شرکت مهندسی
آدلی کنترل باور

Adli Control bavar

مرجع کامل آموزش

سیستم‌های S7-400FH و S7-300F زیمنس

مطابق با منابع آموزشی SITRAIN زیمنس

مولف: دکتر صادق اکبری

PCS7 V 9.0
F-System Library V 1.3
S7 Distributed safety

S7-400 FH Control System Training
Fail-safe & Fault-tolerant

سرشناسنامه

سرشناسنامه : اکبری، صادق، ۱۳۵۴

عنوان و نام پدیدآور: مرجع آموزش سیستم‌های S7-300F و S7-400FH زیمنس، نویسنده: صادق اکبری

مشخصات نشر: تهران، شرکت آدلی کنترل باور، ۱۴۰۲

مشخصات ظاهری : یک جلد ۵۵۱ ص.

وضعیت فهرست‌نویسی : فیپا

فروست: مجموعه کتاب‌های شرکت آدلی کنترل باور

موضوع : مهندسی برق و کنترل

موضوع : سیستم‌های کنترل

موضوع : سیستم‌های ESD/SIS

شناسه افزوده: شرکت مهندسی آدلی کنترل باور

شابک : ۸-۲۴۳۷-۰۰-۶۲۲-۹۷۸

شماره مجوز از مرکز توسعه فرهنگ و هنر درفضای مجازی : ۰۸۰۵۹٤-۵۹۳۸۱-۸

عنوان کتاب	مرجع آموزش سیستم‌های S7-300F و S7-400FH زیمنس
ناشر	شرکت آدلی کنترل باور
نویسنده	صادق اکبری
ویراستارفنی	صادق اکبری
ویراستار ادبی	رقیه اکبری
صفحه‌آرایی و طرح جلد	صادق اکبری
نوبت چاپ اول	تابستان ۱۴۰۲
شمارگان	۵۰۰ نسخه
شابک	۸-۰۰۲۴۳۷-۰۰۶۲۲-۹۷۸
قیمت	۵۰۰ هزار تومان

نشانی مرکز پخش: شهرک گلستان ، بلوار هاشم زاده- بلوار سبزوار پلاک ۳۰ واحد همکف کد پستی ۱۴۹۴۹۱۳۱۸۳

آدرس وب سایت : www.adlitrain.com و www.adli-control.com

پست الکترونیکی info@adli-control.com

تلفن: ۰۲۱-۴۴۷۳۲۹۸۱ و ۰۹۱۲-۳۱۸۲۷۳۴

درباره کتاب

امروزه به‌منظور پیشگیری از وقوع حوادث ناگوار و پیامدهای فاجعه‌بار، به‌کارگیری سیستم‌های کنترل PLC نوع Fail-safe در پلنت‌های نفت،گاز و پتروشیمی و حتی اتوماسیون کارخانه، از طرف سازمان‌ها، مقررات و استانداردهای بین‌المللی به یک الزام تبدیل‌شده است. سیستم‌های کنترل F و FH زیمنس در زمره این کنترل‌کننده‌های PLC می‌باشد. که تحت عنوان سیتسم‌های ESD,HIPPS,BMS,F&G در صنایع مختلف فرایندی، به‌خصوص در صنایع نفت و گاز و پتروشیمی به‌وفور استفاده‌شده است. سیستم‌های Fail-safe که امروزه از آن‌ها تحت عنوان سیستم SIS نام‌برده می‌شود، بسته به‌اندازه پلنت و نوع فرآیند در مدل‌ها و سری‌های مختلف به بازار ارائه‌شده است. سری S7-400FH ازجمله کنترل‌کننده‌های هیبرید مطرح بازار می‌باشد که پیاده‌سازی هم‌زمان لاجیک کنترل استاندارد و لاجیک Faile-safe را در یک کنترل‌کننده فراهم می‌کند.

این کتاب که حاصل مطالعه، تدریس و تجربه عملی چندساله با سیستم S7-400FH می‌باشد، برای فراهم آوردن یک دانش منسجم در راستای آموزش و به‌کارگیری سخت‌افزار و نرم‌افزار این سیستم به رشته تحریر درآمده است. در طول کار در پروژه‌ها و یا تدریس دوره‌های آموزشی در خصوص سیستم‌های کنترل PCS7,S7400H و S7-400FH، درخواست‌های زیادی بابت تهیه یک جزوه یا کتاب فارسی از دانشجویان و کارآموزان داشتم. همچنین با توجه به ساختار مدارک راهنمای زیمنس که دانش یک موضوع به‌صورت منسجم در یک سند وجود ندارد، تصمیم به نگارش این کتاب و ارائه آن در قاب فایل دیجیتال شدم. باشد که گامی دیگر در ارتقاء دانش سیستم‌های کنترل اتوماسیون برداشته باشم.

هدف اصلی این کتاب شناخت معماری سخت‌افزار، نرم‌افزار و شبکه در سیستم‌های کنترل S7-300F و S7-400FH و نحوه پیاده‌سازی لاجیک کنترل Fail-safe با استفاده از بلاک‌های کتابخانه F System در محیط CFC و ماتریس ایمنی و همچنین پیاده‌سازی لاجیک کنترل با استفاده از کتابخانه Distributed safety در محیط SIMATIC Manager می‌باشد.

این کتاب در ۱۱ فصل سازمان‌دهی شده است. فصل اول این کتاب، مفاهیم ایمنی و مبانی سیستم‌های SIS یا Fail-safe را به‌صورت خلاصه توصیف می‌کند. فصل دوم تحت عنوان «ایمنی سیماتیک»، سخت‌افزار و نرم‌افزار انواع سیستم‌های کنترل Fail-safe زیمنس را معرفی می‌کند. که در آن به مواردی چون سطوح SIL تعریف‌شده در سخت‌افزارهای زیمنس و به‌کارگیری پروتکل Prosafe در این سیستم‌ها پرداخته‌شده است. فصل سوم به‌طور

درباره کتاب

مشخص نحوه پیکربندی و برنامه‌نویسی یک سیستم کنترل Fail-safe با کنترل‌کننده‌های S7-300F و S7400F را تشریح می‌کند. کاربرد این کنترل‌کننده‌ها بیشتر در حوزه اتوماسیون کارخانه می‌باشد. فصل چهارم ساختار و معماری یک کنترل‌کننده S7-400H را که پایه و اساس یک سیستم S7-400FH محسوب می‌شود را تشریح می‌کند. در ادامه فصل پنجم نحوه پیکربندی یک سیستم S7-400FH را در محیط ابزارهای برنامه STEP 7 نرم‌افزار PCS7 تشریح می‌کند. توصیف نحوه پیاده‌سازی برنامه و کار با کتابخانه F System زیمنس در فصل ششم جمع‌بندی شده است. در فصل‌های ۷،۸ معماری‌های ارزیابی ایمنی کانال‌های ورودی/خروجی (I/O) به‌صورت سخت‌افزاری و نرم‌افزاری برای رسیدن به دسترس‌پذیری و ایمنی بالا توصیف‌شده است. فصل نهم تشریحی از نحوه پیاده‌سازی یک برنامه یا لاجیک F با استفاده از ماتریس ایمنی می‌باشد. در فصل ۱۰ ساختار و پیکربندی شبکه در سیستم‌های S7-400H, FH و همچنین نحوه پیکربندی سیستم‌های مانیتورینگ جهت اتصال به کنترل‌کننده‌های S7-400FH تشریح شده است. در پایان فصل ۱۱، به برخی نکات و موضوعات در ارتباط با نگهداری سیستم‌های FH اختصاص داده‌شده است.

در انتها از خواهر عزیزم خانم رقیه اکبری که در ویراستاری و تهیه این کتاب پشتیبانی‌های زیادی داشته‌اند، تشکر ویژه دارم. امیدوارم این کتاب برای کارشناسان و متخصصین حوزه کنترل اتوماسیون صنعتي کشور مفید واقع شود.

پیش گفتار نویسنده

چند سال پیش که شروع به برگزاری دوره آموزش و تدریس سیستم‌های کنترل زیمنس و بخصوص سیستم S7-400FH نمودم، به درخواست دانشجویان و مراکز آموزشی در طی برگزاری دوره‌های آموزشی به تهیه جزواتی اقدام نمودم. که این جزوات در طول برگزاری دوره‌های مختلف تکمیل گردید. ازآنجایی‌که این جزوات در دسترس علاقه‌مندان به این حوزه قرارگرفته بود و همچنین تبلیغاتی که در خصوص برگزاری دوره S7-400FH در سایت آموزشی شرکت آدلی کنترل باور (www.adlitrain.com) شده بود، درخواست‌های مکرری در خصوص کتاب و یا فیلم‌های آموزشی S7-400FH از سوی عزیزان و کارشناسان دریافت می‌نمودم. ولی به دلایل مختلف و مشغله کاری، انتشار یک کتاب در این زمینه میسر نگردید. تا این‌که پس از اتمام نگارش پایان‌نامه دکتری تخصصی اینجانب و به درخواست و تشویق عزیزان در کلاس‌های این‌جانب، تصمیم بر گردآوری مطالب جزوات و نگارش آن‌ها در قالب یک کتاب منسجم شدم. امیدوارم که برای کارشناسان صنعتی کشور و علاقه‌مندان به حوزه سیستم‌های Fail-Safe زیمنس مفید بوده باشد.

ازآنجایی‌که تقریباً ۹۰ درصد محتوای این کتاب در طول سال‌های گذشته تهیه شده است. ولی به منظور نشر سریع آن، ساختار و سازماندهی کتاب در یک زمان کوتاهی جمع‌بندی و نگارش شده است، ممکن است دارای اشکالات نگارشی بوده و دارای نواقصی باشد، لذا پیشاپیش از بابت تمامی اشکالات و معایب احتمالی موجود عذرخواهی نموده و از تمامی عزیزان و کارشناسانی که با دقت نظر این کتاب را مطالعه نموده و ما را با ارائه پیشنهادها و انتقادهای سازنده خود در اصلاح و بهبود ویرایش‌های بعدی این کتاب یاری می‌کنند. تشکر و قدردانی می‌کنم.

s.akbari@znu.ac.ir
صادق اکبری

درباره ناشر

معرفی خدمات شرکت آدلی کنترل باور

نام شرکت : آدلی کنترل باور، سهامی خاص به شماره ثبت ۵۵۱۲۰۴

تلفن : 021-44732981 و 09212182734

آدرس وب‌سایت و ایمیل:

Website: www.adli-control.com & www.adlitrain.com

Email: info@adli-control.com , sales@adli-control.com

مدیرعامل : صادق اکبری فارغ‌التحصیل دکترای مهندسی برق و الکترونیک از دانشگاه زنجان– دارای ۲۳ سال تجربه تخصصی در زمینهٔ پیاده‌سازی، اجرا، نصب و راه‌اندازی سیستم‌های کنترل و ابزار دقیق در پروژه‌های نفت، گاز و پتروشیمی و کارخانه، مدرس سیستم‌های کنترل

سرویس‌های مهندسی (Engineering Services)

- پیاده‌سازی و اجرای سیستم‌های کنترل پکیج و پلنت فرآیندی (PLC/DCS/FCS/PCS)
- پیاده‌سازی و اجرای سیستم‌های Fail-Safe (ESD/BMS/F&G)
- پیاده‌سازی و اجرای سیستم‌های اسکادا و مانیتورینگ صنعتی
- تولید مدارک فاز مهندسی پروژه‌های اتوماسیون
- طراحی و مونتاژ تابلوهای برق و کنترل
- اجرای پروژه‌های برق، کنترل و ابزار دقیق
- ارتقاء و بروز آوری سیستم‌های کنترل و ابزار دقیق
- آموزش اتوماسیون صنعتی

عضویت و گواهی‌نامه‌ها

- عضو فهرست بلند تأمین‌کنندگان وزارت نفت
- عضو سامانه ستاد ایران
- دارای گواهی‌نامه پیمانکاری - صنعت و معدن
- گواهی‌نامه مدیریت کیفیت ISO 9001:2015
- دارای گواهی نامه نشر دیجیتال (نشر دیجیتال مبتنی بر حامل، تصدی رسانه برخط کاربر محور، نشر دیجیتال برخط، تکثیر حامل های دیجیتال محدود(Duplicator)

نمایندگی ها

- نمایندگی نرم¬افزار اسکادا/مانیتورینگ ControlMaestro
- نمایندگی فروش محصولات ASTI رومانی

محصولات توسعه داده شده

- **سیستم دشارژ و شارژ بانک باتری با مشخصه ۱-۲۵۰ آمپر و ۲-۱۰۰ ولت**

شرکت آدلی کنترل باور، با اتکا به متخصصین و افراد باتجربه حوزه الکترونیک قدرت، خدمات طراحی و ساخت انواع سیستم‌های شارژ و دشارژ بانک باتری را ارائه می‌کند. در حال حاضر این شرکت در راستای بومی‌سازی فناوری‌های پیشرفته اقدام به تحقیق و توسعه و ساخت سیستم آنالیز دشارژ باتری با بارهای الکترونیکی و قابل‌برنامه‌ریزی با نرم‌افزار نموده است. مشخصه ویژه این سیستم دقت بالای تنظیم جریان ثابت دشارژ در رنج وسیعی از ولتاژها و جریان‌های کاری از ۶ تا ۱۰۰ ولت، ۱ تا ۲۵۰ آمپر و آنالیز هم‌زمان شش بانک باتری می‌باشد.

- **ساخت پکیج‌های آموزشی PLC**
- **نشر کتاب‌ها و محتوای آموزشی در حوزه اتوماسیون صنعتی**

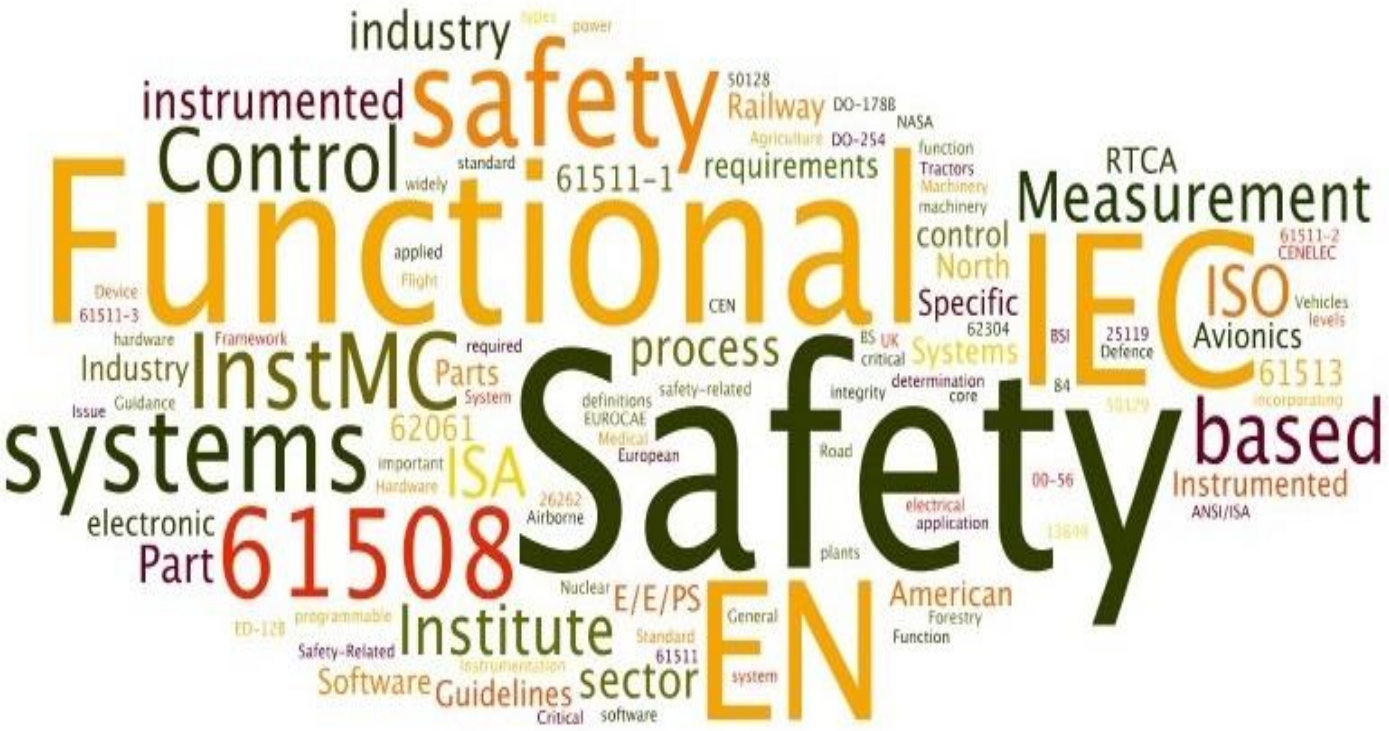
این کتاب را تقدیم می کنم به

همسر و فرزند عزیزم

و پدر و مادر مهربانم

فصل اول

مروری بر مفاهیم ایمنی



Functional Safety Overview

Chapter 1

1 Functional Safety Overview

Learning Targets

محتوای این فصل شامل مباحث زیر است.

- مفاهیم پایه مرتبط با ایمنی فرآیند
- لایه‌های حفاظتی یک پلنت فرآیندی
- روش‌های کاهش ریسک در یک فرآیند
- آشنایی با استانداردهای ایمنی IEC و ISA

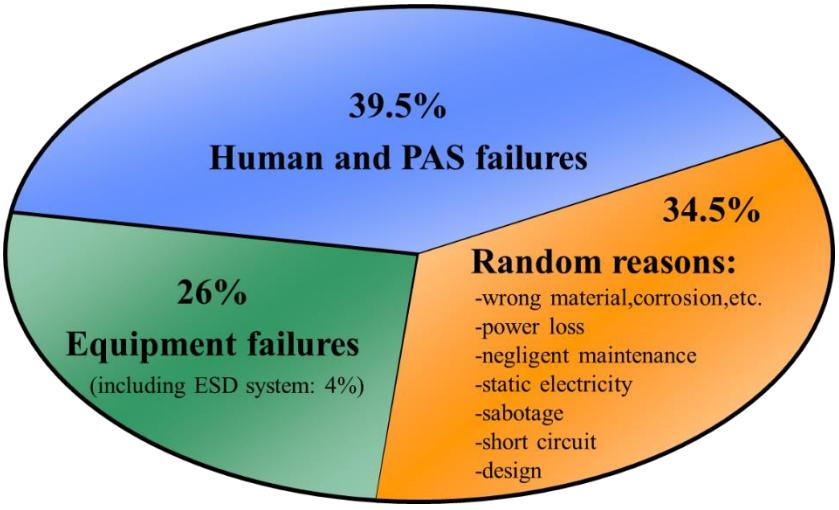
Abbreviations

IEC	International Electrotechnical Commission
ISA	International Studies Association
FH	Fail-Safe & High Available
F	Fail-Safe
SIF	Saftey Instrumented Function
SIS	Saftey Instrumented System
SRS	Safety Related System
BPCS	Basic Process Control System

1.1 Introduction

در بیشتر فرآیندهای صنعتی به علت انتشار مواد خطرناک مانند گازها و مواد شیمیایی، عملیات بهره‌برداری با خطرات ذاتی مانند آتش‌سوزی و انفجار همراه است. به طوری که انفجارها و آتش‌سوزی‌ها هرساله موجب مرگ افراد و از دست رفتن میلیون‌ها دلار در صنایع شیمیایی و صنایع نفت و گاز می‌شود. لذا به دلیل وجود پتانسیل بسیار بالا در از دست رفتن منابع در یک پلنت فرآیندی، به‌کارگیری سیستم‌های مرتبط با ایمنی (SIS,SRS) برای پیشگیری از وقوع حوادث و همچنین هدایت پلنت به یک وضعیت ایمن از قبل تعریف شده با هدف حفاظت از افراد، تجهیزات و محیط زیست ضروری است.

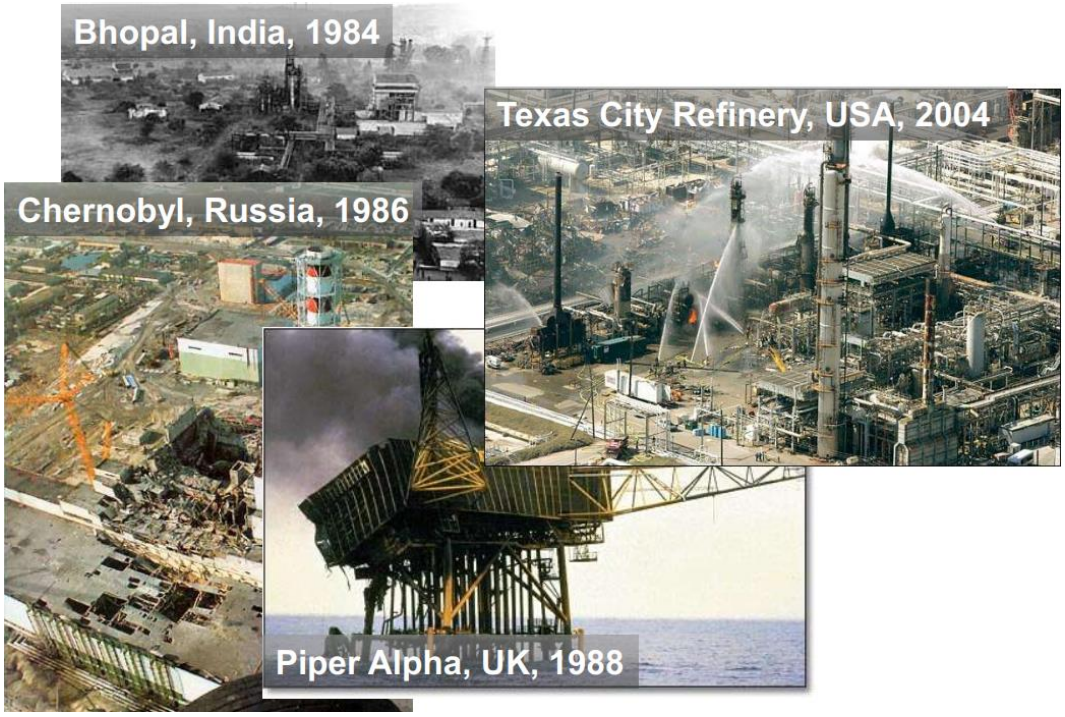
در گذشته از وقوع حوادث بی‌شماری در برخی از پلنت‌های فرآیندی در کشورهای مختلف سرتاسر دنیا گزارش شده است. آمارها از حوادث واقعی رخ داده نشان می‌دهد؛ که دلیل بیشتر حوادث عوامل انسانی بوده است. شکل۱-۱ نتایج حاصل از یک تحقیق و بررسی از ۲۱۶ مورد حادثه در جهان را نشان می‌دهد؛ که توسط موسسه TNO انجام شده است. مطابق این آمار حدود ۴۰ درصد حادثه‌ها به دلیل اشتباهات انسانی رخ داده است. به طوری که تنها ۴ درصد از کل حوادث به دلیل عدم عملکرد درست سیستم‌های SIS در مواقع تقاضا بوده است.



شکل۱-۱: نتایج حاصل از بررسی علل وقوع حادثه در ۲۱۶ مورد

نیروگاه اتمی برق چرنوبیل یک نمونه از پلنت‌هایی است؛ که در آن یک حادثه فاجعه بار رخ داده است. در این پلنت قبل از حادثه اپراتورها تمام سیستم‌های ایمنی را خاموش کرده بودند. به طوری که آخرین سیستم ایمنی درست دقایقی قبل از وقوع انفجار خاموش شده

بود. همچنین اپراتورها سیگنال‌های توقف (Shutdown) را غیرفعال (Override) کرده بودند و از هشدارها چشم‌پوشی شده بود.



شکل۱-۲: نمونه‌هایی از حوادث فاجعه‌بار درپلنت‌های فرآیندی در سراسر دنیا

1.1.1 Safety in the Workplace

ایمنی در محیط کار- در یک پلنت فرآیندی، مناطق ذاتاً پرخطر (Potential areas) بسیاری وجود دارد که می‌تواند باعث آسیب به کارکنان یا اثرات خطرناک احتمالی به محیط یا تجهیزات فیزیکی موجود در آن داشته باشد. یک سیستم ایمنی با طراحی مناسب باید تأثیرات احتمالی هر یک از این مناطق را مد نظر قرار داده و کم کند.

نقص‌های تصادفی سخت‌افزاری (Random hardware faults)، خطاهای سیستماتیک طراحی (systematic design errors) یا اشتباهات انسانی نباید منجر به عملکرد نادرست سیستم مرتبط با ایمنی (safety related) و پیامدهای احتمالی مانند آسیب یا مرگ انسان، آسیب به محیط زیست و از دست دادن تجهیزات یا تولید شوند. نکته کلیدی (key message) این است که هیچ خطا یا خرابی نبایستی باعث عملکرد غلط سیستم مرتبط با ایمنی (SIS) شده و منجر به صدمه یا آسیب احتمالی به نفرات یا تجهیزات شود.

1.1.2 Safety-Related Concepts

What are Hazards on a Machine or Process Plant?

هنگام طراحی یک سیستم ایمنی (SIS) برای یک پلنت صنعتی، باید خطرات یا ریسک احتمالی افراد در نظر گرفته شود. خطرات را می‌توان به صورت زیر دسته‌بندی کرد.

- خطرات فیزیکی (Physical)
  - سقوط یا حرکت اشیاء (Falling / Moving Objects)
  - تصادم یا برخورد (Collisions)
  - فروریختن ساختمان‌ها (Collapsing Struct`ures)
- خطرات الکتریکی (Electrical)
  - صاعقه و سوختگی (Flashover and Burns)
  - برق گرفتگی (Electrocution)
  - اتصال نادرست / اتصال شل (Wrong Connection / Loose Connection)
- خطرات مکانیکی / فرآیندی (Mechanical / Process)
  - گیرافتادن به طور مثال در یک حفره (Pinch Points or Entanglement)
  - سایشی، برش (Abrasion, Grinding, Cutting)
  - حرارتی (Thermal)
  - تأثیرات فشار (ترکیدن مخازن، جت‌های گاز یا مایعات) (Pressure Releasing)
  - جوشکاری، مشعل، گازها و غیره (Welding Torches, Gases etc.)
- خطرات شیمیایی (Chemical)
  - انفجار (Explosion)
  - آتش (Fire)
  - انتشار مواد سمی (Toxic Material Release)
  - مخلوط اشتباه از مواد شیمیایی (Wrong mix of chemicals)

- تابش (Radiation)

What is safety?

- ایمن (Safe): یعنی «عاری از آسیب، صدمه و خطر» یا «قرار نگرفتن در معرض خطر یا آسیب دیدگی»
- ایمنی (safety) : عبارت است از شرایط یا وضعیت ایمن. به عبارت دیگر ایمنی رهایی از ریسک غیرقابل قبول (IEC 61508 / IEC 61511) می‌باشد.
- ایمنی با قابلیت اطمینان متفاوت است. قابلیت اطمینان عبارت است از احتمال اینکه یک سیستم عملکرد مورد نظر خود را در بازه زمانی ماموریت به طور رضایت بخش انجام دهد، می‌باشد.
- ایمنی با امنیت (Security) متفاوت است. امنیت محافظت یا دفاع در برابر حمله، مداخله یا جاسوسی/ خبرگیری است.
- ملاحظه ایمنی زود هنگام یک پلنت ارزانتر از آن است که سعی کنید بعداً آن را ایمن کنید. به این معنی که در زمان طراحی یک پلنت، بایستی مفاهیم ایمنی مدنظر قرار گیرد. نه بعد از اتمام طراحی و ساخت یک پلنت سیستم‌های ایمنی پیاده سازی گردد.
- تجزیه و تحلیل خطر (Hazard Analysis) در یک پلنت، خطرات، نقایص و اقدامات ایمنی را با هم پیوند می‌دهد.

Accident

- حادثه، نوعی از بین رفتن مانند صدمه، مرگ و یا آسیب به تجهیزات است
- خطر (Hazard) مجموعه‌ای از شرایط و / یا رخدادهایی است که منجر به حادثه می‌شود.

Failure

یک خرابی (failure) عدم موفقیت /عدم کارایی (nonperformance) صحیح یک سیستم یا مؤلفه‌ای از سیستم می‌باشد. خرابی یک رخداد هست. به‌عنوان مثال، خرابی در یک تجهیز.

Error

- خطا (**Error**) یک نقص سیستماتیک است. نقص سیستماتیک یک خطای طراحی است.
- خطاها حالت‌ها یا شرایط هستند. به‌عنوان مثال، یک اشکال نرم افزاری.

Fault

☜ یک نقص (fault) یا از نوع یک خرابی است یا خطا. یک نقص دارای ماهیت تصادفی است.

1.2 Functional Safety Definition

IEC 61508 / IEC 61511

استاندار IEC 61508، ایمنی کاربردی (Functional Safety) را به‌عنوان رهایی از ریسک غیرقابل‌قبول (unacceptable) بیان می‌کند. ایمنی کاربردی به‌عنوان بخشی از ایمنی کل، مربوط به فرآیند و سیستم کنترل فرآیند پایه (BPCS/DCS) می‌باشد، که بستگی به عملکرد صحیح سیستم SIS و دیگر لایه‌های حفاظتی دارد.

عبارت عملکرد صحیح در سیستم SIS، اهمیت خاصی دارد. سطح بالایی از ایمنی عملکردی به این معنی است که یک سیستم SIS در صورت وجود تقاضا به یک عملکرد مانند توقف پلنت یا تجهیز، به‌درستی و یا احتمال بالا کار خواهد کرد. بنابراین ایمنی کاربردی، هدف اصلی در طراحی سیستم SIS می‌باشد. نکته مهم این است که ایمنی عملکردی فقط مربوط به سیستم‌های کنترل و ابزار دقیق SIS نیست. بلکه ایمنی عملکردی شامل همه چیز در مورد صلاحیت افراد کنترل‌کننده فرآیند، رویه‌ها و تجهیزات است.

1.2.1 Why do we need Functional Safety?

Out of control

معمولاً سیستم‌های کنترل دچار خطا شده و از کنترل خارج می‌شوند. لذا بایستی از خرابی آنها جلوگیری کرد.

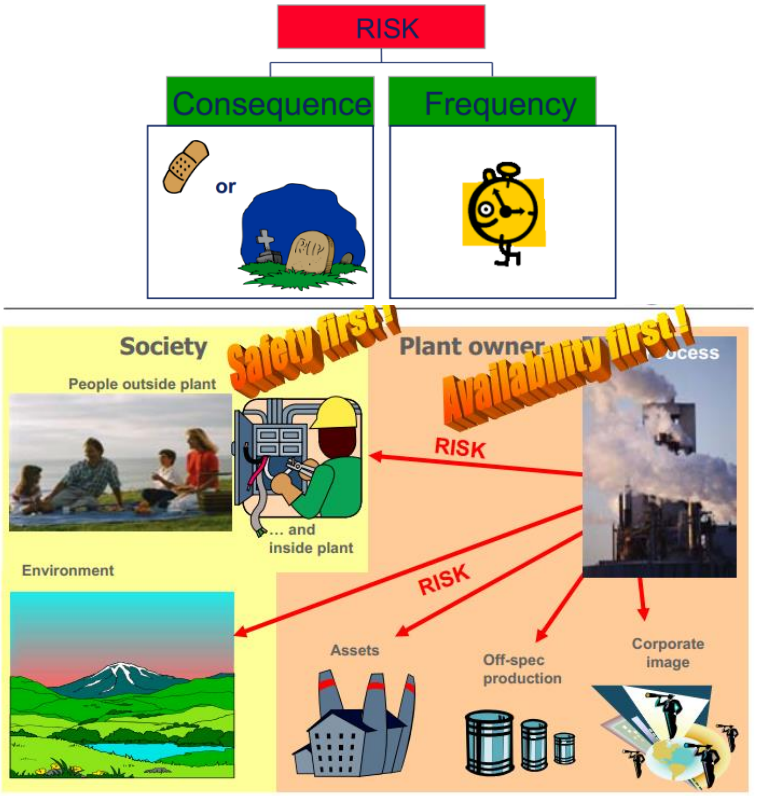
Main Goal: Keep People Safe

هدف اصلی یک سیستم ایمنی (safety system)، ایمن نگه داشتن افراد و تجهیزات است.

1.3 Process Risk

اگر در یک فرآیند صنعتی خطراتی (hazards) وجود دارد، برای عملکرد ایمن پلنت بایستی رویه‌هایی برای کاهش ریسک (Risk Reduction) وجود داشته باشد.

برای تعیین کمیت خطرات موجود در یک ماشین یا پلنت فرآیندی، یک ارزیابی ریسک (Risk Assessment) انجام می‌شود. سپس برای خطرات، لایه‌های محافظتی طراحی می‌شود تا ریسک آنها کاهش یابد.



شکل۱-۳: ریسک‌های ذاتی در یک پلنت فرآیندی

1.3.1 What is Risk? : IEC 61508 / IEC 61511

ریسک یک معیار سنجش از احتمال وقوع و پیامدهای یک حادثه می‌باشد. به تعریف دیگر، احتمال اینکه یک خطر (hazard) یا مخاطره (danger) منجر به بروز یک حادثه گردد، ریسک گفته می‌شود. لذا ریسک ترکیبی از احتمال وقوع یک مخاطره و میزان آسیب به سلامت افراد و تجهیزات تعریف می‌شود.

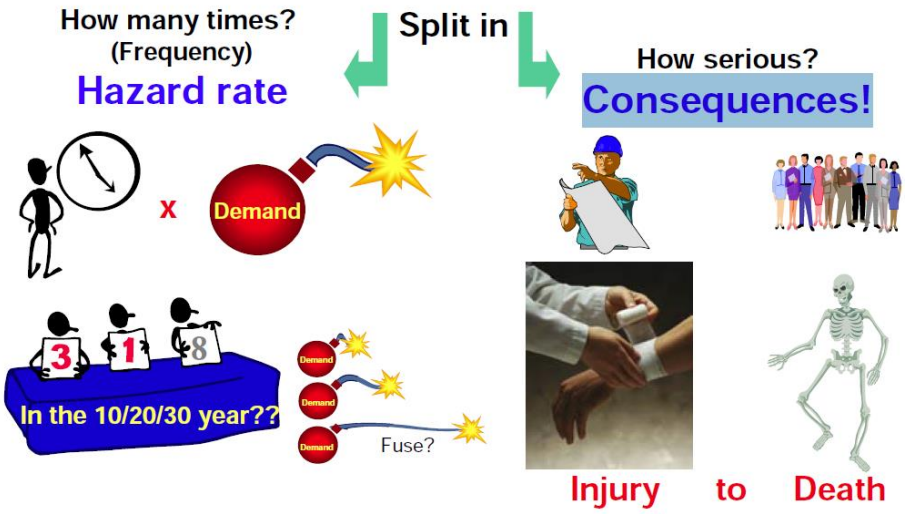
مطابق تعریف استاندارد IEC61508، ریسک عبارت است از یک منبع بالقوه از آسیب (Harm) می‌باشد. به طوری که به حاصل ضرب احتمال وقوع یک رویداد (حادثه یا آسیب) در شدت وقوع آن رویداد، ریسک می‌گویند.

$$Risk = P(a) * S(a)$$

با توجه به تعاریف بالا برای یک ریسک دو مشخصه تعریف می‌شود:

- نرخ وقوع خطر (Hazard rate)
- شدت حادثه (Hazard Severity)

نرخ وقوع خطر به معنی تعداد تکرار وقوع آن خطر در واحد زمان می‌باشد. به‌عنوان مثال یک بار در سال یا سه بار در ۱۰ سال. ولی شدت حادثه (How serious) تعیین می‌کند که پیامدهای (Consequences) بعد از بالفعل شدن خطر که حادثه نامیده می‌شود، چقدر است. پیامدها عبارت است از زخمی شدن افراد، صدمه به تجهیزات، مرگ میر و غیره.

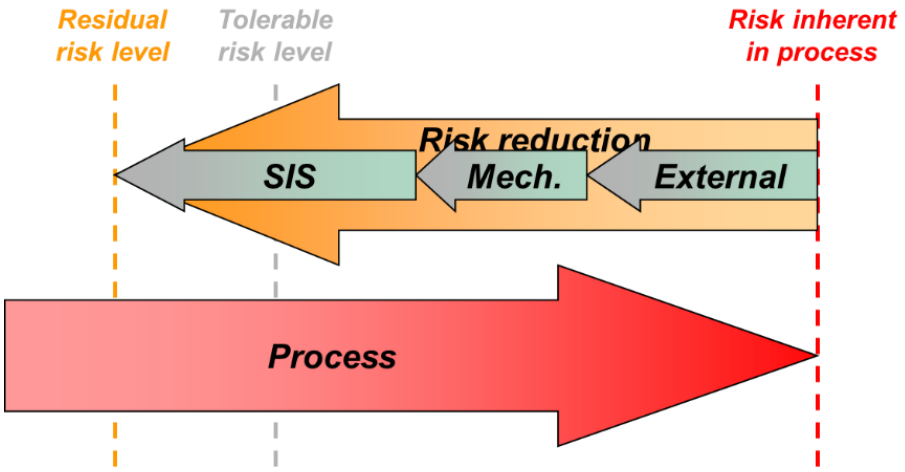


شکل ۱-۴: نمایی از نرخ وقوع خطر و پیامد حاثه

1.3.2 Risk Reduction

یک پلنت فرآیندی همواره با ریسک‌های حتمی همراه می‌باشد که از آن‌ها تحت عنوان ریسک‌های ذاتی یاد می‌شود. این سطح از ریسک به دلایل قوانین دولتی یا شرکتی در یک پلنت فرآیندی غیرقابل قبول می‌باشد. ریسک‌های ذاتی به هیچ وجه به طور کامل قابل حذف نیستند و تنها می‌توان با تمهیداتی، شدت پیامد آن‌ها یا بالفعل شدن خطرات آن‌ها را کاهش داد و یا این که آن‌ها را در یک سطح قابل قبولی تحمل کرد. این که یک ریسک تا چه حدی قابل تحمل (tolerable) است، نیاز به ارزیابی ریسک دارد. امروزه، مخاطرات را بر اساس سطح ریسک آن‌ها ارزیابی می‌کنند و سپس مورد قبول بودن یا نبودن آن را تعیین می‌کنند؛ بنابراین هدف تمام استانداردهای ایمنی نه حذف ریسک، بلکه کاهش ریسک می‌باشد. ریسک‌ها را می‌توان به صورت زیر دسته‌بندی کرد:

- ریسک ذاتی (Inherent Risk)؛
- ریسک مانده / حذف نشده (Residual Risk)؛
- ریسک قابل قبول یا قابل‌تحمل (Tolerable or Acceptable Risk)؛
- ریسک‌های نامعلوم (Uncertain Risk)؛
- ریسک‌های قابل‌اغماض (Negligible)؛
- ریسک‌های غیرقابل‌قبول (Unacceptable)؛



شکل۱-۵: انواع ریسک و روش‌های کاهش آن در یک فرآیند

کاهش ریسک باعث کاهش ریسک ذاتی فرآیند به سطح ریسک باقیمانده می‌شود که برابر یا کمتر از سطح ریسک قابل تحمل است.

Inherent Risk

ریسک ذاتی به ریسکی گفته می‌شود که هنوز هیچ اقدام کنترلی یا روش‌های کاهش ریسک برای کاهش آن اعمال نشده است. یکی از راه‌کارهای کاهش ریسک‌های ذاتی، استفاده از سیستم‌های SIS (ESD,F&G) می‌باشد. وقوع یک رخداد در فرآیند یک تقاضا برای سیستم SIS ایجاد می‌کند.

