# 測位デバイス多重化と鉄道安全関連系国際規格との整合について －GNSS を例に－

森　崇*　　吉永　純*　山口　大助*（(独)自動車技術総合機構 交通安全環境研究所）

The multi-positioning devices usage and conformity with safety-related railway international standards
An example of GNSS devices

Takashi Mori*, Jun Yoshinaga*, Daisuke Yamaguchi*(NTSEL, NALTEC)

GNSS System is widely used for automobile positioning systems, and railway industry tries to use new positioning devices for safety-related applications. When we use them for safety purposes, we have to respect about the accountability of safety evidence. In this paper, we show some conformity technics for international standards and newly developed positioning devices.

**キーワード**：位置検知、安全性、国際規格、GNSS、鉄道保安
(Positioning, safety, international standard, GNSS, railway safety related system)

## 1. はじめに

鉄道において、衛星測位をはじめとした測位デバイスについて、各種提案が活発になされている。これは、鉄道向けや保安装置用途として設計、製造されたデバイスではなく、COTS (Commercial Off-The-Shelf)と呼ばれる市販されるデバイスの活用を目指しているものが多くある。

半面、保安装置として使用するためには、IEC 62425 などに示されている Fail-safety やアイテム間の独立性、リスクアセスメントによる安全機能の確立及びその機能の TFFR (Tolerable Functional Failure Rate)とその TFFR に該当する SIL による技術的手法など、一定の条件があることも事実である。

このため、測位系デバイスについて、測位精度だけではなく、COTS を使用することと、保安装置としての技術的な条件を両立させることを考える必要がある。

本稿では、まず国際規格が述べている保安装置としての条件を述べ、測位デバイスにどのように適用できるかを記述する。

## 2. 国際規格における fail-safety の実現

### 〈2･1〉 IEC 62425(EN 50129)における Fail-safety

IEC 62425 には、リスクの高い SIL(安全性インテグリティレベル: Safety Integrity Level) 3 又は 4 と指定された機能について、その機能を実装するシステム等にある一定のルールに基づき Fail-safety を実現することを求めている。

図 1 に IEC 62425 に示す 3 つの Fail-safety 実現の方法を示している。この 3 つの方法を単独または組み合わせて実現することが規定されている。

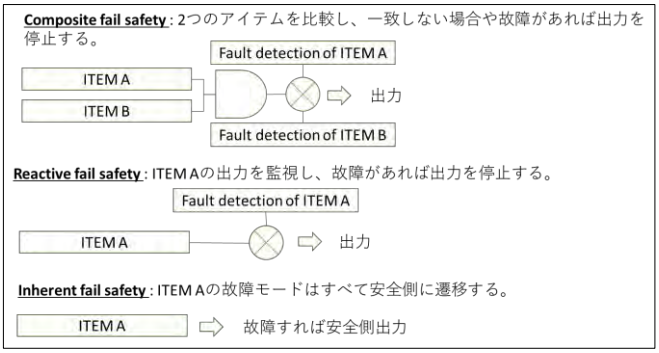


**図 1　IEC 62425 による Fail-safety の技術手法**

Fig. 1.　Technics of Fail-safety in IEC 62425

Composite Fail-safety は、ITEM の比較を行い、ITEM の故障検知を行う際に、その故障を検知し、安全側とされている状態に遷移させることが考え方の中心となり、Reactive Fail-safety においては、ITEM とは独立な故障検知を行うことによって、ITEM の故障を検知し、安全側とされている状態に遷移させることが考え方の中心になっている。これらは一般的に、Detection and Negation といわれる手法である。

これらの Detection and Negation において、いくつか重

要とされている事項がある。それについて簡単に述べる。

(1) ITEM 間の独立について

ITEM の故障を検知する際に、故障検知するデバイスが共通の原因で故障を起こすことがないよう、ITEM 間の独立性が重要とされている。これについては〈2･2〉で後述する。

(2) SDT(Safe Down Time)と安全性の関係

故障検知し安全側遷移する Detection and Negation Time（図 2 参照)を SDT と定義するが、この SDT が、システム構成した際の危険側故障出力をするまでの長さが、システム全体の安全性に影響を与えないかどうか評価する必要がある。

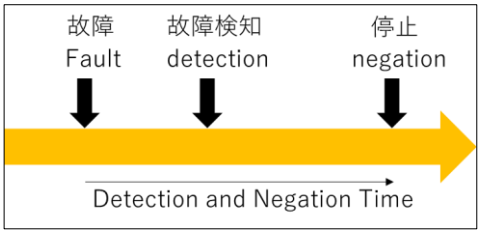


図 2　SDT の概念

Fig. 2.　Concept of SDT

(3) SDR(Safe Down Rate)と安全性の関係

故障検知し安全側遷移する頻度 Detection and Negation Rate を SDR (Safe Down Rate)と定義するが、この SDR が、TFFR と整合しているかどうかの評価を行う必要がある。

