the system of interest.
- 61508における対応する文
  - an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions
    - ☆61508は機能安全規格であるため、integrity level が安全機能の故障率に限定されているが、15026はこの文に対応する一般用語を導入

関連概念図


Residual risk
tolerability region
Initial Risk
low
high
Risk
Extent of reduced risk by Risk reduction measure
Risk criteria
is-about
characterises
Integrity level claim
Adverse consequence
is-a-degree-of-confidence-of
is-expressed-by
leads-to
Integrity level
Dangerous condition
gives-the-required-confidence-of
imposes-on
Integrity level requirement
system-of-interest, development process, etc.

critical qualities in 15288, or critical requirement in 29148 (see [4F] in [1])

is a part of

claim

is about

Tolerable risk

is-a

Risk

is-a

adverse consequence

has-a

severity

has-a

likelihood

has-a

requirement to avoid adverse consequence

requirement to control adverse consequence

requirement to mitigate adverse consequence

an integrity level means the required degree of confidence that the claim is achieved

is associated with

integrity level

risk class (defined by a set of risk)

is determined by both

architectural feature of system

supports (=shows that the claim is achieved)

affects the strength of

may be defined by

is a potential source of

dangerous condition

is-a

random failure

is-a

systematic failure

is provided by meeting ...

argument

has-a

has-a

has-a

assurance case

is specified by

integrity level requirement

