

IEC 61508

für nicht-sichere Programmier- und
Parametrierumgebungen



www.logicals.com

logi.cals®
all the more power



- Über uns
- Safety-Lösungen
- Ein neuer Ansatz
- Änderungsmanagement



Über uns



www.logicals.com

logi.cals®
all the more power



- Wir bieten innovative Lösungen und Technologien für Kunden in der gesamten Automatisierungs-Industrie.
- Unsere Lösungen basieren auf der jahrelangen Erfahrung in diesem Umfeld.
- Unsere internationale Kunden sind Hersteller von Automatisierungs-Produkten und -Lösungen.
- Die Verbindung zwischen Zuverlässigkeit und Verantwortung ist unser absolutes Prinzip.
- Kooperationen mit unseren Kunden sind immer langfristiger Natur.



- HIMA

- Safety für Prozessindustrie und Maschinenbau
- Hochverfügbarkeit
- Seit 1996 Programmiersystem ELOP II (SIL 3)
- Seit 2001 zusätzlich ELOP II Factory (SIL 3, cat. 4)
- Neue Produktlösung ab 2010/2011 gemeinsam mit logi.cals



- Elin EBG Traction

- Safety im Bereich Vollbahnen und Nahverkehr
- Programmiersystem zu ELTAS seit 2002 (SIL 2)



- Neuartiges Safety-Konzept mit logi.SIL

- Parametrieren sicherer Systeme mit Standardprodukten
- Programmieren sicherer Systeme mit Standardprodukten
- ... sicheres Engineering



Safety-Lösungen



www.logicals.com

logi.cals®
all the more power



- nur für Engineering von sicherheitsrelevanten Systemen
- wird oft parallel zur Engineering-Software für den nicht-sicherheitsrelevanten Bereich eingesetzt
- Pros
 - + spezialisierter Funktionsumfang
 - + optimiert für Safety-Engineering
- Cons
 - oft lange Releasezyklen (oder gar „Freeze“ des Produkts)
 - spartanische Ausstattung, meist nicht zeitgemäß
 - abgeschlossene Systeme
 - keine/wenig Erweiterbarkeit
 - stark eingeschränkte Konnektivität
 - „Zweitsystem“
 - Look & Feel anders als beim vorhandenen Standardsystem
 - zusätzlicher Support, Lernaufwand
 - kein/eingeschränkter Datenaustausch mit Standardsystem
- Beispiel: look at the market!



- für Engineering von nicht-sicherheitsrelevanten Systemen
- für Engineering von sicherheitsrelevanten Systemen
- Pros
 - + (meist) komfortable Systeme
 - + kontinuierliche Weiterentwicklung
 - + großer Funktionsumfang
 - + oftmals hohe Verbreitung (und Erfahrungen)
 - + Konnektivität (online bzw. Export/Import)
 - + unabhängige Systeme sind oft einfach erweiterbar
- Cons
 - Release-Zyklen schwierig planbar
 - nicht-sicherheitsrelevante Features aufwändiger zu realisieren
 - hohe Kosten für Test/Prüfung für Änderungen im Standardbereich
 - oftmals mehr Funktionen als der Anwender benötigt
- Beispiel: logi.CAD bzw. Elop II/Elop II Factory



Wie erreicht man diese Ziele?

- Neue Engineering-Software?
 - Standardhardware/-software anpassen
 - Datenkonvertierung
 - Anwenderschulung
 - Support
 - „1.0-Release“

„Never change a winning team!“

Gibt es Alternativen?

Ja!



logi.SIL

Ein neuer Ansatz



www.logicals.com

logi.cals®
all the more power



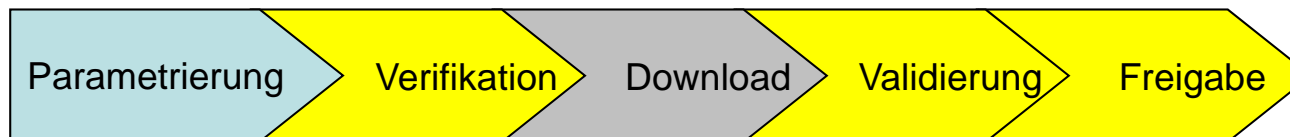
- Safety-Add On für Standard Engineering-Software
- Macht aus dem Standard-Engineering-System ein universelles Standard- und Safety-Engineering-System
- Kein Ersetzen bestehender Software
- vergleichsweise geringer Lernaufwand durch Verwendung eingeführter Technologien und Software