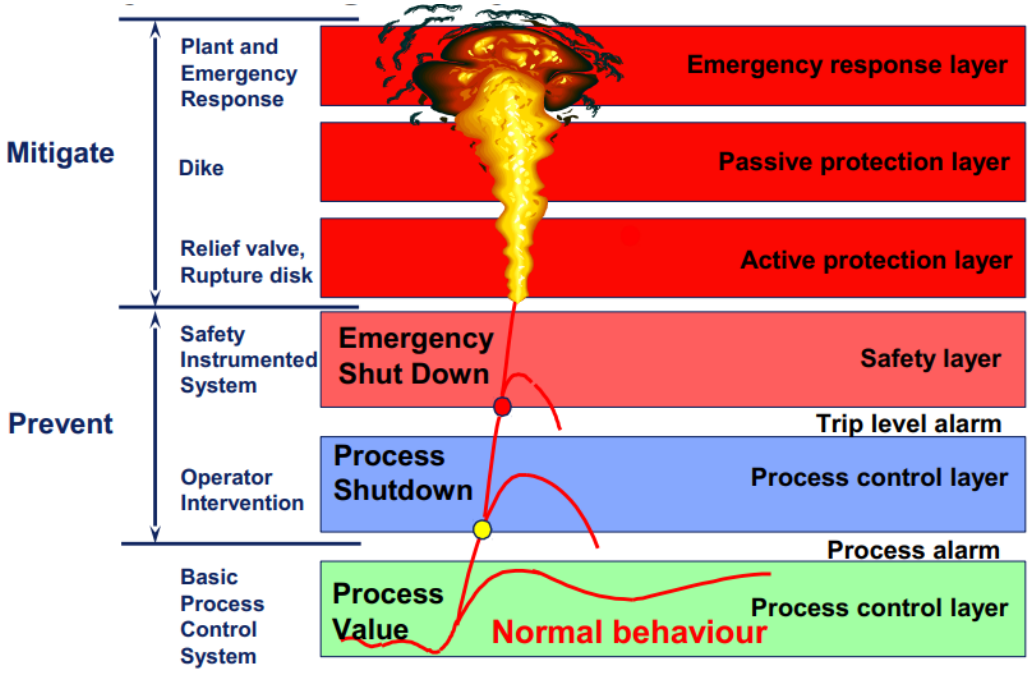
Residual Risk

ریسک مانده به ریسکی گفته می‌شود که پس از اعمال روش‌های کاهش ریسک، کماکان در سیستم ریسک وجود دارد. دقت شود که ریسک‌های قابل قبول نیز نوعی ریسک مانده به شمار می‌آیند.

2.3.2.1 Safety Layers of Protection

هیچ معیار ایمنی واحد، به تنهایی نمی‌تواند اثر خطرات یا ریسک را کاهش داده و در صورت وقوع یک حادثه خطرناک از تجهیزات و کارکنان پلنت در برابر آسیب یا جلوگیری از گسترش آسیب، حفاظت کند. به همین دلیل مطابق استانداردهای ایمنی، روش‌های حفاظتی یک پلنت فرآیندی در لایه‌های مختلف پیاده‌سازی می‌شود. این لایه‌ها که به‌عنوان راه‌کارهای کاهش ریسک در پلنت فرآیندی مطرح می‌باشند، شامل زنجیره‌ای از دستگاه‌های مکانیکی، کنترل‌کننده‌های الکترونیکی (SIS)، سیستم‌های مرتبط با ایمنی و سایر روش‌های کاهش ریسک می‌باشند. در صورت عمل نکردن یک لایه حفاظتی، وظیفه هدایت فرآیند به یک وضعیت ایمن، بر عهده لایه بعدی خواهد بود. با افزایش لایه‌های حفاظتی و قابلیت اطمینان آن‌ها، ایمنی فرآیند نیز افزایش می‌یابد. توالی لایه‌های ایمنی را به ترتیب فعال‌سازی از پایین به بالا نشان می‌دهد.

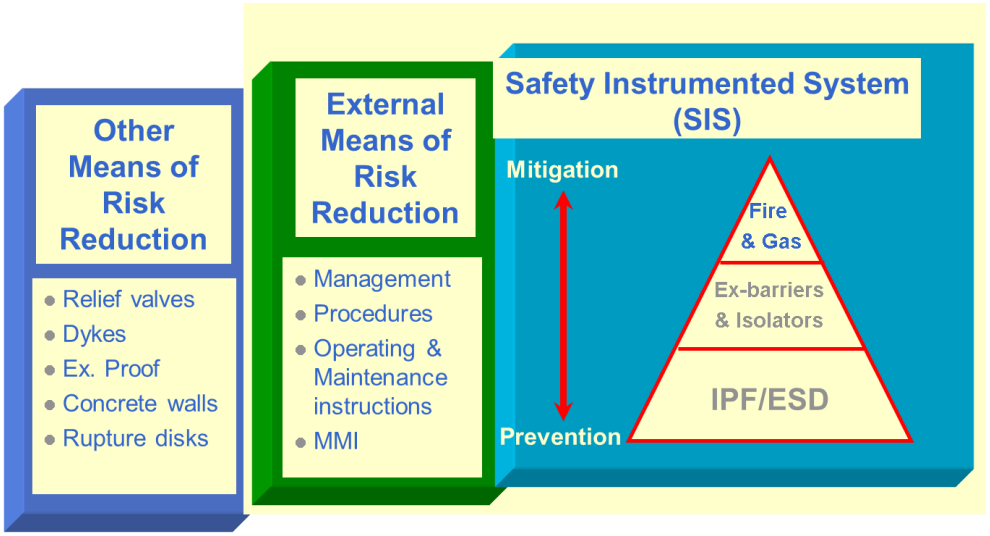
هدف اول از لایه‌های محافظتی، حفظ جان مردم است. مسائل اقتصادی در اولویت دوم قرار دارد. نگرانی‌های زیست محیطی نیز در اولویت سوم است.



شکل۱-۶: لایه‌های حفاظتی در یک پلنت فرآیندی

براساس لایه‌های حفاظتی روش‌های دستیابی به کاهش ریسک را می‌توان به صورت زیر دسته‌بندی کرد:

- استفاده از سیستم‌های کنترل SIS (سیستم‌های ESD و F&G به طور مثال سیستم S7-400FH)
- امکانات کاهش ریسک غیر از SIS (External Risk Reduction) مانند مدیریت، رویه‌ها (Procedures) دستورالعمل‌های بهره‌برداری و تعمیر و نگهداری (Operating & Maintenance)، سیستم مانیتورینگ
- استفاده از تسهیلات فیزیکی کاهش ریسک مانند: شیرهای تخلیه فشار (Relief valves)، خاکریزها (Dykes) دیوراهای بتنی (Concrete walls)، دیسک‌های پاره شونده (Rupture disks)



شکل۱-۷: دسته‌بندی روش‌های کاهش ریسک

1.4 Safety Instrumented Systems: SIS

1.4.1 Brief History or SIS Evolution

از زمان ارائه سیستم‌های خودکار، مهندسین ایمنی حفاظت خودکار را نیز برای سیستم‌ها طراحی کرده‌اند. در ابتدا اغلب سیستم‌های حفاظت خودکار، با استفاده از منطق پنوماتیک و یا رله‌های الکتریکی طراحی می‌شدند. از آنجایی که این قطعات قدیمی تمایل به خرابی (fail) در مد قطع انرژی (de-energized) داشتند. لذا سیستم‌های کنترل ایمنی طوری طراحی شده بودند که با قطع انرژی، سیستم اتوماسیون حفاظتی در وضعیت ایمنی قرار گیرد؛ به عبارت دیگر طوری طراحی شده بودند که در زمان خرابی، شرایط ایمنی (Fail Safe) را برای افراد و تجهیزات ایجاد کنند.

با گذشت زمان، لاجیک کنترل پلنت‌های فرآیندی که پیچیده‌تر شدند، سیستم‌ها بسط یافته و شامل پنل‌های بزرگ‌تر با رله و تایمرهای بیشتر شدند. در این دوره که بین دهه‌های ۵۰ تا ۶۰ میلادی بود، بردهای مدار چاپی و الکترونیک حالت جامد پدیدار شدند. لذا پیاده‌سازی لاجیک سیستم‌های کنترل با بردهای مدارچاپی توسط برخی از مهندسین حرفه‌ای در این زمان معمول شد. متاسفانه، در این طرح‌ها، دانش کمی در خصوص مدهای خرابی قطعات وجود داشت. که بعدها به دلیل وقوع حوادث ناگوار، مهندسین ملزم به طراحی سیستم‌های ایمنی با مشخصات دقیق‌تر نمود. در ادامه به صورت خلاصه مروری بر تاریخچه ارائه سیستم‌های SIS پرداخته شده است.

1960’s: Hardwired relays

سیستم‌های SRS دهه ۱۹۶۰ شامل رله‌ها با سیم‌بندی سخت‌افزاری بود. این رله‌ها در هر جایی که نیاز تشخیص داده می‌شد، نصب می‌شدند.

1970’s: Hardwired relays, Solid State logic

سیستم‌های SRS دهه ۷۰ شامل رله‌ها با سیم‌بندی سخت‌افزاری به همراه قطعات حالت جامد(تراشه‌های الکترونیکی) در بوردهای الکترونیکی بود.

1980's: Started using PLCs

- کنترل‌کننده‌های PLC جایگزین سیستم‌های مبتنی بر رله‌ها و قطعات حالت جامد (solid state) شدند.
- برای نرم‌افزارهای حوزه ایمنی هیچ استانداردی ارائه نشد.

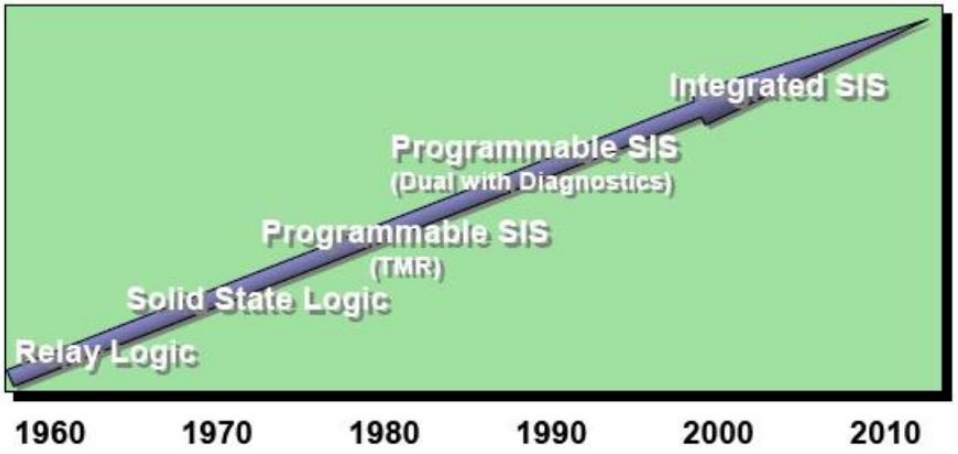
- رویه‌هایی تحلیل ریسک و HAZOP ارائه شد.
- مطالعات نشان می‌دهد که کاهشی در تصادفات دیده نشد.
- از دست دادن افراد و سرمایه همچنان ادامه داشت.

1990’s: Safety PLCs (including “safe” subsets of software)

- استانداردهای ایمنی (Safety) برای PLCها توسعه داده شد.
- توسعه بیشتر تحلیل‌های کمی ریسک (Quantitative Risk Analysis)
- رویکردهای سیستماتیک برای شناسایی ریسک ارائه شد.
- علی‌رغم عرضه سیستم‌های PLC ایمنی، بررسی‌ها نشان داد که استفاده از PLC منجر به کاهش حادثه نشده بود و ضرر مالي و جانی همچنان ادامه داشت.

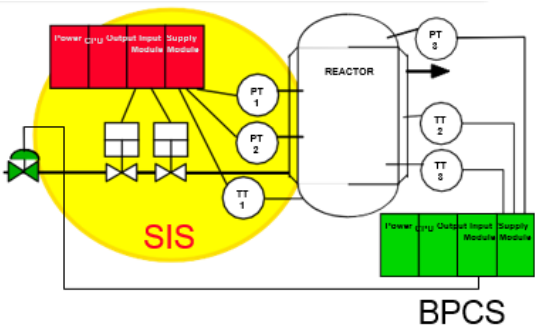
2000's Safety Field Equipment- Transmitters, Valves PLC's - Improved Diagnostics

- در این زمان استانداردهای ایمنی IEC تصویب شد.
- قابلیت‌های تشخیص عیب در سخت‌افزار ایجاد گردید.



شکل۱-۸: تاریخچه سیستم‌های کنترل ایمنی از منطق رله گرفته تا SIS یکپارچه

1.4.2 SIS Definition



یک SIS به سیستمی گفته می‌شود که در صورت خارج شدن فرآیند از وضعیت کنترل نرمال، به‌طور مستقل فرآیند را به یک وضعیت ایمن از قبل تعیین‌شده هدایت کند. یک پلنت فرآیندی که از کنترل خارج شود، منجر به پیامدهای ناگواری مانند صدمه به افراد، خسارت به محیط زیست و تجهیزات، از بین رفتن تولید و از دست رفتن سرمایه و پول می‌شود. همانطور که از شکل مقابل مشخص است، تجهیزات ابزار دقیق بکاررفته در SIS با سیستم کنترل فرآیند (BPCS) کاملا مجزا است.

IEC 61511/ISA 84.01 Definition

SIS یک معماری Failsafe PLC است. که لاجیک کنترل یک یا چند حلقه حفاظتی موسوم به SIF (Safety Instrumented functions) را پیاده‌سازی و اجرا می‌کند. مطابق این استاندارد یک حلقه SIF ترکیبی از حسگرها، اجراکننده لاجیک (Logic Solver) و عناصر کنترل نهایی (عملگرهایی مانند شیرهای ON/OFF) می‌باشد.

فصل دوم

کنترل‌کننده‌های Fail-Safeسیماتیک

SIMATIC Safety Systems

Chapter 2

2 SIMATIC Safety Systems

Learning targets

محتوای این فصل شامل مباحث زیر است:

- تاریخچه سیستم‌های Fail-safe زیمنس
- معرفی سیستم‌های کنترل Fail-safe زیمنس
- پروفایل ProfiSafe برای تبادل داده‌های ایمنی
- زیرسیستم I/O در سیستم‌های Fail-safe زیمنس

Abbreviations

I/O	Input /Output
SIL	Safety Integrated Level
SIS	Saftey Instrumented System
SIF	Safety Instrumented Functions
RIO	Remote I/O
DP	Distributed Peripheral
F	Fail-Safe
PIO	Process Image Output
PII	Process Image Input
PN	Profinet
IEC	International Electronic Committee
IM	Interface Module
NFPA	National Fire Protection Association
FH	Fail-Safe & High Availability

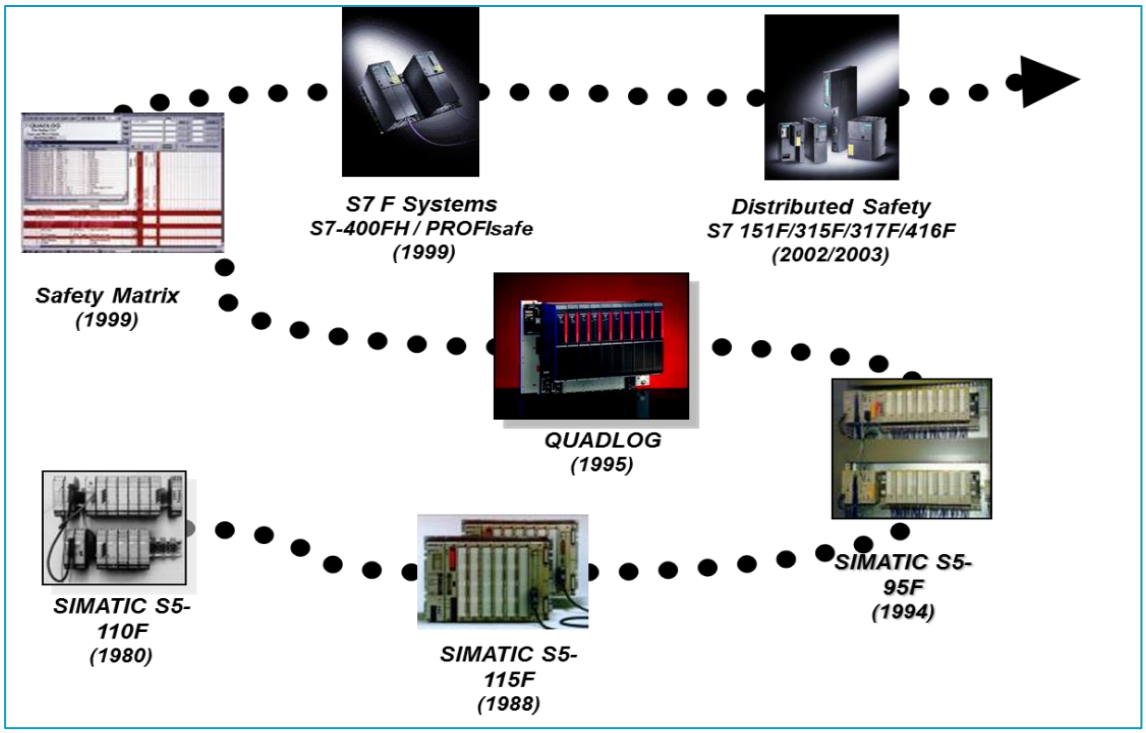
Contents

2.1 Siemens Safety Instrumented Systems

2.1.1 History of Siemens Safety Controllers

آغاز فعالیت زیمنس در حوزه محصولات و PLCهای ایمنی به سال‌های ۱۹۸۰ برمی‌گردد. نخستین پروژه بزرگ زیمنس، پیاده‌سازی سیستم‌های کنترل F، مربوط به پروژه Oseberg Feltsenter است. در حال حاضر نزدیک به ۳۰ درصد از سیستم‌های F نصب‌شده در قسمت نروژی دریای شمال و موارد متعدد در سراسر جهان مبتنی بر سیستم‌های F زیمنس می‌باشد. نمونه اولیه از سیستم‌های F (S5 F) زیمنس شامل دو S5 PLC با سخت‌افزار جانبی بود. به‌طوری‌که دو PLC مستقل از هم اجرا می‌شدند. شکل ۳-۱ تاریخچه سیستم‌های کنترل Fail-Safe شرکت زیمنس را به تصویر کشیده است. سیستم‌های کنترل زیمنس برای حوزه ایمنی شامل سه دسته کنترل‌کننده F می‌باشد. که عبارت است از:

- QUADLOG System (Siemens Moor) Family
- Simatic S5 F Controllers Family
- Simatic S7 F Contollers Family



شکل ۳-۱- تاریخچه سیستم‌های کنترل Fail-safe زیمنس

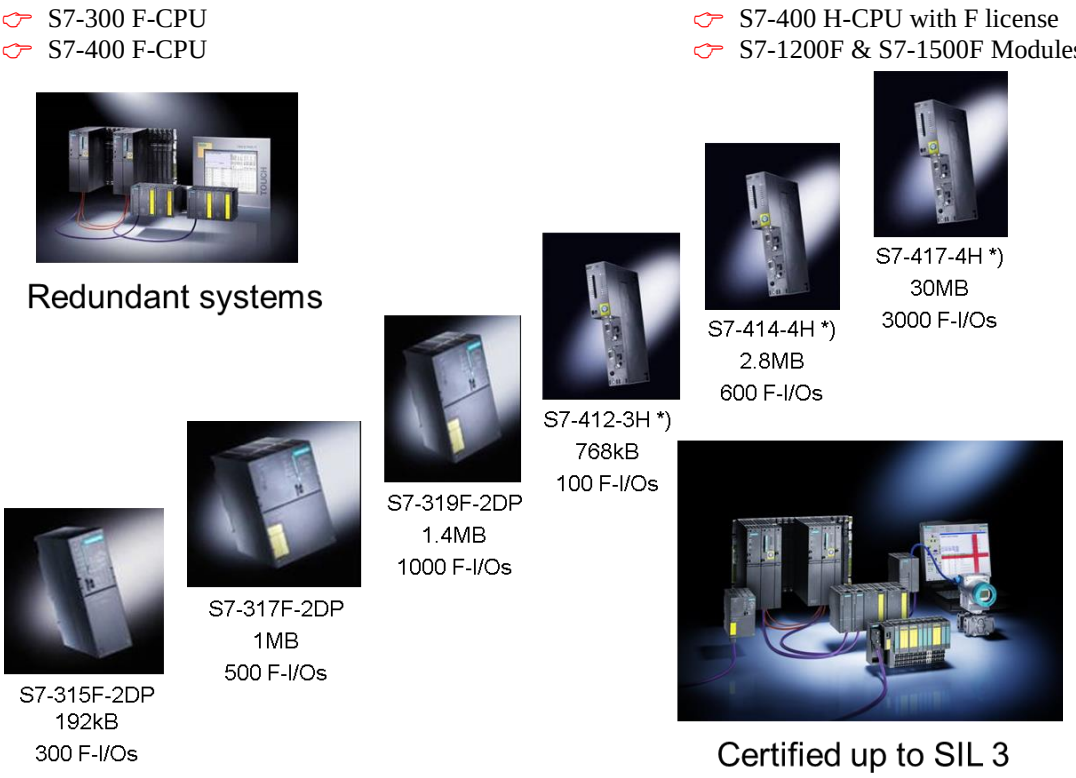
SIMATIC S5 F Controllers Family

خانواده S5 نسخه قبلی سیستم‌های S7 می‌باشد. این سری شامل کنترل‌کننده‌های F و FH زیر می‌باشد.

- S5-95 F, S5-110 F, S5-115 F
- S5-135 FH, S5-155 FH

SIMATIC S7 Safety Controllers: S7- 300/400 F/FH, 1200F, 1500F

این سری شامل طیف کاملی از کنترل‌کننده‌های F و سیستم‌های FH با گواهی‌نامه تائید توف (TÜV) می‌باشد. این سیستم‌ها که مطابق با استاندارد ایمنی IEC 61508 می‌باشند. به چهار دسته کنترل‌کننده تقسیم می‌شوند:



شکل ۳-۲- نمایی از انواع کنترل‌کننده‌های ایمنی خانواده S7 زیمنس

کنترل‌کننده‌های S7-F، محصولاتی هستند که سیستم‌های ایمنی اخیر زیمنس بر پایه این محصولات ارائه‌شده است. این محصولات به‌طور مشخص برای دو حوزه کاربردی جداگانه ارائه می‌شوند؛ که به‌صورت زیر قابل دسته‌بندی می‌باشند:

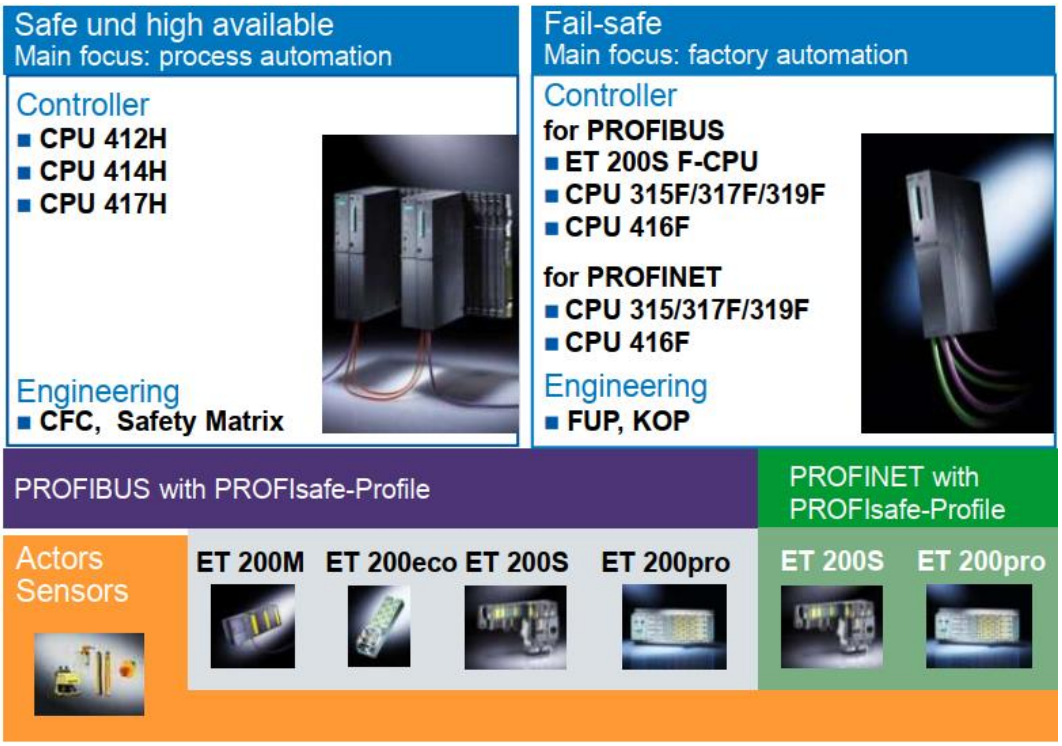
- Safe and high available controllers

- Main focus: process automation

☞ Fail-safe or F Controllers

- Main focus: factory automation

دسته اول که شامل ماژول‌های CPU سری S7-400H سیماتیک می‌باشد. مقصد نهایی این سیستم‌ها حوزه کاربرد ایمنی فرآیند می‌باشد. دسته دوم نیز ماژول‌های F-CPU سری S7-300F و S7-400F می‌باشد. هدف اصلی این کنترل‌کننده‌ها، تأمین ایمنی دستگاه و ماشین در حوزه اتوماسیون کارخانه می‌باشد.



شکل ۲-۱: محصولات S7- F زیمنس برای دو حوزه پلنت‌های فرآیندی و کارخانه

2.1.2 Comparison: Previous Solution versus New Fail-Safe Solution

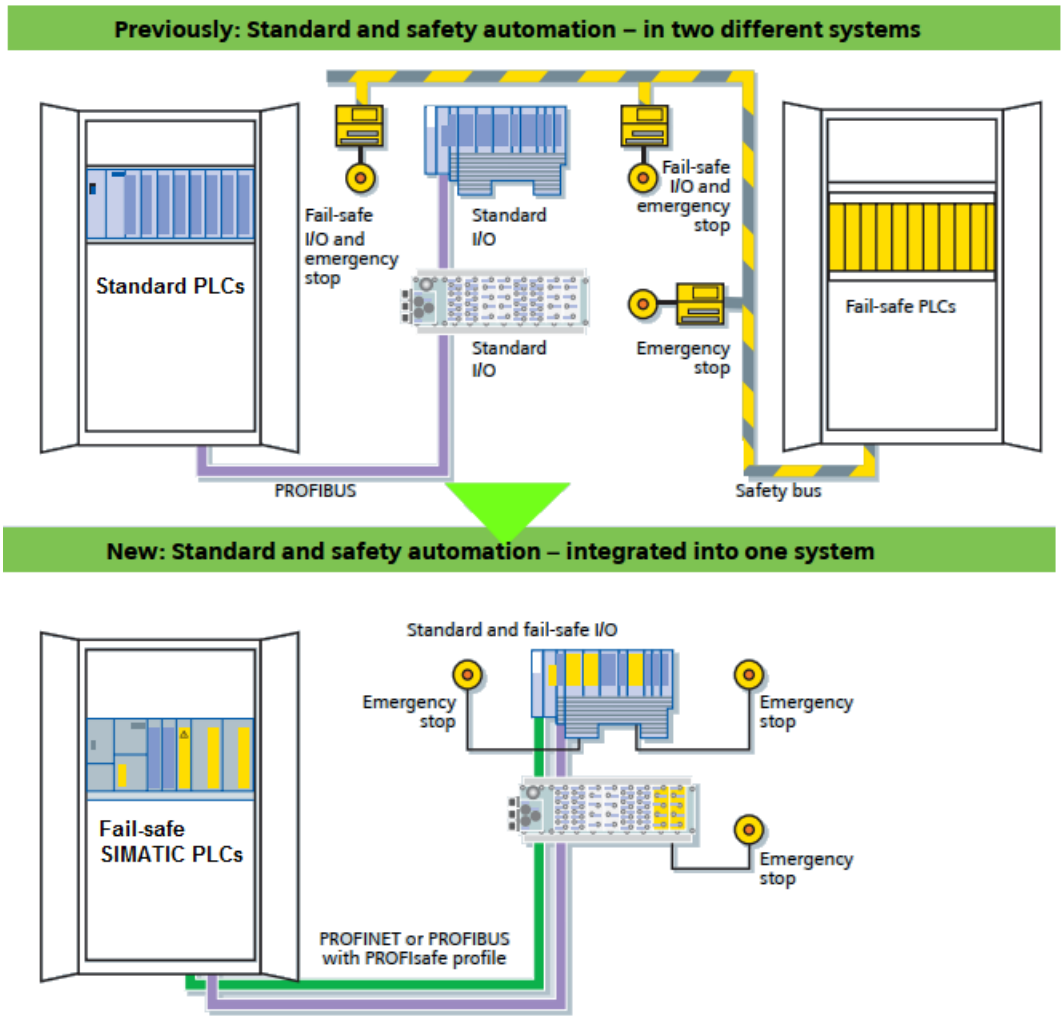
ساختار قدیم و جدید راه‌حل‌های PLC برای کاربردهای ایمنی:

قبل از ارائه معماری «ایمنی یکپارچه سیماتیک» راه‌کارهای قبلی برای پیاده‌سازی یک سیستم Fail-Safe به دو نوع PLC متفاوت (سیستم کنترل استاندارد و ایمنی) نیاز داشت. همچنین در راه‌حل‌های توزیع‌شده به یک باس ایمنی (Safety bus) نیاز بود.

معماری «ایمنی یکپارچه سیماتیک» در مقایسه با معماری قبلی، به‌صورت خلاقانه اتوماسیون استاندارد و فناوری ایمنی را در یک سیستم ترکیب می‌کند. لذا «ایمنی یکپارچه سیماتیک» تنها

به یک PLC نیاز دارد. به‌طوری‌که برای اتوماسیون استاندارد و اتوماسیون مرتبط با ایمنی، از یک بسته مهندسی یک‌شکل و شبکه PROFIBUS یا PROFINET استاندارد با پروفایل PROFIsafe استفاده می‌شود.

توجه شود که در صورت لزوم، سیستم‌ها همانند گذشته می‌توانند به‌صورت جداگانه پیکربندی شوند.



شکل ۲-۲: ساختار قدیم و جدید راه‌حل‌های PLC برای کاربردهای ایمنی

2.1.3 Configuration Example for Factory Automation

در حوزه اتوماسیون کارخانه، شرکت زیمنس دامنه کاملی از محصولات Fail-Safe را مبتنی بر Profinet متشکل از سیستم‌های اتوماسیون S7-300 و S7-400 ارائه می‌دهد. به‌طوری‌که دستگاه‌های Failsafe توزیع‌شده در فیلد را می‌توان مستقیماً به Profinet وصل کرد. دستگاه‌های Failsafe موجود مبتنی بر Profibus نیز می‌توانند در یک پروژه Profinet ادغام شوند.

SIMATIC modules			
Controller		**PROFIBUS**	**PROFINET**
ET 200 S	IM 151-7 F-CPU	■	
S7-300	CPU 315F-2 DP	■	
NEW	CPU 315F-2 PN/DP	■	■
	CPU 317F-2 DP	■	
NEW	CPU 317F-2 PN/DP	■	■
S7-400	CPU 416F-2	■	■ 1)
Distributed I/O			
ET 200S		■	■
ET 200M		■	
ET 200pro NEW		■	■
ET 200eco		■	

شکل ۲- ۳: اجزای سخت‌افزاری سیستم‌های کنترل ایمنی سیماتیک برای کاربردهای اتوماسیون کارخانه

2.1.4 Configuration example for process automation

امروزه از سیستم‌های کنترل ایمنی در حوزه فرآیند تحت عنوان SIS نام‌برده می‌شود. در این راستا «ایمنی یکپارچه سیماتیک» یک راه‌حل SIS را مبتنی بر محصولات S7-400FH و ET 200M/S ارائه می‌دهد. با استفاده از این محصولات می‌توان SIS را به هر سیستم کنترل (DCS) متصل کرد. ویژگی منحصربه‌فرد این سیستم ادغام توابع ایمنی (F) و تحمل‌پذیر در برابر خطا (H) در سیستم کنترل فرآیند SIMATIC PCS 7 است. این ترکیب چندین مزیت را ارائه می‌دهد:

- یک سیستم مهندسی واحد برای کاربردهای استاندارد و ایمنی فرآیند.
- ادغام یک‌شکل فن‌آوری ایمن و تحمل‌پذیر در سیستم اتوماسیون PCS 7 (AS).
- بصری سازی مقادیر ایمنی فرآیند، یکپارچه‌شده در ایستگاه‌های اپراتوری OS (PCS 7).

- ادغام خودکار پیام‌های فالت مربوط به ایمنی (safety-related fault messages) در صفحات نمایش فرآیند، با برچسب زمانی یکسان.
- برقراری لینک ساده بین DCS و SIS بدون هزینه اضافی

Controller

- پیکربندی کنترل‌کننده‌های S7-400FH همانند S7-400 استاندارد با یک ابزار مشترک (HWConfig).
- دستیابی به حداکثر سطح ایمنی SIL 3 فقط با یک کنترل‌کننده امکان‌پذیر است.
- توابع استاندارد، ایمنی و تحمل‌پذیر در برابر خطا در یک کنترل‌کننده قابل‌ترکیب بوده و یا به‌صورت جداگانه پیکربندی می‌شوند.
- کنترل‌کننده‌های FH را می‌توان در یک فاصله ۱۵ کیلومتری جدا از هم پیکربندی کرد.

I/O

- امکان پیکربندی I/O با تعداد زیادی ماژول در ساختار ET 200M و ET 200S.
- دارای ماژول‌های نوع NAMUR (ET 200M) برای مناطق خطرناک (Ex).
- امکان اضافه نمودن ماژول‌های استاندارد و F برحسب الزام کاربردی.
- استفاده از ساختار redundancy/diversity در مدار داخلی ماژول‌های F
- دارای توابع جامع تشخیصی (Comprehensive diagnostics) برای تشخیص فالت‌های داخلی و بیرونی
- امکان پیاده‌سازی توابع ایمنی در ماژول‌های سیگنال F (مانند سیستم 1oo2 Voting)

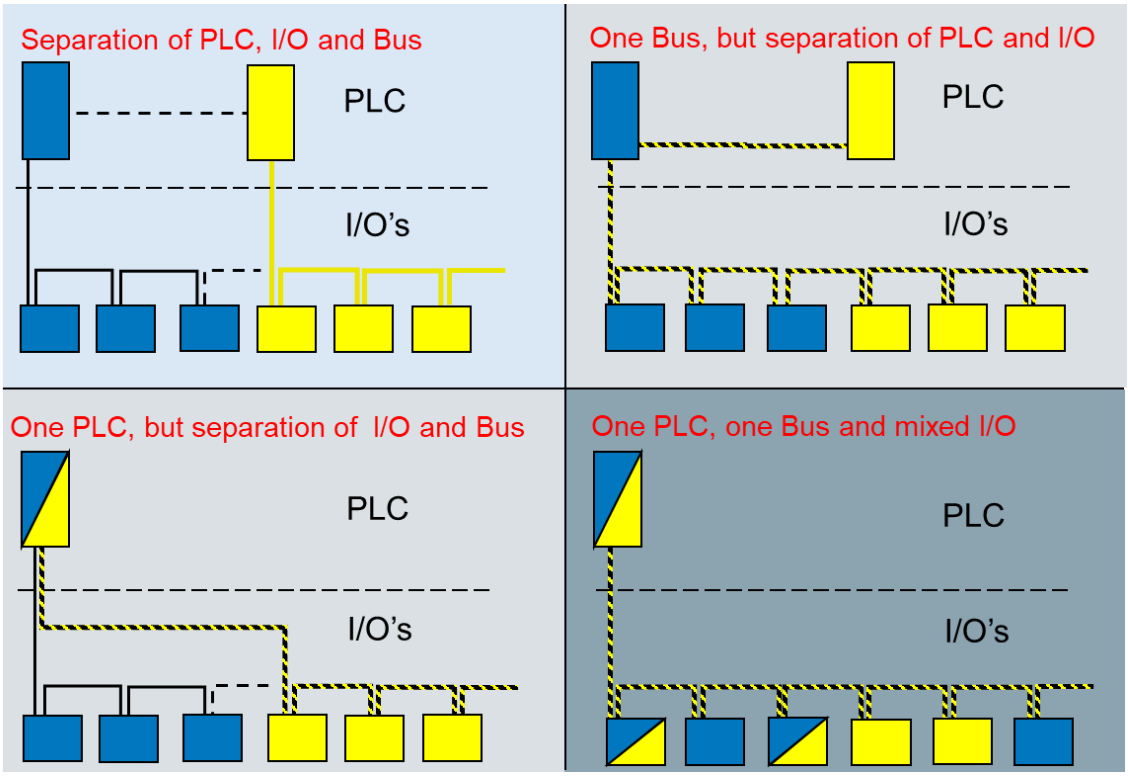
Communication

- استفاده از شبکه استاندارد PROFIBUS DP با پروفایل PROFIsafe

در روش سوم برنامه F و استاندارد در یک CPU اجرا می‌شوند ولی باس و ماژول‌های I/O جداگانه استفاده می‌شود.

در روش چهارم که روش هیبرید نام دارد، می تواند در سری 300F,400F و 400FH محقق شود.

معماری‌های مختلف پیاده‌سازی کنترل‌کننده F و F-I/O با کنترل‌کننده و I/O استاندارد را نشان می‌دهد.



