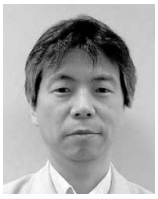
（論文）

クレーンの電子制御システムにおける安全性と信頼性の基本概念

Basic Concepts of Safety and Reliability for Electronic Control Systems Embedded in Mobile Cranes




山下俊郎*1　Toshiro YAMASHITA
下村耕一*2　Koichi SHIMOMURA

This paper describes the design concepts for electronic control systems used in the mobile cranes manufactured by KOBELCO CRANES CO., LTD., focusing on safety and reliability. The main power system of the cranes is hydraulic, but highly functional electronic control systems, including data communication, have been developed and implemented for better control and operation. The highest priority in the design concepts of the electronic control systems is safety and reliability. The contents of the paper include the present status of electronic systems, our basic philosophy of safety and reliability, risks and risk assessment, verification of safety and reliability, and designs for functional safety.

まえがき＝現在の移動式クレーンの主要駆動部は油圧システムであるが，油圧回路だけでは実現できない操作性やエネルギー損失の低減，利便性の向上，および安全性の確保を目的に電子制御化が着々と進んでいる。

一方で，欧州の機械指令を受けて，電子機器を使った機械製品の安全性に関する国際規格が制定されつつある。1999年に制定されたIEC 61508は，安全レベルの定量化概念が強く意識された規格であったが，長い間，特定の分野に限定され個々の産業機械への適用は寛容で緩やかであった。しかし，電気自動車やハイブリッド電気自動車に代表されるように，一般利用される自動車のような機械でも電子制御が必須の技術となっており，安全性に関する国際規格ISO26262が自動車業界で施行されるに至っている。

こうした動きは，安全性に関する国際規格への対応促進の現れであり，様々な分野で安全性の明示化が求められている。移動式クレーンにおいては，欧州移動式クレーン規格EN13000でISO13849-1が引用され，欧州向けの機械に対しては必須の適用要件である。

グローバル戦略を打出すコベルコクレーン㈱としては，安全規格に則りつつ電子制御化を進める必要がある。また，目標とする信頼性を確保するには，電子制御の要となる汎用コントローラを中心とする電気制御システムの安全性および信頼性の考え方を一定に保ち，管理する必要がある。

本稿では，まずクレーン電子制御システムのハードを概括したあと，安全性と信頼性の関係とそれを確実に実現するプロセスを紹介し，具体的な取組を解説する。

1. 電子システム化の現状

移動式クレーンにおいて電子変換される入力情報には，ブーム角度やブーム長さ，各種圧力，安全保護装置用リミットスイッチに代表される状態量，各種切替え，設定などがある。これに対して出力情報には，油圧流量制御のための比例弁の開度，流れの遮断／通過を制御する電磁弁の開閉，表示機，リレーによる安全機能への切替えなどがある。

電子制御の基本的な処理の流れは，入力された物理量を電気的な信号に変換して論理演算を行ったあと，所要の出力（指令）を行う一連のものである。機能をなるべく集中して管理できるよう，コベルコクレーン㈱の汎用コントローラには多くのセンサやアクチュエータが接続され，入出力点数は100を超えている。さらに，インターロックなど安全確認ロジックも増大するため，一つの機能を実現する演算処理に対して多くの入力情報が交錯することになり，共有すべき情報は一つのコントローラではとても処理しきれなくなる。

そこで，コベルコクレーン㈱が新規に開発したホイールクレーンやクローラクレーンにおいては，共通バスCAN[1)]（Controller Area Network）を使った通信でコントローラ間の情報伝達を実現している。また，独自設計した汎用コントローラを複数個搭載し，個々に機能分化した分散システムを構築した。**図1**のクレーンシステム構成例では，汎用コントローラが4台，過負荷防止装置1台，さらにエンジン，走行系で各1台といったネットワークシステムを構築している。配線長が異なるこれらの通信ラインに対しては，ノイズに対応した配線設計を行

