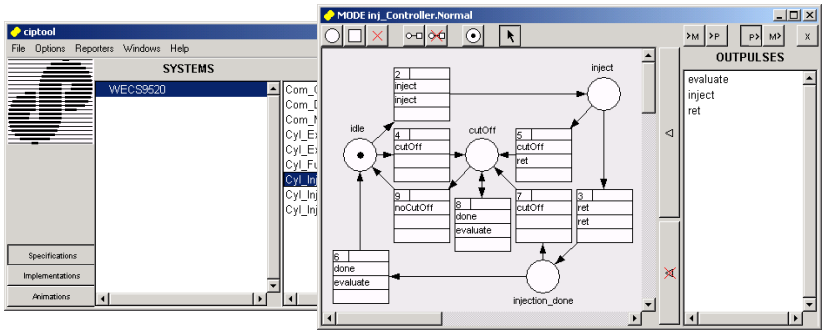
Softwareentwicklung mit CIP

Kunde	Wärtsilä
Ziel-System	Embedded System
Programmier-Sprache	C
Technologien	CIP



Aufgabe

Sotronik erhielt den Auftrag, die elektronische Steuerung für einen Grossdieselmotors zu realisieren. In der Evaluationsphase wurden die Hardware Komponenten, das Software Konzept und die Entwicklungs-Werkzeuge bestimmt. Für die Entwicklung der Steuer Software wurden verschiedene Werkzeuge und Methoden gegenübergestellt. Man entschied sich, die formale Entwicklungsmethode **CIP** (Communicating Interacting Processes) einzusetzen, welche verschiedene Vorteile gegenüber den Konkurrenz-Produkten aufwies.

Entwicklungs-Methode

Bei der Entwicklung von Software verteilter eingebetteter Systeme gibt es verschiedene Aspekte, die mit besonderer Sorgfalt beachtet werden müssen:

- Echtzeitverhalten: Dieser Aspekt ist oft sehr schwer vollständig in den Griff zu bekommen. Einerseits ist die zeitliche Abfolge von Ereignissen der realen Prozesse nicht deterministisch, andererseits ist die Laufzeit der Ereignis-Reaktion in der Software schwer zu bestimmen. Besonders bei Fehlverhalten des Systems gibt es eine Anhäufung von Ereignissen, so dass das korrekte zeitliche Verhalten der Software nicht garantiert werden kann.
- Fehleranfälligkeit: Wie fehleranfällig eine Software ist, wird durch verschiedene Parameter beeinflusst. Bei sicherheitsrelevanten Steuerungen muss diesem Punkt besondere Aufmerksamkeit geschenkt werden.
- Wartbarkeit: Während der Lebensdauer der Steuerung muss die Software mehrmals angepasst und verbessert werden. Deshalb ist es wichtig, dass die Software gut strukturiert und somit wartbar ist. Die Änderung an einer Stelle der Software sollte sich möglichst nicht an anderen Orten auswirken.
- Verständlichkeit: Oft fehlt bei der Kommunikation zwischen Maschinen-Experten und Software-Ingenieuren eine gemeinsame Sprache, welche für beide gut verständlich ist. Der Programm-Code wird von den Maschinen-Experten selten verstanden und ist deshalb nicht geeignet, um über die Funktionalität des Systems zu diskutieren.
- Dokumentation: Die Qualität einer Software zeichnet sich durch gute Dokumentation aus. Das ist wichtig für die Wartbarkeit und hilft die Struktur der Software besser zu verstehen und zu verbessern. Während des Entwicklungsprozesses wird jedoch dafür selten Zeit reserviert. Besonders bei Änderungen der Software, ist das Nachführen der Dokumentation mit viel Aufwand verbunden.

