燃焼安全ソリューションを支えるソフトウェア安全設計

Software Safety Design to Support Combustion Safety Solutions

アズビル株式会社
アドバンスオートメーションカンパニー　山田　晃 Akira Yamada

アズビル株式会社
アドバンスオートメーションカンパニー　中田　知也 Tomoya Nakata

キーワード
燃焼安全，バーナコントローラ，燃焼安全規格，ソフトウェア

工業用燃焼炉の技術革新と安全に対する要求により，燃焼安全計装に求められる機能が変化している。この変化に対応するためバーナコントローラは機能拡張しソフトウェアの重要度が増してきた。しかし，ソフトウェアにはハードウェアとは性質の異なる故障要因が存在し，従来の技法では安全を担保できない問題があった。そこで今回新しいバーナコントローラは機能安全の設計手法を導入した燃焼安全規格に適合するための独自アーキテクチャの採用を行い，安全性を確保している。

Technical innovations in industrial combustion furnaces and the demand for safety have changed the functionality requirements for combustion-related safety instrumentation. In order to address these changes, the functionality of burner controllers has been enhanced and the importance of their software has increased. However, due to the intrinsic differences between software and hardware, the causes of software failure differ from the failure factors for hardware. As a result, conventional techniques have become unable to secure safety. Against this background, we have developed a novel burner controller with a unique architecture that guarantees that the controller is safe to use, in order to comply with combustion safety standards that cover design methods for functional safety.

1. はじめに

工業用燃焼炉（以下工業炉）を取り巻く社会情勢は地球温暖化防止や省エネルギーを要求する世論などにより変化してきている。多大なエネルギーを消費し一度事故が発生すれば重大災害に繋がりかねない工業炉では，より高効率に，そして，より安全に運用することが社会から求められている。

工業炉を設計・製造するメーカーでは，高効率・省エネ化に対応すべくCO_2排出量の少ない燃料への転換や高性能工業炉などの新規技術を盛り込んだ工業炉の導入を進めている。新規技術導入に伴い制御は高速化・複雑化しており，多くのシステムにおいてソフトウェア（コンピュータ）の使用が前提となっている。

このため，ソフトウェアをベースとした際の安全構築とリスク低減が課題となっているが，新規技術とソフトウェアの利用という技術的変化により，従来行ってきた経験ベースの安全対策だけでは安全を担保し切れなくなってきている。

そのため，事故が起こる前に予期して防ぐ努力をしなければならないという考えが世の中に広まってきており，それに合わせて燃焼安全規格も変わりつつある。そこでは，リスクアセスメントに基づいた本質安全設計が求められており，検証と妥当性確認による工数増大や設計を行う人・組織のスキル不足などの課題が存在している。

2. 工業炉を取り巻く安全規格

工業炉やボイラなどの熱源機器においてはISO12100:2010（JIS B9700:2013）を基本とした製品安全規格の整備・改訂が進められている。

2008年には工業用燃焼炉の安全通則（JIS B8415:2008）が改訂された。これにより工業炉を設計・製造するメーカーや使用するユーザーは，設備のリスクアセスメント実施など

これまでと異なる考え方の導入により従来設備の安全見直しを行わねばならなくなった。特に設備への影響の大きい要素としては汎用プログラマブルロジックコントローラ（Programmable Logic Controller，略称:PLC）の安全機能部（インターロック処理など）への使用禁止，中継リレーの原則使用禁止，火炎の個別監視などが挙げられる。

また，2014年には機能安全の設計手法が導入された工業炉および関連するプロセス設備に関する安全規格ISO 13577シリーズの一部が発行され，将来的には工業炉の安全関連部は一般の制御と分離して，センサ，ロジックソルバ，最終要素からなるプロテクティブシステムと呼ばれるループを構築する必要が出てくる。

これにより，形成されたループで使用する機器は個別製品安全規格（例:IEC60730-2-5，EN298など）に適合しているか，SIL3（Safety Integrity Level 3）/PLe（Performance Level e）Capable相当の能力を有する必要があり，かつ，形成されたループ全体として安全上の検証と妥当性の確認が求められることとなる。