*1 技術開発本部　電子技術研究所　*2 コベルコクレーン㈱　開発本部　要素開発部

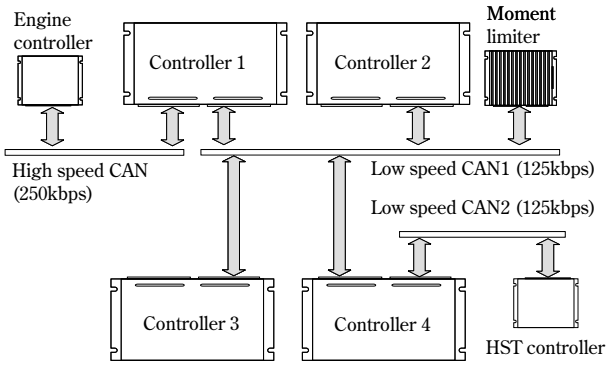


図 1 コントローラネットワークシステム
Fig. 1 Network of controller system

っている。また，高速帯域（250kbps）が必要なラインはエンジン指令といった機器との接続に使用し，低速域（125kbps）のCANラインとは切分けている。

2. 安全性と信頼性の考え方

移動式クレーンは，野外の建設現場で全天候環境下に置かれ，現場の作業者と連携してオペレータが操縦する機械である。また，工事計画の工程に大きく影響を及ぼす機械でもある。

その移動式クレーンの安全性とは，作業中や移動中，組立中など，いかなる状況においても危険な状態に陥らないことである。移動式クレーンにおける危険事象として，主に以下が考えられる。

・意図しない吊り荷の落下
・荷振れ
・機械の転倒
・ブームの旋回・起伏による周辺物との干渉
・走行時の接触・巻込

こうした危険事象を発生させないようにするためには，発生要因の全てを根絶させるか，あるいは許容可能な程度に発生確率を下げる対策を施さねばならない。

一方，移動式クレーンの信頼性とは，機能の継続性である。主な機能である巻上げ・巻下げ，伸縮，起伏，旋回および走行がトラブルなく動作し続ける，あるいは何らかのトラブルに対しても，ある制限下で動作し続けることが必要である。工事計画を遅滞させないことは信頼性のあかしでもある。

以下では，電子機器の信頼性の前提となる安全性に対する取組を述べ，さらに，その信頼性の実現方法の実際について紹介する。

3. 安全性

3.1 電子化に伴う危険源

移動式クレーンは，アフリカの高温地域からシベリアの極低温地域まで，あるいはサバンナの乾燥地域から東南アジアの多湿な地域まで，多彩な環境下で使用される。

また，移動式クレーンは他の建設機械に比べても高さのある構造物であるため，落雷などの危険にさらされる可能性もある。さらに，作業現場への移動に伴う機械の組立や解体の際，配線の断線，地絡，天絡などの電気的なトラブルを引起こさないように注意する必要がある。

通信環境も常に良好な状態に保たれるとは限らない。外界ノイズや配線に関連した不具合などが原因となって通信異常をきたす場合がある。本システムで採用しているCAN通信の規格ではハード的に着信確認を行っていないため，通信データが消失して問題が起きることも考えられる。

すなわち，移動式クレーンは，苛酷な自然環境下での稼動や組立／解体中での損傷，通信データ消失などの危険にさらされることを前提として安全な状態を確保する必要がある。

3.2 リスク低減プロセス

安全設計においては，まず，リスクアセスメントが必要である。危険源を同定してリスクを見積ったあと，リスク評価によって危険源を特定し，その危険源を取除く一連のプロセスの実施が必要である。

一例として移動式クレーンが搭載する過負荷防止装置を考える。この装置は，転倒限界を超えて吊り荷を操作しようとすると自動停止させるものである。ジブやブームの長さおよび角度，旋回角度，シリンダ圧力などをセンサから取得し，機械に作用する転倒モーメントを算出する。その計算結果に基づき，転倒限界内で作業を行っているかを監視している。