### 〈2･2〉 IEC 62425(EN 50129)における ITEM 独立性

IEC 62425 には、ITEM の独立を担保することにより共通原因故障(CCF：Common Cause Failure)を防ぐことが決められている。この ITEM 独立性は、表 1 に示す 4 つの観点で確認することとなっている。

表 1　IEC 62425 における ITEM 独立

Table 1.　ITEM independence in IEC 62425

| | ITEM 間の相互影響(内部影響) | 外部から ITEM への共通な影響 |
|---|---|---|
| 物理的 | Type A | Type C |
| 論理的 | Type B | Type D |

EN 50129 において、SIL3 又は SIL4 の機能を実装するハードウェアについて、ITEM 間の静電結合や電磁結合を防ぐことについては、Type A の対策、ITEM 全体に影響のある環境影響、電源及び入出力について適切に対処を行うことが Type C の対策となる。

Type B は ITEM 間によるデータ伝送によって、情報が共有されることにより独立性が阻害されることに対する影響の評価、Type D については、共通に接続されている外部の機器の機能を活用することによる独立性の阻害について確認する必要がある。

### 〈2･3〉 ITEM とソフトウェアの関係と独立性

Composite Fail-safety を実現する際、同じハードウェアデザインの ITEM を複数使用する場合、同一のソフトウェアを使用する場合と、異なるソフトウェアを使用しソフトウェアダイバシティを確保する場合がある。鉄道保安システムがしばしば参照する IEC 62279 によると、ソフトウェアダイバシティは必須とはされておらず、SIL に応じてソフトウェアの管理と試験の厳格度を調整することによって対処することになっている。

これは、同一のソフトウェアを使用する際、ソフトウェアにエラーがあった場合には必ず CCF となるため、ITEM 間の独立を阻害する大きな原因になりうる。このため、ソフトウェアの品質を向上させることによって CCF の発生する蓋然性を低下させることが IEC 62279 規格の基本的な考え方となっている。

しかしながら、COTS デバイスにおいて、IEC 62279 が規定する管理手法によってソフトウェアが作成されていることはまずないと考えられる。これが COTS デバイスを使用する上での大きな問題点となる。

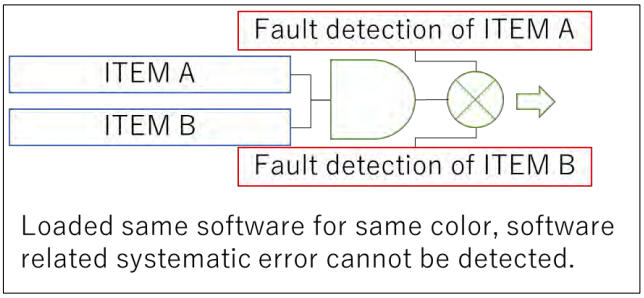


図 3　同一ソフトウェア使用時に生じる CCF

Fig. 3.　CCF using the same software

## 3.　測位デバイスと Fail-safety

### 〈3･1〉　一般的な構成との対比と課題

保安装置に測位デバイスを活用する場合、Composite Fail-safety と Inherent Fail-safety の両者を採用し安全性を確保する方法がある。例えば複数の速度発電機を異なる車軸に取り付けることによるものである（図 4 参照)。

この方法は、速度発電機が故障と判断される場合は、速度

情報を 0 とする SDR を設計と製作により確保し、かつ、Type A の独立性については十分な離隔確保による結合の防止、Type C については、異なる車軸から回転数を確保することにより、物理的な独立性を確保することに基づく。また 2 つの速度を比較し、積分する装置については、既存の保安装置のハードウェアを使用し、ソフトウェアも既存の保安装置と同じ管理手法をとる方法である。この方法は規格が制定される以前からとられている方法であるが、ソフトウェアの管理についての厳密性を除けば、今の規格と照らし合わせてもそれほど矛盾が存在しない。