バーナコントローラや火炎センサに適用される個別製品安全規格も変わってきている。従来までは満たすべきタイミングや電気的特性といった製品に対する要求がまとめられていた。しかし，前述の安全に対する考え方の変化によりこの個別製品安全規格にも機能安全ベースの要求が追加され，リスクアセスメントや検証と妥当性確認が求められるようになった。

一例として，EN298は2012年に改訂され，その際に機能安全規格IEC61508の流れをくむ要求「EN298:2012,6.6 Protection against internal faults for the purpose of functional safety」が新たに追加されている。

3. ソフトウェアのリスク

ハードウェアは，故障モードが比較的容易に判別できる。この特性によりFMEAやFTAなどの技法を用いて的確に安全検証を行うことができる。さらに部品の故障率などからリスク発生を定量的に把握できるので適切な保守作業によりリスク軽減を行うことができる。

ソフトウェアは偶発故障や摩耗故障がなく，設計ミスの対処のみが必要になる。安全仕様の不備やバグなどのソフトウェアの設計ミスは，条件が揃えば100%顕在化するものであり，これらは冗長設計などのハードウェア的なリスク抑制策では対処できない。

したがって，設計段階で，設計ミスを作りこまないようにすることが必要になってくるが，ソフトウェアの設計ミスの発見と除去は非常に困難である。

ソフトウェア設計を難しくしている理由として複雑さの問題がある。単純なシステムなら完全なプログラムを設計することはできるかもしれないが，現在稼働しているシステムは多くの制御要素がありソフトウェアの規模は大きなものとなっている。適切な管理が行われないソフトウェア開発においては，設計が進むにつれて複雑さは増し，人の手に負えなくなり，多くの設計ミスが入り込むだけでなく，それを見つけることも困難にしている。また，全ての入力やパラメータの組合わせは無限に存在し，全てをテストすることは不可能である。

ソフトウェアは容易に変更が可能である。よってシステムの稼働後も頻繁に仕様変更が行われる。通常，生産性が優先されるので，ちょっとした変更は短時間で行うことが求められ，十分なリスク検証が行われない場合がある。ソフトウェアのモジュールは相互に依存関係があり，設計者の意図しないところで影響が波及する場合がある。このようにシステムが寿命を迎えるまで常にソフトウェアの変更リスクがつきまとう。

ソフトウェアのリスクに対する規格の要求事項はあいまいな点が多く理解することが難しいが，基本的には，定められた設計プロセスの中で，適切に設計，検証が行われていることが求められる。さらにコーディングルールや形式化手法などの数百に及ぶ設計技法の使用の要求や，推奨がされている（表1）。

表1　技法例：設計およびコーディング基準

技法 / 措置	SIL1	SIL2	SIL3	SIL4
コーディング基準の使用	HR	HR	HR	HR
動的オブジェクトなし	R	HR	HR	HR
動的変数なし	―	R	HR	HR
動的変数追加時のオンラインチェック	―	R	HR	HR
割込みの使用制限	R	R	HR	HR
ポインタの使用制限	―	R	HR	HR
再帰の使用制限	―	R	HR	HR
高級言語のプログラム内に非構造化制御フローがない	R	HR	HR	HR
自動変換を行っていない	R	HR	HR	HR

HR：強い推奨。不使用には根拠が必要
R：HR より低い推奨
―：推奨も反対もしない
NR：積極的に推奨しない。使用には根拠が必要
SILn：安全度水準。4 が最高水準

近年になって，ソフトウェア開発をサポートする有用なツールが出てきているが，残念ながらソフトウェアの課題を解決する万能薬はない。現在においては適切なプロセス管理により，リスクを正しく認識し，設計の複雑さ，あいまいさを排除し，確実な検証を行うことが現実的なアプローチとなっている。