شکل ۲-۱٤: معماری‌های مختلف پیاده‌سازی کنترل‌کننده F و F-I/O با کنترل‌کننده و I/O استاندارد

2.10 References

[1] SITRAIN ST-PPDS Cource Document, Safety Concept: Distributed Safety, Siemens AG, 2009

[2] Safety Integrated for Process Automation, August 2014, Brochure

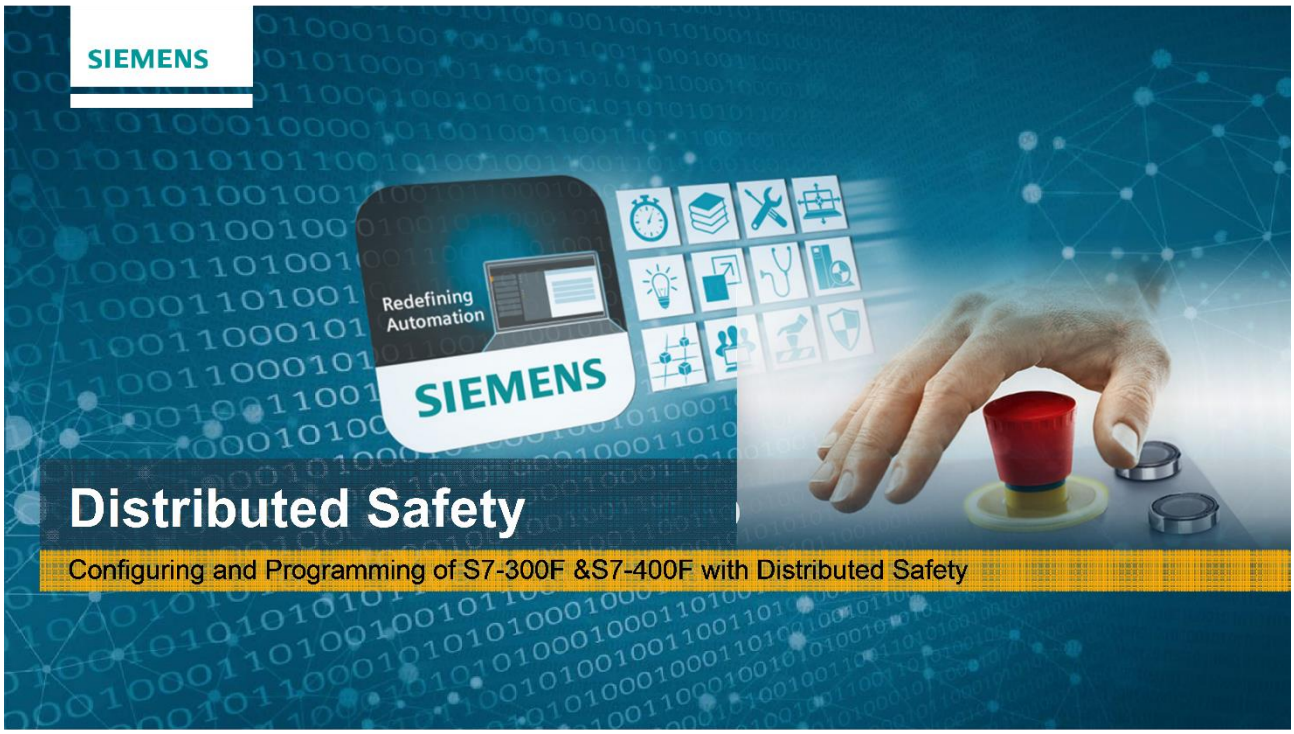
[3] Siemens Forum

[4] Safety Integrated for Process Automation Reliable, Flexible, Easy, Technical Brochure, April 2008

[5] Controllers: Fail-Safe Control Systems (SIMATIC), Kapite 14

فصل سوم

پیکربندی و برنامه نویسی سیستم‌های S7-300F &S7-400F



Configuring and Programming of S7-300F &S7-400F with Distributed Safety

Chapter 3

3 Implementing Failsafe Systems with Distributed Safety

Learning targets

محتوای این فصل شامل مباحث زیر است:

- معرفی سیستم کنترل S7-300F
- پیاده‌سازی سیستم کنترل S7-300F با Distributed Safety
- برنامه‌نویسی سیستم‌های کنترل S7-300F

Abbreviations

AS	Automation Station or Automation System
OS	Operator Station
SIL	Safety integrity level
PCS	Process Control System
FH	Fail-Safe & High Available
SIF	Safety Instrumented Functions
RIO	Remote I/O
DB	Data Block
F	Fail-Safe
DI	Digital Input
DO	Digital Output

Contents

3.1 Implimenting S7 Project with Distributed Safety

در این فصل نحوه پیاده‌سازی کنترل یک ماشین یا پلنت در حوزه اتوماسیون کارخانه با بسته نرم‌افزار Distributed Safety تشریح می‌شود. ولی قبل از پیاده‌سازی سیستم کنترل با یک F-PLC (300F/400F) در ابتدا نحوه پیاده‌سازی آن با روش مرسوم قدیمی یعنی بدون استفاده از یک PLC ایمنی تشریح می‌شود. یادآوری می‌شود که S7 Distributed Safety یک بسته نرم‌افزاری است که برای پیکربندی و برنامه‌ریزی سیستم‌های اتوماسیون S7-300F و S7-400F استفاده می‌شود.

3.1.1 Example-1: Conventional Safety Technology

در این قسمت برای درک ساختار و پیکربندی کاربردهای ایمنی ماشین، موضوع را با یک مثال کاربردی شروع می‌کنیم. شکل ۳-۱ یک مثال از طرح یا معماری پیاده‌سازی کنترل کاربردهای ایمنی به روش مرسوم را نشان می‌دهد که در آن برای کنترل توابع استاندارد یک پلنت یا کارخانه از یک PLC استاندارد با ساختار I/O توزیع‌شده (ET200S) مبتنی بر PROFIBUS DP استفاده‌شده است؛ مطابق شکل در این ساختار یک رله ایمنی (safety relay) وجود دارد که عملکرد ایمنی ماشین پرمخاطره را کنترل می‌کند.

طرح مذکور مثالی از یک کاربرد «تأمین ایمنی در حوزه ماشین» است که برای پیاده‌سازی سیستم کنترل یکپارچه این پلنت، از مجموعه سخت‌افزار و نرم‌افزار پلات‌فرم «ایمنی توزیع‌شده» می‌توان استفاده کرد. در این طرح اجزاء فناوری‌های کنترل استاندارد (PLC معمولی) و ایمنی (رله ایمنی) از هم جدا (Separate Standard and Safety Technology) شده است.

Functional Control

توابع کنترلی پلنت مذکور به شرح زیر است:

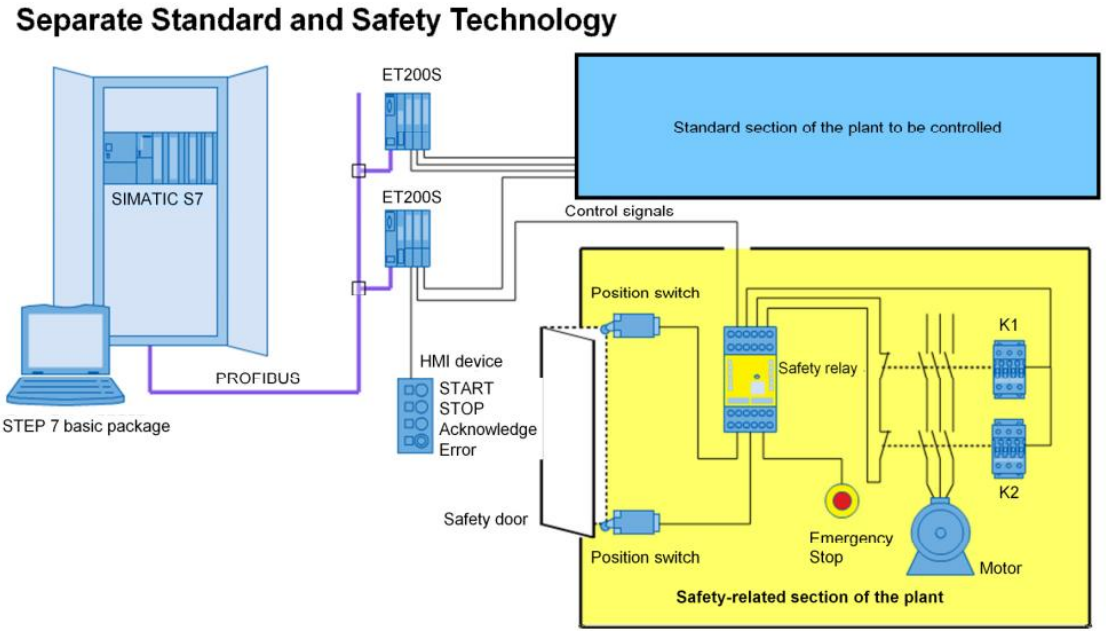
۱- عملکرد دستگاه دارای مخاطره از طریق دو کنتاکت K1 و K2، که به روش ایمن توسط یک رله ایمنی کنترل می‌شود، فعال/غیرفعال (سوئیچ) می‌شود.

۲- رله ایمنی سیگنال‌های فرمان On/Off لازم برای فعال/غیرفعال کردن عملکرد دستگاه از طریق سیم بندی کانال خروجی دیجیتال PLC استاندارد دریافت می‌کند.

۳- یک ماژول CPU استاندارد، سیگنال‌های وضعیت مربوطه را از پلنت دریافت کرده و با لاجیک استاندارد، تجزیه‌وتحلیل می‌کند. به این معنی که عملکرد لاجیکی پلنت توسط یک PLC استاندارد کنترل و پایش می‌شود. مطابق شکل اجزاء اصلی این معماری

عبارت‌انداز:

- کنترل‌کننده استاندارد؛
- ماژول‌های I/O مبتنی بر ET200S؛
- رله ایمنی به همراه کنتاکت‌های K1 و K2؛



شکل ۳-۱- معماری قدیمی برای پیاده‌سازی کنترل عملکرد یک ماشین پرخطر

Protective Functions

توابع محافظتی- در این ساختار جهت محافظت اپراتور از خطرات، عملکرد (Function) دستگاه به یک کلید صدور فرمان توقف اضطراری (Emergency Stop) و یک تجهیز حفاظتی جداساز به‌صورت یک درب ایمنی مجهز شده است. به‌محض وقوع و تشخیص یک خطا در سیم بندی، کلید توقف اضطراری توسط اپراتور فشار داده‌شده و درب ایمنی باز می‌شود. رله ایمنی مستقل از سیگنال‌های کنترلی PLC استاندارد، مطابق Stop-Category 0 قیدشده در استاندارد EN 60204-1 موتور را از طریق کنتاکتورهای K1 و K2 متوقف می‌کند.

قبل از هرگونه تغییر مجدد در کنتاکت‌ها، رله ایمنی، بسته بودن کنتاکت‌های توقف اضطراری و درب ایمنی را چک کرده و همچنین بررسی می‌کند که سیگنال فیدبک بسته شدن آن‌ها دریافت شده است.

Wiring

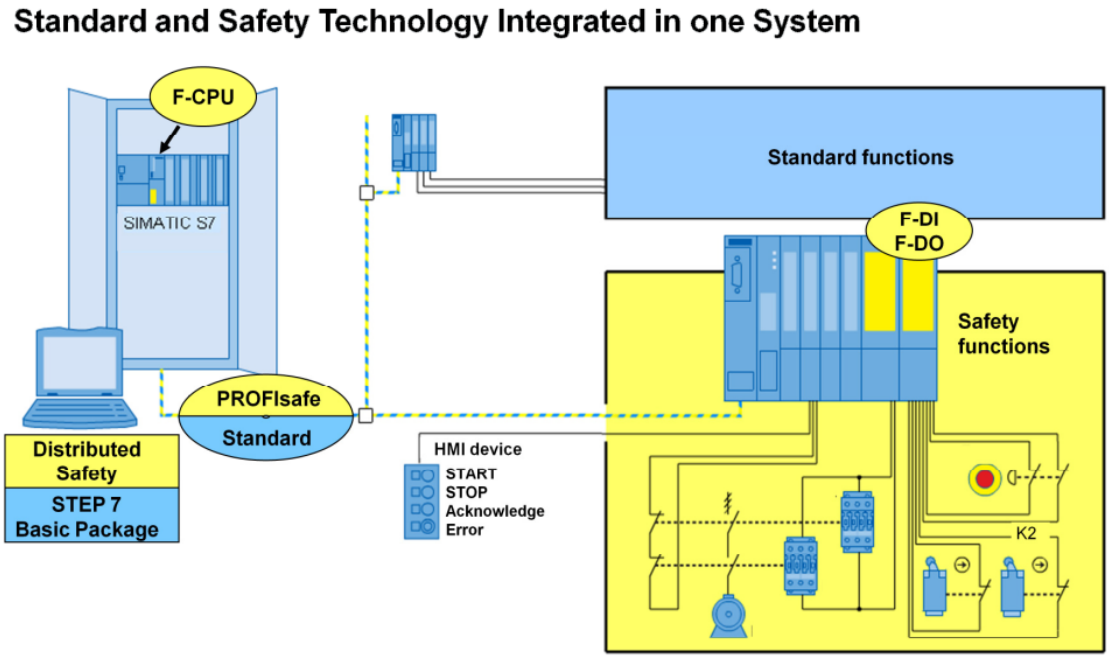
سیم بندی و معماری توابع ایمنی این طرح، مطابق استاندارد EN 61508 در ساختار SIL 3 و یا مطابق EN 954 در ساختار Cat.4 پیاده‌سازی می‌شود. به این صورت که کلید توقف اضطراری و سوئیچ موقعیت درب ایمنی از طریق دو کانال به رله ایمنی سیم بندی می‌شود. برای کنترل عملکرد ماشین نیز دو کنتاکتور به‌صورت سری متصل می‌شود. به‌طوری‌که سیگنال‌های فیدبک یا کنتاکت‌های آینه‌ای آن‌ها به‌عنوان فیدبک به رله ایمنی متصل می‌شود.

3.1.2 Example-2 Safety Integrated Technology

حال در این مثال به‌جای طرح ایمنی بالا که در آن تجهیزات کنترل ایمنی و لاجیک فرمان، جدا از هم بودند، از یک طرح یکپارچه با عنوان «ایمنی توزیع‌شده» جهت عملکرد ایمن دستگاه استفاده می‌شود.

Safety Integrated

مفهوم «ایمنی یکپارچه‌شده» در این طرح به این معنی است که برای کنترل تمامی توابع ایمنی و همچنین توابع استاندارد از یک PLC دارای F-CPU و ایستگاه‌های I/O توزیع‌شده ET200S مبتنی بر PROFIBUS DP با پروفایل PROFisafe استفاده می‌شود.



شکل۳-۲- طرح معماری یکپارچه برای کنترل ایمنی یک دستگاه یا ماشین

Functional Control

در طرح جدید نیز، عملکرد دستگاه خطرساز از طریق دو کنتاکت K1 و K2، سوئیچ می‌شود. ولی

این بار توسط یک رله ایمنی کنترل نمی‌شود. بلکه به‌جای رله یک لاجیک ایمنی بارگذاری شده در F-CPU همراه با ماژول‌های ورودی و خروجی مرتبط با ایمنی عملکرد دستگاه را کنترل می‌کند.

شرایط و وضعیت ورودی/خروجی‌ها برای توابع On و Off هنوز توسط برنامه استاندارد مورد تجزیه‌وتحلیل قرار می‌گیرد. به‌طوری‌که زمان روشن و خاموش شدن کنتاکتورها را از طریق متغیرهایی (مانند بیت‌های حافظه) به برنامه ایمنی اطلاع می‌دهد.

Protective Functions

در این طرح عملکردهای حفاظتی که قبلاً توصیف شد، دیگر توسط رله ایمنی اجرا نمی‌شود، بلکه توسط برنامه ایمنی F-CPU و ماژول‌های ورودی و خروجی F (F-DI/F-DO) صورت می‌گیرد. به‌محض اینکه یک خطای سیم بندی تشخیص داده شود، توقف اضطراری فشار داده‌شده و یا درب ایمنی باز می‌شود. رله ایمنی باید موتور یا کنتاکتورهای K1 و K2 را طبق استاندارد EN 60204-1 در رده Stop-Category 0 - مستقل از سیگنال‌های کنترل برنامه استاندارد خاموش کند. در ساختار جدید عمل پایش قطعی سیم در محرک‌ها و حس‌گرهای ایمنی، توسط ماژول‌های F-DI/DO صورت می‌گیرد.

Wiring

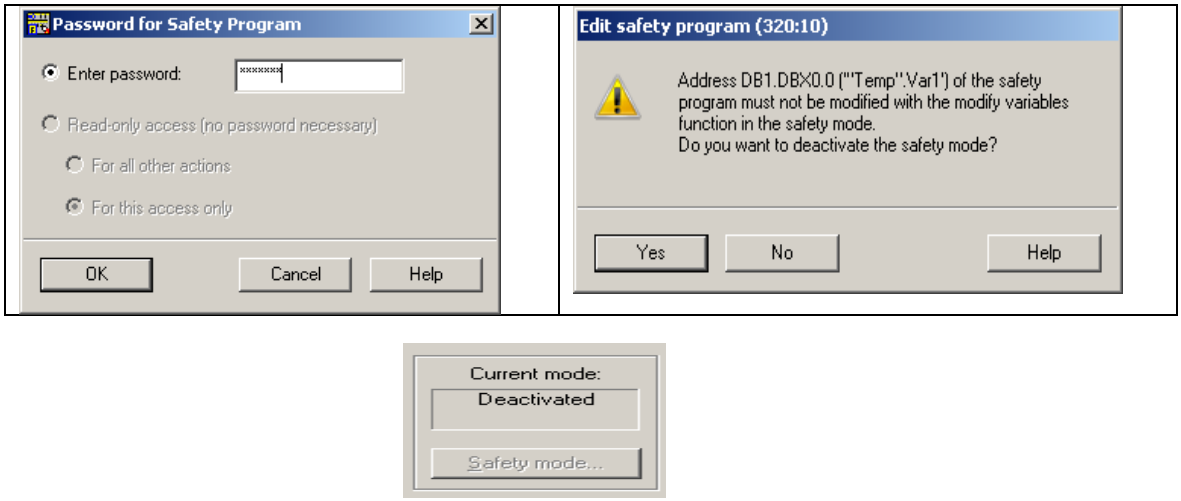
سیم بندی و معماری توابع ایمنی نسبت به طرح قبلی تغییرنیافته و همانند طرح قبلی بر اساس استاندارد EN 61508 در ساختار SIL 3 و یا مطابق EN 954 در ساختار Cat.4 پیاده‌سازی می‌شود. در این طرح نیز کلید فرمان قطع اضطراری (Emergency Off) و سوئیچ موقعیت درب ایمنی به دو کانال سیم بندی می‌شود. ولی این بار نه به یک رله ایمنی، بلکه به دو کانال یک ماژول F-DI واقع در ایستگاه RIO (ET200S) سیم بندی می‌شود.

توجه شود که برای تعویض عملکرد دستگاه، هنوز هم از دو کنتاکتور استفاده می‌شود که به‌صورت سری متصل می‌شوند. ولی در این طرح این دو کنتاکتور توسط یک ماژول F-DO کنترل می‌شوند و سیگنال فیدبک آن‌ها یا کنتاکت‌های آن‌ها در این حالت توسط برنامه ایمنی تجزیه‌وتحلیل می‌شود.

3.2 Hardware Support for Distributed Safety Integrated

برای پیاده‌سازی یک معماری ایمنی بروش Distributed Safety حداقل سخت‌افزار لازم عبارت است از:

برای دیباگ کردن لاجیک F، بلاک FB100 را باز کرده و مانند برنامه استاندارد با استفاده از دستور Debug یا با آیکون عینک مد دیباگ برنامه را فعال می‌کنیم.



شکل۳-۴۷- فعال‌سازی مد دیباگ برنامه F

برای اطلاعات بیشتر در خصوص برنامه‌نویسی سیستم‌های 300F به سند زیر مراجعه شود.

SIMATIC Industrial Software SIMATIC Safety - Configuring and Programming Industrial Software - Safety Engineering in SIMATIC S7

3.5.8 SIMATIC S7-400F

سیستم SIMATIC S7-400F توابع ایمنی (safety-related functions) را با استفاده از یک F-CPU و ماژول‌های F-I/O پیاده‌سازی می‌کند. به‌طوری‌که ماژول‌های F-I/O را می‌توان تنها به‌صورت توزیع‌شده (Distributed) یعنی سیستم‌های ET200M و ET200S. پیکربندی کرد.

توجه شود که در پیکربندی یک سیستم با CPU 416F این سری در پروفایل PCS7 وجود ندرد.

3.5.8.1 Configure a S7-400F Station Manually

خلاصه پیکربندی یک سیستم مبتنی بر S7-400F به‌صورت دستی به شرح زیر می‌باشد:

۱- ایجاد یک پروژه به‌صورت دستی در SIMATIC Manager

۲- درج یک 400 Station در SIMATIC Manager

۳- راست کلیک بر روی ایستگاه ایجادشده و باز کردن آن در محیط HWConfig

۴- درج یک رک UR2

۵- درج ماژول یا ماژول‌های تغذیه استاندارد (PS)

۶- درج یک CPU از مجموعه 400F (416F-2,416F-3 PN/DP)

۷- درج یک رک ET200M از پروفایل ProfibusDP

۸- درج ماژول‌های F-I/O از کاتالوگ به داخل رک ET200M

۹- فعال کردن مد Safety برای ماژول‌های I/O و تنظیم پارامترهای موردنیاز

۱۰- فعال کردن گزینه مرتبط با برنامهF در پنجره پراپرتی CPU

۱۱- ذخیره و کامپایل سخت‌افزار

3.5.8.2 S7-400F Programming

سخت‌افزار این نوع سیستم مبتنی بر ماژول‌های CPU 400F بوده و توسط یک کتابخانه F از پیش پیکربندی شده برنامه‌نویسی می‌شود. عملکرد بلاک‌های برنامه‌نویسی این کتابخانه و همچنین ابزارهای تعریف پارامتر به ماژول‌های ورودی/ خروجی توسط موسسه بازرسی آلمان (TÜV) تأیید شده است. برای اجرای برنامه S7-400F بایستی یک لایسنس F Copy به ماژول CPU بارگذاری شود.

سیستم‌های مبتنی بر ماژول CPU-400F همانند سری S7-300F با زبان‌های برنامه‌نویسی F_LAD و F_FBD برنامه‌نویسی می‌شود.

3.5.9 References

[1] SITRAIN ST-PPDS Cource Document, Safety Concept: Distributed Safety, Siemens AG, 2009

فصل چهارم

معماری سیستم کنترل تحمل‌پذیر خرابی

S7-400H

SIMATIC S7-400H

Fault Tolerant Architecture

Chapter 4

4 S7 Fault Tolerant Control System

4.1 Learning targets

محتوای این فصل شامل مباحث زیر می‌باشد:

- انواع سیستم‌های اتوماسیون S7-400
- اجزای اصلی یک سیستم S7-400H
- مفهوم ریداندانسی
- زیرسیستم I/O برای S7-400H

4.2 Abbreviations

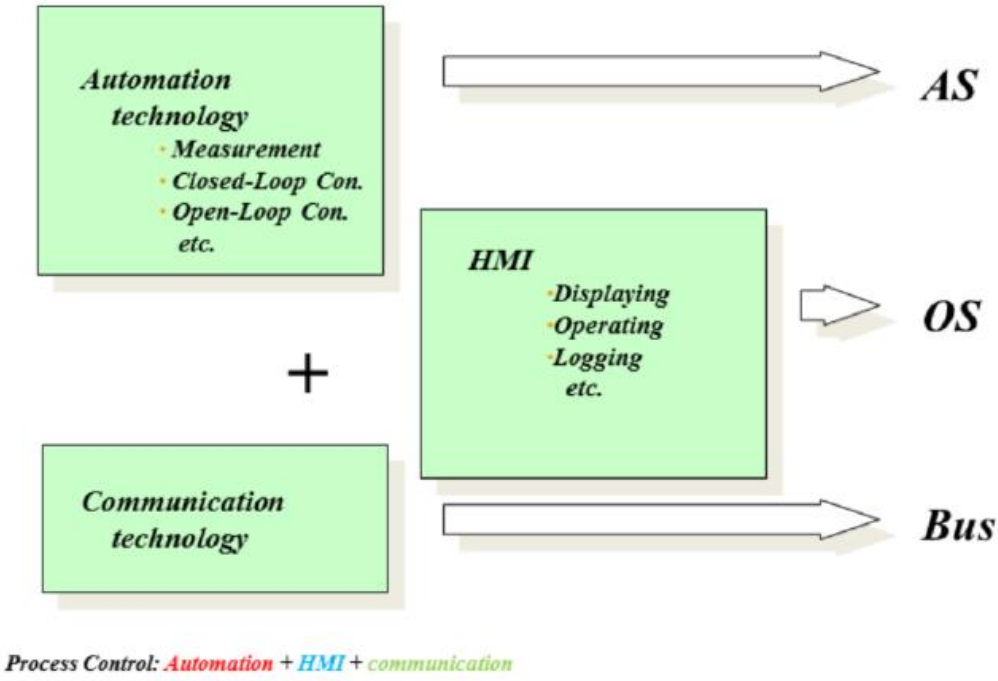
AS	Automation Station or Automation System
OS	Operator Station
H	High Availibility
PCS	Process control System
FH	Fail-Safe & High Available
RIO	Remote I/O

Table of Content

4.3 Introduction: Siemens Process Control System (PCS7)

راه‌کار جامع نرم‌افزاری زیمنس برای پیاده‌سازی یک سیستم کنترل فرآیند مبتنی بر S7-400FH استفاده از معماری نرم‌افزاری PCS7 می‌باشد.به این معنی که برای پیاده‌سازی برنامه کنترل F ساختار نرم‌افزاری جداگانه‌ای وجود ندارد و از همان نرم‌افزار مورداستفاده برای کنترل‌کننده‌های استاندارد DCS بهره می‌برد. این معماری در سه زیرسیستم خلاصه می‌شود:

- ایستگاه اتوماسیون AS (Automation System)
- ایستگاه اپراتوری OS (Operator Station)
- شبکه ارتباطی بین تجهیزات فیلد و ایستگاه‌های AS و OS (SIMATIC Net)



شکل ٤-١: زیرسیستم‌های اصلی تشکیل‌دهنده معماری یک سیستم کنترل فرآیند PCS 7

- ایستگاه اتوماسیون (AS) به یک مجموعه سخت‌افزار مبتنی بر S7-400 اطلاق می‌شود. که شامل ماژول‌های تغذیه (PS)،ماژول/ماژول‌های پردازنده (CPU)، کارت‌های شبکه (CP) و ماژول‌های ورودی/خروجی (RIO) است. وظیفه سیستم AS، اندازه‌گیری و کنترل مقادیر پارامترهای فرآیند به‌صورت حلقه بسته و حلقه باز می‌باشد.

- سیستم OS یک ایستگاه کامپیوتری برای بصری سازی فرآیند و تهیه آرشیو از مقادیر پارامترهای فرآیندی و آلارم‌های فرآیند و همچنین نمایش آن‌ها به اپراتور را بر عهده دارد.
- شبکه سیماتیک نیز بستر ارتباط داده بین تجهیزات فیلد و سیستم‌های AS و OS را باقابلیت اطمینان بالا فراهم می‌کند.

4.3.1 S7 400 Automation Systems

هسته مرکزی ایستگاه اتوماسیون (AS) را ماژول‌های S7-400 CPU تشکیل می‌دهد. این ماژول‌ها در معماری S7 در چهار نوع قابل دسته‌بندی می‌باشد:

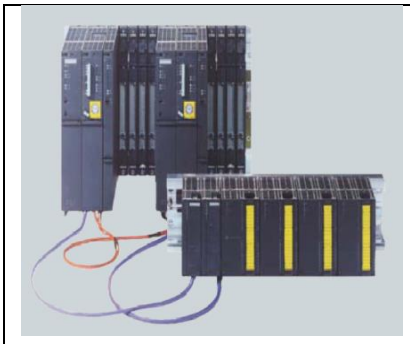
- کنترل‌کننده استاندارد AS400 (Standard System) مبتنی بر ماژول‌های 400-CPU معمولی؛
- کنترل‌کننده تحمل‌پذیر خرابی AS400H (fault-Tollerant or Redundant System)
- سیستم تحمل‌پذیر و ایمن در خرابی AS400-FH مبتنی بر ماژول‌های 400H-CPU به همراه نرم‌افزار F-System؛
- کنترل‌کننده AS400F (Failsafe) بر اساس ماژول‌های 400F-CPU به همراه نرم‌افزار Distributed Safety؛

دسته اول، ماژول‌های CPU معمولی به‌اصطلاح استاندارد هستند که قابلیت پیاده‌سازی پیکربندی ریداندانت سخت‌افزاری را ندارند.

سری دوم، CPUهای 400H هستند که قابلیت پیکربندی ریداندانت به‌صورت سخت‌افزاری را دارند.

سری سوم که با عنوان FH مطرح می‌شود، از لحاظ سخت‌افزاری همان ماژول‌های H-CPU هستند. با این تفاوت که برنامه کاربر با استفاده از بسته نرم‌افزاری F-System، به‌صورت Fail-safe پیاده‌سازی می‌شود. کنترل‌کننده‌های FH در فرآیندهایی استفاده می‌شود که به هر دو قابلیت «در دسترس‌پذیری بالا» (H) و «ایمنی» (F) نیاز می‌باشد. سری چهارم ماژول‌های CPU نوع Fail-Safe یا به‌اختصار F می‌باشند. که معمولاً در کاربردهای تأمین ایمنی برای حوزه اتوماسیون کارخانه (Factory Automation) استفاده می‌شود.

نکته: توجه شود که در مجموعه محصولات خانواده کنترل سیماتیک، ماژول CPU سخت‌افزاری با عنوان FH وجود ندارد. درواقع هسته اصلی یک سیستم FH همان CPUهای سری H زیمنس است که با لایسنس Fail-Safe و نرم‌افزار F-system پیکربندی می‌شوند.



AS-400FH

AS-400H

AS-400

شکل ٤-٢: انواع سیستم اتوماسیون مبتنی بر S7-400

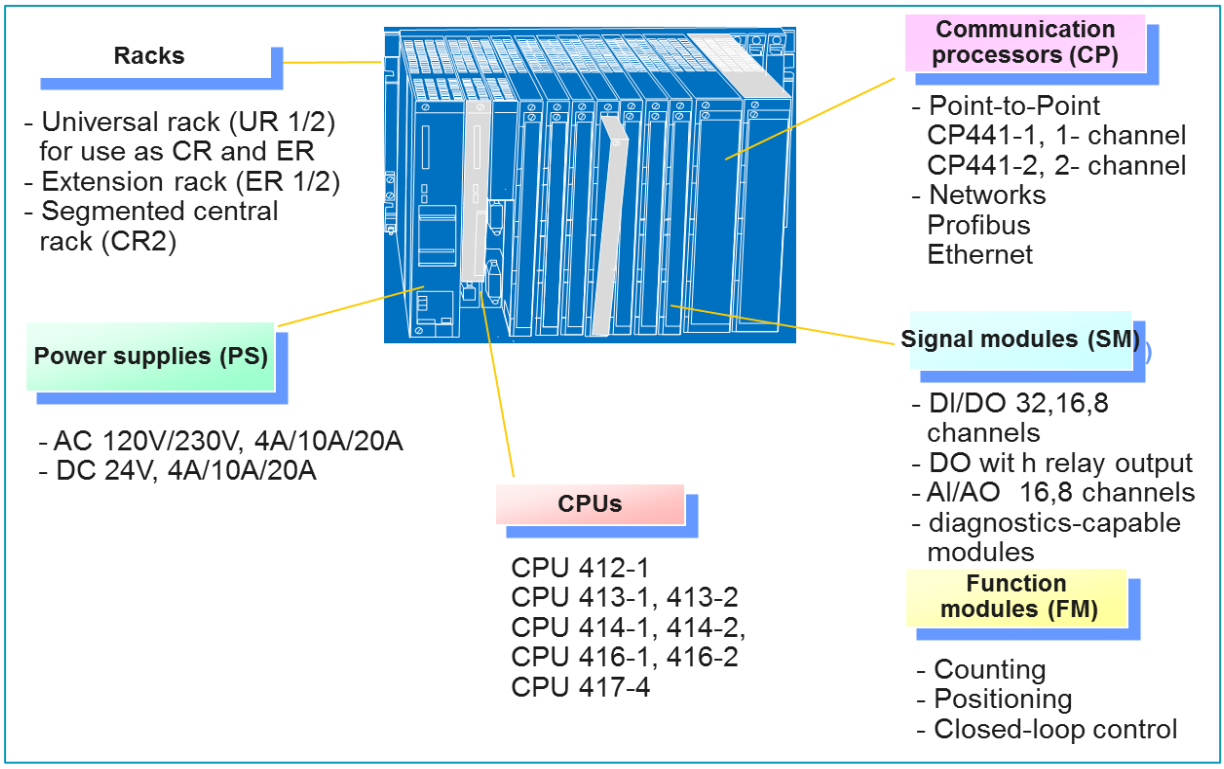
4.3.2 AS-400 Standard Automation System

سیستم اتوماسیون استاندارد: در این پیکربندی، یک AS، تنها دارای یک ماژول CPU بوده و در کاربردهایی که به مشخصه «دسترس‌پذیری بالا» (H) نیازی نباشد، استفاده می‌شود. همه ماژول‌های این سری قابلیت پیکربندی به‌صورت PLC را دارا می‌باشند. ولی توجه شود که تنها تعدادی از آن‌ها را می‌توان در معماری PCS7 پیکربندی کرد. ماژول‌های CPU این سری که می‌توان در معماری PCS7 پیکربندی کرد شامل مدل‌های زیر است:

Standard CPU Modules

- ✓ CPU 414-3 DP; CPU 414-3 PN/DP; CPU 416-2 DP; CPU 416-3 DP; CPU 416-3 PN/DP; CPU 417-4;

شکل ۴-۳ اجزای یک سیستم AS-400 استاندارد را به تصویر کشیده است.



شکل ۴- ۳: اجزای یک سیستم S47-400 استاندارد

4.3.2.1 S7-400 Racks

سیستم S7-400 برای ساختارهای مختلف دارای سه نوع رک برای جایگذاری ماژول‌ها می‌باشد.

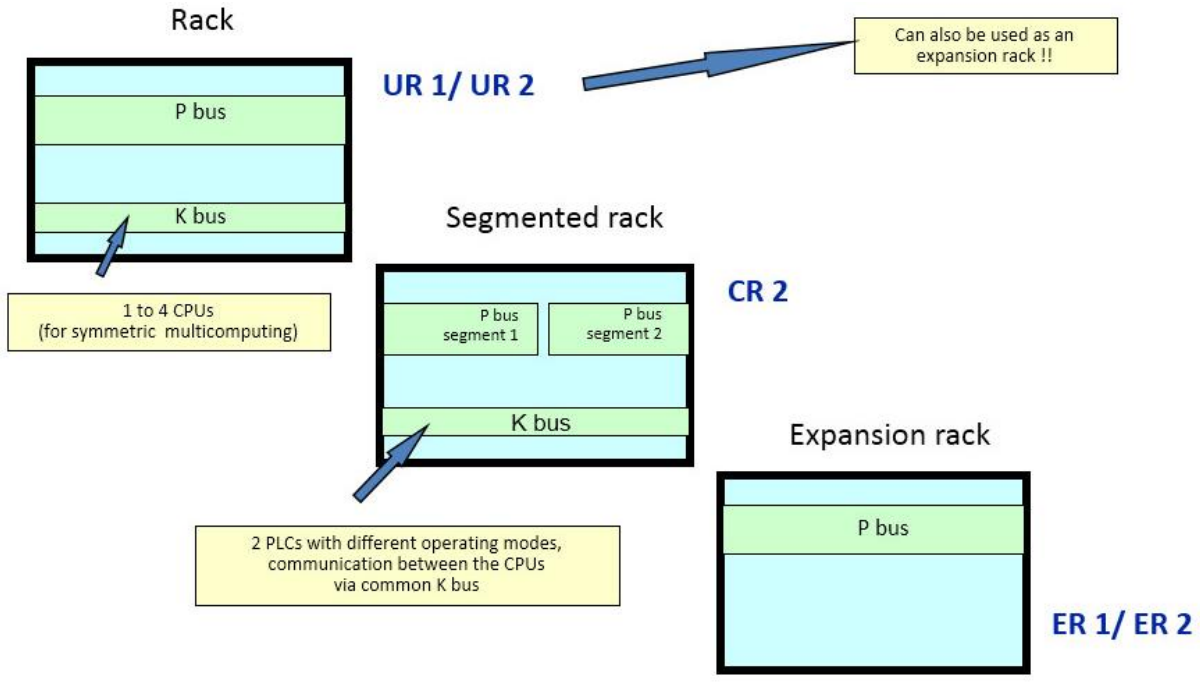
- CR: Central Rack
- ER: Expansion Rack
- UR: Universal Rack

- رک CR، به‌عنوان رک سیستمی (Main Rack) تنها برای نصب CPU و ماژول‌های شبکه استفاده می‌شود و بایستی به‌عنوان اولین رک نصب شود. این نوع رک در پیکربندی چندلایه (Multi tire) به‌عنوان رک Expansion نمی‌تواند مورداستفاده قرار گیرد. رک CR دارای هر دو باس P و C می‌باشد.
- رک ER فقط به‌عنوان رک Expansion جهت نصب ماژول‌های I/O استفاده می‌شود و تنها دارای باس یا گذرگاه P می‌باشد.
- رک UR به‌عنوان رک سیستمی و رک Expansion استفاده می‌شود. رک UR دارای هر دو باس P و C می‌باشد. لذا کلیه ماژول‌های I/O، CP و FM بر روی این رک قابل‌نصب می‌باشد.

- UR2: Universal rack, 9 slots, not suitable for redundant Power Supply Modules

- UR2: Universal rack, 9 slots
- UR2ALU: Universal aluminum rack, 9 slots
- UR1: Universal rack, 18 slots, not suitable for redundant power supply modules
- UR1: Universal rack, 18 slots
- UR1ALU: Aluminum universal rack, 18 slots
- UR2-H: Central rack, 2*9 slots, split backplane bus, suitable for compact configuration of standard and redundant PLCs
- UR1ALU: Central aluminum rack, 2*9 slots, split backplane bus, suitable for compact configuration of standard and redundant PLCs

معمولاً برای سیستم‌های H از رک‌های UR2H استفاده می‌شود. رک UR2-H امکان نصب دو زیرسیستم S7400H را به‌صورت ریداندانت با ۹ اسلات پشتیبانی می‌کند که برای نصب در کابینت ۱۹ اینچی مناسب است. توجه شود که سیستم S7-400H را می‌توان با دو رک جداگانه UR1 و UR2 نیز پیکربندی کرد.



شکل ۴- ۴: انواع رک در S7-400

4.3.2.2 S7-400 Rack buses

بر روی رک‌های S7-400 دو نوع باس (P & C) وجود دارد:

- گذرگاه P-bus یا IO Bus: این باس تبادل داده بین CPU و ماژول‌های I/O را بر عهده دارد.

در IM153-2 HF هر دو DP Master فعال بوده و به‌درستی عمل می‌کنند؛ و عملیات I/O به شرح زیر صورت می‌گیرد:

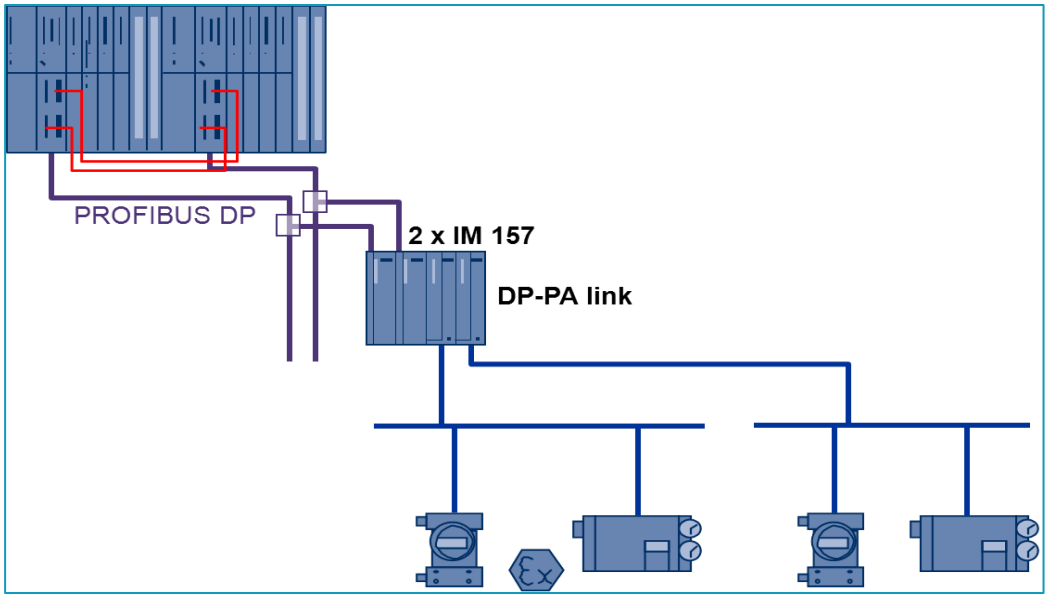
- **قرائت ورودی (Reading inputs):** ورودی‌ها تنها از کانال IM فعال خوانده می‌شوند.