ここで，これらセンサの異常も転倒原因となる危険源の一つとなる。そこで，転倒につながる危険源のリスクレベルを決定するため，ISO13849-1に定められるリスクグラフを使ったリスク分析（見積・評価）を行う。リスクグラフは，影響度，頻度，回避性によって判別され，移動式クレーンにおける最悪状態のリスクレベル（要求パフォーマンスレベル*PLr*）は**図 2**のように順位付けられる。レベルが*PLr*＝＜d＞以上ならば，基本的に危険源を取除きたい。もし取除けない場合は，1時間あたりの平均の危険側故障率を100万分の1以下に抑えるべきであることをISO13849-1は要求している。

またセンサ異常という危険源は，先にあげた断線，地絡，天絡，水濡れ，CPU異常などの考慮が必要との結論に至るが，例えば断線などの事象に対しては，センサ異常の検出機構を電子機器に設け，入力ポートが開放された際に電圧が想定範囲外になるように設計する。これによって，配線が断線していないかが検知でき，機械が危険状態に陥る可能性を排除することができる。

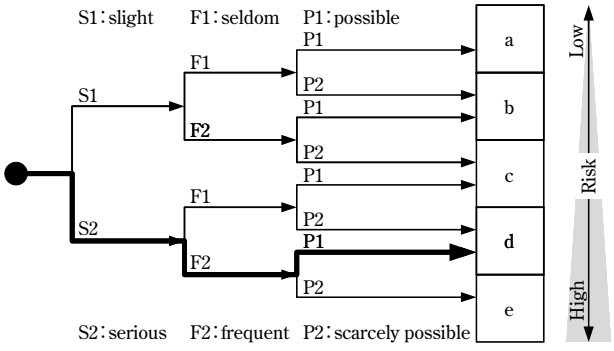


図 2 リスクグラフ
Fig. 2 Risk graph

3.3　システムの安全性検証

前節で述べたリスク低減プロセスに従って設計を実施した後，それらの安全性を確認するためには，各種のDR（Design Review）を通して設計方針の一貫性を保つ活動が有効である。しかし上述のように，移動式クレーンの電子化が進み，これまでの油圧・機械のシステムに比べて見えにくい危険源が増えてきた。このため，DRを実施する前に，一定の安全水準を確保する定式的な手法である故障モード影響解析[2]（Failure Mode and Effects Analysis，以下FMEAという）による安全性確認を行っている。危険源をコントローラ内部の部品の故障レベルとして，その影響度，頻度，回避性をFMEAによってランク付けし，危険源の影響を考察する。

コベルコクレーン㈱の電子制御システムは機能分化したシステム構成のため，一つのコントローラにかかわるFMEAを実施すれば，その結果はあるまとまった機能に着目した検証になる。例えば走行コントローラのFMEAを実施すれば，走行系機能に着目した解析ができる。機能分化しているため，あえて階層化で分離するより，コントローラ内部の部品異常から機械全体に及ぼす影響までが確認できる。

走行系システムにおけるFMEAの適用例として，補助排気ブレーキ力が過大になる故障モード，すなわち最終段のアクチュエータ部分に対する水侵入を原因として，電流リーク，天絡，あるいはアクチュエータの機械的な故障などが発生し，制御不能な状態になる場合を考える。この故障モードの場合，結果として車両は止まる方向に作用するため，安全側故障として判断できる。しかし，さらに踏込んで，故障が発生したとしても不安全な状態に陥ることなく，機能の制限のみで使用し続けられるかという概念がある。この概念はディペンダビリティと呼ばれ，これに対する検討も行う必要がある。このケースでいえば，大きなブレーキ力が急にかかることによって走行安定性に問題が発生しないか，あるいはオペレータが慌てることによって問題が発生しないかという点までを検討する。最終的には，補助排気ブレーキ力が過大になることによって発生しうる最大のブレーキ力を実機検証の段階における確認項目として抽出した。実際の検証では，ブレーキ力がオペレータに及ぼす衝撃力の影響を確認した。

4. 信頼性

4.1　ハードウェア

電子機器の信頼性は一般的に，**図3**に示したようなバスタブ曲線[3]で表現される。バスタブ曲線は，初期故障（Early failure），偶発故障（Chance failure），および摩耗故障（Wear-out failure）の三つに区分するモデルで表され，実状ともよく一致している。これまでのクレーンでは，機械，あるいは油圧による制御機器が主に用いられていたが，これらの構成部品は自然環境による偶発的な故障は非常に少ない。このため，それらの寿命は摩耗故障によって決定するといってよく，緩やかな変化を経て故障に至る場合が多い。

