生産システムにおける
セーフティ・セキュリティの技術動向

生産システムにおけるセーフティ・セキュリティ調査専門委員会編

目　　次

生産システムにおけるセーフティ・セキュリティ
調査専門委員会

委員長	宮澤　以鋼(神奈川県産総研)	委　員	神余　浩夫(三菱電機)
幹　事	森　泰二(富士電機アドテク)		月花　正志(富士電機機器制御)
幹　事	河重　隆一郎(山武)		小城　千明(オムロン)
委　員	関口　隆(よこはまＴＬＯ)		原　裕和(いすゞ自動車)
	藤本　康孝(横浜国立大学)		山田　稔久(新日鉄ｿﾘｭｰｼｮﾝｽﾞ)
	武田　有志(東京都立産技研究所)		脇屋　繁(石川島播磨重工業)
	赤羽　国治(横河電機)		塩見　勝(光洋電子工業)
	甘利　康文(セコム)		宮脇　信芳(ＪＴＥＫＴ)
	山崎　泰廣(綜警電気工事)		村上　正志(デジタル)
	梅田　裕二(東芝)		
	大槻ｼﾞｮﾝ琢也(i2 テクノロジーズ)		

なお,所属は設立当時。

1　はじめに

1.1　報告書の発行にあたって

『生産システムにおけるセーフティ・セキュリティ調査専門委員会』は，平成１７年３月～平成１９年２月の間に活動し，終了してから既に３年経つ。調査専門報告書をまとめている最中に機能安全に関する国際規格が大幅に修正され，その影響から，生産システムに関する機能安全の国際規格も，未だに決着していない。調査を続けているが，その他のテーマや課題は不変なものも多く，情報をまとめて提供する重要性からここに報告書を発行することにした。さらに，継続調査による新たな安全規格の動きなど，最新情報を極力まとめて盛り込むことにした。

具体的には，機能安全（Functional Safety）の国際規格 IEC 61508 シリーズが改訂となり，機能安全の考え方を含めてその内容が大幅に変更された。この影響を受けて，その下位の製品規格としての PLC（Programmable Controller）機能安全の規格 IEC 61131-6 の制定作業も遅れて未だに結論が得られていない。議論が収束せず，その先も見通せないことから，現在の情報を提供する目的で報告書をまとめることとした。他の調査報告内容は不変なものも多く，このまま発行することとするが，さらに新しい状況も生まれたことから，これらも極力まとめて提供することとした。一方，セーフティ・セキュリティについては多くのことが今も進行中で，その技術をすべて網羅することはとても無理であり，ここで調査を一段落として区切りを付けることとした。

以上の経緯から発行が遅れ，関係者各位に多大なご迷惑をおかけいたしたことを心からお詫び申し上げる。

1.2　生産システムの範囲

本調査は生産システムに限定して行ってきたが，生産システムという概念の範囲は必ずしも明確ではない。これについて委員会では時間を費やして議論をし，最終結論を得るには至らなかった。ただし，共通認識は，セーフティやセキュリティのそれぞれの意図とするテーマや課題によってその範囲が異なり，必ずしも明確に定義できるものではない。

しかし，電気学会の立場から見たときの生産システムは一般に生産における電気技術及びこれから派生した技術を中心にして論じられることから，生産システムは生産設備など生産技術とその周辺を対象としている。個別のテーマや課題によって，例えばその周辺として人間の介在を入れて考慮する場合があったとしても，セキュリティの観点の一つからいえば故意による人的被害は本調査報告書の範囲外となろう。

また，生産システム自体の曖昧さから，原料の供給などどこまで含まれているかも必ずしも明言はできないが，それぞれのテーマや課題が必要なところを範囲と定めることに任せることとし，その都度の生産システムの範囲は揺れ動くものと理解できる。すなわち，もっとも典型例として想定される生産システムは工場など一つの閉じた生産空間を想定し，必要によってその外延が列挙され，再定義されるものである。

さらにこれに影響を与えているのがネットワークの普及である。ネットワークの使用により，生産システムの範囲は無限に広がることと想定できる。また，近年の生産は在庫を最小にする考えから発注の段階の情報まで生産計画に組み込むことが主流になりつつあるが，本報告書は基本的にはそこまでは広げず，テーマや課題によって言及することに留めておく。

1.3　調査報告書の構成

本報告書は，概念，事例紹介，規格紹介及びリスクマネジメントの４部構成とした。

概念はセキュリティとセーフティのそれぞれについてその定義を与えておいた。事例紹介は異なる分野から選んで紹介した。さらに，規格は生産技術に直結するものを中心に詳細に説明した。最後のリスクマネジメントは，生産システムの範囲をより広範に捉えて一つの考え方として読者に供することとした。

とりわけ，規格紹介においては近年の動きを盛り込んだ。セーフティについては改定後の IEC 61508 機能安全及びその JIS 化の動きについて紹介する。さらに，安全全般については中国の提唱による IEC 61010 がアサインされ，現在その作業の状況について概観する。IEC 61010 は中国 GB の安全規格をまとめて IEC への登録を提唱してきたことによって指定された新しい安全の規格群である。現在作業が始まったところではあるが，特に DCS（Distributed Control System）までも含む PLC の安全全般に関する IEC 61010-2-201 が先行して制定作業が行われており，本報告書では，CD（Committee Draft）現段階の内容について紹介する。

一方，産業用ネットワークが既に広く普及されており，その上位層，さらにインターネットへのシームレスな接続も提唱されている中で，生産システムにおけるセキュリティの問題もクローズアップされつつある。本報告書では，生産システムにかかわるこれらの国際規格や関連団体の活動についても紹介する。