نوشتن خروجی‌ها (Writing outputs): داده توسط هر دو کانال دریافت می‌شود ولی تنها از کانال IM فعال به خروجی‌ها ارسال می‌شود.

4.6.7 Profibus PA Connection to H System

در سیستم‌های S7 سیگنال‌های I/O بر روی باس Profibus PA نمی‌توانند مستقیم به CPU متصل شنود. لذا اتصال به اجزای این باس از طریق باس DP صورت می‌گیرد. برای این کار از ماژول واسط IM 157 (DP-PA Link) استفاده می‌شود.

- IM 157: 6ES7 157-0AA82-0XA0
- Bus module BM IM 157: 6ES7 195-7HD80-0XA0

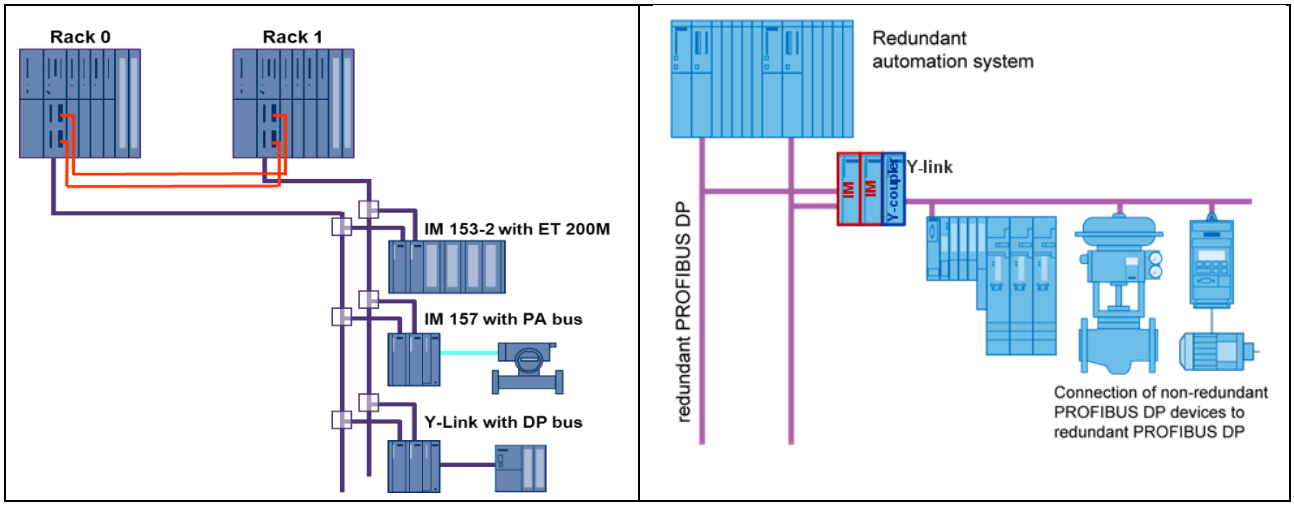


شکل ۴-۳۲: اتصال PROFIBUS PA از طریق یک لینک PA به سیستم H

4.6.8 Y-Link

کار این ماژول همانند DP-PA Link می‌باشد. ماژول Y-Link زمانی استفاده می‌شود که بخواهیم یک شبکه DP غیر ریداندانت (تک کانال) را به یک شبکه پروفی‌باس ریداندانت (دو کانال) متصل کنیم.

- Y-Link: 6ES7 197-1LB00-0XA0
- Bus module BM Y-Link: 6ES7 654-7HY00-0XA0



شکل ٤-٣٣: اتصال شبکه DP تکی به یک شبکه DP ریداندانت از طریق واسط Y-Link

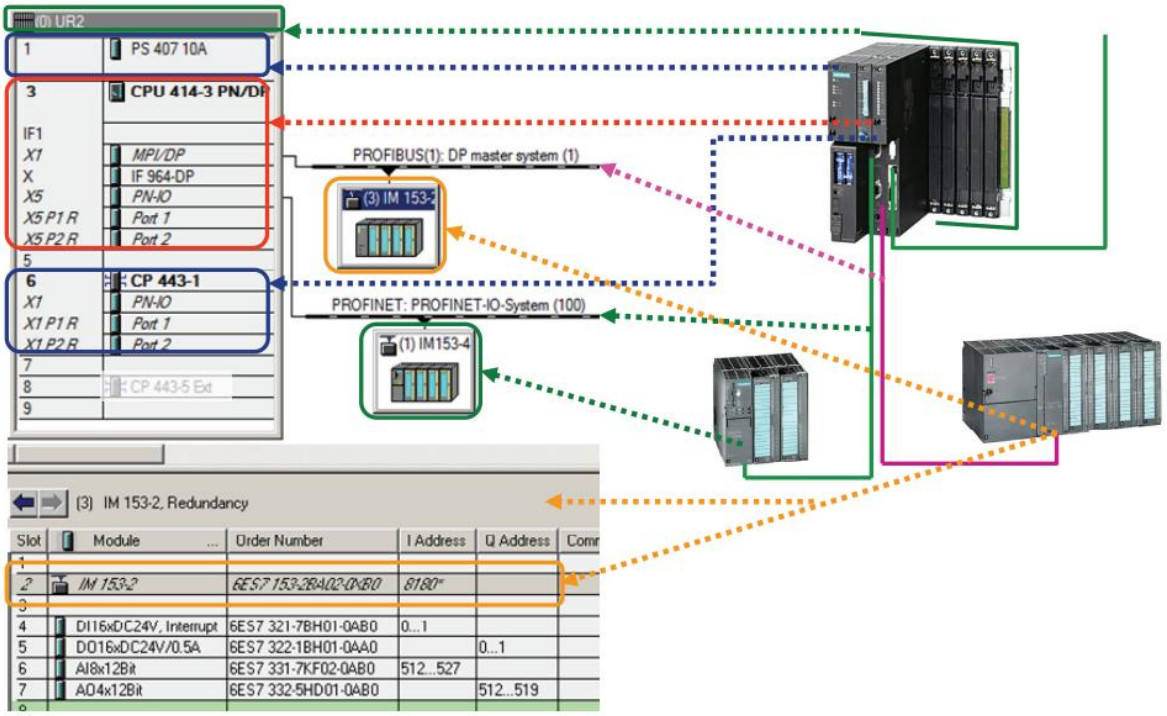
4.7 References

[1] Siemens Manuals

فصل پنجم

پیکربندی سیستم کنترل

S7-400FH



S7-400-FH Automation Stations Configuration

Chapter 5

5 S7-400FH hardware Configuration

5.1 Learning targets

محتوای این فصل شامل مباحث زیر می‌باشد:

- تعریف و ایجاد یک پروژه مبتنی بر سیستم 400FH
- پیکربندی سخت‌افزار سیستم 400FH
- زیرسیستم I/O در S7-400FH
- پیکربندی و تنظیم پارامترهای I/O

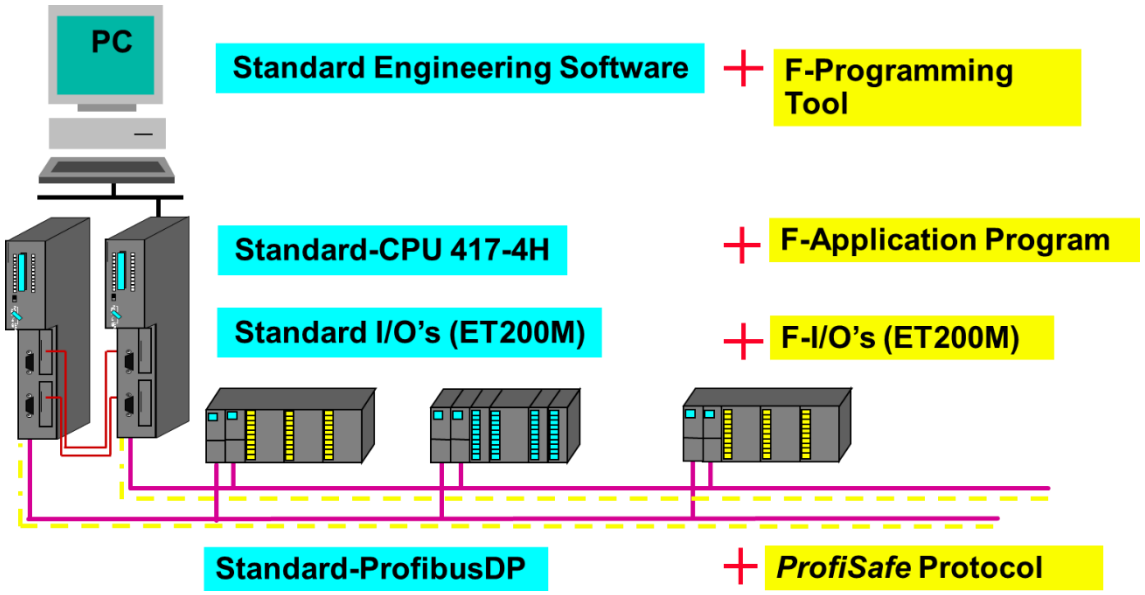
5.2 Abbreviations

AS	Automation Station or Automation System
OS	Operator Station
SIL	Safety Integrity Level
PCS	Process control System
FH	Fail-Safe & High Available
PCS	Process Control System
SIF	Safety Instrumented Function
RIO	Remote I/O

5.3 S7-400 FH System Structure / Modularity

یک سیستم کنترل 400FH یک سیستم ترکیبی می‌باشد. که با استفاده از آن می‌توان هم‌زمان لاجیک استاندارد یعنی حلقه‌های کنترل فیدبک (DCS/PCS) و لاجیک Fail-Safe (SIF) یعنی حلقه‌های تامین ایمنی موسوم به SIF را محقق کرد. لذا سخت‌افزار یک کنترل‌کننده S7-400H در دو نقش DCS و ESD می‌تواند بکار گرفته شود. به‌عبارت‌دیگر سیستم اتوماسیون 400FH ترکیبی از یک سیستم تحمل‌پذیر خرابی (H) و یک سیستم ایمن در خرابی (Fail-Safe) می‌باشد. معماری S7-400FH، در دسترس‌پذیری بالا و فن‌آوری ایمنی را در یک سیستم اتوماسیون واحد ترکیب می‌کند. به‌طوری‌که با حفظ ایمنی در برابر خرابی‌ها تحمل‌پذیر است. در این نوع سیستم ارتباط داده بین CPU و ماژول‌های I/O بر اساس پروتکل PROFIsafe صورت می‌گیرد. این به این معنی است که امکان ایجاد یک سیستم کنترل کاملاً یکپارچه برای یک پلنت وجود دارد. به‌طوری‌که هر دو برنامه H و F را می‌توان با استفاده از یک ابزار استاندارد یکسان، پیکربندی و برنامه‌نویسی کرد. سیستم S7-400F/FH الزامات ایمنی زیر را برآورده می‌کند:

- Safety Requirement Class: SIL 1 to SIL 3 acc. to IEC 61508
- Category: 2 to 4 acc. to EN 954-1
- Requirement Class: AK 1 to AK 6 acc. to DIN V 19250/DIN V VDE 0801



شکل ۵-۱- ساختار ماژولار سیستم ترکیبی S7-400FH

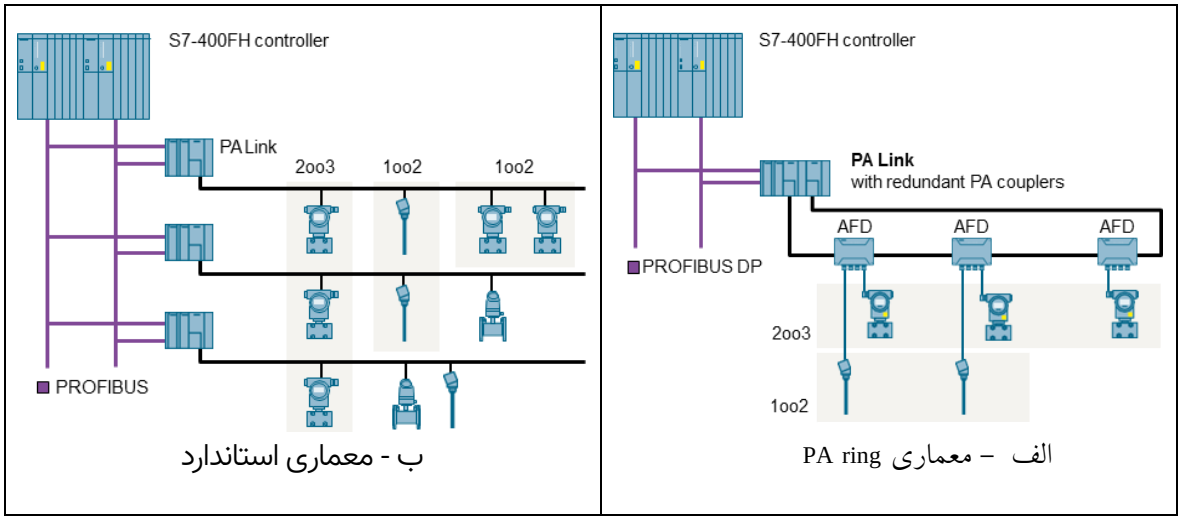
5.4 S7-400F/FH Main Components

یک سیستم S7-400 FH شامل سه مؤلفه اصلی زیر می‌باشد:

- MTBF of a central processing unit: 15 years
- MTBF of an I/O module: 50 years

5.6.8 Direct device interfacing via fieldbus with high safety and availability

شکل ۵-۴۲ روش‌های پیکربندی مختلف PROFIBUS PA در کاربردهای FH را نشان می‌دهد. شکل الف - روش اتصال استاندارد و شکل ب- روش استفاده از روترهای ریداندانت (Redundant routers) با یک توپولوژی حلقه را نشان می‌دهد. این روش پیاده‌سازی کاربردهای safety-related و fault-tolerant را نسبت به معماری استاندارد قبلی ارزان‌تر می‌کنند.



شکل ۵-۴۲- معماری پیکربندی‌های Profibus PA

شبکه PROFIBUS PA با توپولوژی حلقه از طریق روتر PA Link به دو سیگمنت ریداندانت profibus یک کنترل‌کننده S7-400FH متصل می‌شود. وسایل AFD4، AFD8 و AFDiS (active field distributor) می‌توانند حداکثر ۳۱ دستگاه را در حلقه PROFIBUS PA متصل کنند.

برای اطلاعات بیشتر در خصوص سیم‌بندی کانال‌های I/O در سیستم S7-400H به سند زیر مراجعه شود.

SIMATIC Fault-tolerant systems S7-400H, system manual, S7_400_h_en_en-US.pdf, 2014 version

Chapter 13.4.1 Signal modules for redundancy

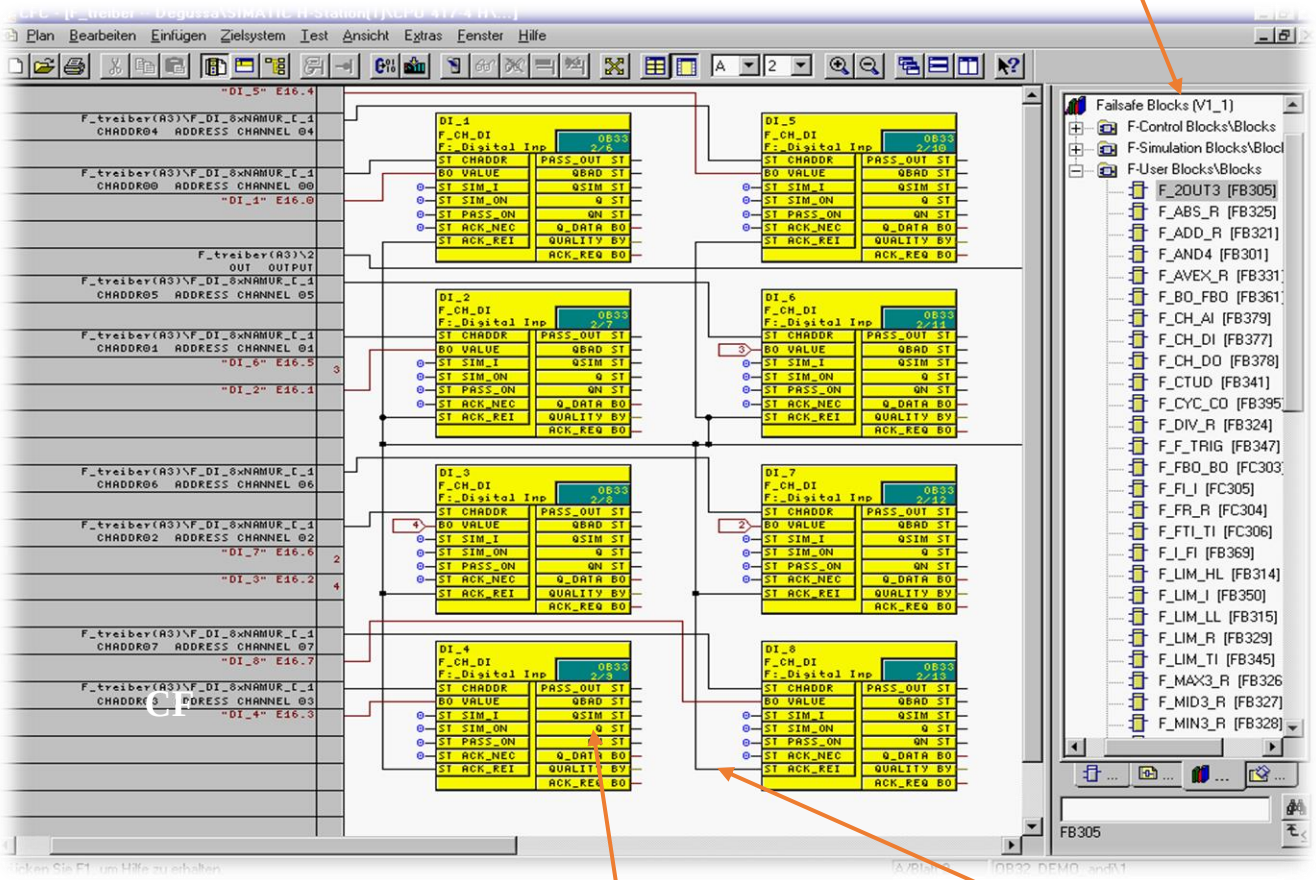
5.7 References

[1] Configuration of Redundant I/O Modules in PCS 7, Application description 10/2013

فصل ششم

برنامه نویسی با کتابخانه

F System



Implementing User Program with F-System library

Chapter 6

6 Implementing User Program with F-System library

Learning Targets

محتوای این فصل شامل مباحث زیر هست.

- بسته نرم‌افزاری F-System
- ساختار برنامه F در سیستم S7-400 FH
- کار با کتابخانه بلاک‌های پیاده‌سازی برنامه F
- کامپایل و دانلود برنامه F
- مفاهیم F-Runtime و F-Shutdown
- Passivation و Regeneration در کارت‌های F

Abbreviations

AS	Automation Station or Automation System
OS	Operator Station
ES	Engineering Station
PCS	Process Control System
FH	Fail-Safe & High Available
SDW	Safety Data Write
MOS	Maintenance Override Switch
RIO	Remote I/O
F	Fail-Safe
HMI	Human Machine Interface
SIF	Safety Instrumented Function
SIS	Safety Instrumented Systems
CH	Channel
AI	Analog Input
DI	Digital Input

6.1 F Systems Software Overviw

برای پیاده‌سازی برنامه F با PLCهای سیماتیک(S7)، دو بسته نرم‌افزاری ارائه‌شده است. که عبارت‌انداز:

- بسته Distributed Safety برای اتوماسیون کارخانه مبتنی بر ماژول‌های CPU سری 300F و 400F؛
- بسته S7 F System برای اتوماسیون فرآیند مبتنی بر ماژول‌های CPU سری S7-400H؛

6.1.1 Installing the S7-F Systems Package

برای پیاده‌سازی یک برنامه F برای حوزه کنترل فرآیند مبتنی بر S7-400-FH بایستی بسته نرم‌افزار F System بر روی کامپیوتر مهندسی (ES) نصب گردد. آخرین ویرایش بسته نرم‌افزار F-System . تا سال ۲۰۱۹ نسخه 6.2 می‌باشد. این بسته شامل برنامه‌های زیر می‌باشد:

- S7 F Systems (V6.2 Upd1 last version
- S7 F Configuration Pack (V5.5 SP13)
- S7 F Systems Lib V1_3 (SP2)

Prerequisite

پیش‌نیاز بسته F برای نصب در سیستم مهندسی شامل موارد زیر می‌باشد.

- On the ES
  - STEP 7 V5.5 SP3 or higher
  - CFC V8.0 SP4 or higher
  - Optional: PCS 7 V8.0 SP2 or higher
- On the OS (for S7 F Systems HMI)
  - PCS 7 V8.0 SP2 or higher
  - For off-Line testing
  - S7 PLCSIM V5.4 or higher

F system, HMI Package

درصورتی‌که در پروژه از امکان SDW یا MOS استفاده می‌شود، بایستی بسته S7 F Systems HMI V6.1 SP1 و بسته Safety Matrix Viewer V6.2 SP1 روی کامپیوتر OS نصب شود. قابلیت SDW و MOS امکان تغییر یک متغیر F و پارامترهای F-CPU را در مد Safety از سیستم OS فراهم می‌کند.

- SDW: Safety Data Write
- MOS: Maintenance Override Switch

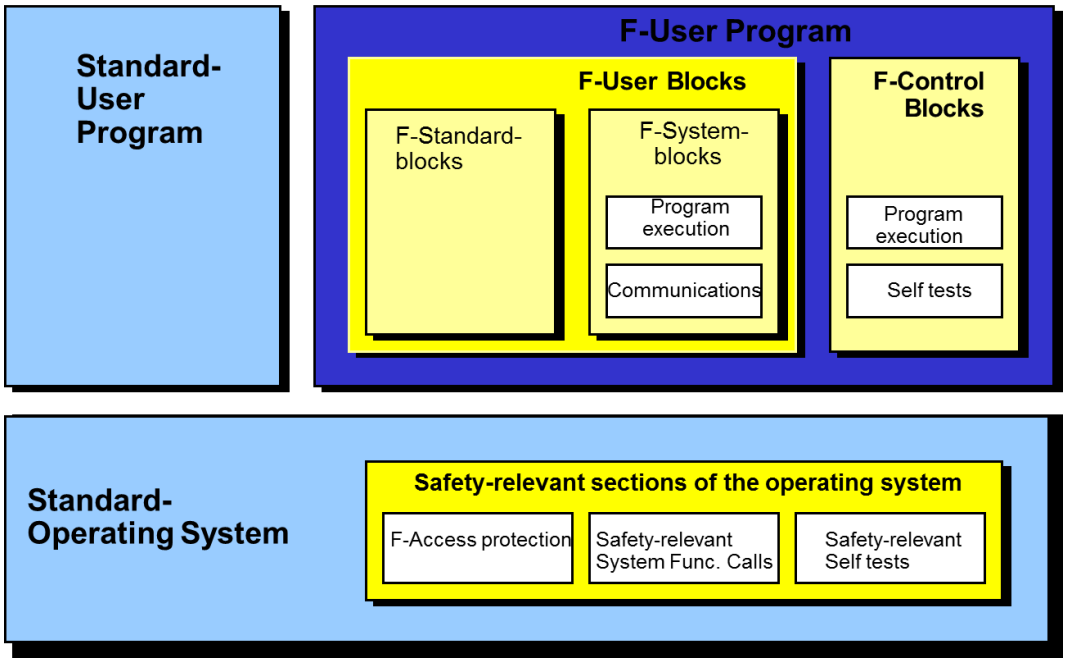
6.2 S7-400FH Program Structure

6.2.1 CPU-Software Architecture

مطابق شکل ۶-۱ یک سیستم S7-400 FH قادر به اجرای هم‌زمان هر دو لاجیک F و استاندارد می‌باشد. لذا یک برنامه S7 در سیستم‌های FH متشکل از دو نوع لاجیک می‌باشد:

- لاجیک نوشته‌شده با بلاک‌های استاندارد؛
- لاجیک متشکل از توابع کتابخانه F-System؛

به‌عبارت‌دیگر یک برنامه در کنترل‌کننده S7-400FH متشکل از بلاک‌های FC و FB می‌باشد. که با استفاده از بلاک‌های کتابخانه F-System و بلاک‌های استاندارد به‌صورت کاملاً یکپارچه ایجاد می‌شوند. بلاک‌های F در گروه‌های اجرایی (Runtime Groups) جدا از بلاک‌های استاندارد پیکربندی و اجرا می‌شوند. بین بخش F و بخش استاندارد برنامه S7 یک روش تبادل داده ایمن وجود دارد. همچنین برای انتقال داده بین بخش استاندارد و برنامه F از بلاک‌های تبدیل (Convert) کتابخانه F استفاده می‌شود.



شکل ۶-۱- ساختار یک برنامه مبتنی بر S7-400 FH

در یک سیستم S7-400 FH پیاده‌سازی لاجیک حلقه‌های SIF تنها از طریق برنامه‌نویسی با بلاک‌های کتابخانه F-System در ویرایشگر CFC انجام می‌شود. به این صورت که برای نوشتن یک برنامه F ابتدا کاربر از کتابخانه F-System بلاک‌ها را انتخاب و آن‌ها را در داخل یک چارت

CFC درج می‌کند. سپس با اتصال بلاک‌های F به همدیگر منطق برنامه F پیاده‌سازی می‌شود. علاوه بر توابع F، کتابخانه F شامل توابعی برای تشخیص و واکنش به خطاها هستند. این توابع تشخیص فالت (Diagnostics)، تضمین می‌کنند که خرابی‌ها (Failures) و خطاها شناسایی‌شده و برای هدایت پلنت به یک وضعیت ایمن، واکنش مناسب را تریگر می‌کنند. توابع خاص تشخیص و واکنش به خطاها در طول کامپایل در داخل چارت‌های سیستمی با پیشوند @ به‌طور خودکار درج و به برنامه F اضافه می‌شوند.

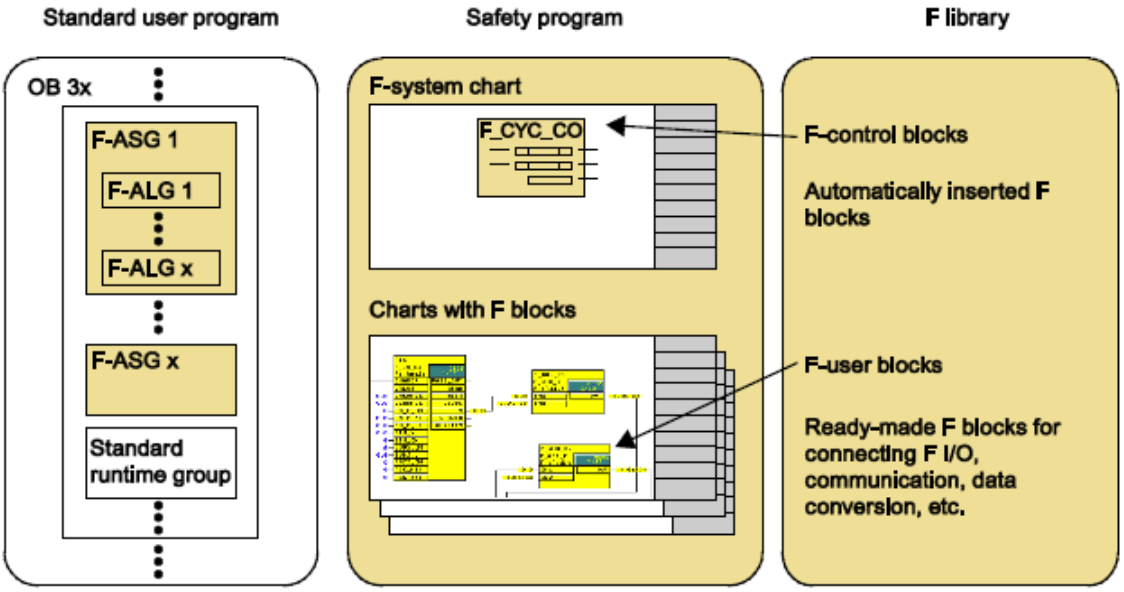
6.2.2 Safety Program Execution Structure

یک برنامه مبتنی بر S7-400 FH بایستی در چارت‌های CFC برنامه‌نویسی شود. این برنامه ممکن است شامل هر دو لاجیک استاندارد و F باشد. که در چارت‌های CFC جداگانه برنامه‌نویسی و اجرا می‌شود. به‌طوری‌که از دید سیستم اجرایی S7 در دو گروه اجرای (Runtime Group) جداگانه اجرا می‌شود. شکل ۶-۲ ساختار اجرایی یک برنامه S7-400 FH متشکل از چارت‌های استاندارد و F را به تصویر کشیده است.

نکته:: از دید سیستم اجرایی S7 یک چارت CFC در زمان اجرا به‌عنوان یک گروه پردازش در CPU تلقی می‌شود. لذا با درج هر چارت CFC در برنامه یک Runtime Group ایجاد می‌شود. بنابراین در زمان اجرا دو دسته گروه اجرا در CPU وجود خواهد داشت.

- Standard Runtime Groups
- F-Runtime Groups

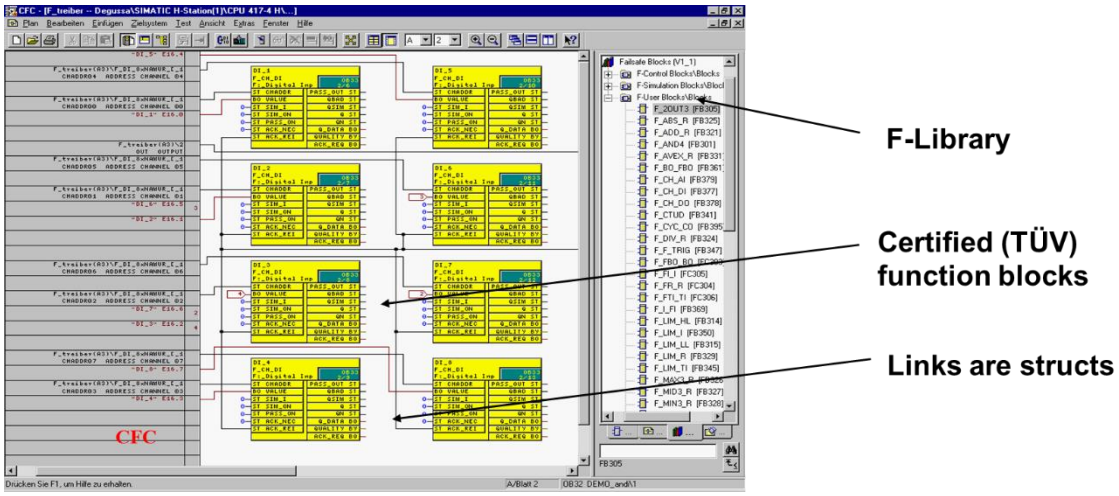
گروه‌های استاندارد شامل بلاک‌های درج‌شده از کتابخانه‌های استاندارد و گروه‌های F حاوی بلاک‌های درج‌شده از کتابخانه F-System می‌باشد.



شکل ۶-۲- دیاگرام معماری اجرای یک برنامه ایمنی در S7-400FH

6.3 Implementing Fail-Safe Program with F-System Library

6.3.1 Programming: Graphical programming CFC acc. to IEC 1131

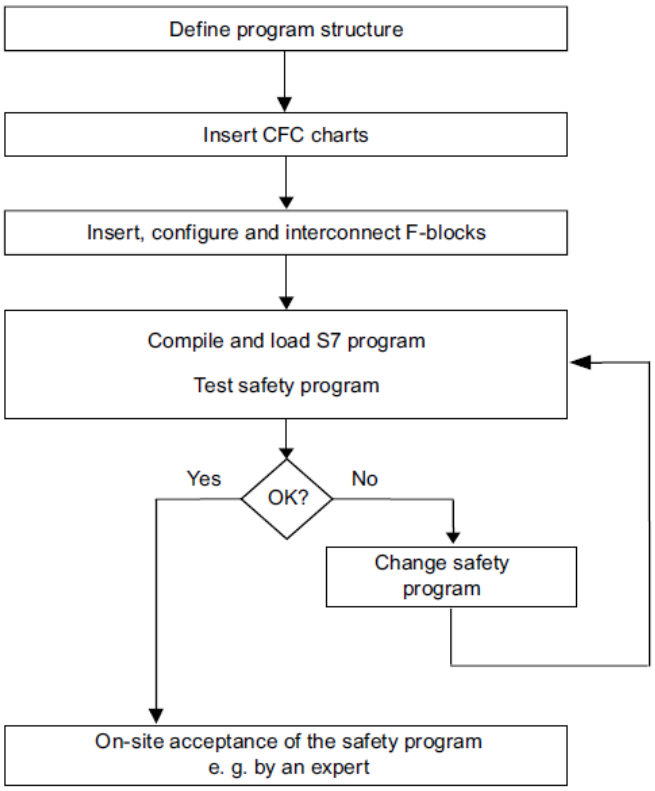


پس از اتمام پیکربندی سخت‌افزار یک سیستم S7-400H، گام بعدی برنامه‌نویسی لاجیک در محیط ویرایشگر CFC می‌باشد. یادآوری می‌شود که پیاده‌سازی یک سیستم کنترل S7-400FH شامل مراحل زیر می‌باشد:

- نصب نرم‌افزار PCS7 در یک سیستم کامپیوتری (EWS)؛
- نصب بسته نرم‌افزار S7-F Systems ؛
- ایجاد یک پروژه Single یا MultiProject (استفاده از ویزارد PCS7 پیشنهاد می‌شود)؛
- ویرایش و پیکربندی سخت‌افزار در محیط HWConfig؛

- ایجاد پوشه‌های ساختار سلسله‌مراتبی پلنت در پنجره Plant View؛
- پیاده‌سازی لاجیک در چارت‌های CFC با استفاده از کتابخانه F-System؛
- کامپایل، آزمون و عیب‌یابی و دانلود برنامه به CPU؛

در فصل قبل پیکربندی سخت‌افزار یک سیستم S7-400FH به‌طور کامل تشریح شد. در ادامه در این فصل پیاده‌سازی لاجیک F و نحوه کار با بلاک‌های کتابخانه F-System تشریح می‌شود. شکل ۶-۳ یک فرآیند پایه برای ایجاد یک برنامه FH را به تصویر کشیده است.



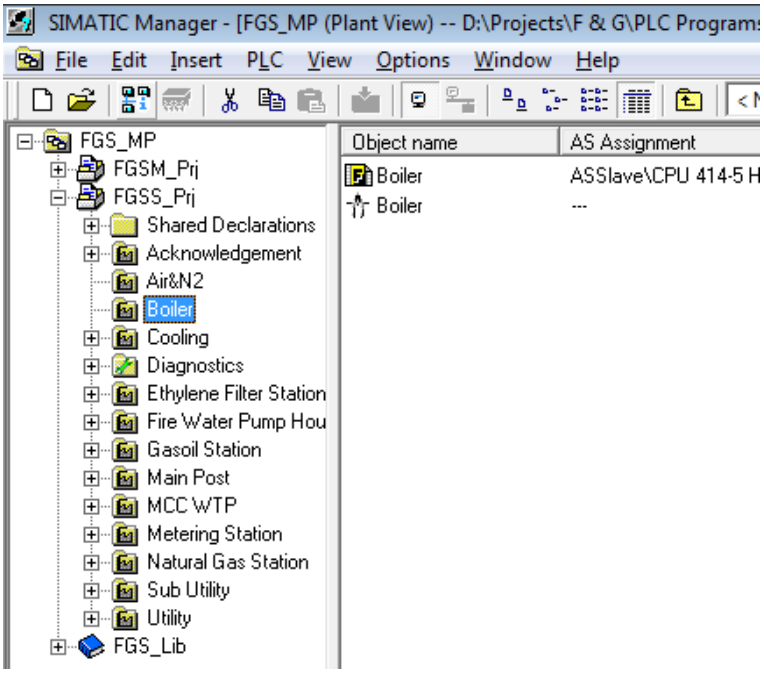
شکل ۶-۳- فرآیند پایه برای ایجاد برنامه FH

6.3.2 Create Plant Hierarchy

درصورتی‌که بخواهیم برنامه‌نویسی را به سبک PCS7 اجرا کنیم. ابتدا ساختار سلسله‌مراتبی پلنت را در پنجره Plant View در قالب پوشه‌های مختلف پیاده‌سازی می‌کنیم. شکل ۶-۴ یک ساختار نمونه پیاده‌سازی شده در یک پروژه F&G مبتنی بر سیستم FH رانشان می‌دهد.

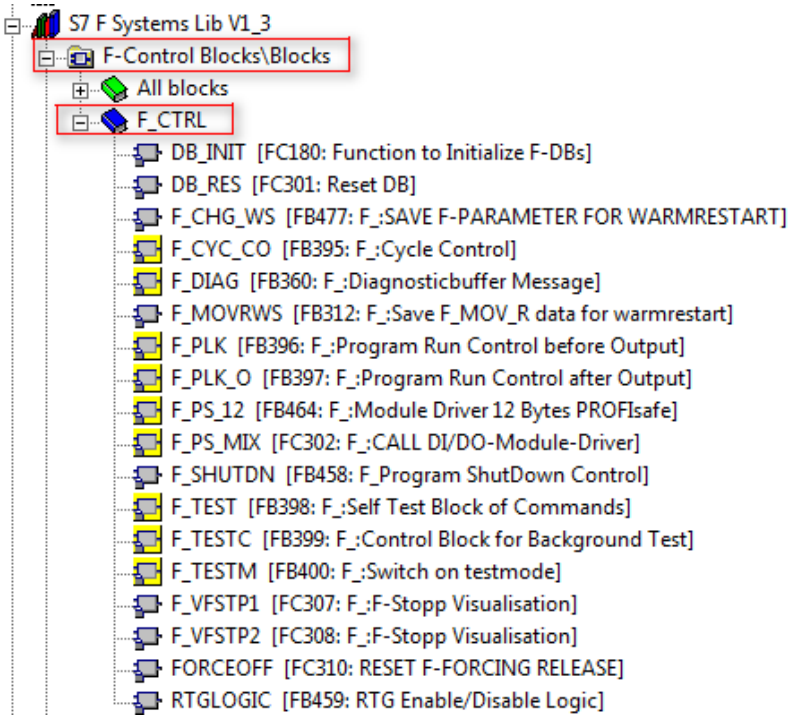
پس از ایجاد ساختار سلسه مراتبی پلنت، برای پیاده‌سازی لاجیک بایستی ابتدا بر اساس طرح لاجیک پلنت، چارت‌های CFC را در داخل پوشه‌های مختلف درج و سپس با استفاده از

بلاک‌های کتابخانه F منطق موردنظر را پیاده‌سازی می‌کنیم. یادآوری می‌شود که پس از درج یک بلاک F در یک چارت CFC، به یک چارت F تبدیل‌شده و آیکون ظاهری آن تغییر می‌کند.