domain specific standard

uses

shows integrity level requirement is satisfied

evidence

legend

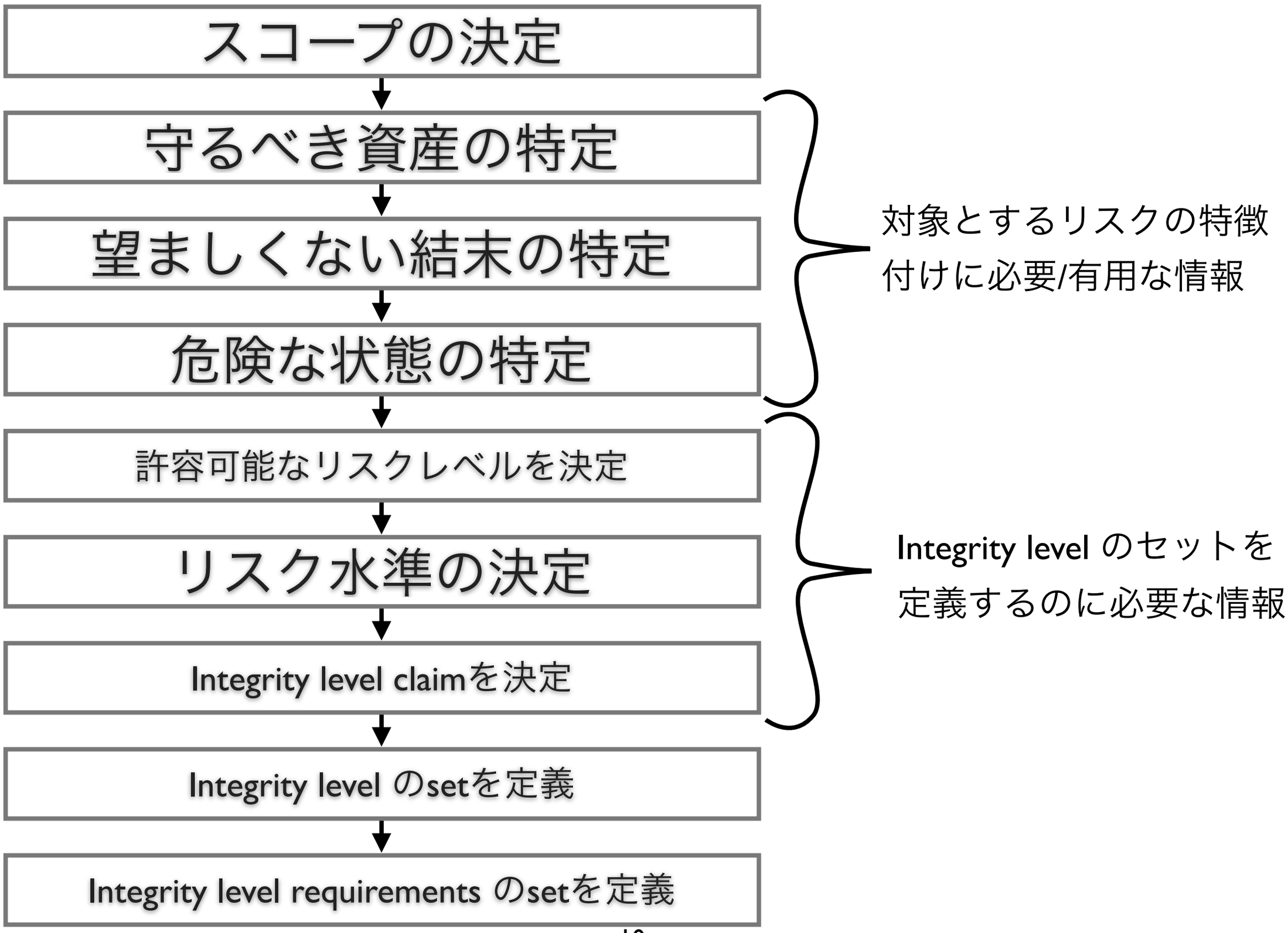
key concept in 15026-3

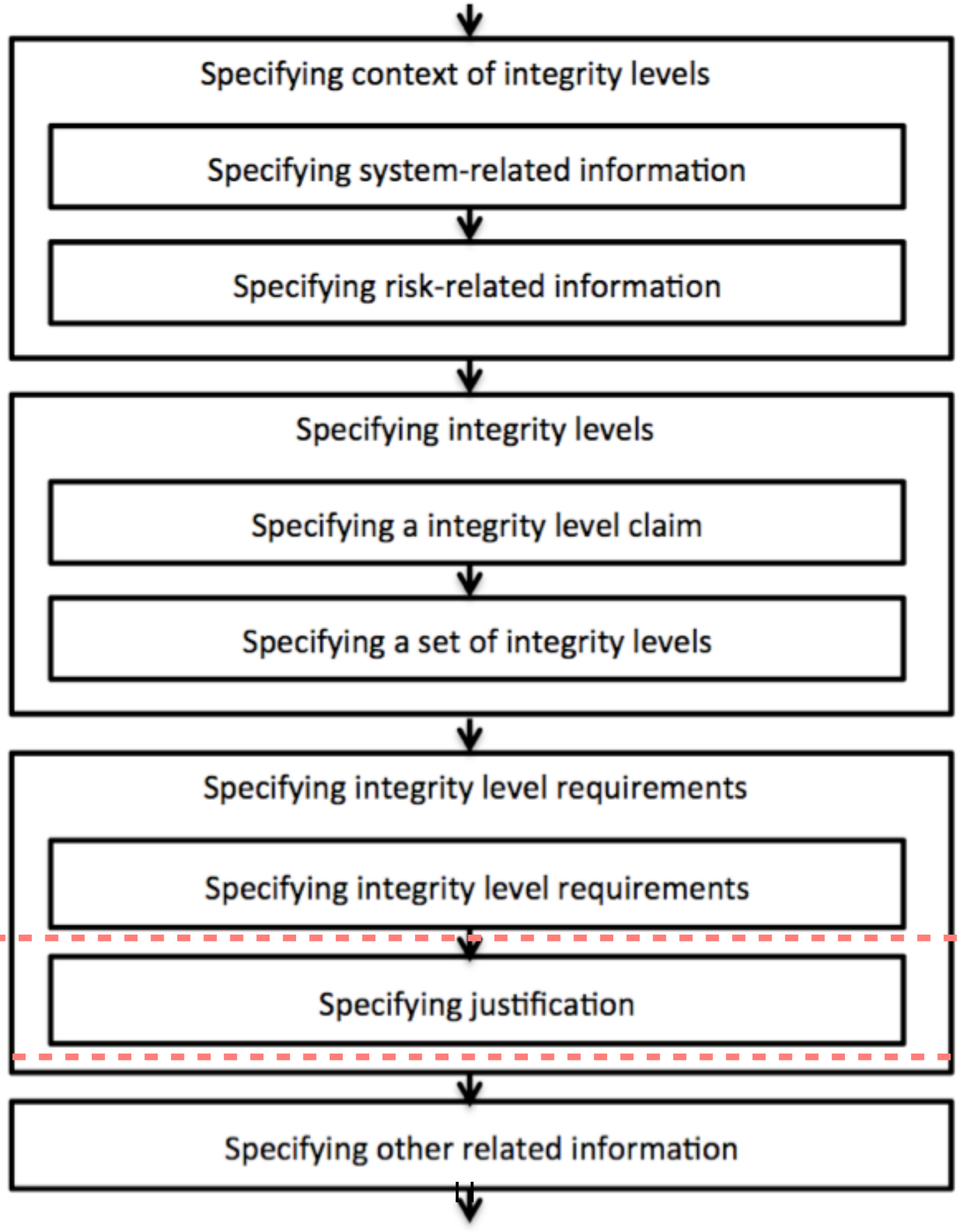
general noun or term defined in other standards

関連概念規格間対応表

ISO/IEC15026-3	IEC61508 (functional safety)	ISO26262 (road vehicles functional safety)	ISO/IEC15408 (Evaluation criteria for IT security)
tolerable risk	tolerable risk	(?)	(?)
risk	risk	risk	risk
adverse consequence	harm	harm	loss of asset
dangerous condition	1) hazard 2) hazardous situation	1) hazard 2) hazardous event	1) vulnerability ? 2) threat ?
claim	1) E/E/PE system safety requirements specification 2) E/E/PE system safety functions requirements specification	1) safety goal 2) functional safety requirement	security target(ST)
integrity level	safety integrity level (SIL)	automotive safety integrity level (ASIL)	evaluation assurance level (EAL) ?
integrity level requirement	recommended activities in IEC61508, E/E/PE system safety integrity requirements specification	necessary requirement of ISO26262, functional safety concept	security functional requirement (SFR) ?
system-of-interest	EUC	item	target of evaluation (TOE)

Integrity level 定義プロセス





integrity level requirementsの妥当性を要求している

まとめ

- ISO/IEC15026は、Integrity levelの一般的な枠組みを提供
  - リスクの程度に関する利害関係者間の合意形成のための共通言語の一つ
  - 多様なシステムに対するオーダーメイドのIntegrity levelを想定
- 現在改訂中であり、日本からの意見を反映できるチャンスですので皆様御協力を！
  - ドラフトをお送りします