4. 燃焼安全計装の変遷と課題

4.1　従来計装の問題点

安全規格，ソフトウェアのリスク以外の問題点として，従来の燃焼安全計装の問題点が存在する。

従来のバーナコントローラはハードウェアを主体とした安全設計で，機能も単体のバーナ制御および燃料遮断のみを受け持つといったシンプルな構成だった。そして装置の制御だけでなく，インターロックの取込みといった安全機能までも汎用PLCで行われる場合が多かった（図1）。

しかし，汎用PLCでは安全性が保障されないことより，工業用燃焼炉の安全通則（JIS B8415）では安全関連部への汎用PLCの使用を禁止した。

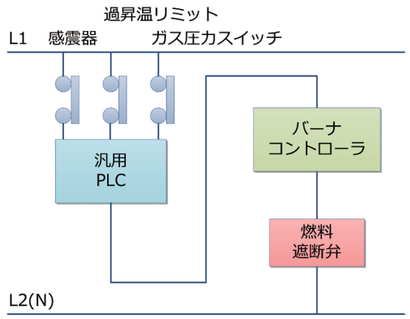

図1　汎用 PLC を中心とした従来計装

インターロックについては，従来の負荷電源直切り（図2）は本質的に安全であるが，設備の要求に満足できなくなってきている。ある条件下で監視が必要なインターロックや，接点のチャタリングを防止するためにフィルタが必要な場合がある。また，システムの異常により同時に複数のインターロックが作動する場合があり，異常のメカニズムを正しく認識するには，どのような順でインターロックが作動したのかを知る必要がある。これらの点についてハードワイヤリングによるインターロック構成は限界にきており，ソフトウェアによるインターロック監視が必要になってきている。

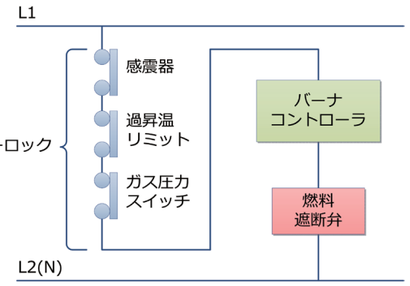

図2　インターロック構成

これらの問題を解決できる機器として，安全PLCまたはazbilグループが新規開発を行ったバーナコントローラが挙げられる。

4.2　安全PLCの課題

安全PLCは汎用PLCとは異なり，ハードウェアの多重化，安全関連部品の自己診断，アプリケーションの多重化演算といった安全機能を有しているのが特徴と言える。ラダーやファンクションブロックダイアグラムといった言語で組んだソフトウェアアプリケーションを自ら構築することができるため，制御における柔軟性は高く，前述の設備の多様化・多機能化にも対応することが可能である。

しかし，このように作成したアプリケーションはソフトウェアのため，製品開発を行う場合と同様の検証・妥当性確認を実施する必要がある。もし燃焼安全機能に関してのアプリケーションを構築するのであれば，その部分は個別製品安全規格に対応して検証と妥当性確認を行う必要がある。

燃焼関連に関しては，メーカーより認証済みファンクションブロックが提供されていれば，その部分についての検証と妥当性確認を省くことができるが，周辺ファンクションブロックとの接続や他の安全関連アプリケーションについては検証と妥当性確認が必要なことには変わりがない。

このアプリケーション適合を行うためには，専門技能を有する人材の確保や多くの工数がかかるため，安全PLC導入における大きな負担になると考える。

4.3　新バーナコントローラによる解決

これまでに述べた課題に対応すべく，当社では従来製品と同等の安全性を確保しつつ制御性を高めたバーナコントローラRXシリーズを2010年に，BC-Rシリーズを2013年にリリースした。

新たなバーナコントローラは安全機能の実装においてもソフトウェアの占める割合が高くなっている。ソフトウェアも含めて製品開発段階で個別製品安全規格のEN298に適合しているため，バーナコントローラ導入時にソフトウェアのアセスメントを行う必要がないのが利点である。