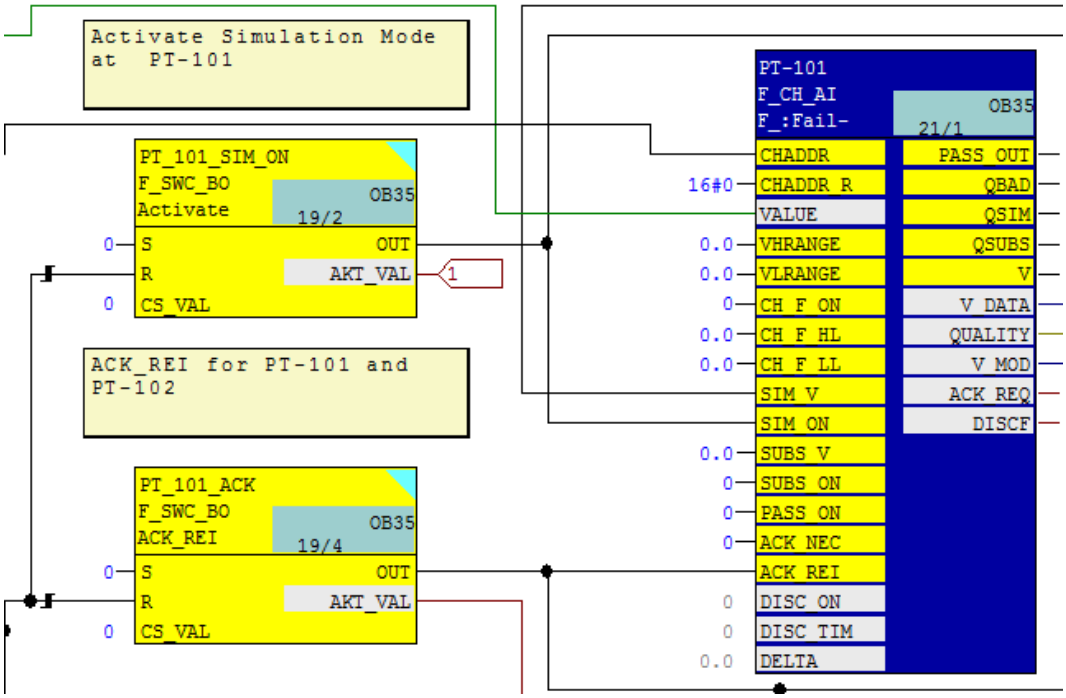


شکل ۶-۴- نمونه ساختار سلسله‌مراتبی پوشه‌های فرآیندی

6.4 F System Library

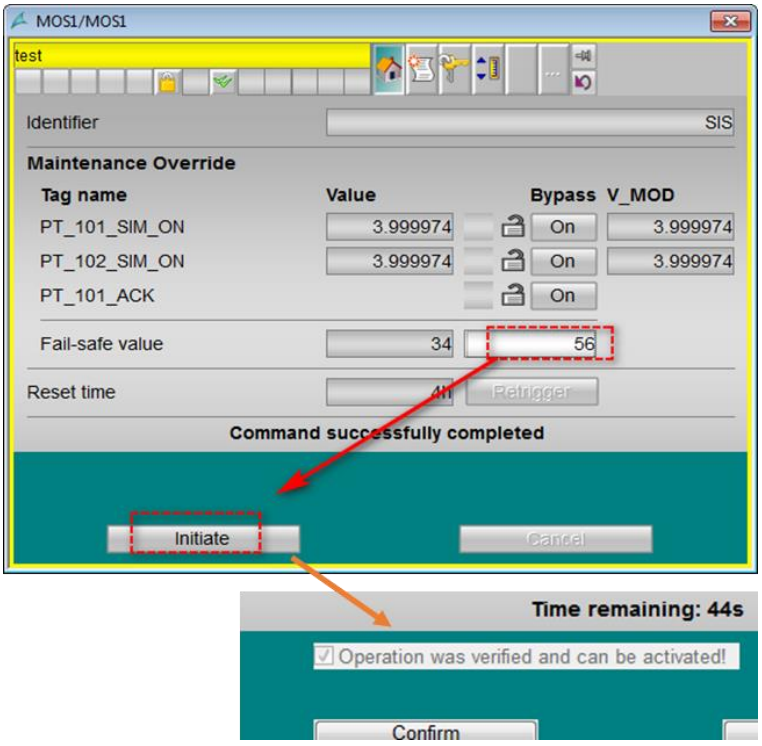


شکل ۶-۵- بلاک‌های سیستمی کتابخانه F-System



شکل ۶-۸۱- استفاده از بلاک‌های F_SWC_BO برای فعال‌سازی شبیه‌سازی در بلاک درایور F_CH_AI

برای اعمال بای‌پس، مطابق شکل مقدار بای‌پس را در کارد Fail-safe value وارد کرده و Enter می‌کنیم. با این کار دکمه Initiate فعال می‌شود.



شکل ۶-۸۲- پنجره faceplate بلاک SWC_MOS پیکربندی شده برای مثال

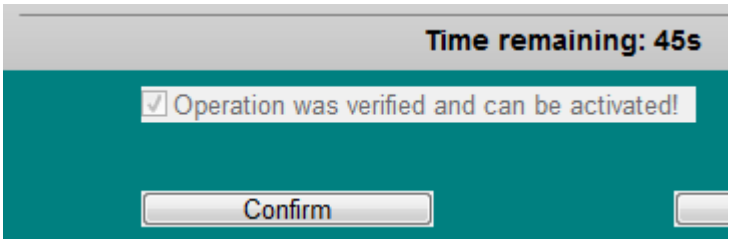
حداکثر مدت زمان فعال‌سازی برای سه مقدار BOOL با استفاده از قالب SWC_TR کتابخانه F System محدود می‌شود. پس از قرار دادن این قالب در چارت و اتصال خروجی AKT_TR به ورودی AKT_TR بلاک SWC_MOS، اتصالات دیگر این قالب به طور خودکار در هنگام کامپایل چارت برقرار می‌شود.

پس از سپری شدن این مدت زمان، عمل بای‌پس به صورت خودکار غیرفعال می‌شود. در طول این مدت زمان (به عنوان مثال یک ساعت) می‌توان از طریق گزینه reintegrate در faceplate عمل بای‌پس را غیرفعال کرد.

Transaction for MOS

در صورتی که توالی خاصی از عملیات را در سیستم OS در مدت زمانی مشخص انجام دهید، از MOS می‌توانید برای تغییر یک پارامتر F در برنامه ایمنی یک F-CPU استفاده کنید. کل عملیات تغییر به عنوان یک «تراکنش» شناخته می‌شود.

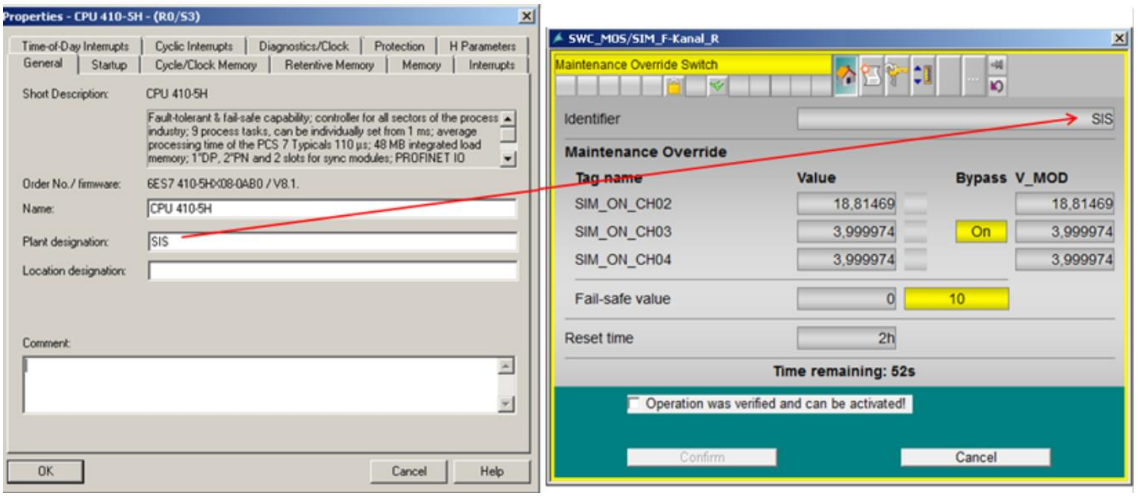
به عنوان مثال پس از اجرای فرمان Initiate در faceplate، شصت ثانیه فرصت هست که تراکنش تایید شود.



Operator types for MOS

تراکنش فقط می‌تواند توسط یک اپراتور که عملیات (initiate,checks, confirm) تغییر را اجرا می‌کند، انجام شود. با این حال، یک تراکنش توسط دو اپراتور نیز قابل انجام است. اولین اپراتور عمل تغییر (initiator) را آغاز می‌کند و دومی (confirmer) عمل ورود مقدا و تأیید را انجام می‌دهد.

مجوزهای مربوط به اپراتور در ویژگی‌های Faceplate تنظیم می‌شود. برخلاف SDW، شناسه اتصال بین بلاک و Faceplate، به طور خودکار توسط سیستم تولید می‌شود. در این فرآیند، سیستم از ویژگی"CPU Plant Designation" یا ورودی "IDENT" از بلاک "F_SWC_P" استفاده می کند. در صورتی‌که در پنجره پراپرتی CPU در HW Config ویژگی"CPU Plant Designation" تنظیم شود، نیازی به تعریف مقدار در ورودی "IDENT" در بلاک "F_SWC_P" نیست.



شکل ۶-۸۳- تنظیم ویژگی"CPU Plant Designation" پنجره پراپرتی CPU در HW Config

برای اطلاعات بیشتر در این خصوص به مراجع زیر مراجعه شود:

[1] Industrial software S7 F/FH Systems - Configuring and Programming, Programming and Operating Manual, 06/2016

[2] Process Control System PCS 7 Compendium Part B -Process Safety (V8.1)

6.15 References

[1] Automation System S7-400H Fault-tolerant Systems

[2] Configuring Hardware and Communication Connections with STEP 7

[3] Fault-tolerant Systems S7-400H

[4] S7 Distributed Safety Configuring and Programming

[5] Industrial software S7 F/FH Systems - Configuring and Programming

[6] Industrial Software S7 Distributed Safety – configuring and programming - Programming and Operating Manual

[7] Industrial Software Safety Engineering in SIMATIC S7

[8] Safety Engineering in SIMATIC S7

فصل هفتم
سیم‌بندی و معماری‌های ارزیابی ایمنی
ورودی‌های آنالوگ

Wiring and Voting Architectures for failsafe Analog Input Modules (F AI) of the ET 200M

SIMATIC Safety Integrated for process automation

Chapter 7

7 Wiring and Voting Architectures for Failsafe Analog Input Modules (F-AI)

Learning targets

پس از مطالعه این فصل خواننده توانایی‌های زیر را کسب خواهد کرد.

- اتصالات مختلف کانال‌های ورودی آنالوگ برای دستیابی به یک سطح SIL
- پیاده‌سازی معماری‌های Fail-Safe در ماژول‌های S7-300 F AI

Abbreviations

AS	Automation Station or Automation System
OS	Operator Station
PCS	Process Control System
FH	Fail-Safe & High Available
HART	Highway Addressable Remote Transducer Protocol
RIO	Remote I/O
F	Fail-Safe
MTA	Marshalled Termination Assemblies
PFD	of Probability of Failure on Demand (PFD)
CFC	Continuous Function Chart
DEST	Destination
ADD	Address
SIL	Safety Integrated Level
DI	Digital input
AI	Analog Input

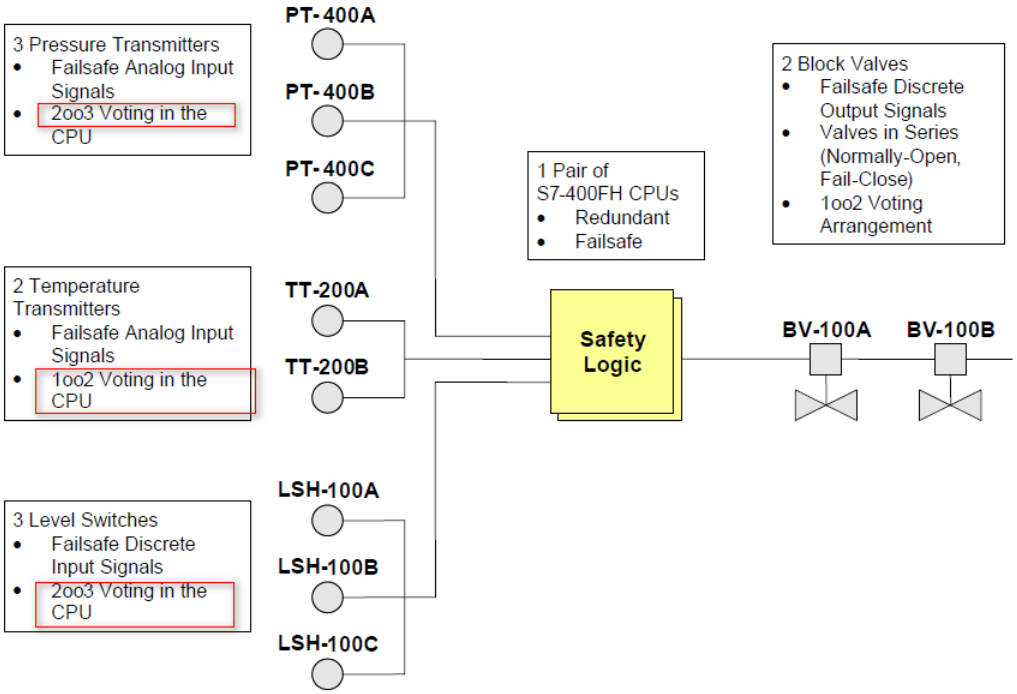
1. Automation functions

1.1 Abstract

در سیستم‌های کنترل با مشخصه تحمل‌پذیرخرابی (Fault-tolerant) برای رسیدن به هدف دسترس‌پذیری (Availability) بالا و همچنین در سیستم‌های کنترل Fail-safe جهت بالا بردن میزان درجه ایمنی SIL معماری‌های اتصال سیم‌بندی مختلفی را برای دستگاه‌های ورودی/خروجی و همچنین سیگنال‌های ورودی/خروجی دیجتال و آنالوگ در سیستم کنترل می‌توان پیاده‌سازی کرد.

در این فصل معماری‌های ارزیابی Fail-Safe برای سیگنال‌های آنالوگ ورودی و نحوه ارتباط سیگنال‌ها در یک حلقه SIF توصیف می‌شود.

برای مثال فرض کنید که برای رسیدن به یک سطح ایمنی در یک پلنت بایستی چند سیگنال آنالوگ مانیتور شود. بسته به سطح SIL موردنیاز در حلقه‌های ایمنی (SIF)، چندین معماری برای سیم‌بندی و ارزیابی سیگنال‌های ورودی آنالوگ وجود دارد. شکل ۷-۱ یک نمونه پیکربندی از ارزیابی Failsafe حلقه‌های SIF را به تصویر کشیده است. در این پیکربندی بسته به مقادیر سیگنال‌های ورودی آنالوگ به شیرهای سولنوئید (BV-100A و BV-100B) فرمان تریپ صادر می‌شود. در این فصل اتصالات مختلف کانال‌های ورودی آنالوگ جهت ارزیابی معماری‌های Fail-safe در سیستم‌های سیماتیک با ماژول‌های S7-300 F I/O تشریح می‌گردد.

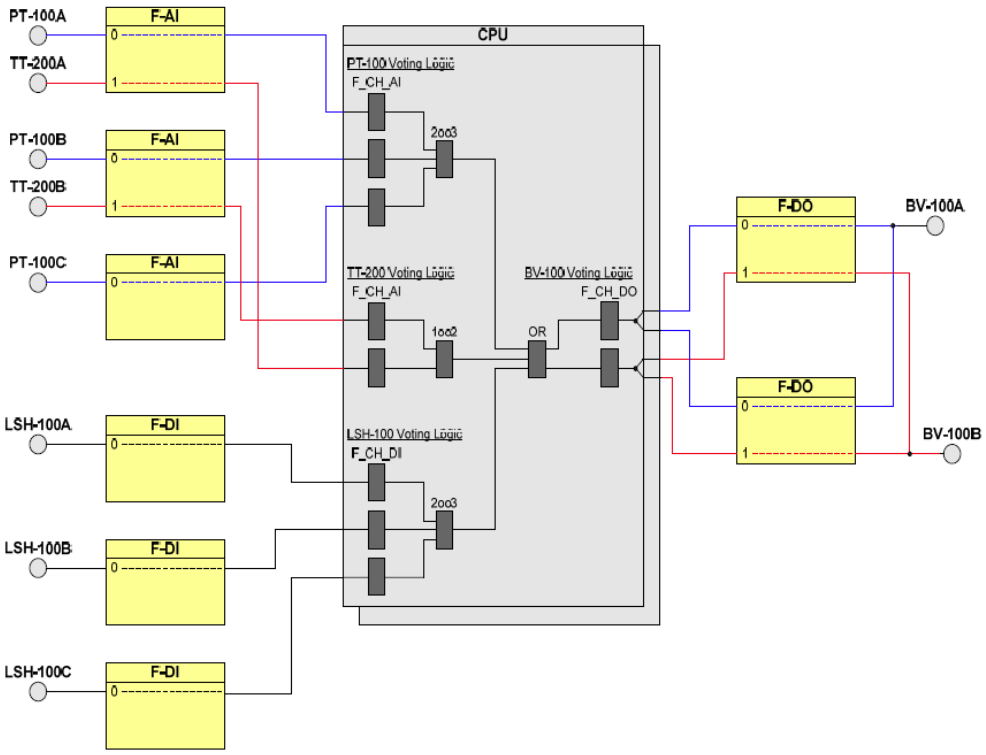


شکل ۷-۱ : یک مثال از سیم‌بندی و ارزیابی سیگنال‌ها در حلقه‌های SIF

برای ارزیابی سیگنال‌های F-AI چند معماری وجود دارد. که عبارت‌انداز:

- ارزیابی مقدار و وضعیت سیگنال و صدور رأی در داخل ماژول ورودی آنالوگ برای معماری 1oo2
- ارزیابی مقدار و وضعیت سیگنال و صدور رأی در برنامه لاجیک CFC (در ماژول CPU)
- ارزیابی و صدور رأی (Voting) در ماژول CPU برای معماری 2oo3

شکل ۷-۲پیاده‌سازی‌های احتمالی از اجرای Voting برای سناریو شکل ۷-۱ را در محیط CFC نشان می‌دهد. که در آن اتصالات سیگنال‌های آنالوگ و دیجیتال برای معماری‌های مختلف ارزیابی F استفاده‌شده است.



شکل ۷-۲ : پیاده‌سازی ساختارهای Voting در برنامه لاجیک

1.2 F-AI Architectures

معماری‌های پیشنهادشده برای ارزیابی سیگنال‌های ورودی آنالوگ در مثال کاربردی یادشده در بالا عبارت است از:

One sensor (1oo1)

معماری تک سنسور - کاربردهای معمول این معماری برای مواردی است که تنها با استفاده از یک سنسور، سطح SIL موردنیاز برآورده می‌شود. همچنین مشخصه دسترس‌پذیری بالا (Increased availability) موردنیاز نیست.

Two sensors (1oo2) evaluation in the F-AI

در این معماری، برای حصول عملکرد ایمنی موردنیاز، مقدار دو سنسور آنالوگ ورودی در داخل خود ماژول F-AI ارزیابی می‌گردد. کاربردهای معمول این معماری برای مواردی است که برای رسیدن به سطح SIL موردنظر، به ارزیابی مقدار دو سنسور AI نیاز می‌باشد. ولی به مشخصه دسترس‌پذیری بالا در کارت‌های AI نیازی نیست. دقت شود که در این

معماری از دو کانال کارت AI برای ارزیابی مقدار دو سنسور جهت حصول مقدار SIL موردنظر استفاده می‌شود. این موضوع با معماری که در آن جهت افزایش دسترس‌پذیری در سطح کارت‌های I/O، یک سنسور به دو کانال از دو کارت متصل می‌شود، متفاوت می‌باشد.

Two sensors (1oo2) evaluation in the user program

در این معماری، به جای رروش قبلی که ارزیابی در داخل خود کارت انجام می‌شود، برای حصول عملکرد/تابع ایمنی موردنیاز، مقادیر دو سنسور در داخل برنامه ارزیابی می‌شود. کاربردهای معمول این معماری برای مواقعی است که در آن برای رسیدن به SIL موردنیاز به دو سنسور نیاز بوده و نمایش مقدار هر دو سنسور در سیستم مانیتورینگ ضروری است. درصورتی‌که تنها یک سنسور واحد، سطح SIL موردنظر را برآورده کند، می‌توان برای افزایش دسترس‌پذیری، این معماری را به‌صورت 2oo2 نیز پیکربندی کرد.

Three sensors (2oo3) evaluation in the user program

در این معماری، برای حصول عملکرد/تابع ایمنی موردنیاز در یک واحد فرآیندی، نیاز است که مقدار سه سنسور (2oo3) در برنامه کاربر ارزیابی شود. کاربردهای معمول این معماری برای مواردی است که علاوه بر تأمین سطح SIL مطلوب با سه سنسور، مشخصه دسترس‌پذیری در کارت‌های F-AI نیز مدنظر است.

1.3 Properties of the failsafe analog input module

در سیستم S7-300 I/O دو نوع ماژول ورودی آنالوگ F وجود دارد که عبارت است از:

- SM 336F, AI 6x13Bit (6ES7 336-1HE00-0AB0)
- SM 336F, AI 6x0/4...20mA HART (6ES7 336-4GE00-0AB0)

نکته: در مثال‌های این فصل، ماژول ورودی آنالوگ F از نوع هارت در نظر گرفته‌شده است.

مشخصات ماژول‌های ورودی آنالوگ F به شرح زیر می‌باشد:

11.3 Protective & Clean earth

ارت تمیز و ارت کثیف- زمین حفاظتی که زمین کثیف (dirty earth) نیز نامیده می‌شود، به برق AC مربوط می‌شود و برای محافظت از کارکنان و تجهیزات استفاده می‌شود. زمین حفاظتی برای حفاظت از کارکنان در برابر شوک الکتریکی در زمان وقوع یک فالت در نظر گرفته‌شده است. همواره از لوازم الکتریکی از طریق هادی زمین یک اتصال به پایانه زمین اصلی در اتاق تأمین برق وجود دارد. به‌طوری‌که جریان ناشی از فالت از طریق این هادی به جرم زمین جاری خواهد شد.

در مدارک راهنمای کارت‌های سیماتیک زیمنس زمین Functional همان زمین Clean است. که به‌عنوان یک زمین مرجع برای سیگنال‌های دیجیتال و آنالوگ استفاده می‌شود. این زمین همچنین برای کاهش اعوجاج در سیگنال لازم است. زمین کاربردی (Functional Earth) برای مواردی چون کاهش نویز فرکانس رادیویی، فیلتر کامپیوتر به‌منظور افزایش وضوح سیگنال و یا دیگر تجهیزات که همواره جریان نشتی 10mA دارند، در نظر گرفته‌شده است. زمین کاربردی باید از زمین حفاظت به‌جز در نقطه زمین اتصال پایانه اصلی جدا شوند.

شکل زیر دیاگرام مدار یک ماژول خروجی آنالوگ SM332 AO 8x16Bit را برای خروجی جریان نشان می‌دهد.

12. References

[1] Wiring and evaluation architectures for failsafe analog input modules (F-AI) of ET 200M, functional Example No AS-FE-II-001-V21-EN

[2]

فصل هشتم

معماری‌های سیم‌بندی و ارزیابی ورودی/خروجی‌های دیجیتال

Wiring and Evaluation Architectures for Failsafe Digital Input (F-DI) and Output Modules (F-DO)

SIMATIC Safety Integrated for process automation

Chapter 8

8 Evaluation Architectures for F-DI and F-DO

Learning targets

این فصل به تشریح موضوعات زیر می‌پردازد.

- سیم‌بندی‌های مختلف کانال‌های ورودی/خروجی دیجیتال در یک سیستم Failsafe
- پیاده‌سازی معماری‌های Fail-safe برای حلقه‌های SIF با ماژول‌های F-DIO

Abbreviations

AS	Automation Station or Automation System
OS	Operator Station
SIL	Safety Integrity Level
PCS	Process control System
FH	Fail-Safe & High Available
RIO	Remote I/O
HFT	Hardware fault tolerant
DC	Diagnostic coverage
SFF	Safe failure fraction
EUC	Equipment Under Control
FSK	Frequency-Shift-Keying
SIL	Safety Integrated Level
DI	Digital input
AI	Analog Input
MTA	Marshalled Termination Assemblies

1. Automation functions

1.1 Abstract

در سیستم‌های کنترل با مشخصه تحمل‌پذیر خرابی (Fault-tolerant) برای رسیدن به هدف دسترس‌پذیری (Availability) بالا و همچنین در سیستم‌های کنترل Fail-safe جهت بالا بردن میزان درجه ایمنی SIL، معماری‌های اتصال سیم‌بندی مختلفی را برای دستگاه‌های ورودی/خروجی و همچنین سیگنال‌های ورودی/خروجی دیجیتال و آنالوگ در سیستم کنترل می‌توان پیاده‌سازی کرد.

در این فصل معماری‌های ارزیابی Fail-Safe برای سیگنال‌های دیجیتال ورودی/خروجی و نحوه ارتباط سیگنال‌ها در یک حلقه SIF توصیف می‌شود.

نکته: در تمام بخش‌های این کتاب به‌جای عبارت Fail-Safe از حرف F استفاده‌شده است.

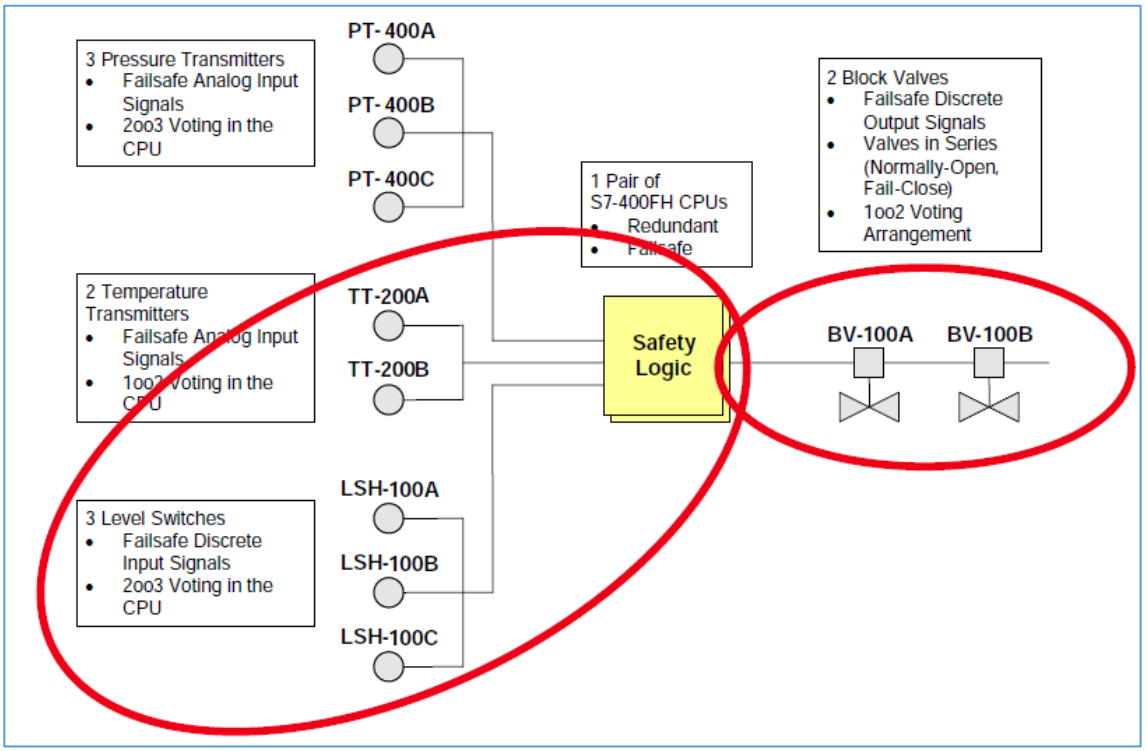
1.2 Functionality of the application example

1.2.1 Task

شکل ۸-۱ یک مثال از پیکربندی حلقه‌های SIF متشکل از سیگنال‌های آنالوگ و دیجیتال در یک پلنت را نشان می‌دهد. در این مثال چندین سیگنال ورودی دیجیتال F وجود دارد که باید مانیتور شوند و چند عملگر F وجود دارد که باید در یک پلنت کنترل شوند. به‌عبارت‌دیگر در این ساختار برای حصول به یک نتیجه مورد انتظار از عملکرد ایمنی بایستی سیگنال‌های دیجیتال ورودی مانیتور شده و به یک یا چند کانال خروجی (عملگر) فرمان تریپ مناسب صادر شود. در این شکل سیگنال‌های دیجیتال با دایره‌های قرمزرنگ مشخص‌شده است.

بسته به اهمیت و میزان ریسک خرابی‌ها (سطح SIL موردنیاز)، معماری‌های مختلف سیم‌بندی و ارزیابی یا صدور رأی (voting) برای سیگنال‌های دیجیتال وجود دارد. برای مثال رأی‌گیری می‌تواند، در داخل ماژول‌های ورودی دیجیتال و یا در CPU انجام شود. که در ادامه تشریح می‌شود.

در پیکربندی شکل ۸-۱ لاجیک F با پایش وضعیت فرایند از طریق کانال‌های ورودی، بسته به مقدار فشار، سطح و دما و یا در صورت تشخیص یک خرابی، به‌صورت ایمن فرمان تریپ به شیرهای ESD (BV-100A و BV-100B) در یک مخزن را صادر می‌کند.

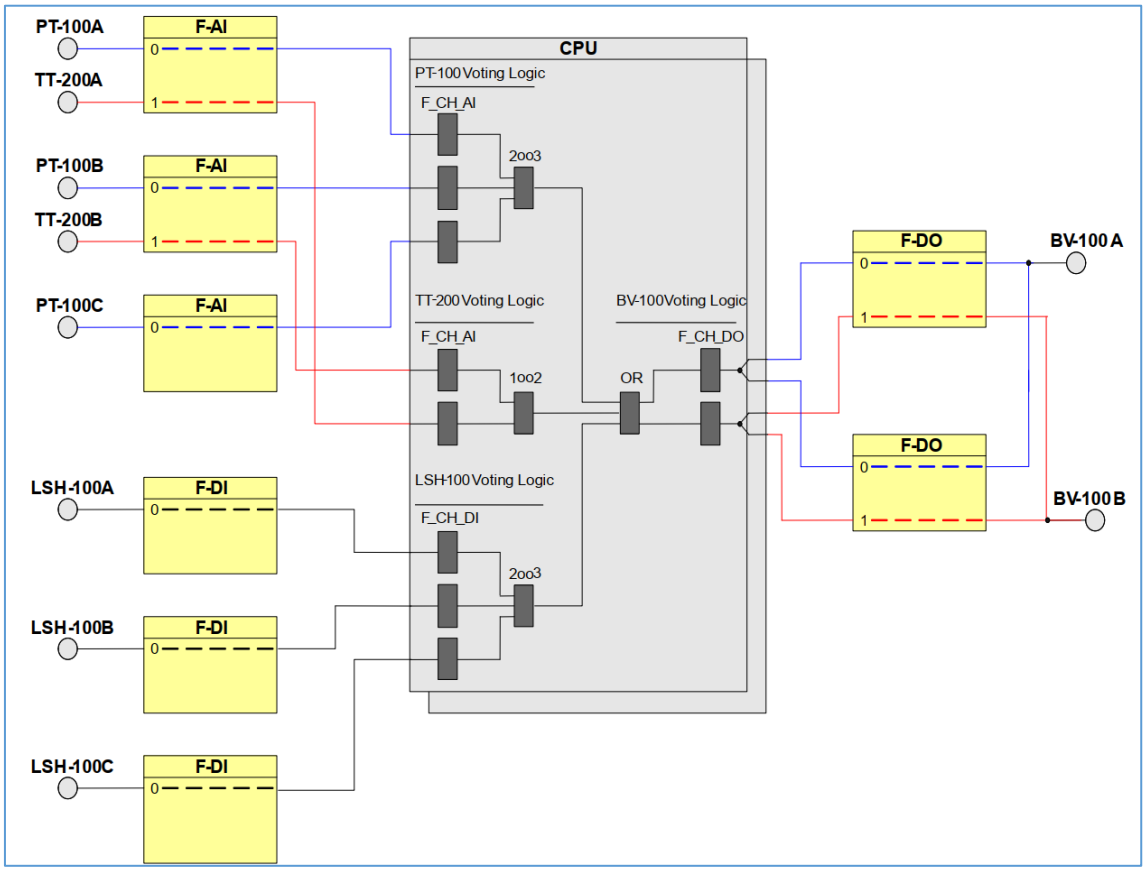


شکل ۸-۱: ساختار نمونه از حلقه‌های ایمنی (SIF)

نکته: در تمام مثال‌های این بخش، از ماژول ورودی خروجی دیجیتال با کد سفارش زیر استفاده‌شده است.

- ☑ SM 326 -F-DI 24 x DC- 24V: 6ES7 326-1BK02-0AB0
- ☑ SM 32- F-DO - 6ES7 326-2BF01-0AB0

امکان‌های مختلف سیم‌بندی و رأی‌گیری سیگنال‌های دیجیتال F در این ساختار در شکل ۸-۲ نشان داده‌شده است.



شکل ۸-۲: روش‌های مختلف سیم‌بندی و رأی‌گیری سیگنال‌های دیجیتال F

1.3 Presented Architectures

برای پیاده‌سازی مثال مطرح‌شده در بالا و برای ارزیابی سیگنال‌های ورودی/خروجی دیجیتال F (F-DIO)، معماری‌های زیر توصیف می‌شود.

One sensor (1oo1) Architecture

معماری تک کانال/ تک حس‌گر- در این معماری یک حس‌گر به یک کانال از یک ماژول سیگنال F متصل می‌شود. کاربردهای نوعی این معماری برای مواردی است که در آن یک حس‌گر واحد، سطح SIL موردنیاز را برآورده می‌کند و ساختار ریداندانت برای بالا بردن دسترس‌پذیری (Availability) موردنیاز نیست.

نکته: ماژول دیجیتال ورودی SM 326 مطرح‌شده در این معماری دارای گواهینامه SIL2 می‌باشد. لذا با پیکربندی 1oo1، برای یک حلقه SIF حداکثر سطح SIL2 حاصل می‌شود.

ولی در صورت اتصال یک حس‌گر به دو کانال از دو کارت ریداندانت، سطح SIL 3 نیز قابل حصول می‌باشد. توجه شود که برای سازگاری با SIL، بایستی تمام اجزای حلقه SIF ازجمله تجهیزات فیلد، مطابق با استانداردهای IEC 61511 / IEC 61508 ارزیابی شود.

one sensor (1oo1) and redundant F-DI (2oo2) Architecture

معماری تک حس‌گر با دو کانال ریداندانت - درصورتی‌که یک حس‌گر در یک حلقه SIF بتواند، سطح SIL موردنیاز را برآورده کند و نیاز به دسترس‌پذیری بالا در سیستم کنترل باشد. در آن صورت می‌توان برای افزایش در دسترس‌پذیری در کانال‌های کارت، معماری 2oo2 را پیکربندی کرد.

Two sensors (1oo2) and one F-DI with evaluation in the F-DI (1oo1)

معماری دو حس‌گر- کاربرد معمول این ساختار، زمانی است که یک حس‌گر منفرد سطح یکپارچگی ایمنی یا SIL لازم را برآورده نمی‌کند و همچنین نیازی به افزایش دسترسی وجود ندارد.

Two sensors (1oo2) Architecture

معماری دو کانال/ ارزیابی با دو حس‌گر - در این معماری دو حس‌گر به دو ورودی مقابل هم از یک ماژول یا به دو کانال از دو ماژول ریداندانت متصل می‌شود. ارزیابی دو سیگنال می‌تواند به‌صورت سخت‌افزاری در داخل ماژول ورودی دیجیتال و یا در برنامه F (CFC) انجام شود.

- ارزیابی 1oo2 با دو حس‌گر در داخل کارت F-DI
- ارزیابی (1oo2) با دو حس‌گر در برنامه کاربر(User Program)

Two sensors (1oo2) and redundant F-DI with evaluation in the F-DI (2oo2)

کاربرد معمول این ساختار، زمانی است که یک حس‌گر منفرد سطح یکپارچگی ایمنی لازم را برآورده نمی‌کند. ولی برای افزایش دسترس‌پذیری نیاز به ریداندانسی کارت وجود دارد.

Two sensors (1oo2) with evaluation in the user program

معماری دو کانال/ ارزیابی با دو حس‌گر - کاربرد معمول این ساختار، زمانی است که یک حس‌گر منفرد سطح یکپارچگی ایمنی لازم را برآورده نمی‌کند و داده‌های هر دو حس‌گر باید در سیستم

مانیتورینگ قابل‌مشاهده باشد. در این معماری دو حس‌گر به دو کانال از یک کارت متصل می‌گردد.

Two sensors (1oo2) and redundant F-DI (2oo2) with evaluation in the user program

معماری دو کانال/ ارزیابی با دو حس‌گر - کاربرد معمول این ساختار، زمانی است که یک حس‌گر منفرد سطح یکپارچگی ایمنی لازم را برآورده نمی‌کند و داده‌های هر دو حس‌گر باید در سیستم مانیتورینگ قابل‌مشاهده باشد. در این ساختار برای افزایش دسترسی، کارت‌های F-DI ریداندانت هم (2oo2) پیکربندی می‌گردد.

Control of a single actuator or final element (1oo1) on an F-DO (1oo1)

معماری تک کانال برای المان نهایی (1oo1) - از دیدگاه یک سیستم ایمنی سیماتیک، تمامی طرح‌های صدور رأی در المان نهایی کنترل (final element voting) ترکیبی از خروجی‌های 1oo1 می‌باشند. المان نهایی باید به شیوه‌ای که لاجیک ایمنی فرمان می‌دهد، عمل کند.

Control of a single actuator (1oo1) with redundant F-DO (2oo2

این طرح معماری برای افزایش دسترسی در کارت‌های FDO می‌باشد. عملگر توسط یک جفت F-DO ریداندانت هم کنترل می‌شود.