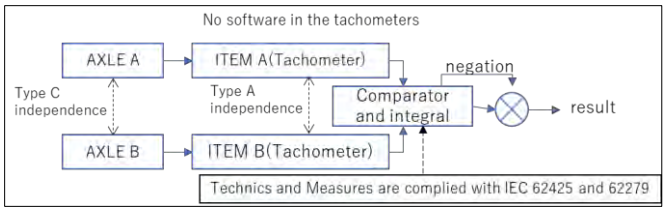


**図 4**　速度発電機による距離測定

Fig. 4.　Distance measurement with tachometers

次に GNSS について検討を行う。

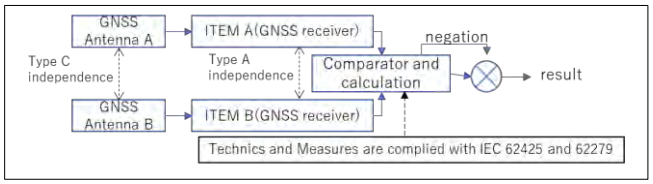


**図 5**　GNSS による距離測定のアイディア例

Fig. 5.　An example of idea of positioning with GNSS

図 5 では、単純に速度発電機を GNSS に変更して構成を考えてみた例である。速度発電機の構成と異なる面は以下の 2 つに集約される。

(1)　Type C の独立性についての差異

図 5 は受信している GNSS 衛星は共通であり、また電波伝搬経路も GNSS のアンテナ離隔が確保できない限りほぼ同一である場合があると考えられる。電離層における影響など、広範囲にわたるものについては、複数のアンテナを設置しても、列車の前後程度の離隔では排除できないと考えられる。

このため、GNSS 衛星受信システムの観点では、GNSS の電波伝搬系及び GNSS の衛星システムは、複数の受信システムを導入したとしても、入力における共通原因故障の排除は困難であると推定される。

(2)　測位センサがソフトウェアを持っていること

GNSS 受信機は速度発電機とは異なり、ソフトウェアを持っている。このため、安全機能の SIL に整合したソフトウェアの IEC 62279 の管理手法を採用し、安全性の正当化をする方法がある。

GNSS 受信ハードウェアのみを使用し、測位アルゴリズムを IEC 62279 に整合した管理手法で作成することは、COTS を使用するコストメリットを減殺してしまうことになる。将来において、IEC 61508 や IEC 62279 の認証を取得した受信機が市販される可能性は否定できないが、COTS であるデバイスを使用し、安全性を宣言する方法が現実的であると考える。

### 〈3･2〉　COTS を利用しての Fail-safety

図 5 で示した方法について、課題があることを述べた。その解決案についてこの項では提案する。

(1)　外部影響による独立性の阻害(Type C)の解決提案

外部影響として、衛星系の故障と、電波伝搬上の電離層の異常伝搬を述べた。これらの故障を検知し、システムを停止させる(Detection and Negation)ことが安全機能となる。

このため、衛星系の故障と電波伝搬上の異常伝搬を検知する方法を別途考えればよいことになる。

衛星系の故障は、測位衛星「みちびき」の仕様書によると、予期せずサービスエラーとなることを示す指標である ISF（Integrity Status Flag）が 1 の際のサービスエラー頻度は $10^{-8}$/h 以下とされている。この値は重要な保安装置に設定される THR（Tolerable Hazard Rate）と比較しほぼ上限であるため、THR の概念のみでいえば、衛星の不安全故障は一定程度担保されているといえる。ただし、より悪い状況である ISF=0 となった場合、ユーザーのシステムが Detection and Negation を行うとすると、この機能が TFFR を満たすように処置することは依然課題として残る。

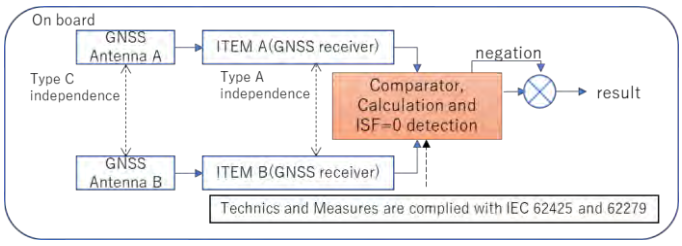


**図 6**　みちびきにおける ISF 活用の例

Fig. 6.　An example of positioning using QZSS with ISF data

また、ISF=1 の際のサービスエラー頻度が $10^{-8}$/h 以下としても、このことだけで、IEC 62425 規格適合とすることができず、規格適合性を条件にされた場合についての課題は残ることとなる。

次に、衛星系の規格適合は考えず、一定の THR は担

保されていると考え、ISF=0 となった時の安全動作を GNSS 受信機で規格に適合するような方法で担保することが考えられる。GNSS 受信機において ISF=0 であれば安全側動作するということになると、下記(2)にも関係するが、図 6 において GNSS 受信機である ITEM A, B が所要の TFFR を満たしながら ISF を出力できるかどうかの、ソフトウェア及びハードウェアの安全性の議論が生じてしまう。ここまでいけば、ある一定の割り切りを行うことも考えとしてあり、それを否定するものではないが、規格適合性としては課題が生じる。