次項では，バーナコントローラRXシリーズと汎用PLCを用いた燃焼安全ソリューションについてまとめる。

5. azbil が提案する燃焼安全ソリューション

工業炉の技術進歩に伴い，システムの高速化や高精度化が進んでいる。一方，安全に関する規制は年々厳しくなる傾向がある。一般的に，制御性と安全性はトレードオフの関係にあると言われる。制御スピードを上げると安全性が損なわれ，逆に，安全性を重視すると制御性が悪くなる傾向がある。制御性と安全性をうまく調和させることが求められるが，これを実現したモジュールタイプのバーナコントローラRXシリーズを使用した計装を図3に示す。工業炉の中でも規模の大きい加熱炉や熱処理炉では，複数の燃焼室（マルチゾーン）で構成される場合が多い。このような炉を含む生産システムにおいては，原料（ワーク）の搬送，エアー設備など燃焼以外の関連設備があり，これらは汎用PLCによって制御されている。また効率良く生産を行うためにシステム全体を監視する分散制御システム（Distributed Control System，略称:DCS）も利用されている。

(1) 制御系と安全系の分離

システムの安全設計として制御系と安全系を完全に分離することが必要である。バーナコントローラなどの安全機器のみがインターロックや燃料遮断弁を接続することができる。本例に示すように汎用PLCなどのプログラマブルコントローラで実行される制御系と，バーナコントローラが担当す

特集論文

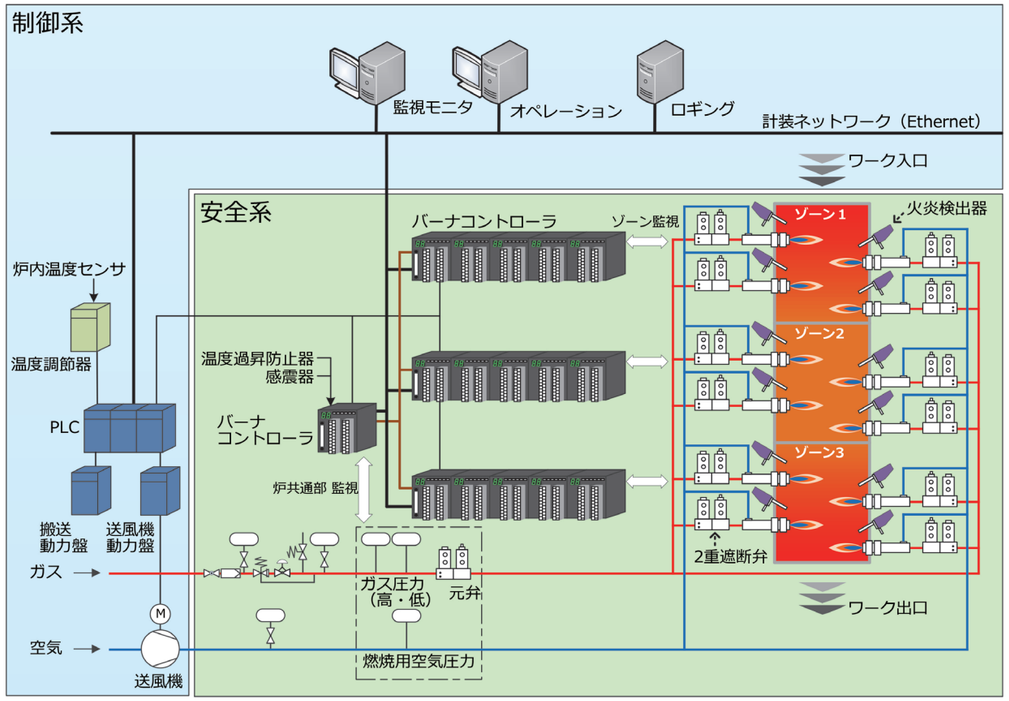

図３　ソリューション事例

る安全系は，明確に分離されていることが必要である。通常は，制御系(汎用PLC)が炉全体の運転シーケンスを実行し，その運転指令に基づき安全系(バーナコントローラ)は燃焼装置の制御を実行する。安全系(バーナコントローラ)では，燃焼安全に関わる必要最小限の制御を行い，制御系(汎用PLC)の設計自由度が高くなるように配慮している。