Notes

۱- توجه شود که در تمام طرح‌ها و مثال‌های این فصل فرض شده است که سیگنال ورودی دیجیتال، برای رأی به صدور فرمان تریپ (Failsafe)، بی‌برق (de-energize to trip) می‌شود. به این معنی که در حالت عادی تا زمانی که شرایط غیر نرمال توسط حس‌گر تشخیص داده نشده است، مقدار ورودی ازلحاظ منطقی یک می‌باشد و به‌محض تشخیص وضعیت غیر نرمال، ورودی صفر شده و رأی به‌فرمان تریپ صادر می‌شود

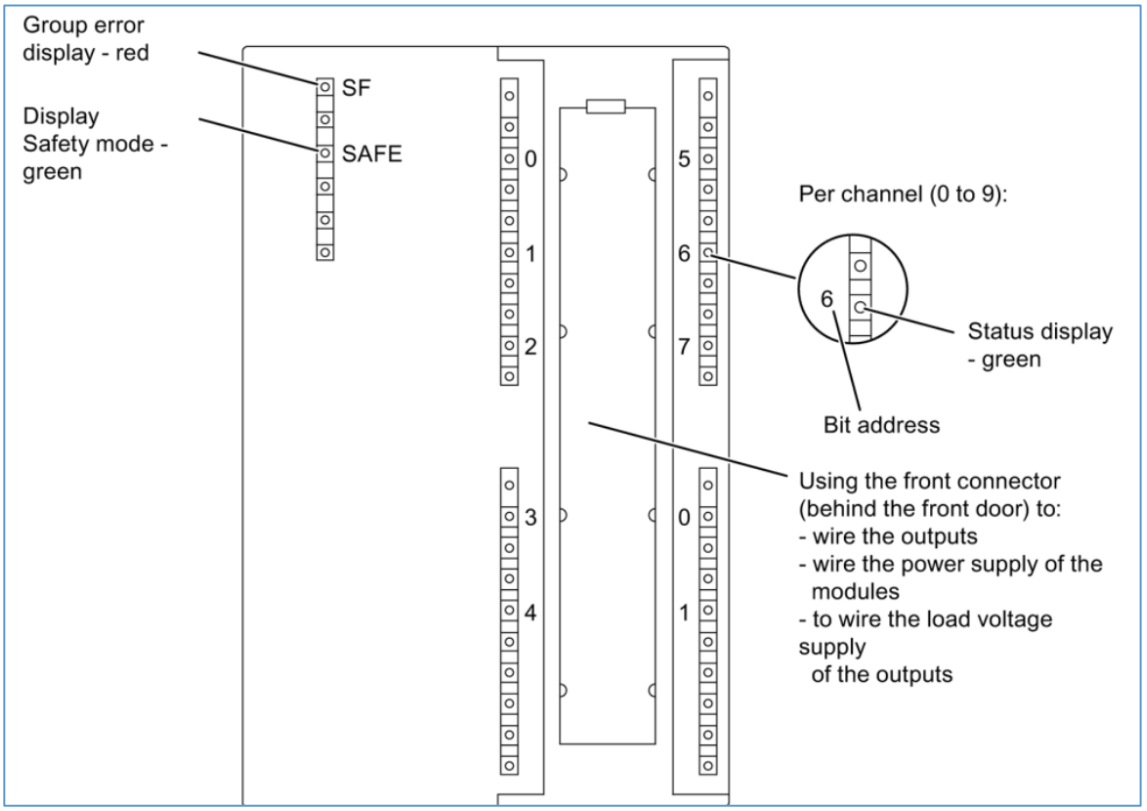
Input Signal Value: Normal = 1 & Vote to trip = 0

۲- در طرح‌های ارزیابی، المان حس‌گر رأی به تریپ می‌دهد و لاجیک داخل ماژول CPU فرمان تریپ به لاجیک Shutdown را صادر می‌کند. به‌عبارت‌دیگر از دید یک مدرک cause & effect

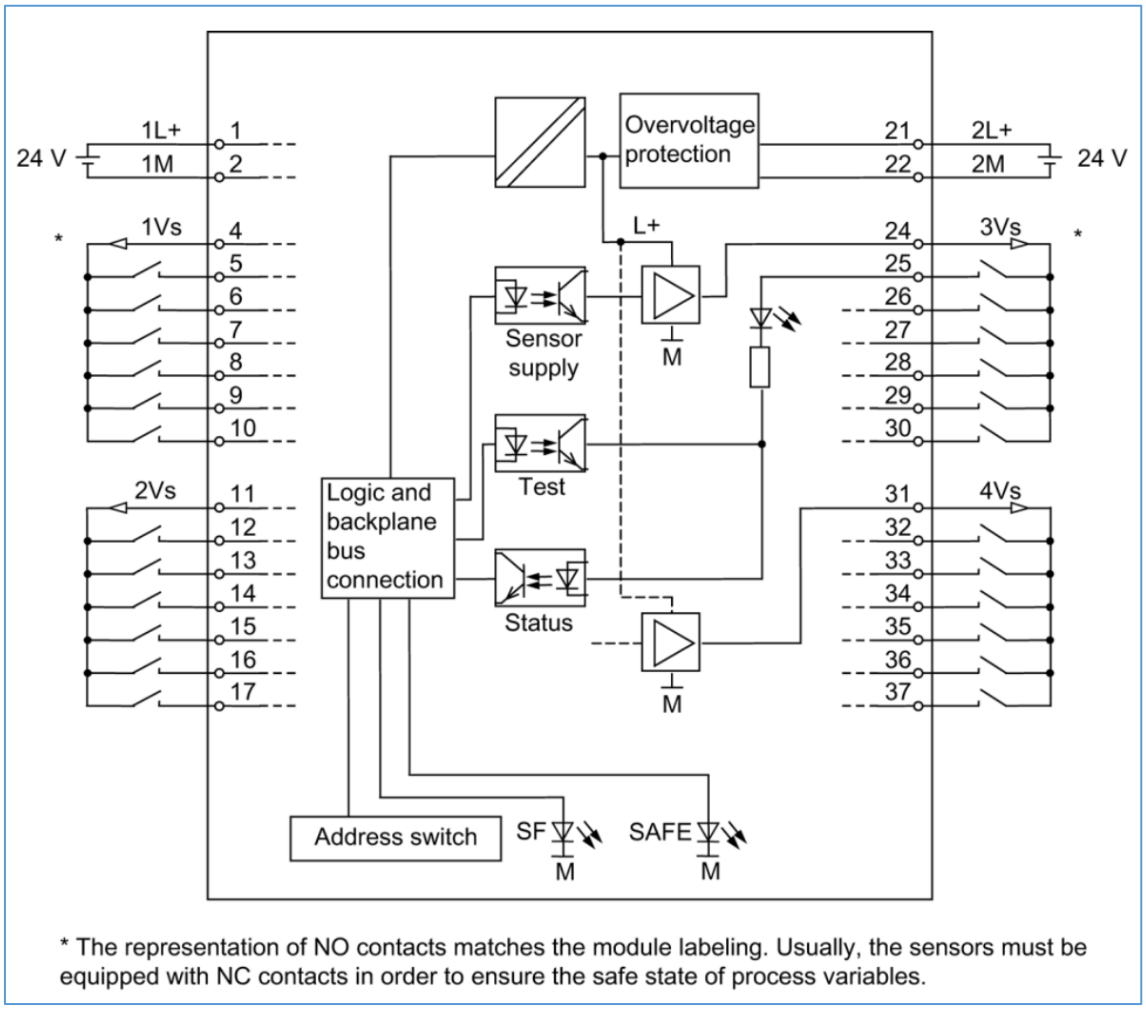
وقتی حس‌گر دیجیتال رأی به تریپ می‌دهد، Cause تعریف‌شده فعال می‌شود و درنتیجه Effectهای مرتبط با این Cause تریگر می‌شود.

1.4 Properties for the fail-safe digital input module

ماژول ورودی S7-300F که توضیح داده شد، SM 326 - DI 24 x DC 24V است. این ماژول دارای ۲۴ کانال است و می‌توان آن را برای طرح‌های ارزیابی مانند 1oo2 پیکربندی کرد. برای ساده‌سازی، در این فصل از این ماژول تحت عنوان F-DI اشاره خواهد شد. شکل ۸-۳نمای جلوی F-DI و شکل ۸-۴ دیاگرام اتصال و شماتیک کارت FDI را نشان می‌دهد.



شکل ۸-۳: نمای جلویی کارت FDI



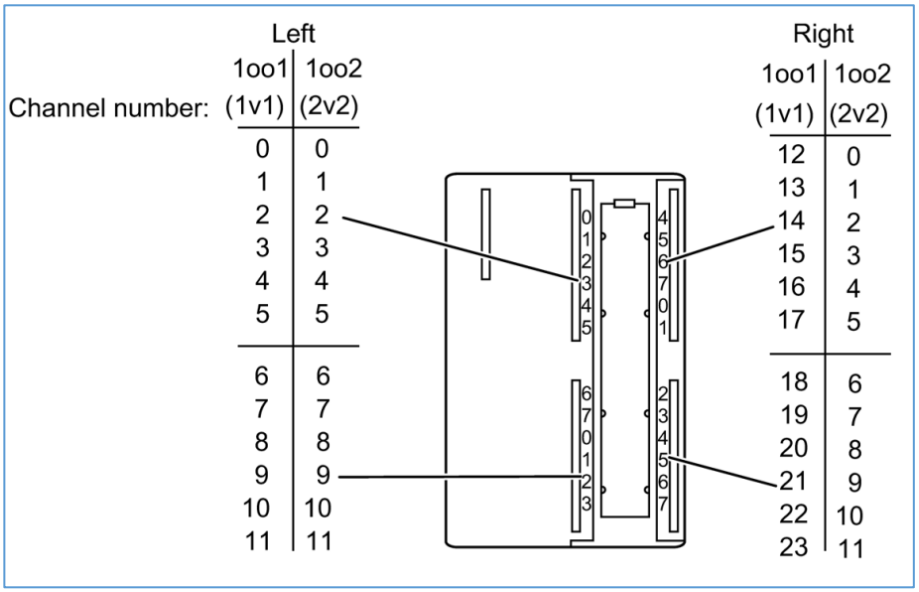
شکل ۸-٤: پایه‌های اتصال و دیاگرام شماتیک کارت FDI

کارت F-DI باید از دونقطه تغذیه شود. پایه‌های 1L+/1M (۱ و ۲) تغذیه به کانال‌های سمت چپ ماژول (ترمینال‌های ۴ تا ۱۷) را تأمین می‌کند. پایه‌های 2L+/2M (۲۱ و ۲۲) تغذیه کانال‌های سمت راست ماژول (ترمینال‌های ۲۴ تا ۳۷) را تأمین می‌کنند. دستگاه‌های فیلد را می‌توان از طریق پایه‌های xVs (۴، ۱۱، ۲۴ و ۳۱) تغذیه کرد. این پایه‌ها تغذیه را برای هر گروه شش کانال ورودی را تأمین می‌کنند.

کانال‌ها را می‌توان به‌صورت جداگانه (1oo1) یا به‌صورت جفتی (یعنی کانال ۰ و ۱۲، کانال ۱ و ۱۳ و یا به‌طورکلی کانال x و کانال x+ 12) برای معماری 1oo2 ارزیابی کرد. ارزیابی 1oo1 شامل معماری‌های تک حس‌گر با ارزیابی اختیاری 1oo2 در CPU است. در ارزیابی 1oo2، به‌طورکلی

دو حس‌گر موردنیاز است. که در آن وضعیت سیگنال آن‌ها در خود ماژول نیز قابل ارزیابی است.

شکل ۸-۵ انتساب شماره کانال‌های FDI را برای ارزیابی 1oo1 و 1oo2 در F-DI نشان می‌دهد



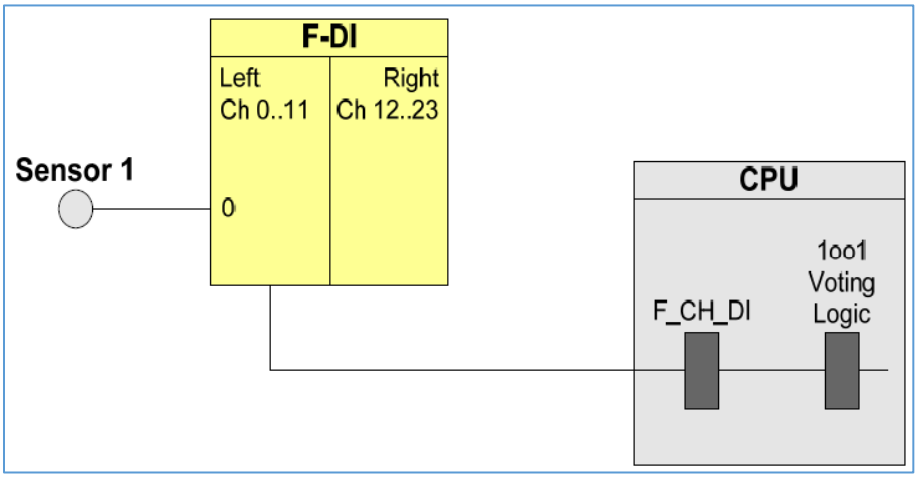
شکل ۸-۵: شماره کانال برای ارزیابی 1oo1 و 1oo2 در F-DI

2. Hardware configuration and wiring of one sensor (1oo1) and one F-DI (1oo1)

سیم‌بندی تک حس‌گر یا طرح صدور رأی 1oo1 (voting)، برای کاربردهایی است که در آن یک حس‌گر سطح SIL موردنیاز را برآورده می‌کند و به ریداندانسی حس‌گر نیازی نیست. ارزیابی 1oo1 بدان معنی است که برای صدور فرمان تریپ تنها به یک حس‌گر نیاز است. در صورت تشخیص شرایط تریپ توسط حس‌گر، لاجیک ایمنی فرمان تریپ را صادر می‌کند. مطابق شکل ۸-۶ تنها یک حس‌گر به کانال صفر یک ماژول F-DI متصل می‌شود.

نکته: ماژول دیجیتال ورودی SM 326 مطرح‌شده در این معماری دارای گواهینامه SIL2 می‌باشد. لذا با پیکربندی 1oo1، برای یک حلقه SIF حداکثر سطح ایمنی SIL2 حاصل می‌شود. ولی در صورت اتصال یک سنسور به دو کانال از یک کارت یا دو کارت ریداندانت، سطح SIL 3

نیز قابل حصول می‌باشد. توجه شود که برای سازگاری با SIL، بایستی تمام اجزای حلقه SIF ازجمله تجهیزات فیلد، مطابق با استانداردهای IEC 61511 / IEC 61508 ارزیابی شود.



شکل ۸-٦: اتصال ورودی دیجیتال به ماژول FDI در معماری ارزیابی 1oo1

با پیکربندی سخت‌افزاری مطابق شکل ۸-۶، تنها دستیابی به حداکثر SIL2 امکان‌پذیر است.

جدول زیر نشان می‌دهد که چه زمانی عملکرد ایمنی می‌تواند توسط لاجیک مربوطه فعال شود.

Sensor 1	F-DI	Error reaction function has been triggered?
No	No	No
X	Yes	Yes
Yes	X	Yes

شکل ۸-۷: مدهای خرابی و پاسخ تابع واکنش به خطا در معماری 1oo1

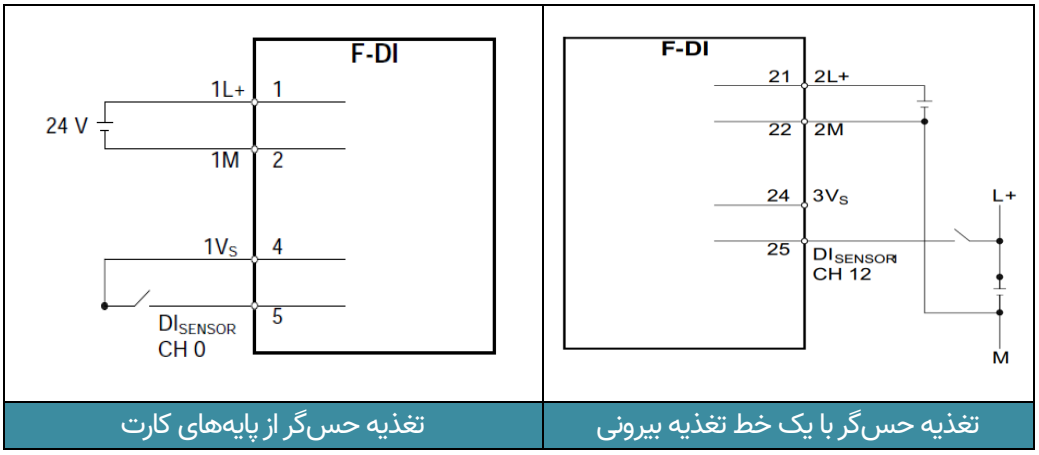
2.1 1oo1 Wiring

2.1.1 Conventional wiring

در اتصال یک حس‌گر به یک کانال F-DI، خط تغذیه حس‌گر را به دو صورت می‌توان سیم‌بندی کرد. تغذیه از طریق کارت F-DI با پایه‌های Vs و استفاده از یک خط تغذیه از منبع بیرونی.

نحوه اتصال حس‌گر به کانال دیجیتال را در معماری 1oo1 نشان می‌دهد. حس‌گر به کانال صفر (ترمینال ۵) متصل می‌شود. در طرح تغذیه حس‌گر از پایه‌های کارت، تغذیه موردنیاز از خط

1L+/1M تأمین‌شده و از پایه 1Vs (ترمینال ۴) به حس‌گر اعمال می‌شود. ولی در طرح دوم، حس‌گر از یک منبع بیرونی تغذیه می‌شود.

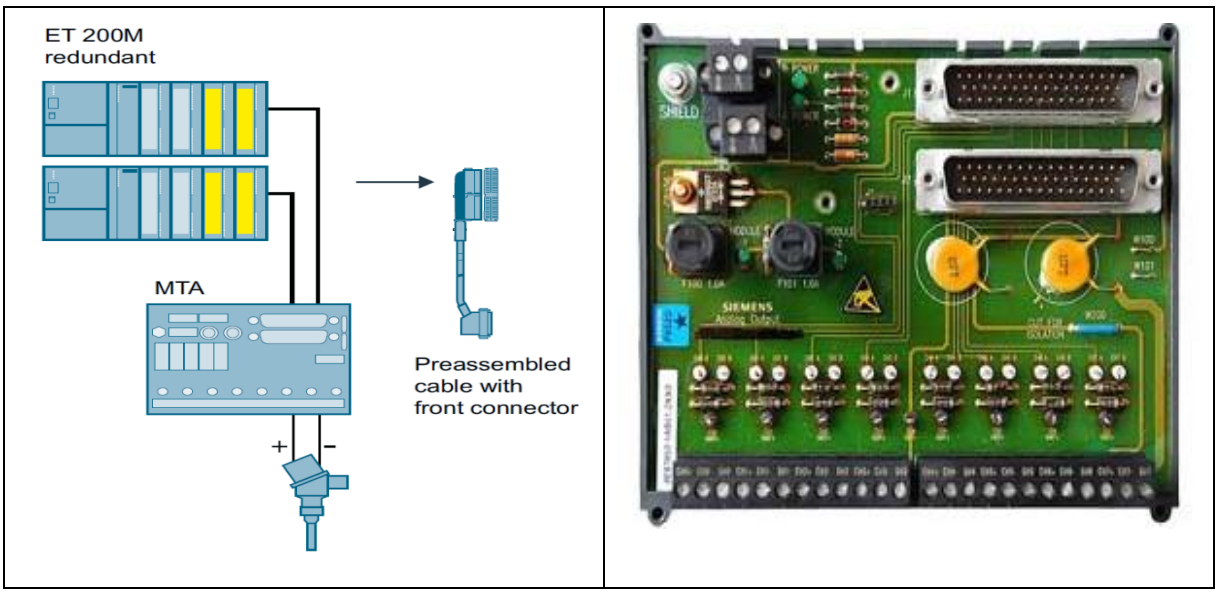


تغذیه حس‌گر از پایه‌های کارت | تغذیه حس‌گر با یک خط تغذیه بیرونی

شکل ۸-۸: اتصال یک حس‌گر دیجیتال به یک کانال از کارت F-DI (طرح 1oo1)

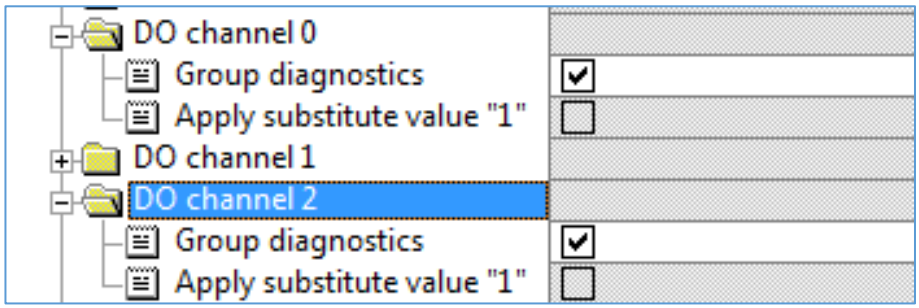
2.1.2 Wiring using an MTA (Marshalled Termination Assembly)

علاوه‌بر روش مرسوم سیم‌بندی سنسور به کانال‌های کارت‌های ورودی/خروجی، شرکت زیمنس استفاده از بردهای MTA را نیز ارائه می‌دهد. در این روش سیم‌کشی بین سنسورها و ماژول‌های سیگنال روی ET200M با استفاده از F-DI MTA بسیار ساده شده است.



شکل ۸-۹: اتصال یک حس‌گر به ماژول F-DI به روش MTA

توجه: این گزینه قابلیت تشخیص عیب در سطح ماژول را فعال می‌کند. با فعال کردن این گزینه، بایستی این پارامتر برای تک‌تک کانال‌ها نیز انتخاب شود. پارامتر Diagnostic interrupt بایستی برای تمام کانال‌های سیم‌بندی شده ماژول F-DO فعال گردد.



شکل ۸-۶۷: تنظیم Group Diagnostic برای کارت‌های F-DO

Behavior at CPU STOP

این گزینه تنها برای ماژول‌ها در مد استاندارد قابل انتخاب می‌باشد. برای یک ماژول F-DO در مد ایمنی، به‌صورت پیش‌فرض گزینه Apply Substitute value انتخاب‌شده است. به‌طوری‌که در صورت وقوع خطا یا متوقف شدن CPU، مقدار صفر در همه خروجی‌های ماژول جایگزین می‌شود.

Maximum test time (s)

با این پارامتر، زمان سیکل تکرار سیکل‌های تست بیت خروجی تنظیم می‌شود.(complete bit pattern test). مقدار این پارامتر در بازه ۱۰۰۰ / ۱۰۰ ا(۱۰۰۰) است.

Diagnostics load voltage failure

این پارامتر مانیتورینگ تشخیص خرابی در ولتاژ بار (voltage load) را برای کانال‌های 0-4 (2L+) و کانال‌های 5-9 (3L+) فعال می‌کند.

Light test activated

12.1 F Input/output Modules LEDs

بر روی ماژول‌های ورودی/خروجی F نشانگرهایی به شرح زیر وجود دارد.

1	SF: Group fault	به معنی System fault بوده و در صورت وجود فالت در ماژول، روشن می‌شود.
2	SAFE: Safety mode	مد کارت را مشخص می‌کند. این چراغ در مد safety روشن و در مد استاندارد خاموش می‌شود. درصورتی‌که دیپ‌سویئچ مربوط به آدرس PROFIsafe درست تنظیم‌نشده باشد. این چراغ روشن نمی‌شود.
4	Green LED Status	وضعیت فعال یا غیرفعال بودن هر کانال را نشان می‌دهد.
	Sensor supply display (Vs)	در صورت تغذیه حس‌گر از طریق پایه‌های VS روشن می‌شود.

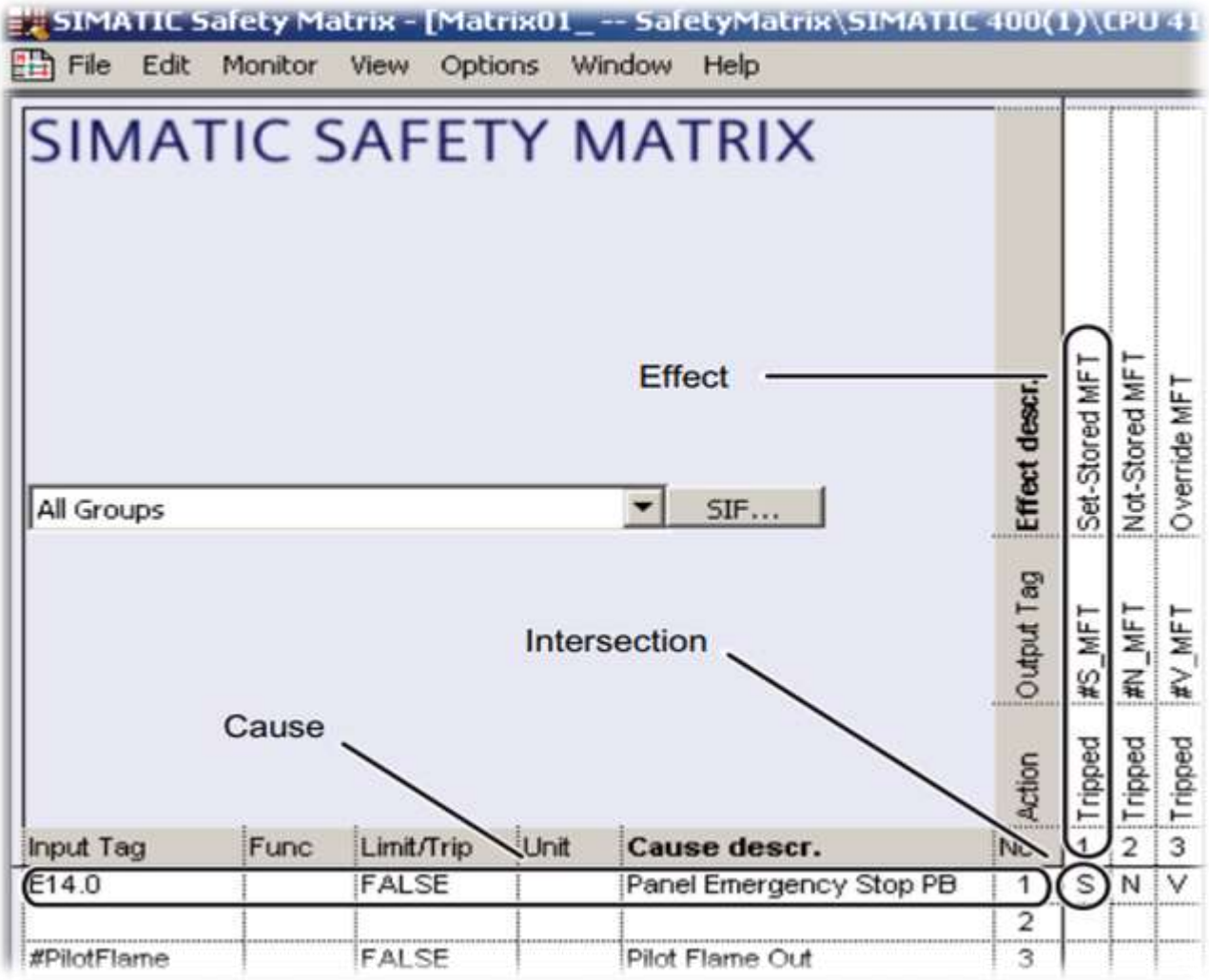
13. References

[1] Wiring and Evaluation Architectures for Failsafe Digital Input (F-DI)- and Output-Modules (F-DO) of ET 200M, Functional Example No AS-FE-II-002-V10-EN

[2] Wiring and Voting Architectures for failsafe Digital Input (F-DI) and Output Modules (F-DO) of the ET 200M

فصل نهم

کار با ماتریس ایمنی



Working with Safety Matrix

Chapter 9

09 Safety Matrix

Learning targets

محتوای این فصل شامل مباحث زیر می‌باشد.

- معرفی ماژول نرم‌افزاری
- تشریح ویرایشگر ماتریس ایمنی
- پیکربندی ماتریس ایمنی
- برنامه‌نویسی، کامپایل و دانلود ماتریس ایمنی

Abstract

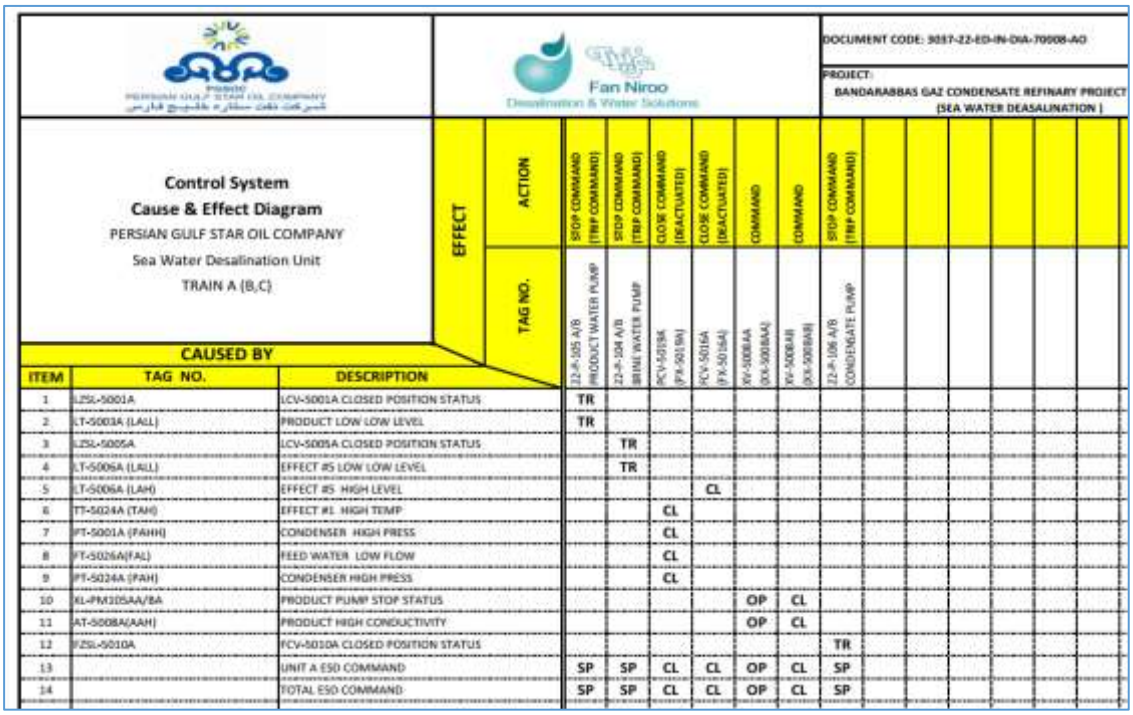
ماتریس ایمنی یک ابزار قدرتمند و اثبات شده برای پیاده‌سازی ایمنی فرآیند با سیستم Simatic PCS 7 F است. ماتریس ایمنی که برای صنایع فرآیند طراحی شده است، امکان ساده‌سازی بسیاری از مراحل مهم را که در چرخه عمر ایمنی (safety lifecycle) ANSI / ISA S84 تعریف شده است، را فراهم می‌کند.

Abbreviations

1oo2	1 out of 2
2oo3	2 out of 3
AS	Automation Station or Automation System
CFC	Continious Function Charts
CPU	Centeral Processing Unit
ES	Engineering Station
ESD	Emergency Shutdown System
FH	Fail-Safe & High Available
OS	Operator Station
PCS	Process control System
RIO	Remote I/O
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
LOPA	layer of protection analysis

9.1 Cause and Effect Matrix Methodology

ماتریس علت و اثر، برای تعریف چگونگی (how) و زمان (when) اجرای اقدامات (Actions) در یک سیستم ایمنی استفاده می‌شود. این روش شامل سازمان‌دهی رویدادهای فرایند به دسته‌های علت‌ها و اثرات و سپس اتصال این علل و اثرات به همدیگر است. لینک‌های بین علل و اثرات، تقاطع‌ها (intersections) نامیده می‌شود. به‌طوری‌که effectها اثراتی را که از علت فعال‌شده حاصل می‌شود، نشان می‌دهد. از این داده‌ها، می‌توان لاجیکی را استخراج کرد. که جهت جلوگیری از وقوع رخدادها قبل از ایجاد آسیب به افراد و فرایند، برای ایجاد یک برنامه ایمنی استفاده می‌شود. شکل ۹-۱ نمایی از یک ماتریس علت و اثر را نشان می‌دهد.



DOCUMENT CODE: 3037-22-ED-IN-DIA-70008-A0

PROJECT: BANDARABBAS GAZ CONDENSATE REFINARY PROJECT (SEA WATER DEASALINATION)

Control System
Cause & Effect Diagram
PERSIAN GULF STAR OIL COMPANY
Sea Water Desalination Unit
TRAIN A (B,C)

EFFECT / ACTION / TAG NO. / CAUSED BY

ITEM	TAG NO.	DESCRIPTION	22-P-105 A/B PRODUCT WATER PUMP: STOP COMMAND (TRIP COMMAND)	22-P-104 A/B BRINE WATER PUMP: STOP COMMAND (TRIP COMMAND)	FCV-5015A (FX-5015A): CLOSE COMMAND (DEACTUATED)	FCV-5016A (FX-5016A): CLOSE COMMAND (DEACTUATED)	XV-5008AA (XX-5008AA): COMMAND	XV-5008AB (XX-5008AB): COMMAND	22-P-106 A/B CONDENSATE PUMP: STOP COMMAND (TRIP COMMAND)
1	LZSL-5001A	LCV-5001A CLOSED POSITION STATUS	TR						
2	LT-5003A (LALL)	PRODUCT LOW LOW LEVEL	TR						
3	LZSL-5005A	LCV-5005A CLOSED POSITION STATUS		TR					
4	LT-5006A (LALL)	EFFECT #5 LOW LOW LEVEL		TR					
5	LT-5006A (LAH)	EFFECT #5 HIGH LEVEL				CL			
6	TT-5024A (TAH)	EFFECT #1 HIGH TEMP			CL				
7	PT-5001A (PAHH)	CONDENSER HIGH PRESS			CL				
8	FT-5026A(FAL)	FEED WATER LOW FLOW			CL				
9	PT-5024A (PAH)	CONDENSER HIGH PRESS			CL				
10	XL-PM3DSAA/BA	PRODUCT PUMP STOP STATUS					OP	CL	
11	AT-5008A(AAH)	PRODUCT HIGH CONDUCTIVITY					OP	CL	
12	FZSL-5010A	FCV-5010A CLOSED POSITION STATUS							TR
13		UNIT A ESD COMMAND	SP	SP	CL	CL	OP	CL	SP
14		TOTAL ESD COMMAND	SP	SP	CL	CL	OP	CL	SP

شکل ۹-۱- نمایی از ماتریس Cause & Effect

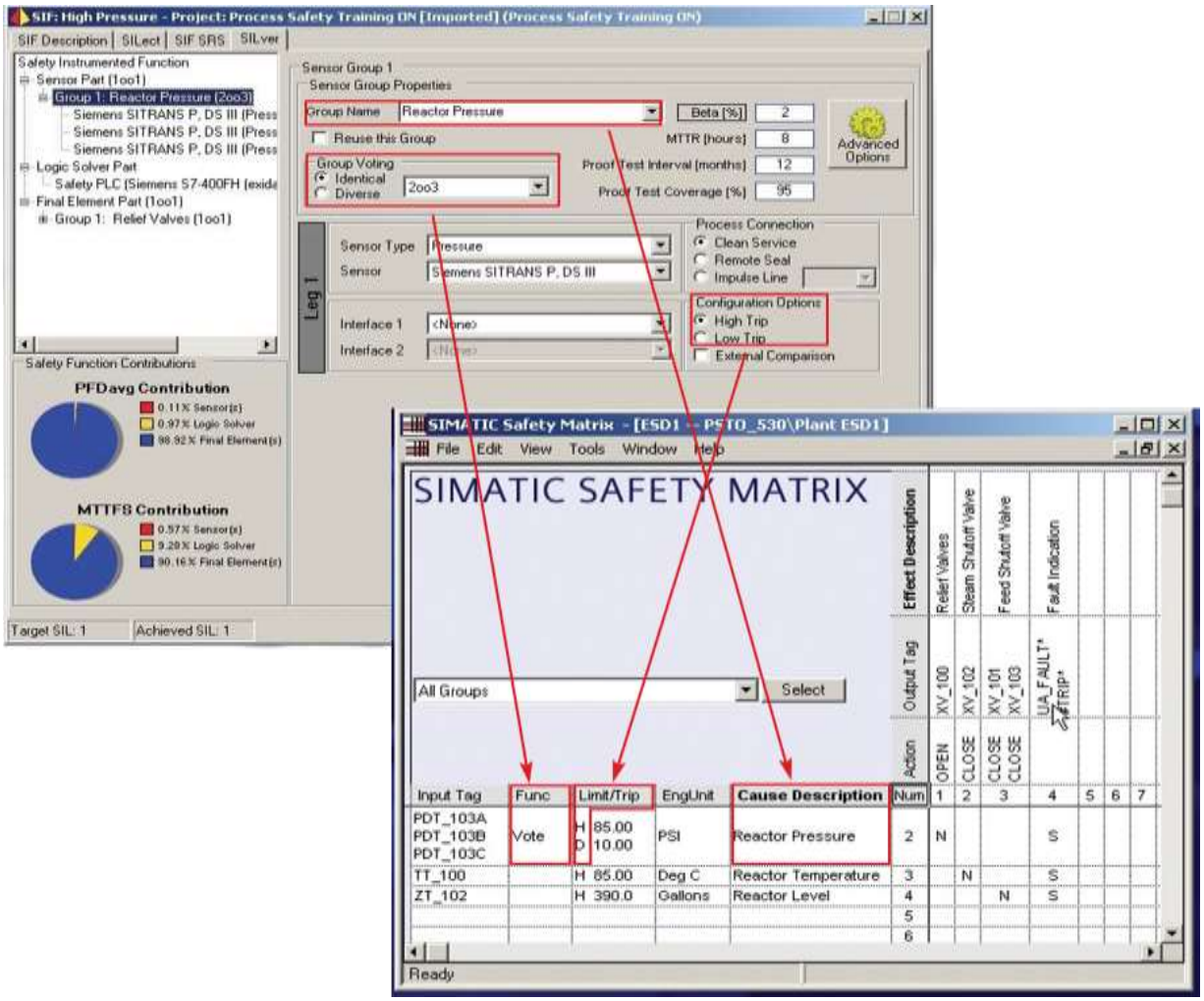
9.2 Introduction to Safety Matrix

ماتریس ایمنی (Safety Matrix) یک ابزار نرم‌افزاری (toolkit) است که ساختار ظاهری آن شبیه به یک جدول یا ماتریس علت - اثر (Cause & Effect) می‌باشد. به طوری‌که مدت زمان تکمیل مراحل انجام پروژه را با ادغام تک‌تک مراحل پیکربندی، برنامه‌نویسی، آزمون، تعمیر و نگهداری را از طریق ایجاد یک ماتریس علت و اثر کاهش می‌دهد. در واقع ابزار نرم‌افزاری ماتریس ایمنی روند ایجاد یک ماتریس علت - اثر را با فراهم نمودن یک الگوی ورود اطلاعات (template for data entry) آسان‌تر می‌کند. به عبارت ساده‌تر ماتریس ایمنی، روش خودکار برای ایجاد لاجیک CFC مربوط به طرح‌های ارزیابی ایمنی می‌باشد.

9.2.1 Safety Lifecycle Integration

امروزه برای کمک به کاربران در تمام مراحل مختلف چرخه عمر ایمنی، انواع ابزارهای نرم‌افزاری وجود دارد. به عنوان مثال تجزیه و تحلیل خطر فرآیند (process hazard analysis)، LOPA و ابزار تعیین SIL.

این ابزارها برای صرفه‌جویی در وقت و ساده‌سازی فعالیت‌ها در چرخه عمر ایمنی طراحی شده است. با این حال، از آنجایی که توسط شرکت‌های مختلف توسعه یافته است، این ابزارها به طور معمول با هم ادغام نمی‌شوند. در نتیجه، کاربر را مجبور می‌کند ورود اطلاعات ایمنی را چندین بار تکرار کند، با این که در بیشتر موارد داده‌های ایمنی ثابت می‌باشد. به عنوان مثال ورود اطلاعات توصیف فرآیند، لاجیک صدور رای (voting logic) و محدودیت‌های تریپ.



شکل ۹-۲- ایجاد ماتریس ایمنی از روی ابزارهای چرخه عمر ایمنی

دپارتمان اتوماسیون و انرژی زیمنس (Siemens Energy & Automation) این ابزار نرم‌افزاری را با انتقال مستقیم (import) داده‌ها از یک ابزار چرخه عمر ایمنی مستقل به ماتریس ایمنی ایجاد نموده است.

برای این کار زیمنس با شرکت Exida همکاری کرد تا نشان دهد که چگونه کاربران می‌توانند ابزار چرخه ایمنی خود را (exSILentia) در ماتریس ایمنی ادغام کنند. در نتیجه، ثابت شد که با ماتریس ایمنی، می‌توان در زمان صرفه جویی کنید و پیچیدگی را کاهش دهید.