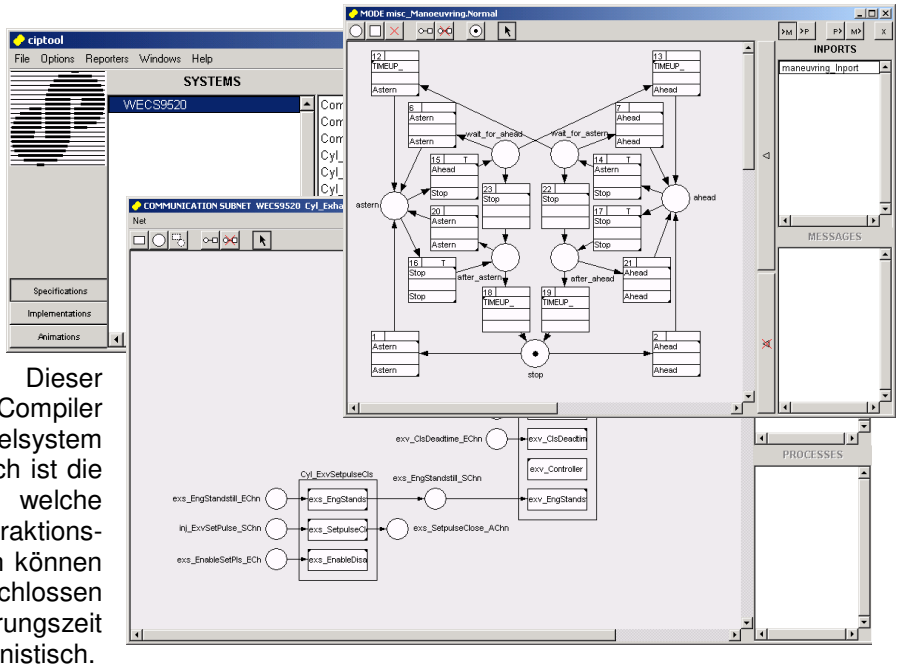
Um diesen Aspekten Rechnung zu tragen, wurde für die Entwicklung der neuen Motor Steuerung die formale Entwicklungsmethode CIP eingesetzt. CIP ist eine industrielle Software-Entwicklungsmethode für Prozessrechnersysteme. Die Steuerung und Leitung von Geräten und Anlageteilen wird durch graphische Modelle spezifiziert. Das Entwicklungswerkzeug von CIP generiert dabei aus den spezifizierten Modellen automatisch fehlerfreien und ausführbaren C-Code. CIP-Modelle bestehen aus erweiterten Zustandsmaschinen, die mittels synchron übertragender Ereignisse interagieren. Das formale und kompositionelle Arbeiten in den frühen Projektphasen reduziert die Entwicklungszeiten und verbessert die Softwarequalität entscheidend:

- Graphische Modelle -> verständliche Systeme
- Codegenerierung -> kürzere Entwicklungszeiten, Sicherheit
- Kompositionelle Struktur -> einfache Wartung

Der methodische Nutzen modellbasierter Entwicklung besteht darin, dass sich der Entwickler bereits in den frühen problemorientierten Entwicklungsphasen grundlegend mit Fragen der Verhaltensstruktur auseinandersetzt. Da die Modelle im Kontext der Anforderung gebildet werden, entstehen naturgemäss weniger Fehler, die erst am implementierten System entdeckt werden. Zudem erlaubt die formal abgestützte Arbeitsweise den Entwicklungsprozess zu automatisieren.

CIP Tool

CIP ist nicht nur eine Methode, sondern stellt auch ein Entwicklungswerkzeug zur Verfügung. Mit diesem kann man die externen Prozesse modellieren, das Gesamtverhalten (funktionale Lösung) beschreiben, und die Schnittstelle (Aktionen und Ereignisse) definieren. Auf Knopf-Druck wird dann automatisch ausführbarer C-Code generiert. Dieser Source-Code kann mit einem Compiler übersetzt und auf ein beliebiges Zielsystem implementiert werden. Sehr Hilfsreich ist die automatische Interaktions-Analyse, welche zur Konstruktionszeit erlaubt, Interaktions-Sequenzen zu verifizieren. Dadurch können zyklische Interaktionspfade ausgeschlossen werden, und die maximale Ausführungszeit einer Ereignis Reaktion wird deterministisch.



Nutzen für die Entwicklung der Motor Steuerung

Durch den Einsatz der CIP Entwicklungsmethode konnten folgende grosse Vorteile erzielt werden:

- Das Modellieren der externen Prozesse mit den erweiterten Zustandsmaschinen führte zu einem fundierteren Verständnis des Software Ingenieurs über die physikalischen Prozesse des Grossdieselmotors. Das verringerte Fehler, die erst im implementierten System entdeckt werden.
- Die Software kann mit minimalem Aufwand gewartet werden. Wenn das funktionale Verhalten der Steuerung ändert, kann nach dem Anpassen der Zustandsmaschinen durch Knopfdruck der neue Code generiert werden. Dieser Code ist fehlerfrei.
- Das zeitliche Verhalten der Steuerung konnte besser kontrolliert werden. Durch die Möglichkeit der Interaktionsanalyse mit dem CIP-Tool konnten die maximalen Laufzeiten der Reaktionen auf die externen Ereignisse bestimmt werden.
- Das CIP Tool bietet die Möglichkeit einer einfachen visuellen Animation, mit welcher der Software-Ingenieur die CIP Modelle mit dem Maschinen-Spezialisten kontrollieren konnte. Damit war eine gemeinsame Sprache gegeben, mit der interdisziplinär miteinander kommuniziert werden konnte.
- Die mit dem CIP Tool entwickelte Software konnte per Knopfdruck automatisch dokumentiert werden. Das nahm uns sehr viel Zeit ab, insbesondere war das bei den vielen Änderungen während der Entwicklungszeit sehr nützlich.
- CIP ist sehr einfach und leicht verständlich, sodass keine grosse Einarbeitung notwendig war.