(2) 階層化されたインターロック監視

安定的に生産を行うために，生産ラインを冗長化するなどの工夫が行われる。そこでは一部のインターロックが作動してもシステム全体を止めることなく，該当する燃焼炉のみを停止させることができる(一方，感震器などシステム全体を停止させるインターロックもある)。

モジュールタイプのRXシリーズは，インターロックの対象範囲を階層化し，システムに応じてフレキシブルに安全設計を行うことができる。

(3) ソリューションの効果

従来製品では，多くのリレーやタイマなどの外部回路を組み合わせてシステム構築を行っていた。配線は膨大となり複雑化していたため安全検証が困難あるいは不可能な状況にあった。当社のバーナコントローラ，火炎検出器，燃料遮断弁を組み合わせることで，省配線/省スペースを実現できる。また，プログラムレスであらかじめ作り込まれている安全機能を選択するだけで機能実現でき，ユーザーにおけるソフトウェアの設計･検証のためのエンジニアリング工数やリスクを大幅に低減できるものとなっている。

図４　azbil 燃焼安全計装ソリューション

6. バーナコントローラ RX・BC-R の開発

6.1　安全性の確保

前述の通り，新たなバーナコントローラはソフトウェアの占める割合が高くなりリスクも増大しているため，独自の安全アーキテクチャを導入することと，個別製品安全規格のEN298およびIEC60730-2-5で規定されているCPUおよび関連ハードウェアとそのソフトウェアの障害対策に適合することにより安全性の確保を行っている。

6.2　安全レベルの要求

バーナコントローラは爆発を防ぐための機器であり，万が一の事故が発生した場合は人命を損なう可能性があるため，EN298ではソフトウェアクラスCという一番厳しい安全レベルを満たすことと位置づけられている。また，EN298が参照するIEC61508に当てはめると，安全度水準はSIL3を満たす必要がある。

そのため，規格認証においても厳格なチェックが求められる。

6.3　安全アーキテクチャ

燃焼安全機器として求められる安全レベルを満足するために当社では，1oo2D（診断機能付デュアルチャンネル）のアーキテクチャを採用した(図5)。

入力部はシングルチャンネルとなるが，ロジックと出力部はデュアルチャンネルとなり，各チャンネルの出力結果が一致しないとアクチュエータは駆動できない構成となる。

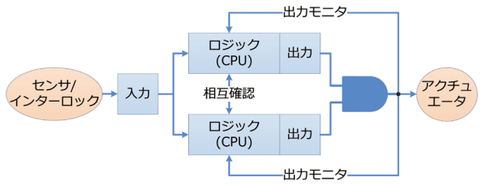

図５　安全アーキテクチャ

診断として，出力モニタ，ロジック（CPU）のセルフチェックおよびロジック（CPU）間の相互チェックが行われる。入力信号，出力信号および出力モニタなどの安全関連部の信号はパルス信号(ダイナミック信号)を基本とする。これにより診断系も含めて部品の危険側故障を検出することができる。規格上二つまでの故障に対して安全確保が求められる。二つ目の故障は一つ目の故障から1時間経過後に発生するものとしていることから診断周期は1時間未満が求められると思われたが，認証機関の審査官によるとデュアルチャンネルにしたことでCPUの診断周期として24時間以内で良いとされている。シングルチャンネルに比べて診断周期の時間制約や高度な診断手法は要求されないことで，ソフトウェアの構造はシンプルな設計とすることができる。割込み処理も必要最小限とし，OS（オペレーティングシステム）を使用しないなど，ソフトウェアの複雑さを極力排除することを心掛けた。デュアルチャンネルのアーキテクチャであってもCPUの全ての構成要素は，可能な限り診断しなければならない。以下に診断の内容について示す。