نمودار C&E در مرحله اول یک روش عالی برای مستند کردن تمام توابع SIS در یک فرایند است. این اطلاعات در گام بعدی توسط یک کامپایلر به کد لاجیک ترجمه می‌شود. به‌طوری‌که PLC ایمنی (Logic Solver) می‌تواند این کد را درک کند. امروز برای اکثر سیستم‌های کنترل موجود در بازار، این کار نیاز به ترجمه و کد کردن علت و اثرات و تبدیل آنها به لاجیک PLC به زبان LAD یا FBD دارد. همچنین یک زمان زمان اضافی لازم است تا این تبدیل و ترجمه دقیق را تضمین کند. ولی در ماتریس ایمنی با یک کلیک ماوس، ابزار ماتریس ایمنی به طور خودکار تمام جزئیات پیچیده را برای هر علت (ورودی) و هر اثر (خروجی) استخراج می‌کند و یک بلاک تابع (FB) تایید شده TÜV را تولید می‌کند.

هر فانکشن‌بلاک، می‌تواند تا ۱۲۸ علت و ۱۲۸ اثر را با حداکثر ۵۰۰ تقاطع پشتیبانی کند. یک کنترل کننده ایمنی S7-400 می‌تواند چندین نمودار علت و اثرات متعدد را اجرا کند.

در روند تکمیل لاجیک SIS، صفحات پیکربندی ساده و گرافیکی ابزار ماتریس ایمنی، رابط کاربری ساده‌ای را برای پیکربندی الزامات رایج در یک SIS مانند شرایط آلارم و تریپ، توابع bypass و overrides و جزئیات لاجیک مانند voting logic و تاخیرهای زمانی (time delays) ارائه می‌دهد.

9.2.2 Safety Matrix Software: Product Overview

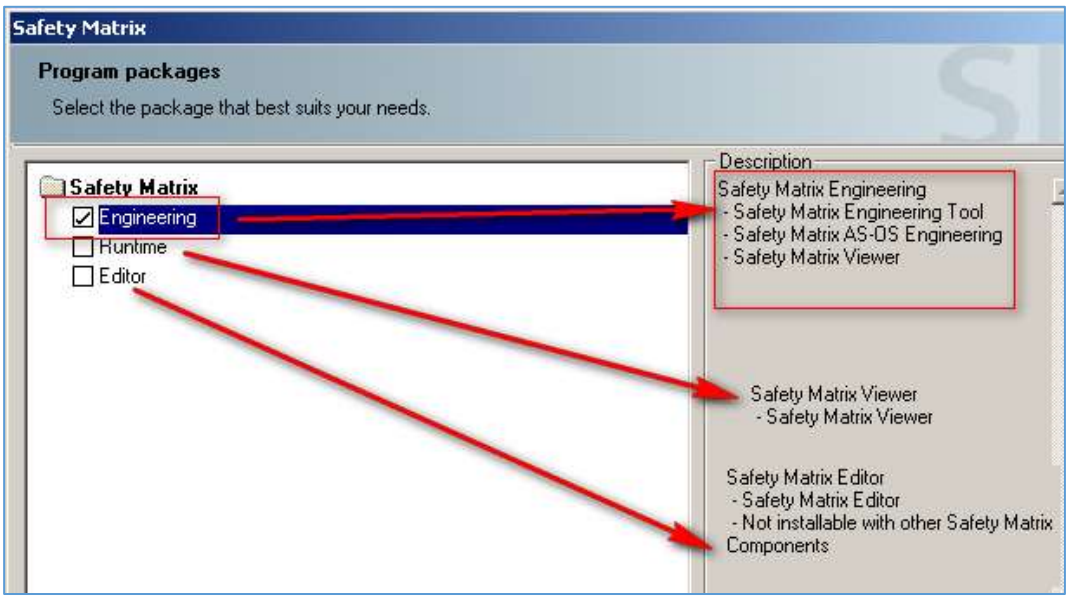
برنامه Safety Matrix به‌صورت یک بسته نرم‌افزاری جداگانه همراه بسته F-System ارائه و نصب می‌شود. آخرین نسخه نرم‌افزار Safety Matix عرضه‌شده به بازار تا سال ۲۰۱۸ نسخه 6.2 SP2 می‌باشد. این بسته شامل سه ابزار نرم‌افزاری می‌باشد. که عبارت است از:

☞ Safety Matrix Engineering Tool ☞ Safety Matrix Viewer ☞ Safety Matrix Editor	Safety Matrix ☑ Safety Matrix Engineering Tool V6.2 SP2 ☑ Safety Matrix Viewer V6.2 SP2 ☑ Safety Matrix AS-OS Engineering V6.2 SP2 Safety Matrix Editor ☐ Safety Matrix Editor V6.2 SP2 Tools ☐ Automation License Manager V5.3

سه ابزار مذکور موقع نصب بسته نرم‌افزار مطابق شکل ۹-۳ به سه صورت قابل انتخاب می‌باشد.

☜ برای کامپیوتر مهندسی گزینه Engineering نصب می‌شود.

☜ برای کامپیوتر OS گزینه Runtime نصب می‌شود.

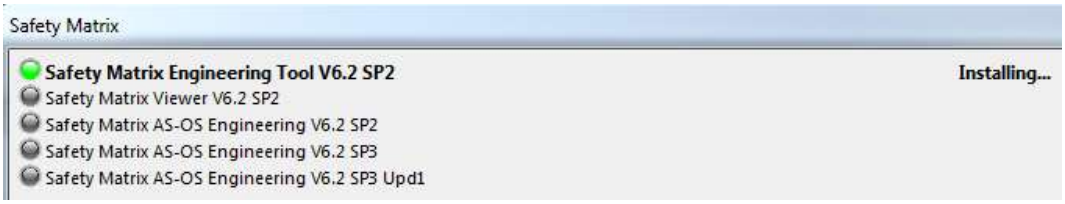


شکل ۹-۳- گزینه‌های نصب نرم‌افزار Safety Matrix

https://support.industry.siemens.com/cs/ww/en/view/101509838

Safety Matrix Engineering Tool

«ابزار مهندسی ماتریس ایمنی» مجموعه کامل ابزارهای نرم‌افزاری را برای ایجاد، پیکربندی، کامپایل و دانلود ماتریس ایمنی به CPU را از یک ایستگاه مهندسی STEP 7 (ES) فراهم می‌کند. علاوه‌براین این ابزار، قابلیت ارتباط آنلاین با PLC را برای آزمون آنلاین ماتریس ایمنی پشتیبانی می‌کند. با انتخاب گزینه Engineering برای نصب، مطابق شکل ۹-۴ ابزارهای مختلف در کامپیوتر مهندسی نصب می‌شود.



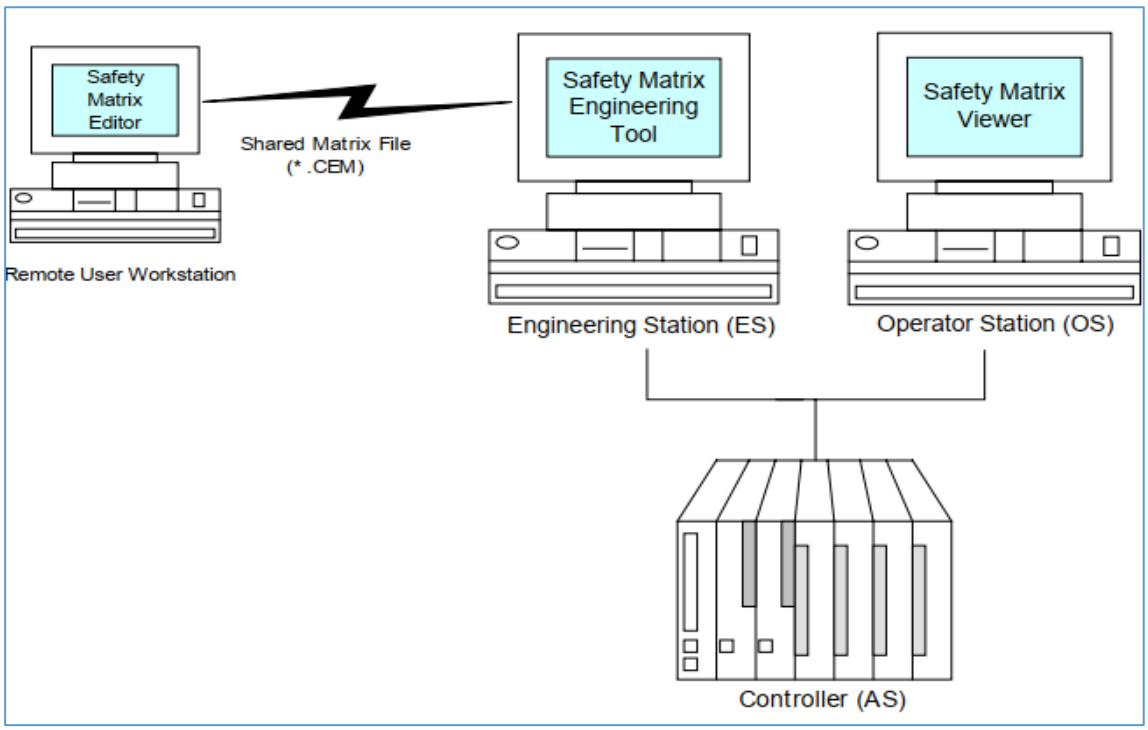
شکل ۹-٤- نمایی از پنجره نصب ابزارهای ایمنی ماتریس ایمنی

Safety Matrix Viewer

این ابزار برای نمایش ماتریس ایمنی در محیط OS (PCS 7 WinCC) استفاده می‌شود. ابزار Viewr لاجیک ماتریس ایمنی را در مد Runtime و در یک قالب سازگار با ابزار مهندسی «ماتریس ایمنی» نمایش می‌دهد. سطوح مختلف عملکرد اپراتور در خصوص «ماتریس ایمنی» از طریق حقوق کاربر در OS تعیین می‌شود.

Safety Matrix Editor

امکان ایجاد و مشاهده ماتریس ایمنی را در یک ایستگاه کاری راه دور (Remote Workstation)، بدون نیاز به محیط SIMATIC STEP 7 یا PCS 7 فراهم می‌کند. ماتریس‌های ایجادشده در ویرایشگر ماتریس ایمنی را می‌توان به‌راحتی با ایمیل یا روش دیگر به اشتراک گذاشت. تا در یک پروژه سیماتیک دیگر استفاده شود. شکل ۹-۵ جایگاه سه ابزار مرتبط با ماتریس ایمنی را به تصویر کشیده است.



شکل ۹-۵- ابزارهای ماتریس ایمنی در سیستم کنترل

9.3 Getting Started: Configuration

9.3.1 Creating a New Safety Matrix

در یک پروژه Step 7، لاجیک Cause and Effect در یک شیء ماتریس (Matrix) قرار می‌گیرد، جایی که در آن لاجیک مربوطه پیکربندی و به شکل یک فانکشن‌بلاک به یک چارت CFC انتقال داده می‌شود. هر ماتریس ایمنی تا ۱۲۸عدد cause و ۱۲۸عدد effect را با حداکثر ۵۰۰ سلول تقاطع پشتیبانی می‌کند. یک کنترل‌کننده برحسب ظرفیت حافظه کنترل‌کننده از ایجاد و اجرای چندین ماتریس ایمنی پشتیبانی می‌کند.

9.3.1.1 Step 1: Adding a Matrix object to a Project

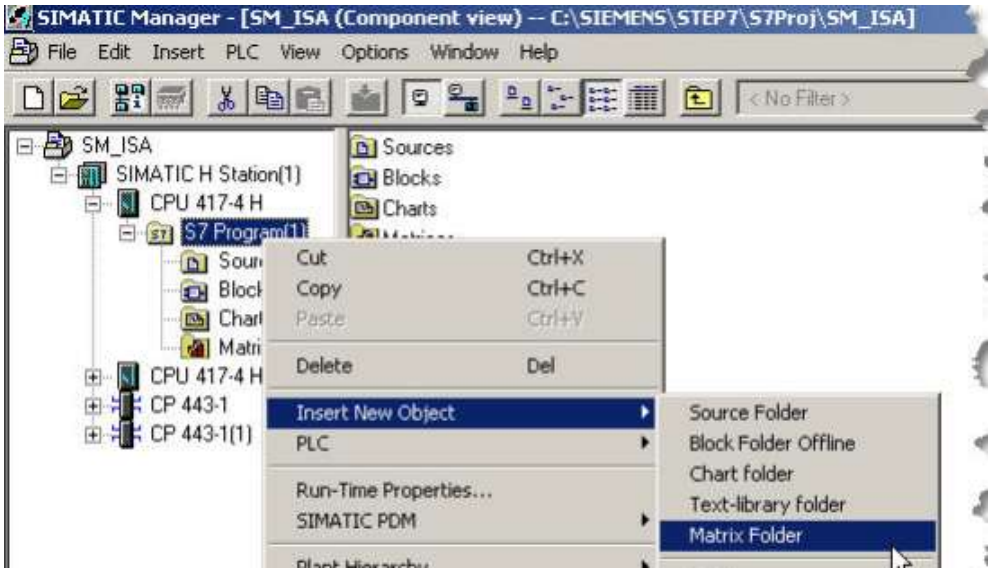
برای ایجاد یک ماتریس ایمنی (Logic Matrix1) به دو روش می‌توان عمل کرد.

روش اول ایجاد ماتریس ایمنی – ایجاد پوشه و ماتریس

در این روش ابتدا یک پوشه Matrix مشابه پوشه Charts ایجاد می‌کنیم و سپس یک ماتریس در داخل این پوشه ایجاد می‌گردد. برای ایجاد یک ماتریس ایمنی، گام‌های زیر اجرا می‌شود.

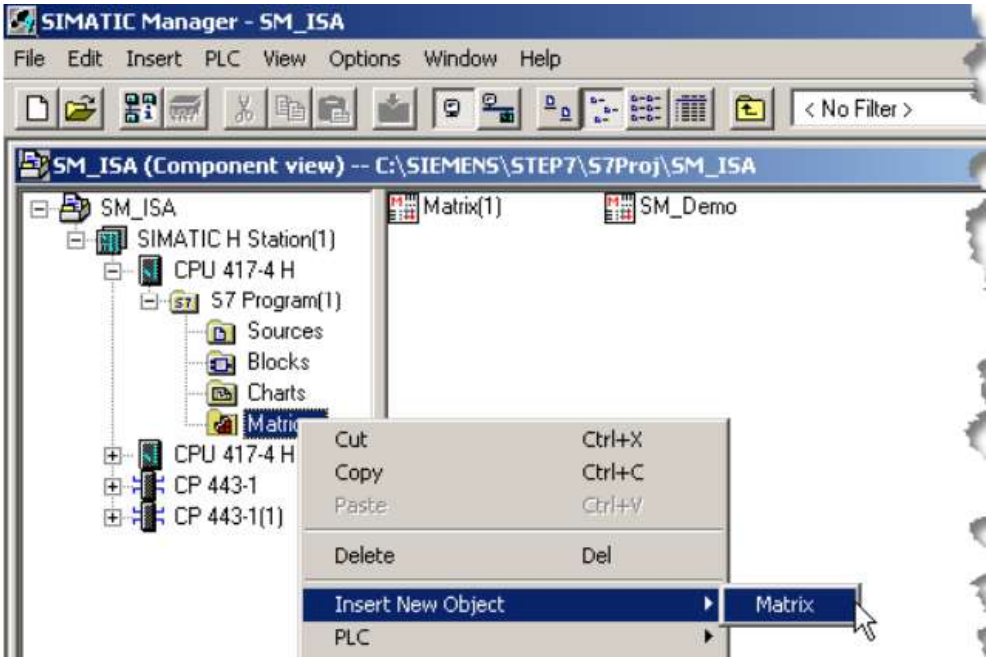
1. Open the project in SIMATIC Manager.
2. Navigate to the S7 Program folder within the project.
3. Right-click the S7 Program folder, and select Insert New Object >> Matrix Folder.

   A matrix folder will be added to the S7 Program.



شکل ۹-۶- ایجاد پوشه Matrix در پوشه S7-Programs

4. Right-click the **Matrix** folder, and select **Insert New Object** >> **Matrix**



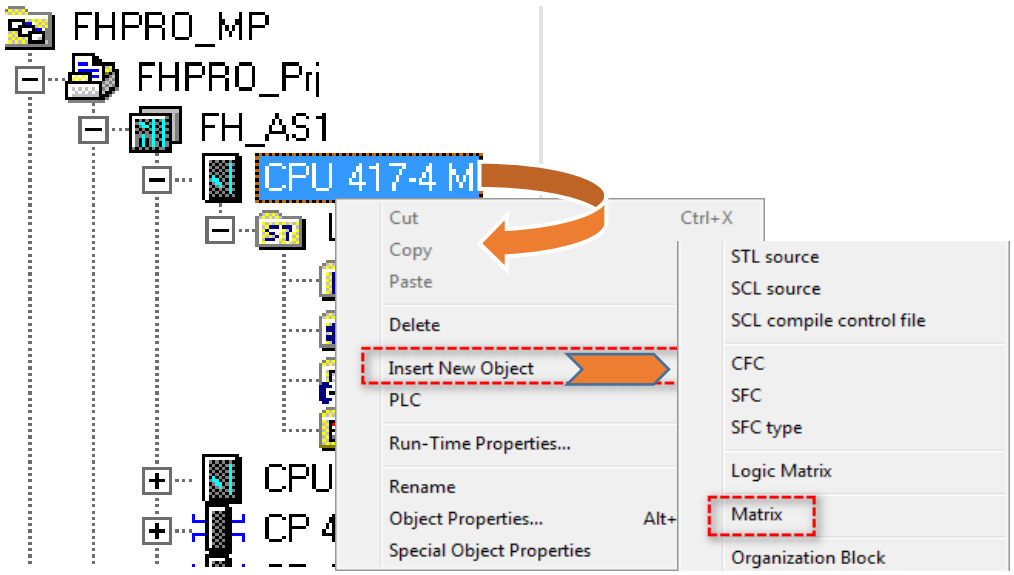
شکل ۹-۷- ایجاد یک پوشه ماتریس و شئ ماتریس در داخل آن

روش دوم – ایجاد یک ماتریس به‌صورت مستقیم در داخل CPU

در این روش پوشه Matrix به‌صورت خودکار ایجاد می‌شود. گام‌های زیر ایجاد ماتریس ایمنی را نشان می‌دهد.

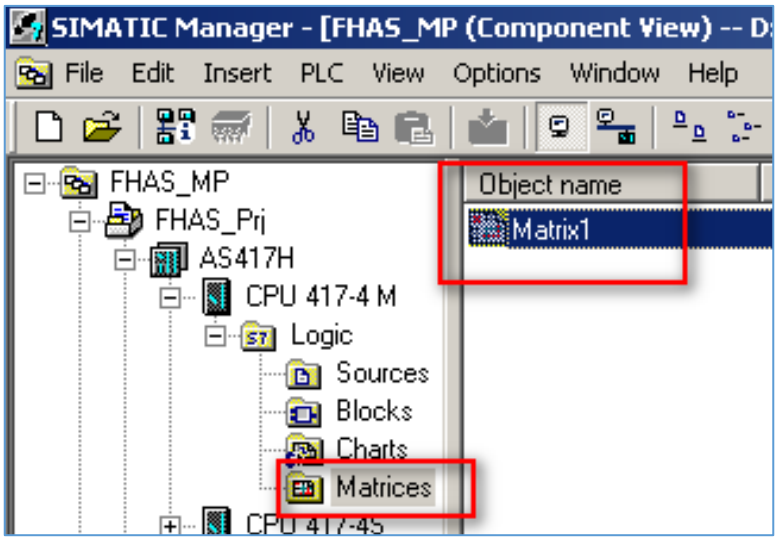
1. Open the Project in SIMATIC Manager.
2. Navigate to the S7 CPU within the Project.
3. Right-click the S7 CPU, and select Insert New Object >> Matrix.

   A matrix folder will be added to the S7 Program and A matrix Created whitin it.



شکل ۹-۸- درج یک ماتریس ایمنی به داخل یک CPU

با این کار یک پوشه در زیرمجموعه CPU بنام Matrices اضافه‌شده و در داخل آن یک فایل Matrix1 ایجاد می‌شود. توجه شود که پس از تکمیل ماتریس و کامپایل آن یک فایل CFC به همین نام در پوشه Charts ایجاد می‌گردد. نام آن را به یک نام دلخواه مانند Matix1_CFC تغییر می‌دهیم.



شکل ۹-۹- فایل Matrix1 در پوشه Matrices برای پیاده‌سازی لاجیک ارزیابی

Note

اجرای دستوراتی مانند copy/past بر روی بلاک‌های برنامه در ماتریس ایمنی (Matrix blocks) توصیه نمی‌شود. با این کار اتصال بین پروژه سیماتیک و ابزار مهندسی Safety Matrix از بین خواهد رفت و لاجیک درست کار نخواهد کرد. درصورتی‌که می‌خواهید از یک ماتریس یک کپی ایجاد کنید، برای این کار در محیط ابزار مهندسی Safety Matrix، ماتریس موجود را تحت نام دیگری ذخیره کنید.

9.3.2 Safety Matrix Editor Overview

پس از ایجاد یک ماتریس ایمنی در پنجره سیماتیک، با دوبار کلیک روی آن، ماتریس ایمنی در ویرایشگر مربوطه باز می‌شود. شکل ۹-۱۰ نمایی از پنجره اصلی ویرایشگر Safety Matrix را نشان می‌دهد. مطابق شکل سه فیلد اطلاعاتی در این ماتریس وجود دارد که عبارت است از:

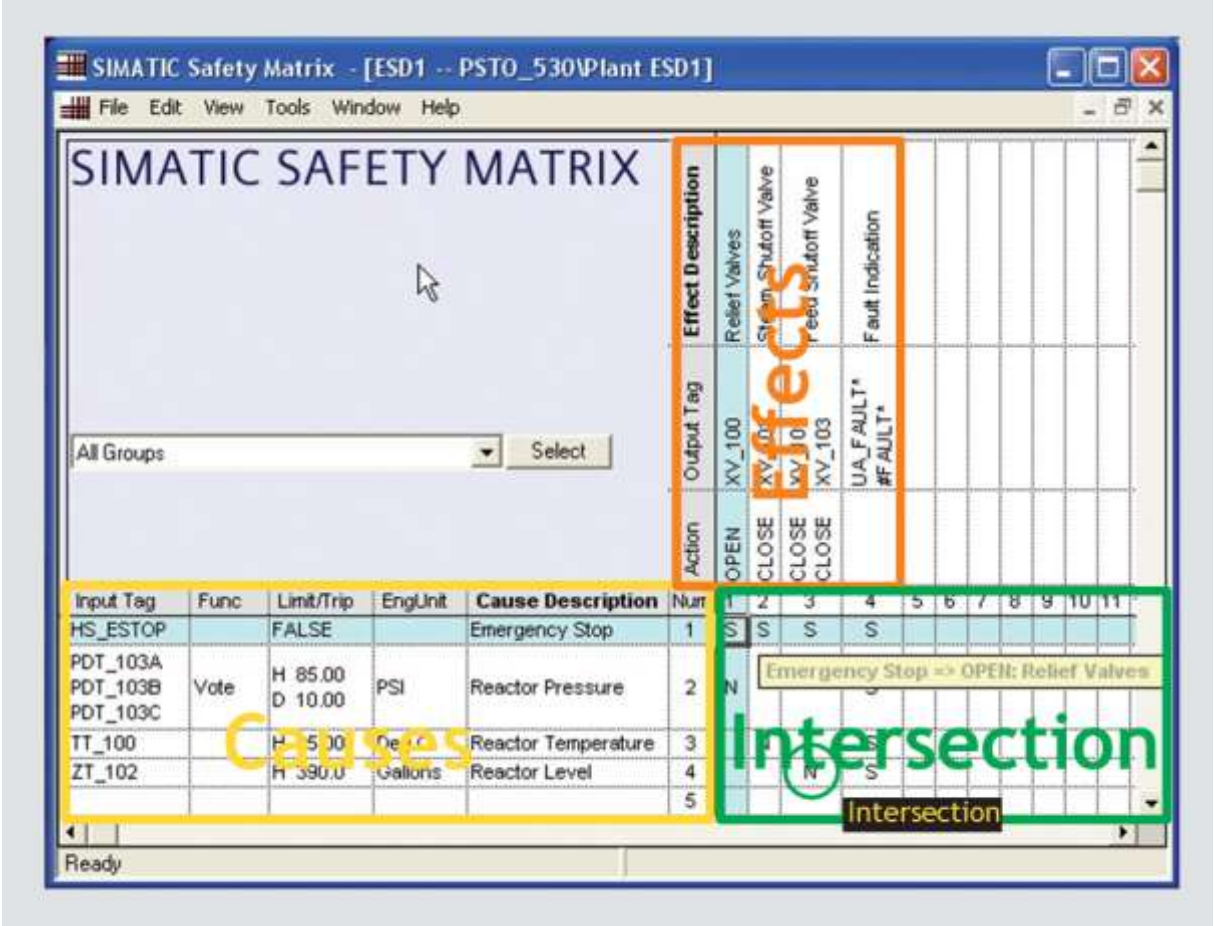
- Causes
- Effects
- Intersections

1- Cause

یک علت یک ردیف از ماتریس را اشغال می‌کند. فعال شدن فیلد علت، یک انحراف از فرایند را نشان می‌دهد. زمانی که وضعیت تگ تعریف‌شده برای یک علت فرآیندی (cause tag) (مانند بالا رفتن فشار) با شرایط پیکربندی‌شده توسط کاربر در فرآیند مطابقت دارد، فعال می‌شود.

2- Effect

یک اثر، یک ستون از ماتریس را اشغال می‌کند. این فیلد منعکس‌کننده انجام عملی در فرایند درنتیجه فعال شدن یک علت می‌باشد. با فعال شدن یک اثر، تگ مربوطه (Effect tag) به مقدار تعریف‌شده (Failsafe) تنظیم خواهند شد.



شکل ۹-۱۰- سه فیلد اطلاعاتی یک ماتریس ایمنی

3- Intersection

تقاطع، سلولی است که بین سطر و ستون «علت – اثر» مشترک است. این فیلد تعیین می‌کند که چگونه اثر به علت پاسخ می‌دهد. اگر تقاطع خالی باشد، به این معنی است که علت تأثیری در اثر ندارد. در سلول تقاطع حروف زیر درج می‌شود.

☞ N (not stored)

- S (set stored)
- V (override) or R (resetable override)

اگر یکی از موارد N، S در تقاطع درج شود، یک عامل فعال‌شده، باعث تریگر شدن اثر مرتبط شده و فرمان اثر اجرا می‌شود. حرف V نیز موجب اجرا نشدن اثر می‌گردد.

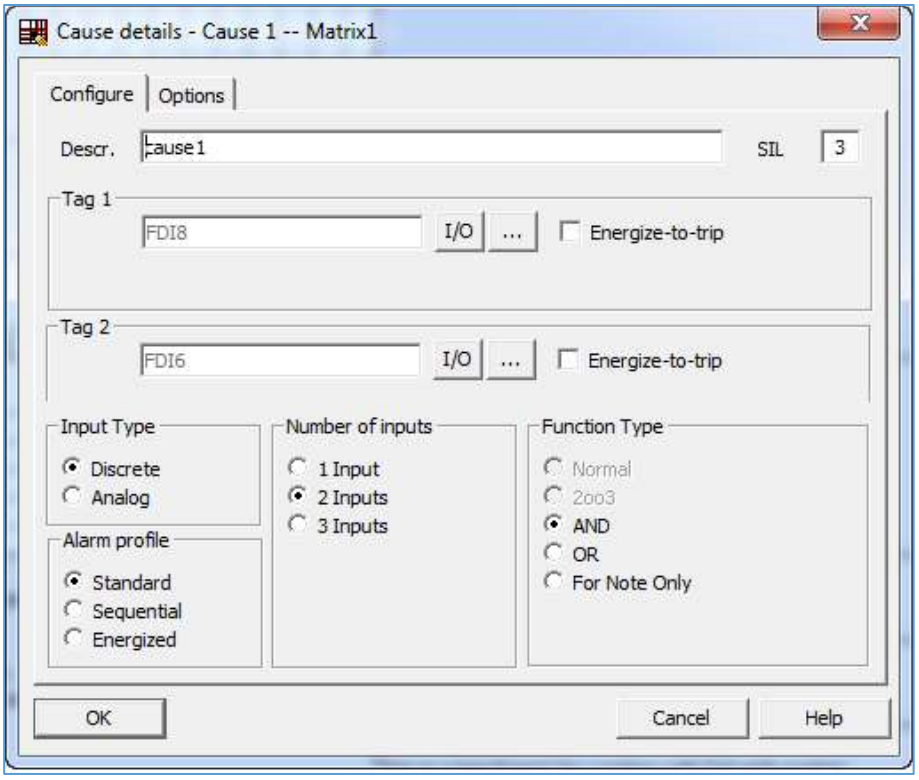
9.4 Configuring the Safety Matrix Logic

9.4.1 Adding Causes

گام اول برای پیکربندی یک ماتریس ایمنی اضافه کردن Causeها در سطرهای ماتریس و Effectها در ستون‌های آن می‌باشد.

9.4.1.1 Configure Tab

برای اضافه کردن یک Cause در یک سلول از سطر خالی اول دوبار کلیک می‌کنیم. پنجره پیکربندی به‌صورت شکل ۹-۱۱ نمایش داده می‌شود. این پنجره همچنین از طریق راست کلیک بر روی یک Cause موجود و انتخاب گزینه Edit Cause یا Change Cause باز می‌شود. مشاهده می‌شود که به هر سطر یک عنوان Cause با شماره سطر آن یک نام اختصاص می‌دهد.



شکل ۹-۱۱- پنجره تعریف و ایجاد یک Cause

9.7.7 Password for safety program

Password assignment

تعریف رمز برای برنامه F در پنجره SIMATIC Manager از طریق منو فرمان زیر انجام می‌شود.

SIMATIC Manager >> Options > Edit Safety Program

When Password requested?

مجوز دسترسی برنامه F پس از ورود صحیح رمز عبور برای یک ساعت معتبر می‌باشد. پس‌ازاین مدت‌زمان با هر اقدامی که نیاز به ورود رمز داشته باشد، پس از ورود رمز مجدد به یک بازه یک‌ساعته دیگر تنظیم مجدد می‌شود. در هر حالت می‌توان اعتبار زمانی رمز برنامه F را به‌صورت زیر لغو کرد.

۱- ابتدا از مسیر زیر پنجره Edit safety program باز می‌کنیم.

SIMATIC Manager >> Options > Edit safety program

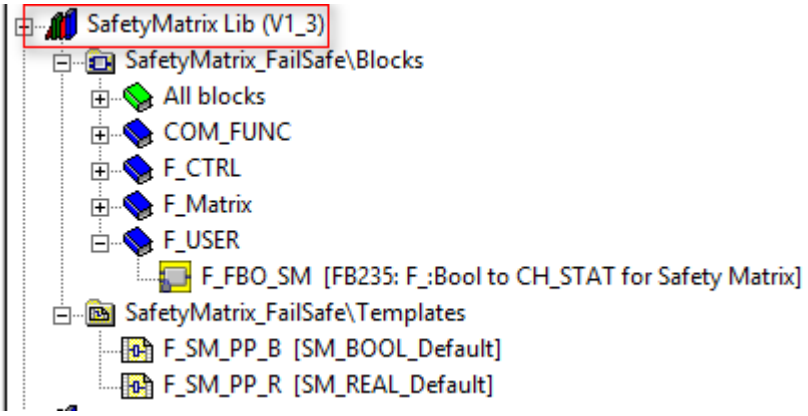
۲- سپس بر روی دکمه Password کلیک کرده و در پنجره بازشده بر روی Logout کلیک می‌کنیم.

در مواقع زیر رمز برنامه F از کاربر درخواست می‌شود.

- ذخیره تغییرات اساسی در یک ماتریس ایمنی
- انتقال ماتریس ایمنی به برنامه ایمنی (Safety Matrix to safety program)
- کامپایل تغییرات در برنامه ایمنی
- دانلود تغییرات در برنامه ایمنی
- شروع اولین عملیات اپراتوری روی ماتریس ایمنی از طریق Secure Write در حالت آنلاین
- فعال و غیرفعال کردن حالت ایمنی

9.8 Safety Matrix Library

با نصب بسته نرم‌افزاری Safety Matrix کتابخانه مربوطه نیز نصب‌شده و در محیط ویرایشگر CFC ظاهر می‌شود. بلاک‌های این کتابخانه همانند دیگر کتابخانه‌ها در گروه‌های مختلف دسته‌بندی‌شده است. به طور معمول خود سیستم از این بلاک‌ها در پیاده‌سازی لاجیک ماتریس ایمنی در CFC استفاده می‌کند.



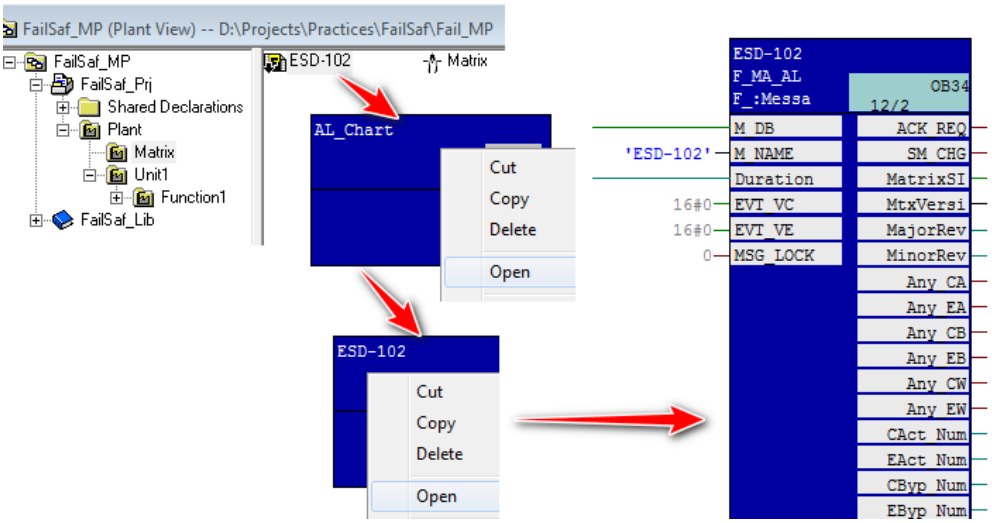
شکل ۹-۵۹- کتابخانه بلاک‌های ماتریس ایمنی

9.8.1 F_Matrix Family

9.8.1.1 Safety Matrix message block F_MA_AL

یک بلاک آلارم برای تولید پیام‌های ماتریس ایمنی و انتقال آن‌ها به سیستم OS می‌باشد. بلاک آیکونی هم که برای یک ماتریس ایمنی در OS ایجاد می‌شود، مرتبط با این بلاک می‌باشد.

بلاک F_MA_AL به‌صورت خودکار پس از انتقال ماتریس ایمنی به برنامه در داخل چارت تودرتوی AL_Chart واقع در چارت هم نام ماتریس ایمنی درج‌شده و ورودی/خروجی‌های آن پیکربندی می‌شود.



شکل ۹-۶۰: بلاک آلارم یک ماتریس ایمنی

نکته: در صورت حذف تیک Create Block icon در پنجره پراپرتی این بلاک، برای ماتریس ایمنی بلاک آیکون ایجاد نمی‌شود.

M_Name: Matrix name

در این ورودی نام ماتریس ایمنی ('ESD-102') وارد می‌شود.

MSG_LOCK

درصورتی‌که به این ورودی مقدار 1 داده شود. ایجاد پیام‌ها غیرفعال می‌شود.

9.8.1.2 Cause Message block: F_SC_AL

با فعال کردن گزینه Alarm Palcing در پنجره سربرگ Cause به‌صورت خودکار یک بلاک F_SC_AL در داخل چارت تودرتوی AL_Chart برای هر Cause درج می‌شود. پس از کامپایل OS برای هر Cause یک بلاک آیکون نیز ایجاد می‌شود.

M_Name: Cause name

به این ورودی نام Cause (‘LS101’) وارد می‌شود.

9.8.1.3 Effect message block F_SE_AL Block

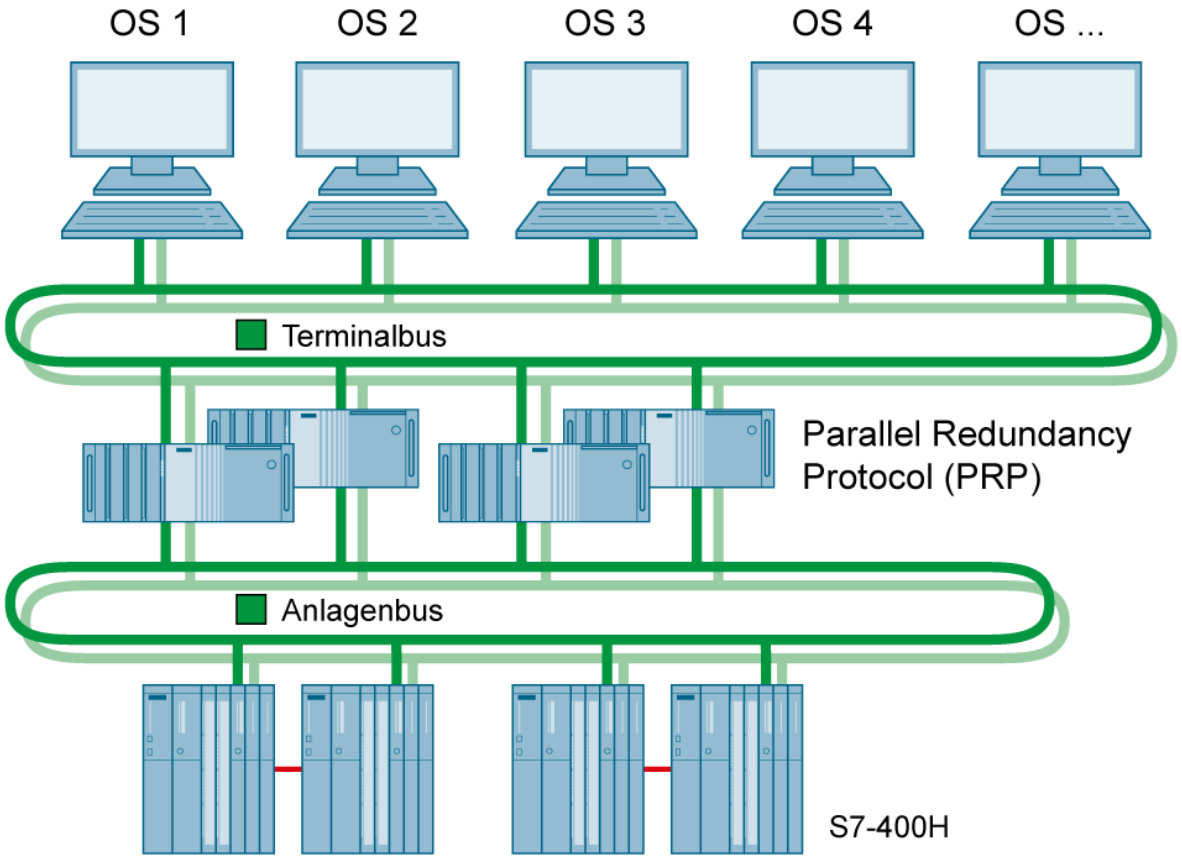
با فعال کردن گزینه Alarm Palcing در پنجره سربرگ Effect، به‌صورت خودکار یک بلاک F_SE_AL در داخل چارت تودرتوی AL_Chart برای هر Effect درج می‌شود. پس از کامپایل OS برای هر Effect یک بلاک آیکون نیز ایجاد می‌شود.