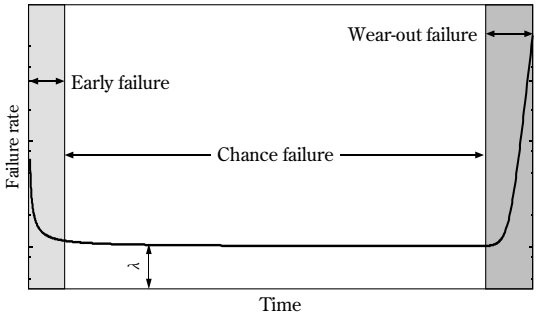


図3　バスタブ曲線
Fig. 3　Bathtub curve

これに対して，電子機器の信頼性においては偶発故障期の故障率の扱い方が重要となる。クレーンにおける電子システムは，コントローラに代表されるように一様ではない多種の部品を集めたシステムである。それらの部品は，電波や雷などの電気的な要因による影響を他の機械類より受けやすい。システム設計時に想定しうる事象をあげ，そのレベルや頻度に応じた設計を行うのであるが，全ての自然事象のレベルを想定することは困難である。このため電子部品の故障は，偶発故障期に一定の故障率をもって事象が発現することを考える。

我々の使用する電子装置においては，データベースを基に各部品の故障率を計算し，機能停止を観点に影響度を考えて対処を行っている。ここでもFMEAを活用し，機能停止に対する顧客の損害を考慮して全体のレベルに一貫性をもたせている。

こういった特殊な状況をできる限り考慮に入れたうえで装置寿命を延ばす手法としてディレーティングがある。これは，温度，電圧などの加速（ストレス）要因に対して，定格の数分の1の状態で使用することによって装置の寿命を延ばすことが期待できるとする考え方に基づくものであり，実際に多くの場合に適用できる。したがって，ディレーティングを考慮することは設計を行ううえで重要である。また，ディレーティングを考慮することは，危険源に対するマージンが数倍に確保されるということでもあり，システム全体としての堅牢性を向上させることが期待できる。

電子部品の劣化では，抵抗の熱劣化や基板配線のマイグレーション，電界コンデンサのドライアップなどの典型的な劣化メカニズムが知られている。例えば，電界コンデンサは摩耗故障期的な現象で容量低下を招く。容量対コストの関係から，電源周辺にはアルミ電界コンデンサを使用することが多いなか，電子部品の中では温度上昇しやすい電源部には熱的劣化を考慮する必要がある。すなわち，アレニウス則を適用することによって想定寿命におけるコンデンサ容量を割り出さなければならない。容量の減少から想定される電源リップルなどの基本性能は設計時の確認試験項目として重要であり，偶発故障期の平均故障間隔[4]（Mean Time Between Failure，以下MTBFという）の考え方と区別して考察している。