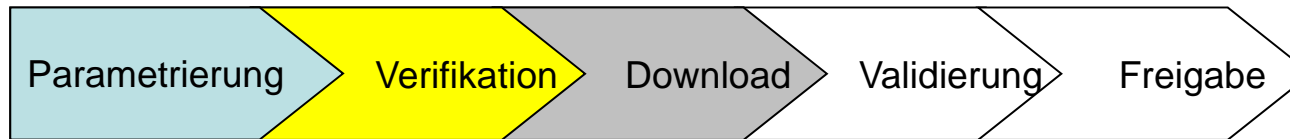
- für einfache (bzw. kleine) Systeme
- Parametrierung statt Programmierung
 - I/O-Verschaltung
 - Reaktionszeiten
 - Funktionen und Algorithmen
- Parametrierungsoberfläche
 - spezifisch für einen Gerätetyp
 - ideal abgestimmt auf die Anwendung und den Anwender
 - existiert bereits oder wird vom Gerätehersteller erstellt
- Typische Verarbeitungsschritte (nicht sicherheitsrelevant)
 - Parametrierung
 - Download
 - Validierung (Test am Gerät)



- Weiterverwendung der Parametrierungsoberfläche
 - Safety-Add On „zwischen“ Parametrierung und Gerät
- Typische Verarbeitungsschritte
 - Parametrierung
 - Verifikation der Parametrierung im Safety-Add On (optional)
 - Download
 - Validierung (Test am Gerät)
 - (formaler) Abschluss der Prüfung und Freigabe



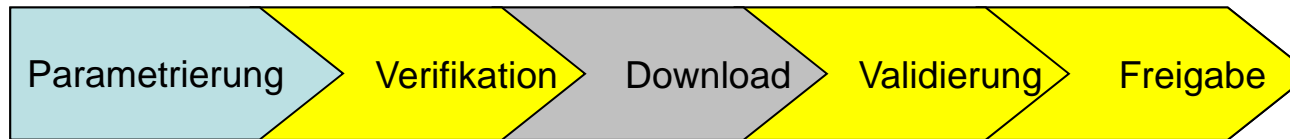
Use Case: Parametrierung



- Parametrierung
 - keine sicherheitsrelevante Funktion
- Verifikation
 - Daten werden vom Parametrierwerkzeug nach XML exportiert
 - XML-Daten werden in Safety-Add On importiert
 - mit Prüfsummen versehen
 - verfälschungssicher und identifizierbar
 - Verifikation der Korrektheit der Daten
 - automatisch bzw. durch den Anwender
 - Parametrierungsdaten werden als Listen/Grids präsentiert
- Download
 - Daten sind in sich geschützt
 - Download ist keine sicherheitsrelevante Funktion



Use Case: Parametrierung



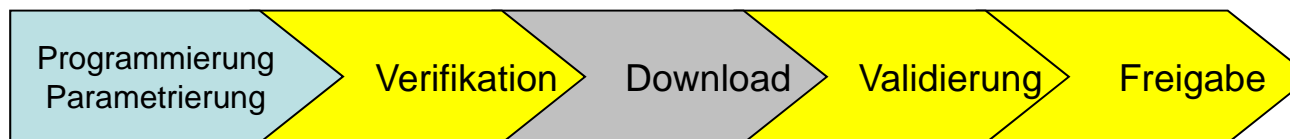
- Validierung
 - Test der Anwendung (Parametrierung) am Gerät
 - gesicherte Kommunikation mit dem Gerät über „schwarzen Kanal“
- Freigabe
 - Formalakt durch einen Anwender
 - üblicherweise nach Prüfung der korrekten Durchführung von Verifikation und Validierung
- (Parametrierungs)daten
 - ab dem Import in das Safety-Add On verfälschungssicher
 - jede Änderung kann erkannt werden
 - Parametrierungsdaten sind auch eindeutig identifizierbar



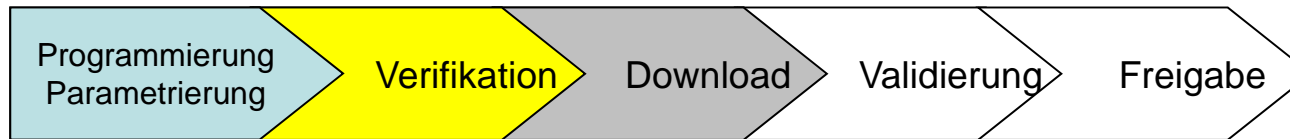
- für komplexere und mächtigere Systeme
- Parametrierung und Programmierung
 - z.B. mit grafischen Sprachen der IEC 61131-3 (FBD, KOP)
- Engineering-System
 - spezifisch für einen Gerätetyp (Parametrierung)
 - ideal abgestimmt auf die Anwendung und den Anwender
 - existiert bereits oder wird vom Gerätehersteller erstellt
 - hochflexibel
 - ev. Standardprodukt
- Typische Verarbeitungsschritte (nicht sicherheitsrelevant)
 - Programmierung und Parametrierung
 - Download
 - Validierung (Test am Gerät)