- 演算/制御結果について自己および相互チェック
- 安全パラメータの自己および相互チェック
- プログラム実行順のチェック
- 内蔵RAM，レジスタの固着チェック
- CRCコードによるFlashROM，EEPROMのチェック
- 割込み処理層のデッドロックチェック
- スタックレジスタのチェック
- 命令コードの動作チェック
- タイマ割込み処理の周期チェック
- CPU間通信のフォールト抑制

6.4　独自の安全アーキテクチャ

規格に適合するだけではなく独自のアーキテクチャを採用することでさらなる安全性の追求を行っている。設計の一例として，クロックの相互チェックと多様化について示す。シーケンスタイミングを守ることは安全上重要なことであり，シーケンスの実行周期は厳密にチェックされる。図6に，シーケンス処理とタイミング監視の構成を示す。デュアルチャンネルの各CPUにおいてソフトウェアは三つの処理層（二つのタイマ割込みとバックグランド処理）をもつ。シーケンス実行部は20msタイマ割込み処理に含まれる。処理層は相互にタイミングをチェックし，CPU間は基準クロックを交換しタイミングをチェックすることでシーケンス実行周期の正しさを保障する。

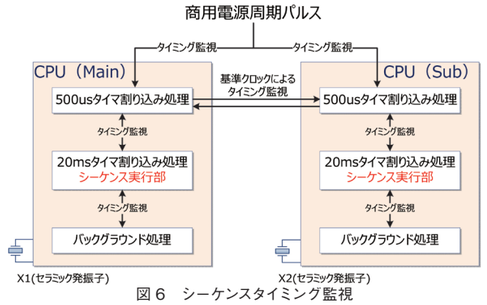

図６　シーケンスタイミング監視

ここで各CPUにクロックを供給するセラミック発振子は故障や温度特性，経年変化の特性は似たものとなるので相互比較では異常検出できない危険性がある(図7)。単一の要因によって冗長系が失われてしまう故障(障害)を共通原因故障と言う。そこで動作原理の異なる商用電源周期パルスのチェックを加え，クロック信号の多様化により対策としている。

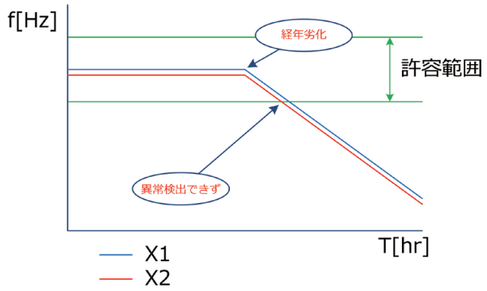

図７　クロック故障例

6.5　ソフトウェアのプロセス管理

前述の通り，ソフトウェアには偶発的な故障はなく，すべて設計ミスで作り込まれた故障となる。そのためソフトウェアに対しての安全要求が設計され検証がなされていることを証明することが必要となる。規格EN298:2012はソフトウェアに関してはIEC61508-3を参照しており，規定されているVモデル（図8）に従って，要求仕様から設計，実装に至る製品の具現化の方法と，それぞれに対して検証および妥当性確認が適切に行われているか体系的に示すことが求められる。

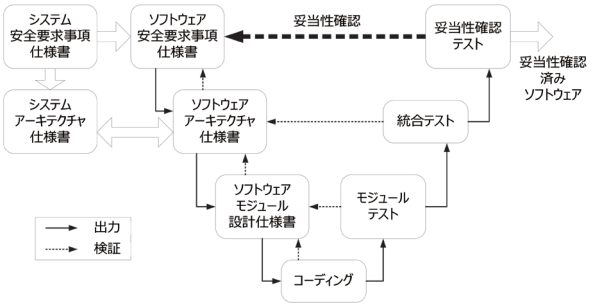

図８　Ｖモデル

開発プロセスを仕様定義，アーキテクチャ設計，モジュール設計などに階層化しプロセスの成果物を理解しやすく可視化することで検証の抜けや誤りを防止することが求められる。