4.2　ソフトウェア

機能・仕組みとして，また上述の活動例を通じてハードウェア的な信頼性が十分に確保できた。その一方で，

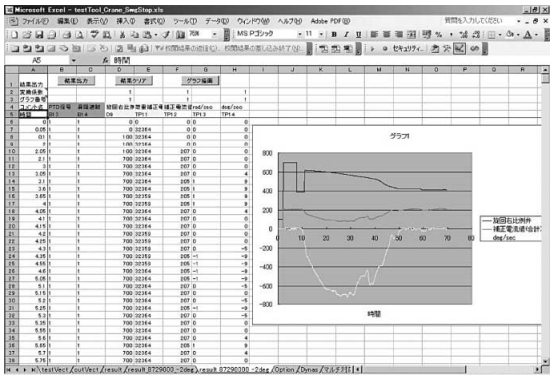


図 4 Kme ツールの画面例
Fig. 4 Screen shot of KmeTool

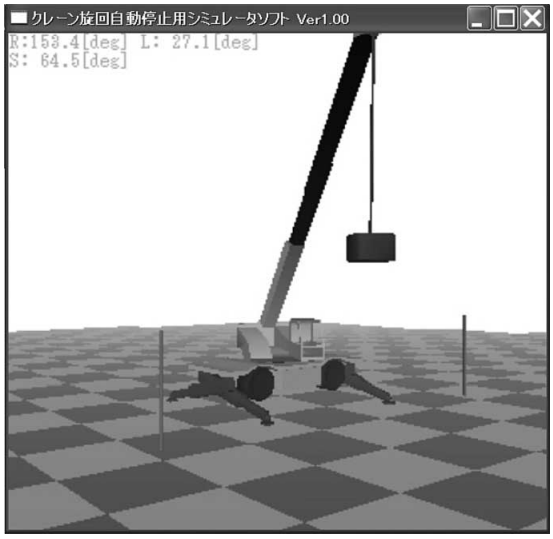


図 5 事前解析画面例
Fig. 5 Screen shot of Crane Simulator

コントローラに対してはさらに，ソフトウェアによる機能の実現が必要となり，ソフトウェアに対する評価が求められる。ソフトウェアは，まずは要求仕様に基づいた静的な検証がなされるべきである。しかし，それだけでは仕様に織込められていなかった問題を洗い出すことはできない。実機試験で全ての動作を検証することができれば問題ないが，あらゆる動作を検証することは事実上不可能である。

このため，ソフトウェア開発においてはシミュレータによる動的な検証が有効である。当社では，ソフトウェアの記述の正確さを確認する論理検証シミュレータとして「Kme ツール[5]」（**図 4**）を独自開発している。入力範囲と出力範囲が実環境下での論理範囲に入っているかどうかを確認できる。既存の機械からの情報を元に，現実的な数値範囲を検証している。さらに，動的な振舞いに対しても，実機試験の前にシミュレータによる検証を行うことは実機試験での確認ポイントを明らかにするうえでも重要であると考える。**図 5** に，コベルコクレーン㈱が開発したクレーンを対象とした動作シミュレータ[5] の画面例を示す。

5. 安全性と信頼性の両立

安全性を確実にするには，まず安全を“本質安全”と“機能安全”に切分けて考える必要がある。

まず，本質安全とは，危険源を根本的に排除する考え方である。例えば，移動式クレーンには，吊り荷の落下防止のためのカウンタバランス弁と呼ばれる油圧機構を設けている。これは，吊り荷時に発生する油圧のバランスを取る機構であり，途中の油圧配管が損傷した場合でも吊り荷が落下することを防ぐ。すなわち，カウンタバランス弁は，途中配管の損傷といった危険要因に対して，吊り荷の落下を根本的に解消することによって本質安全を確保している。

これに対して，本質安全としては対処できない，すなわち機械の目的機能を遂行する限り排除できない危険源や危険事象が存在する場合に，その危険事象の影響度，頻度，回避性を知ったうえで，その発生確率を許容できる範囲まで低減するとの考え方が機能安全である。

クレーン作業中のオペレータは，転倒の可能性のある体勢や荷重超過とならないよう注意を払って作業を進めているが，何らかの操作ミスによって安全領域を外れた場合においても，その危険を認識して停止させるのが先にあげた過負荷防止装置である。転倒しないよう，センサ計測によってブームの角度，荷重などを常時監視して安全を確保するには必須の装置である。ここでもし，センサが本来の値より軽いと判断する故障が発生したとき，不安定な領域でも動作が可能になってしまう。すなわち，過負荷防止装置が機能を失い，転倒事故という重大な危険事象に陥る。

そこで，転倒事故の影響度，頻度，回避性に応じた許容発生確率を導出し，その値が許容値以下となるようなセンサ系の冗長性や判断ロジックを設計するのが機能安全である。危険事象の発生確率を許容範囲まで低減するには，信頼性の確保に用いたのと同様の手法が適用できる。ただし，安全側故障と危険側故障を区別して扱う必要がある。上述の過負荷防止装置の例では，センサが本来の値より“重い”と判断する故障は，機能が停止したり制限されたりするが，危険事象には至らない安全側故障である。事前の安全性検討の段階で，危険側故障と安全側故障の比率を指標に，後者が多くなるようシステム設計することが肝要である。