- Weiterverwendung der Engineeringoberfläche
 - Safety-Add On „zwischen“ Programmierung/Parametrierung und Gerät
- Typische Verarbeitungsschritte
 - Programmierung und Parametrierung
 - Verifikation der Programmierung und Parametrierung im Safety-Add On (optional)
 - Download
 - Validierung (Test am Gerät)
 - (formaler) Abschluss der Prüfung und Freigabe



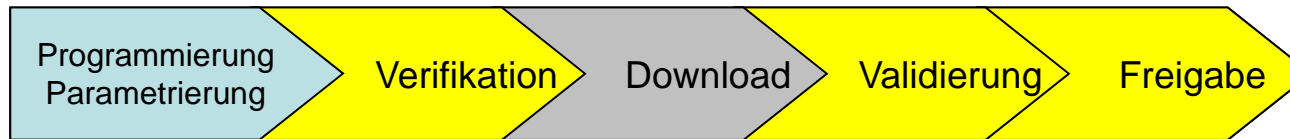
Use Case: Programmierung



- Programmierung und Parametrierung
 - keine sicherheitsrelevanten Funktionen
- Verifikation
 - Daten werden vom Engineeringwerkzeug nach XML exportiert
 - XML-Daten werden in Safety-Add On importiert
 - mit Prüfsummen versehen
 - verfälschungssicher und identifizierbar
 - Verifikation der Korrektheit der Daten
 - automatisch bzw. durch den Anwender
 - Programmierungsdaten werden als „Quellcode“ angezeigt (FBD-Grafik, KOP)
 - Konfigurations- und Parametrierungsdaten werden als Listen angezeigt
- Download
 - Daten sind in sich geschützt
 - Download ist keine sicherheitsrelevante Funktion



Use Case: Programmierung



- Validierung
 - Test der Anwendung am Gerät
 - gesicherte Kommunikation mit dem Gerät über „schwarzen Kanal“
- Freigabe
 - Formalakt durch einen Anwender
 - üblicherweise nach Prüfung der korrekten Durchführung von Verifikation und Validierung
- (Programm- und Parametrierungs)daten
 - ab dem Import in das Safety-Add On verfälschungssicher
 - jede Änderung kann erkannt werden
 - Programm- und Parametrierungsdaten sind auch eindeutig identifizierbar



Änderungsmanagement



www.logicals.com

logi.cals[®]
all the more power



- Erstellung der Software (Parametrierung oder Programmierung) ist nur erster Schritt
- Änderungen an Geräten (Software, Parameter) werden oft gemacht
 - während des Tests (Fehlerbehebung)
 - bei der Inbetriebnahme (Anpassung an die Umwelt)
 - im Betrieb (neue Anforderungen und Funktionen)
- Verifikation
 - kann sich auf Änderungen beschränken
 - ungeändertes entspricht (formal) dem alten Stand
- Validierung
 - je nach Anwendung/Änderung kann Validierung vereinfacht/verkürzt werden



- Vergleichsfunktion
 - „Referenzdaten“ beim Import in das Safety-Add On
 - zuletzt freigegebener Stand
 - zuletzt freigegebener Stand und zuletzt bearbeiteter Stand
 - nicht unähnlich der Änderungsnachverfolgung in Microsoft Word
 - benötigt keine Unterstützung durch das Programmier- und Parametrierwerkzeug
- Kennzeichnen der Änderungen
 - Verifikation kann sich auf die Änderungen beschränken
 - Validierung kann meist signifikant vereinfacht werden
- weniger Aufwand bei der Verifikation und Validierung
→ effizienter
- unbeabsichtigte Änderungen werden aufgedeckt
→ sicherer



- Pros
 - + (meist) komfortable Systeme
 - + kontinuierliche Weiterentwicklung
 - + großer Funktionsumfang
 - + oftmals hohe Verbreitung (und Erfahrungen)
 - + Konnektivität (online bzw. Export/Import)
 - + unabhängige Systeme sind oft einfach erweiterbar
 - + Weiter- und Wiederverwendung von Projekten/Daten (in beide Richtungen)
 - + Ergänzung statt Replacement: Support, Erfahrungen
 - + Änderungsmanagement/-verifikation
- Cons
 - Integration in Standardsystem muss für gute Usability gemacht werden
 - Datenexport
 - Zeichnungen (Funktionsplan) kann sich optisch leicht unterscheiden
 - zusätzlicher Verifikationsschritt (Add On)



logi.cals Austria

Mailüfterlweg 1, 3124 Oberwölbling,
ÖSTERREICH

T: +43 2786 77147

F: +43 2786 77147-16

E: info@logicals.com

logi.cals Germany

Poststraße 53, 40764 Langenfeld,
DEUTSCHLAND

T: +49 2173 9191-0

F: +49 2173 9191-19

E: germany@logicals.com



all the more power



www.logicals.com

logi.cals[®]
all the more power