規格に適合するためには、衛星系の故障を把握し、その情報を用いて確実に Detection and Negation をすることを定量的に述べることが必要となる。

(2) 測位センサがソフトウェアを持つことへの対策

GNSS 受信機は、RF 信号を中間周波数までダウンコンバートし、IQ 復調を行い、拡散符号と相関をとり、符号を取り出すところまでは一般の無線受信機と同じである。反面、GNSS の測位アルゴリズムの実装はアプリケーションソフトウェアそのものであり、仮にワンチップ化されていてもロジックの実装という意味ではソフトウェアと大きく変わるところがない。保安装置に GNSS 受信機を使用する場合、測位が誤った値を出すと、一般的には非常に重大な結果をもたらすと評価されることとなり、測位機能に厳しい TFFR が求められることとなる。このため、この TFFR に相当する SIL 及び Software SIL(SSIL)が割り当てられ、GNSS 受信機には SSIL のレベルに合わせた規格の要求する管理手法などが必要となる。しかしながら COTS 中心の GNSS 受信機のソフトウェアを、規格の要求する管理手法で作成することは現時点ではあまり現実的な解とは言えない。

このため、ソフトウェアにより測位結果が誤ったとしても ITEM A と B が共通原因故障とならないような対処をすることにより、測位結果を比較するロジックに安全要求を行い、測位結果自体には安全要求を行わないという考え方をとることが考えられる。すなわち、測位結果が誤ったところで、同時に誤ることの蓋然性が非常に低いため、比較装置のみに安全性を求めるという考え方である。これは、ITEM A,B とソフトウェアダイバシティをとることにより対処が可能であると考えられる。

### 〈3･3〉 提案する方式

提案する方式を図 7 に示す。衛星系の故障及び電波伝搬上の異常は、固定された GNSS 受信装置で連続的に位置受信を行うことで、あるべき値との比較を行うことで、異常を検知する。これは電波伝搬上の電離層の影響が同一であると考えられる間隔で設置する。ただし、車載の GNSS 受信装置において、電離層の伝搬異常だけではなく、伝搬経路が複数あることによる影響による誤差拡大なども考えられる。これについて、鉄道は同一ルートしか走行しないため、衛星配置上受信しない天空位置を決めておくなどの対処がある。

衛星系の故障及び電波伝搬上の異常が発生する判定装置は、Detection and Negation の中心であり、異常の判定を行い、システムを停止させる機能には安全要求が生じる。このため、この部分には規格上要求される要求事項を満たすように設計及び製作を行う。

また、車上装置の GNSS 受信機は COTS を採用することを前提とし、複数設けるとともに、ソフトウェアダイバシティを行うことにより、複数のランダム故障及びシステマティック故障を防止する。

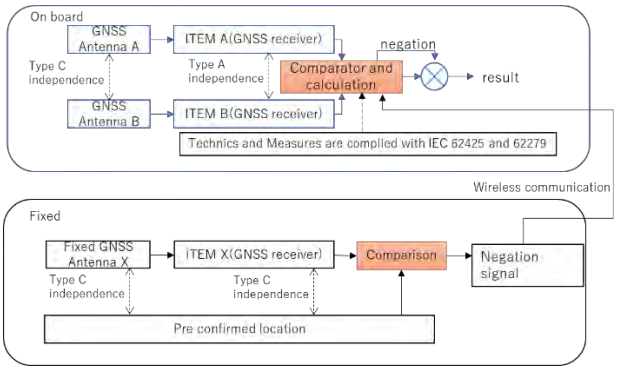


**図 7** みちびきを活用した安全関連位置検知の一例

Fig. 7. An example for safety related positioning system using QZSS

## 3. 終わりに

本稿では、IEC 62425 及び 62279 規格に整合できる可能性のあるシステム構成を示した。しかしながら、安全機能として、ここまで必要であるかという議論はあると考える。ただしいずれにしても、安全に対する説明の必要性は変わらない。今後とも規格適合性審査を通して努力してまいりたい。

## 文　　献

(1) 速度発電機と慣性センサを併用した高精度列車位置検知システム, 第 272 回 鉄道総研月例発表会, 2013
https://www.rtri.or.jp/events/getsurei/2013/summary272.html

(2) Quasi-Zenith Satellite System Performance Standard (PS-QZSS-003), Cabinet office, Japanese Government, Mar 17, 2022