機能安全は確率的手法に基づいているため，信頼性確保と同様にシステムの冗長化（並列化）対策が有効である。しかし，冗長化は一般に部品点数を増加させるため，各部品の信頼性が同じであれば，安全側故障をむやみに増やしてシステム全体に対する信頼性の低下（どこかが故障する状態が頻発し，すぐに機械が停止してしまう状態）に陥ることが懸念される。ここに，安全性と信頼性の“やっかいな軋轢（あつれき）”問題が生じる。

当社は以下の安全設計方針に基づき，安全性と信頼性の両立を目指す。

まず本質安全の追求を試み，そこに至ることのできなかった事象に絞って機能安全を検討する。危険度に応じて危険側故障の目標確率を定め，目標を明示化する。重大危険事象に対しては厳しい低確率化が要求されるため，その対策は過大な検討労力や装備を伴う。このため，機能安全として捉えるべき事象は厳選することが肝

要である。そのためには，システム全体にわたる構成のシンプルさの追求が一つの指導原理となる。例えば，信号入力から出力までの直列構成の部品点数の削減を検討する，あるいは，まずは実績の多い汎用的で信頼性の高い部品での検討を行う，といった思想が大切である。安全信頼性レベルの可視化確認には，まず定性的にはFMEAなどを用いたDR（Design Review）を行い，次に定量的判断としてMTBFなどによる数値比較を行うことが有効である。

ソフトウェア品質確保においても，上記ハードウェア同様の安全確保の思想継承が必要である。その場合，開発を補助するツール（エミュレータやシミュレータ）の開発が有効であり，制御アルゴリズムの論理の確実な実装と，その系統的な動作確認を周到に記録できることが重要である。開発期間の短縮，初期不良の削減，および偶発期におけるシステムの堅牢性の確保は常に改善が要求される問題である。こうした問題に対してシミュレーション技術を活用することにより，要求事項を可視化して確認できることから効果を上げている。設計仕様にフィードバックする際にもこれらシミュレーション技術が役立っている。

以上，安全性と信頼性を両立させるには，プロセスやツールを活用した設計方針を首尾一貫させることが欠かせないと結論する。ただ，設計仕様作成や実装などの各プロセスにおいては，技能レベルによって手戻りが多く発生するなど，品質を改善する余地がまだまだある。事業環境が変化するなかで安全性確保のプロセス自体の改善は継続的に続けていくことが必要である。

むすび＝安全性に関する国際規格においては，安全レベルの定量化とその明示化が進んでいる。そうしたなか，移動式クレーンにおける安全性の考えを示し，当社における取組み方を実例を交えて述べてきた。さらに，大規模になりつつある電子制御装置を用いたシステムに対する信頼性についても，その考え方と設計の基本コンセプトを述べた。

また，製品の安全性と信頼性の両立は重要な課題であり，全体システムとして品質を確保するためには各機能レベルに一貫性をもたせる活動が重要であることを述べた。コベルコクレーン㈱では，国内でも早い段階から機能安全規格に対する検討を進めてきており，全体システムとして品質を確保する活動を行っている。そして，そうした活動を通して，欧州移動式クレーン規格を満足する安全電子システムを構築すると同時に，より機械停止の少ない高い信頼性を確保する取組を続けている。そうした取組に不可欠となる支援ツールなどの開発によってこそ，安全性と信頼性を両立させた機械がより効率的に提供できるものと考え，プロセスの改善を継続する所存である。

参 考 文 献

1） Robert Bosch GmbH. CAN Specification 2.0. Part B, 1991.
2） 鈴木順二郎ほか．FMEA・FTA 実施法―信頼性・安全性解析と評価，日科技連，1982.
3） 原田耕介ほか．信頼性工学．養賢堂，1977, p.8.
4） 原田耕介ほか．信頼性工学，養賢堂，1977, p.6.
5） 下村耕一．新型ホイールクレーンにおける安全技術ー走行およびクレーン作業における安全性追求（特集 建設機械の安全技術）．建設機械．日本工業出版．2010, Vol.46, No.2, p.30.