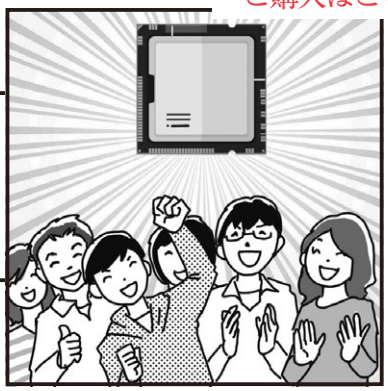
もう一度重要になる気がする

プロセッサ開発のセンス



第8回 自動車に見る…プロセッサの安全機構

丸目 佳

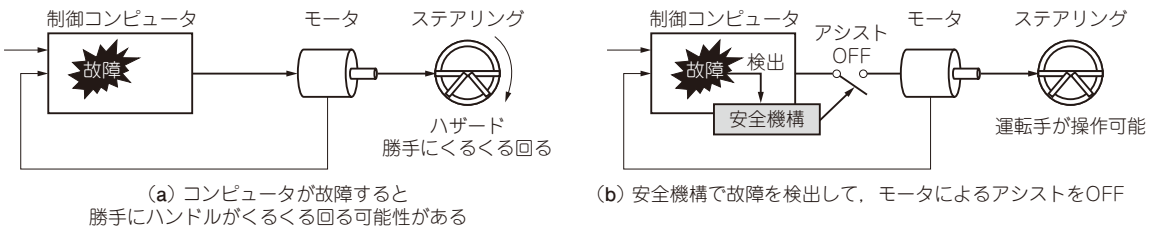


図1　電動パワー・ステアリング・システム概略図

今回は安心・安全がポイントです．故障が起きた後も人に被害が及ばないコンピュータに使われるプロセッサや，その上で動くソフトウェアの設計について説明します．

現在の車はさまざまなコンピュータにより走る，曲がる，止まるが制御されています．もし運転中にこれらのコンピュータに故障が起きた場合，運転手や周りの歩行者の命を脅かす事故に発展する可能性があります．このような車に搭載するコンピュータには，故障が起きにくいこと（高い信頼性）と故障が起きても人に被害が起きないこと（機能安全）が求められます．

機能安全…故障を検出して安全な状態にする工夫

人命に影響を及ぼす可能性のあるコンピュータに必要な機能安全について簡単に説明します．

機能安全という言葉の定義を話し始めると難しくなってしまうので，ここではコンピュータが動作中に何かしらの故障が発生しても人に被害が及ばないように工夫することと覚えておいてください．コンピュータを構成するハードウェアとソフトウェアに何かしらの故障が起きたとき（ここではソフトウェアのバグも故障と呼ぶことにする），故障を検出して安全な状態にする工夫（安全機構）を施して車を安全な状態にしなければなりません．

機能安全が必要な例…自動車

● 自動車の安全機構

図1に挙げた，自動車の電動パワー・ステアリング・システムのコンピュータを例に，この仕組みについて説明します．

このシステムでは運転手のステアリング操作量と現在のモータのアシスト量を元に，次のモータのアシスト量を計算します（実際はこの他に車速やその他さまざまな車の状態を元に制御するが，ここでは話を簡単にする）．動作中にコンピュータ内部に故障が発生した場合，最悪のケースではステアリングが勝手にくるくる回るセルフステア状態や，全く操作がきかなくなるステアリング・ロック状態になってしまう可能性があります．

そこで，コンピュータ（正確にはセンサやモータなど関係する部品全部）のハードウェア故障や，ハードウェアまたはソフトウェアのバグに起因する故障（動作異常）が起きた場合，安全機構によって，それらの動作異常を検出し，モータのアシスト動作を停止して（ステアリング操作は重くなるが），運転手が車を安全に停車，もしくは運転を継続できるようにします．

● 自動車は機能安全規格で安全レベルを規定

自動車の機能安全規格であるISO 26262では，システムの故障が人命に及ぼすリスクの大きさによってASIL（Automotive Safety Integrity Level）がA，B，

第1回　今どきのプロセッサ開発に求められること（2022年6月号）
第2回　先見性か自己満足か…プロセッサのコンセプト開発（2022年7月号）
第3回　みんな大好き？ CPU開発（2022年9月号）