6.6　ソフトウェアの文書管理

Vモデルを用いた安全要求の検証と妥当性の確認が正しく行われたことを示すために全ての成果物に対する文書化が必要となる。文書化に関する規格の要求事項を次に示す。

1)正確であり，曖昧さがなく利用者が明確に理解できること
2)要求事項が識別できること，評価基準が明確であり検証可能であること
3)管理基準(バージョン管理，改訂履歴など)が規定されていること
4)要求事項，設計仕様およびテストの関連についてのトレーサビリティ

特に重要な点として4)項のトレーサビリティが挙げられる。要求仕様がどのように解釈され実装に至ったのか，またそれぞれのテストフェーズにおいて，どのような方法を用いて仕様の確認を行ったのか，作業のモレや誤りを検出するためには，これらの関係がトレースできなければならない。また，開発段階や開発完了後も仕様変更や改良が入る。トレーサビリティの管理により変更による安全機能への影響箇所を見極めることが可能になり，安全機能に対する検証の抜けを防止することができる。また，変更作業を，Vモデルのどのフェーズから始めればよいのか判断することができる。

工業炉の安全設計を行う場合，燃焼技術，ハードウェア，ソフトウェア，システム設計，人間工学など広範囲の知識が必要となり，複数の人が関わる共同作業が必要となってきている。フェーズの移行にあたってのチェックゲートとして成果物のレビューを行う。ここでは，ソフトウェア技術者だけでなく，様々な専門分野の人が参加し，多様な視点により審査が行われる。

妥当性確認により最終的な確認が行われ，ソフトウェア開発が完了する。

6.7　規格認証

バーナコントローラは，個別製品安全規格EN298に適合するため欧州の第三者認証機関の監査を受けている。利用した第三者認証機関の特徴として実地確認を行うことが挙げられる。

監査は事前送付したドキュメントに対する審査と来日した認証エンジニアによる実地確認とで行われる。

実地確認は丸一週間かけて行われ，機能面では正常動作確認およびフォールト動作確認を行い，規格上求められている要求が満たされているかを一つずつ確認した。フォールト動作確認ではフォールトの挿入方法の確認やフォールト条件を変えた抜打ち試験といった，開発者の対応能力が試される場面もあった。ソフトウェアに関しては，コードウォークスルーやコーディング方法，プロセス･文章管理方法の確認が行われた。

第三者認証機関による妥当性確認が終わり問題なければ，第三者認証機関は最終レポートと認証書の発行を行い認証は完了となる。

7. おわりに

本論文で示したように工業炉の現場における従来計装のソフトウェア･エンジニアリングには多くの課題が残されている。当社はこれからも，グループ理念である「人を中心としたオートメーション」の下，燃焼安全ソリューションを発展させ，工業炉の現場における課題解決力を強化し，お客さまの安全。安心の実現に貢献していきたい。

＜参考文献＞

(1)熊澤雄一:燃焼安全制御技術を用いたコントローラの開発，azbil Technical Review，2011年1月号
(2)山田晃ほか:燃焼安全技術の開発と燃焼安全ソリューションへの応用，計測と制御第53巻 第12号2014年12 月号
(3)安全PLCを用いた機械･設備の安全回路事例集，(一社)日本電機工業会 技11-01
(4)JIS B8415:2008 工業用燃焼炉の安全通則
(5)EN298:2003 Automatic gas burner control system for gas burners and gas burning appliances with or without fans
(6)EN298:2012 Automatic burner control system for burners and appliances burning gaseous or liquid fuels
(7)IEC60730-1:2011 Automatic electrical controls for household and similar use –Part 1: General requirements
(8)IEC60730-2-5:2000 Automatic electrical controls for household and similar use –Part 2-5: Particular requirements for automatic electrical burner control system
(9)IEC61508-3:2010 Functional safety of electrical/electronic/programmable electronic safety-related system – Part 3: Software requirements
(10)二村元規:工業炉の国際規格(ISO13577)の動向，計測展2014 OSAKA テクニカルセミナー資料

＜著者所属＞

山田　晃　　アドバンスオートメーションカンパニー 開発3部
中田　知也　　アドバンスオートメーションカンパニー 開発3部