9.9 References

[1] SIMATIC Industrial Software Safety Matrix, Configuration Manual, 06/2015, A5E33216084-AB

فصل دهم

شبکه در سیستم S7-400 H/FH



Communication Principle

Chapter 10

Learning targets

محتوای این فصل شامل مباحث زیر می‌باشد:

- پیکربندی‌های مختلف شبکه ریداندانت بین سیستم‌های S7-400H
- پیکربندی اتصال ریداندانت سیستم OS به سیستم H
- پیکربندی‌های مختلف اتصال دستگاه‌های HMI به سیستم H

Abbreviations

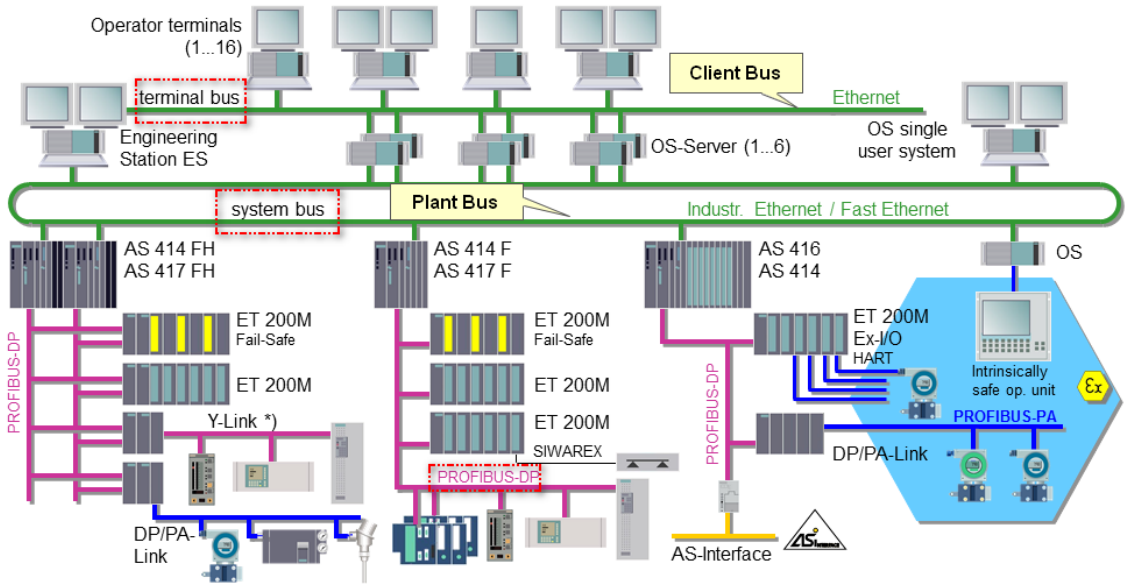
CCR	Centeral Control Room
UCP	Unit Control Panel
AS	Automation Station or Automation System
OS	Operator Station
SFC	System Function
PCS	Process control System
FH	Fail-Safe & High Available
OB	Organization Block
RIO	Remote I/O
EUC	Equipment Under Control
SFB	System Function Block

10.1 PCS7 Networks

به‌طورکلی در یک پلنت مبتنی بر سیستم PCS7 در صورت استفاده از معماری Client/Server (سطح مانیتورینگ) چهار شبکه خواهیم داشت.

- شبکه فیلدباس PA یا ASI در سطح فیلد؛
- شبکه Profibus DP برای ارتباط بین کنترل‌کننده S7-400H/FH و رک‌های ET 200،دستگاه‌های درایو و ....
- شبکه در سطح کنترل (Plant Bus/System Bus) مبتنی بر پروتکل اترنت صنعتی برای ارتباط بین کنترل‌کننده‌ها و ایستگاه‌های OS Server؛
- شبکه اترنت با عنوان Client/Terminal Bus برای ارتباط بین OS Serverها و ایستگاه‌های Client

شکل ۱۰-۱ نمونه معماری شبکه در یک سیستم PCS7 مبتنی بر کنترل‌کننده‌های S7-400H/FH نشان می‌دهد.



شکل ۱۰-۱- انواع شبکه‌ها در یک سیستم PCS7 مبتنی بر S7400FH/H

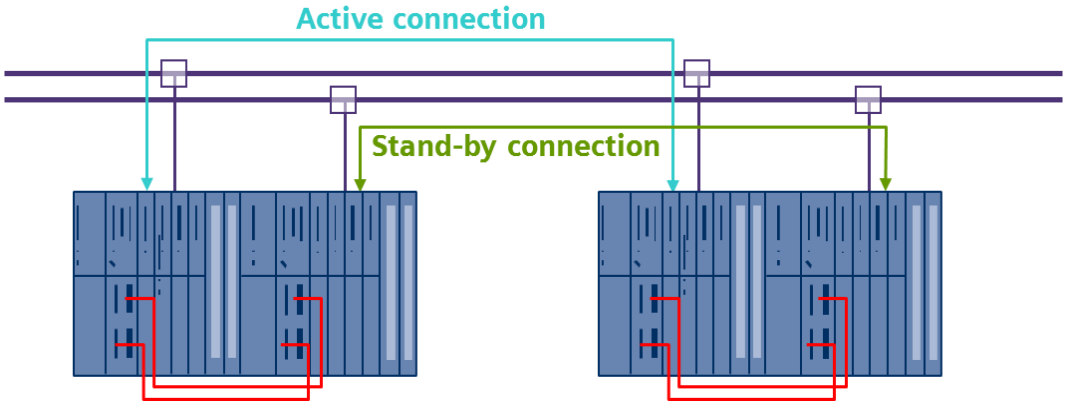
10.2 Fault-tolerant Connections

برقراری ارتباطات تحمل‌پذیر خطا (Fault-tolerant) بین دو یا چند سیستم از طریق ایجاد اتصال ریداندانت حاصل می‌شود. بین ایستگاه‌های مختلف AS و OS دو نوع اتصال ریداندانت (Redundant) می‌توان ایجاد کرد.

☑ اتصال ریداندانت از یک سیستم AS به یک یا چند سیستم AS دیگر (Other H stations)؛

☑ اتصال ریداندانت از یک سیستم AS به یک یا چند سیستم OS؛

نوع اول جهت اتصال به دیگر سیستم‌های 400H/FH و اتصال نوع دوم جهت اتصال به کامپیوترهای OS استفاده می‌شود. در اتصال نوع دوم نصب نرم‌افزار S7-REDCONNECT و لایسنس مربوطه موردنیاز است.



شکل ۱۰-۲- اتصالات ریداندانت بین دو سیستم ریداندانت H

توجه شود که برای داشتن یک سیستم تحمل‌پذیر خطای مبتنی بر 400H، در هر دو زیرسیستم بایستی اجزای پیکربندی سخت‌افزار یکسان باشد. بسته به نوع شبکه‌ای که برای ایجاد ارتباط ریداندانت استفاده می‌شود، از ماژول‌های CP زیر می‌توان استفاده کرد:

- For Industrial Ethernet >> CP 443-1
- For PROFIBUS :CP 443-5 Extended (not configured as DP master system)

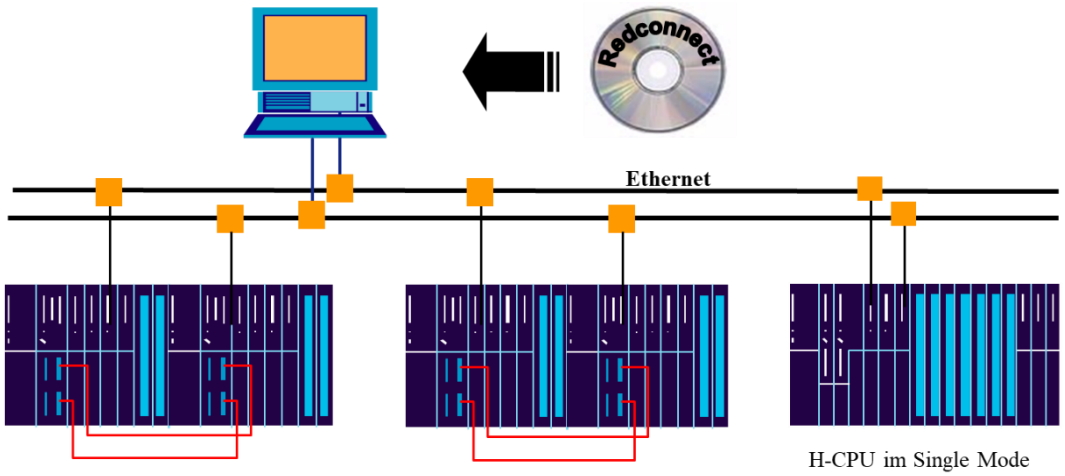
10.2.1 Ethernet Communication Configurations: High Available Communication

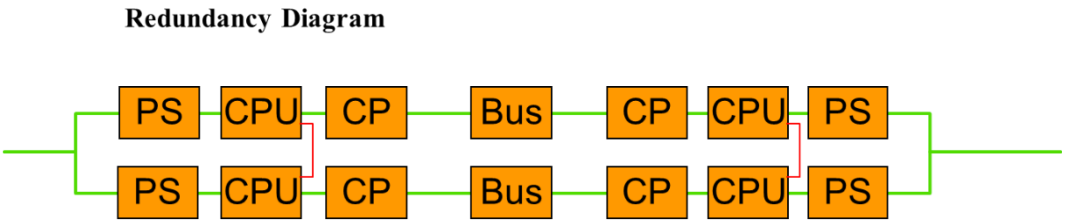
برای پیاده‌سازی ارتباط ریداندانت مبتنی بر اترنت بین دو یا چند سیستم H، با توجه به کابل شبکه و ماژول‌های CP اترنت، پیکربندی‌های مختلفی را می‌توان پیاده کرد. برخی از ساختارها برای پیکربندی ارتباط ریداندانت عبارت است از:

1- Redundant communication Configuration with redundant bus
2- Redundant communication Configuration with redundant bus & CP modules
3- Redundant communication Configuration with single bus
4- Redundant communication Configuration with ring bus

High Available Communication Configuration with redundant Bus

شکل ۱۰-۳ یک پیکربندی از شبکه اتوماسیون S7-400H/FH را نشان می‌دهد که در آن شبکه ارتباطی (کابل اترنت) ریداندانت می‌باشد.

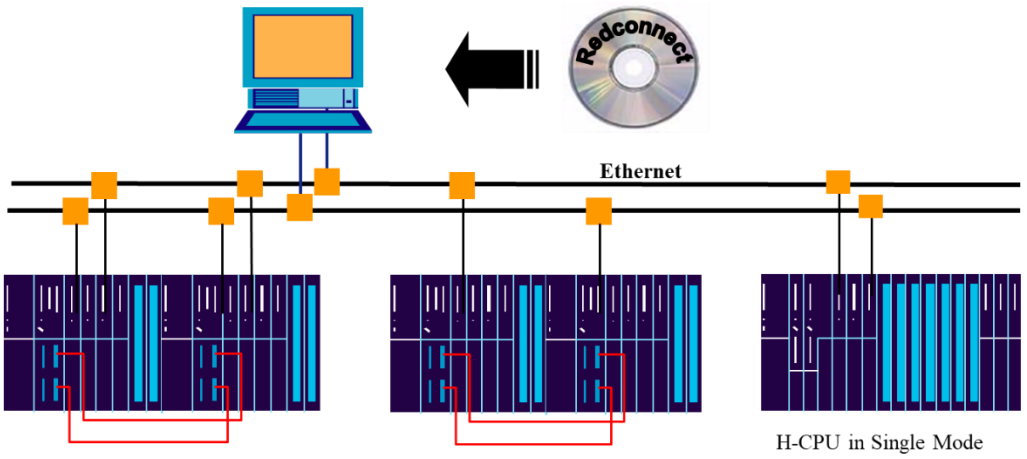


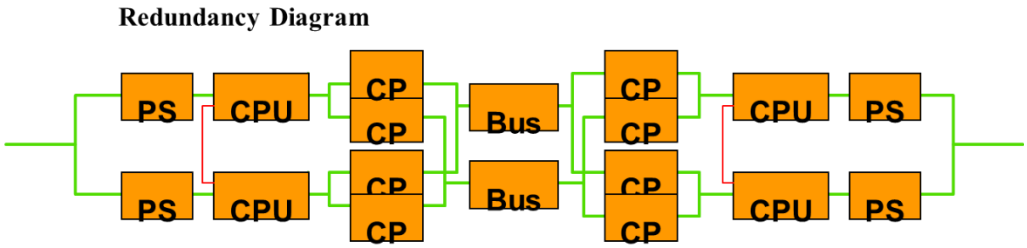


شکل ۱۰-۳- پیکربندی ارتباط ریداندانت بین دو سیستمH/400FH

2. High Available Communication - Configuration with redundant Bus and redundant CP

شکل ۱۰-۴ یک پیکربندی از شبکه اتوماسیون S7-400H/FH را نشان می‌دهد که برای افزایش در دسترس بودن در سطح ماژول شبکه، در هر سمت از ماژول CPU، از دو عدد CP443-1 استفاده‌شده است. این طرح ارتباطی هم در سطح شبکه و هم در سطح ماژول شبکه، ریداندانت می‌باشد.

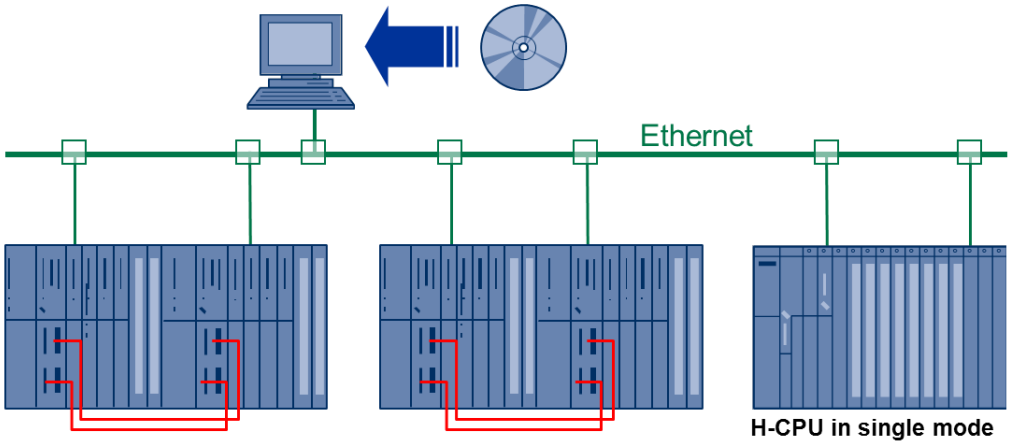




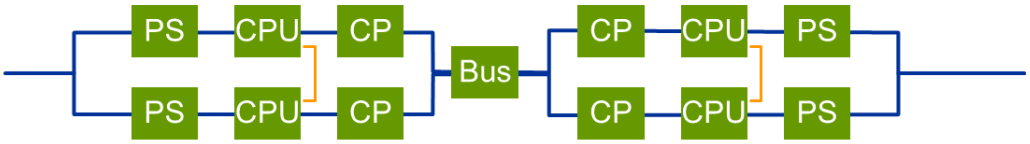
شکل ۱۰-٤- پیکربندی ارتباطات اترنت با ریداندانسی در سطح کارت CP و شبکه

3. Redundant communication Configuration with single bus

پیکربندی شکل ۱۰-۵ حالتی را نشان می‌دهد که در آن سیستم‌های S7-400FH/H ریداندانت تنها از طریق یک کابل به هم متصل شده‌اند. لذا این طرح ارتباطی، در سطح کابل شبکه و ماژول اترنت ریداندانت نمی‌باشد.



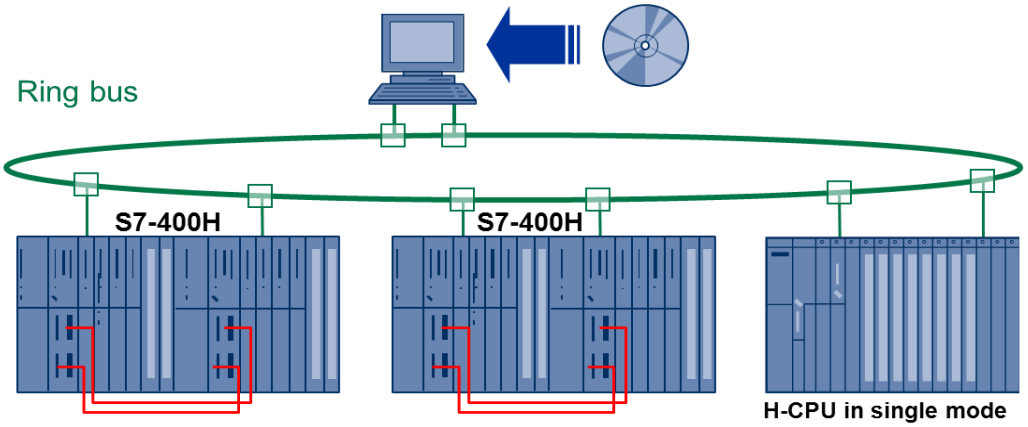
Equivalent circuit diagram:



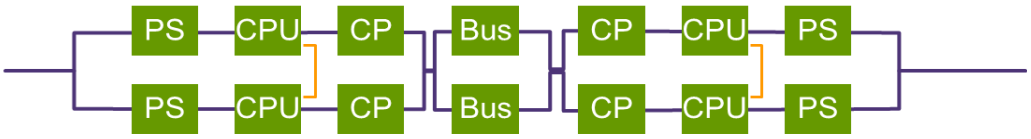
شکل ۱۰-۵- پیکربندی سیستم H با باس تکی

4. Redundant Communication Configuration with ring bus

شکل ۱۰-۶ نیز حالتی را نشان می‌دهد که در آن سیستم‌های ریداندانت S7-400FH/H دارای کابل و ماژول شبکه ریداندانت نیستند. ولی با استفاده از یک کابل در یک ساختار حلقوی به هم متصل شده‌اند. لذا این طرح ارتباطی در سطح شبکه از نوع تحمل‌پذیر خطا هست ولی در سطح ماژول اترنت ریداندانت نمی‌باشد.



Equivalent circuit diagram:



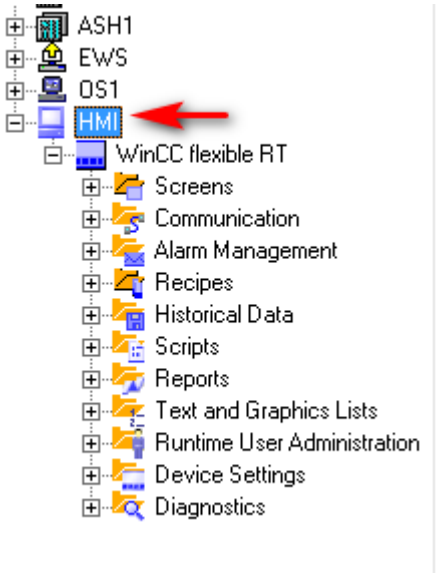
شکل ۱۰-۶- پیکربندی سیستم H با باس حلقوی (Ring)

10.3 Connecting HMI or Monitoring PC to H-Stations

10.3.1 Introduction

یکي از اجزای اصلی یک سیستم اتوماسیون فرآیند، سیستم مانیتورینگ (HMI/SCADA) می‌باشد. بسته به‌اندازه یک پروژه FH، سیستم مانیتورینگ ممکن است به دو صورت کلی پیاده‌سازی شود:

۱- برای پلنت‌های بزرگ مبتنی بر سیستم‌های DCS در یک اتاق کنترل مرکزی موسوم به CCR پیاده‌سازی می‌شود. در این حالت از کامپیوترهای مختلف مانند OS Server و OS Client (در سیستم PCS7 زیمنس) استفاده می‌شود.



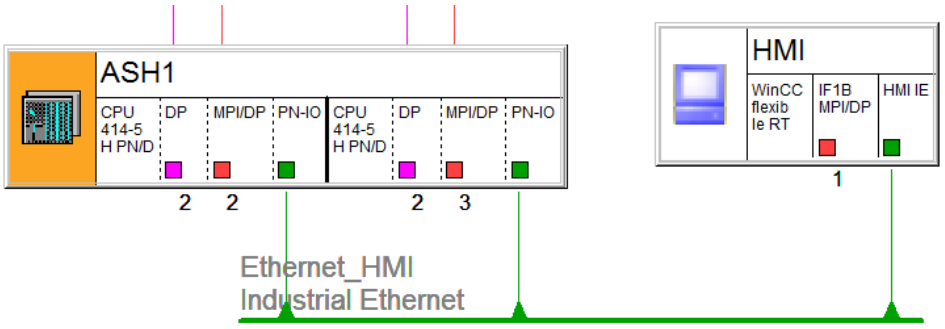
شکل ۱۰-۳۱- درج ایستگاه SIMATIC HMI

۳- سیستم H را با دو عدد CP 443-1 پیکربندی و IP ماژول‌های CP 443-1 را به‌صورت زیر تنظیم کنید.

- CPU_1: 192.168.0.130
- CPU_2: 192.168.0.131

۴- پروژه را در پنجره NetPro بازکرده و ایستگاه H را از طریق ماژول‌های اترنت به یک شبکه اترنت متصل کنید. همچنین پنل اپراتوری را به همان شبکه اترنت متصل کنید.

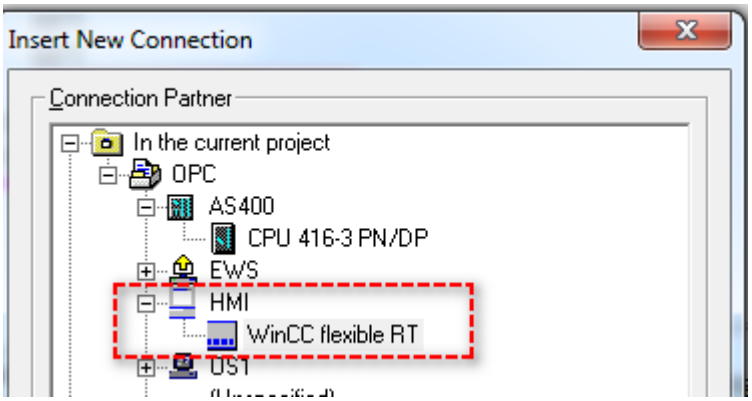
- MP: 192.168.0.3



شکل ۱۰-۳۲- پیکربندی ارتباط بین HMI و سیستم H از طریق اترنت

۵- دو عدد اتصال از نوع S7 Connection با مشخصات زیر در NetPro ایجاد می‌کنیم.

- S7 connection_1 → CPU417-4 H to "WinCC flexible RT"
- S7 connection_2 → CPU417-4 H(1) to "WinCC flexible RT



Local ID	Partner ID	Partner	Type	Active connection	Subnet
S7 connection_1	1	ASH1 / CPU 414-5 H PN/DP	S7 connection	Yes	Ethernet_HMI [IE]
S7 connection_2	2	ASH1 / CPU 414-5 H PN/D...	S7 connection	Yes	Ethernet_HMI [IE]

شکل ۱۰-۳۳- ایجاد اتصال از CPUهای H به ایستگاه HMI در NetPro

Step 2: WinCC Flexible Configuration

۱- در پنجره NetPro تنظیمات را Save & Compile کرده و آن را می‌بندیم.

۲- پروژه WinCC Flexible RT را بازکرده و از بخش Communication گزینه Connections را با دو بار کلیک باز می‌کنیم.

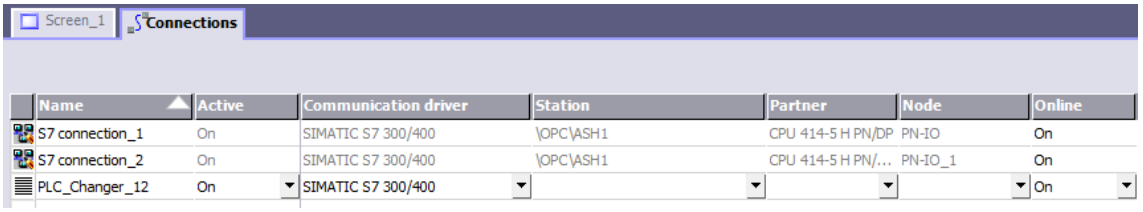
۳- مشاهده می‌شود که در قسمت Connections به‌صورت خودکار (درنتیجه کامپایل NetPro) دو اتصال به شرح زیر ایجادشده است.

- S7_Connection_1
- S7_Connection_2

اتصال PLC_1 به CPU اول و اتصال PLC_2 به CPU دوم متصل می‌شود.

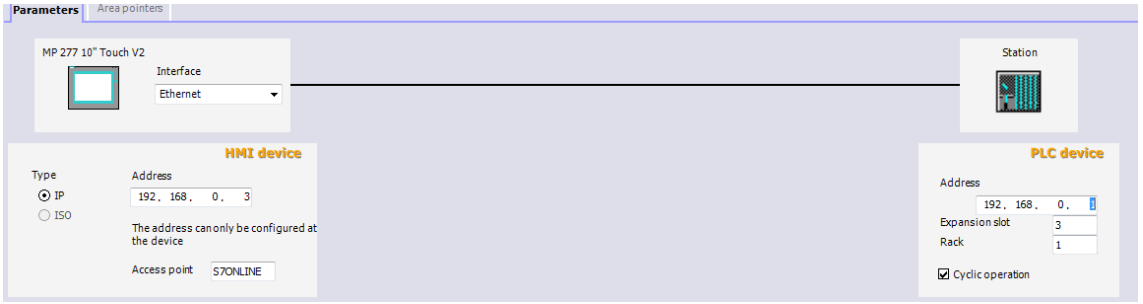
۴- حال با توجه به اینکه دو تا اتصال تعریف‌شده است بایستی تگ‌های WinCC برای هر اتصال جداگانه یعنی دو بار تعریف شود. برای حل این مشکل یک اتصال دیگر بنام PLC_Changer_12 را به‌صورت دستی ایجاد می‌کنیم. به‌طوری‌که تگ‌های WinCC در این اتصال ساخته می‌شوند و عمل تعویض بین CPUها به‌صورت نرم‌افزاری صورت می‌گیرد.

توجه شود که این اتصال به هیچ‌یک از CPUهای سیستم H متصل نشده است و تنها برای آن درایور ارتباطی S7-300/400 تعریف‌شده است.



شکل ۱۰-۳٤- اتصال‌های ایجاد شده در محیط WinCC Flexible

آدرس IP اتصال سوم PLC_Changer_12 بایستی مطابق با آدرس IP یکی از دو اتصال اول باشد. همچنین اطمینان حاصل شود که اسلات و شماره رک سیستم H را به‌درستی وارد کنید.



شکل ۱۰-۳۵- تنظیمات اتصال سوم

Step 3: Tag parameterization in WinCC flexible

برای تشخیص فالت و انتقال خودکار از یک CPU به CPU دیگر نیاز است که یک سری تگ در WinCC ایجاد کنیم. برای این کار در درخت پروژه زیرمجموعه Communication > Tags را بازکرده و تگ‌های مطابق جدول زیر را ایجاد می‌کنیم.

جدول ۹-۱: ایجاد تگ‌های WinCC برای تعویض اتصال ریداندانت

Variable name	Connection	Data type/ address	Acquisition	Acquisition cycle	Use
trigger_PLC1	S7_Connection_1	Bool/M0.4	Cyclic continuous	500ms	Trigger for the VB scripts
trigger_PLC2	S7_Connection_2	Bool/M0.4	Cyclic continuous	500ms	Trigger for the VB scripts
con_state_PLC1	Internal tag	Integer	Cyclic when used	1s	Connection status tags
con_state_PLC2	Internal tag	Integer	Cyclic when used	1s	Connection status tags
connected_to	Internal tag	String	Cyclic when used	1s	Connection memory of the data link
Clock memory	PLC_Chang er_12	Byte/MB0	Cyclic continuous	100ms	Clock memory

Step 4: Script creation and implementation in WinCC flexible

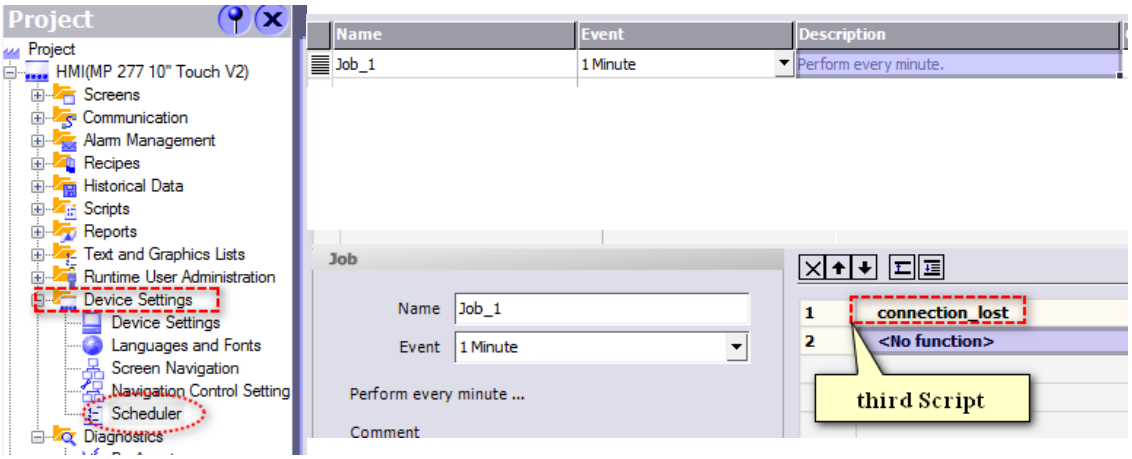
سه فایل اسکریپت را در درخت پروژه در زیرمجموعه Scripts > Add script اضافه می‌کنیم. برای محتوای کد هر اسکریپت از فایل‌های txt معرفی‌شده در بالا (قسمت 9.7.1) استفاده کنید. توجه شود که اجرای اسکریپت‌های VB در WinCC به یک تریگر سیکلیک نیاز دارند. برای این کار، باید اسکریپت‌های Connection_plc1 و Connection_plc2 را به تگ‌های تریگر متصل کنیم.

- Communication > Tags “trigger_PLC1” Properties> Events > Change in Value> Select script Connection_PLC1.
- Communication > Tags “trigger_PLC2” Properties > Events > Change in Value> Select script “Connection_PLC2”.

اسکریپت سوم که connection_lost نام دارد، برای تشخیص قطعی اتصال استفاده می‌شود. برای این کار ابتدا یک اسکریپت به همین نام ایجاد کرده و محتوای کد آن را از فایل txt مربوطه کپی می‌کنیم.

سپس یک scheduler ایجاد کرده و این اسکریپت را معرفی می‌کنیم..

Device Settings > Scheduler > Add task with the event "1 Minute" and the function “connection_lost”



شکل ۱۰-۳۶- پیکربندی یک scheduler

نکته: پنل و ایستگاه SIMATIC H باید از طریق اتصال PLC_Changer_12 ارتباط برقرار کنند. اتصالات S7_Connection_1 و S7_Connection_2 برای عمل تعویض بین دو CPU در مواقع خطا هستند. بنابراین نباید بار(Load) این اتصالات را با سایر ارتباطات دیگر افزایش داد. همچنین توجه شود که آدرس‌های IP برای تغییر اتصال بایستی در اسکریپت‌های “connection_PLC1” و “connection_PLC1” در تابع ChangeConnection تنظیم شوند.

10.6 References

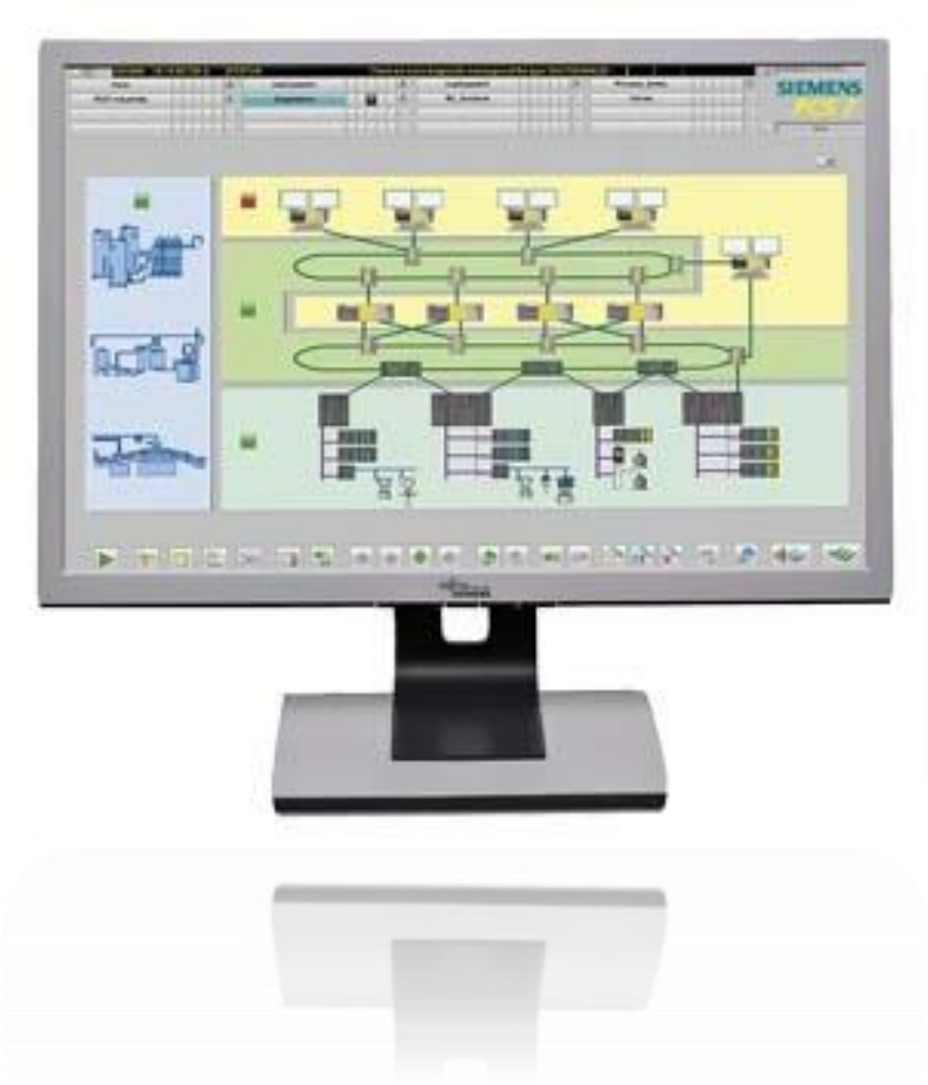
[1] How do you connect a panel to a SIMATIC H station, FAQ March 2010?

[2] How do you connect an operator panel (ProTool) to an H system (S7-400H)?

فصل یازدهم

تعمیرات و نگهداری سیستم

S7-400FH



S7-400 FH

Diagnostic & Maintenance

Chapter 11

11 Startup & Maintenance

Learning targets

محتوای این فصل شامل مباحث زیر می‌باشد.

- راه‌اندازی سیستم‌های S7-400FH
- عیب‌یابی سیستم S7-400H/FH با صفحات Diagnostic
- خواندن وضعیت سیستم با تابع سیستمی SFC 51
- روش‌های به‌روزآوری سیستم‌عامل CPU
- استفاده از حافظه Flash برای برنامه‌های F
- نحوه تعویض کارت‌های حافظه CPU

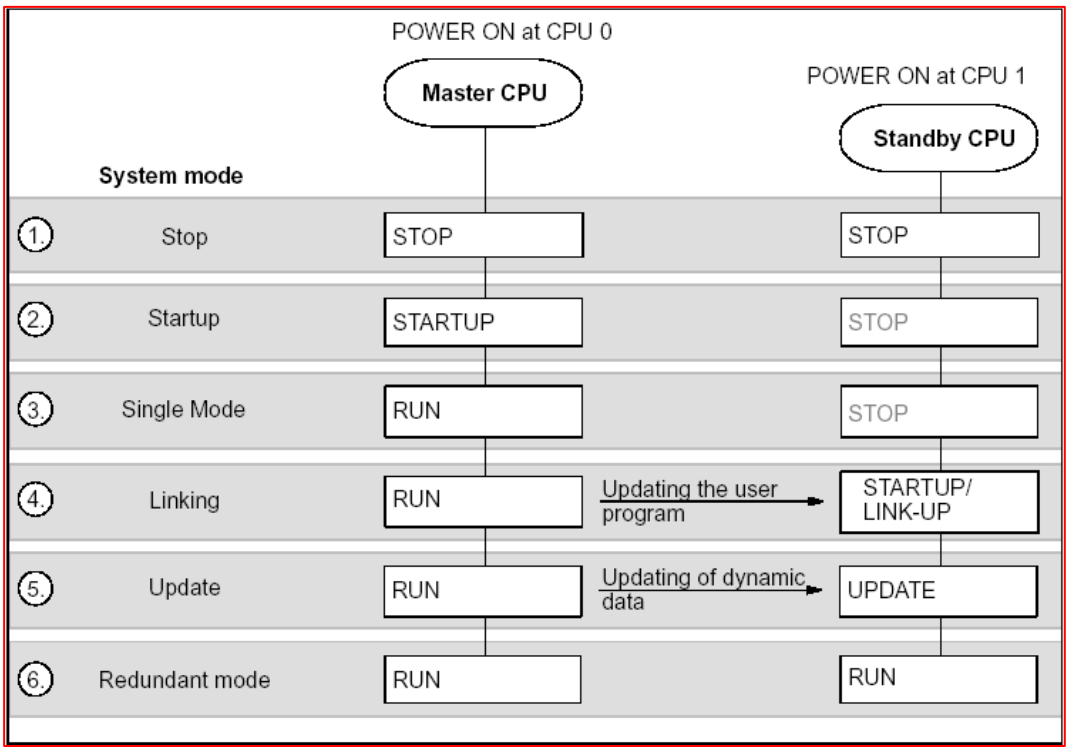
Abbreviations

AS	Automation Station or Automation System
BAF	Batery fault
BUSF	Bus fault
CPU	Centeral Processing Unit
DC	Direct Current
DR	Data Record
EXTF	External Fault
FH	Fail-Safe & High Available
FRCE	Force
INTF	Internal Fault
MS	Maintenance Station
MRES	Memory Reset
OB	Organization Block
OS	Operator Station
PCS	Process control System
REDF	Readundancy Fault
RIO	Remote I/O
SFB	System Function Block
SFC	System Function

Contents

11.1 S7400H Startup

پس از نصب و مونتاژ اجزاء سخت‌افزاری یک سیستم S7-400H، برای راه‌اندازی سیستم H ابتدا منبع تغذیه واقع در رک ۰ و سپس رک ۱ را روشن می‌کنیم. بعد از روشن شدن سیستم، چراغ تغذیه (DC 5V و DC 24V) به رنگ سبز روشن‌شده و سیستم H مطابق شکل ۱۱-۱ راه‌اندازی می‌شود.



شکل ۱۱-۱: مراحل بالا آمدن سیستم S7 400H

جدول ۱۱-۱ یک توصیف خلاصه از مراحل بالا آمدن سیستم S7 400H را نشان می‌دهد.

جدول ۱۱-۱: توصیف مراحل راه‌اندازی سیستم S7-400H

Step	Description
1	بعد از روشن شدن تغذیه، هر دو CPU (CPU 0 and CPU 1) در وضعیت STOP قرار دارد.
2	ماژول CPU 0 به وضعیت Startup منتقل‌شده و OB 100 یا OB 102 بر اساس مد راه‌اندازی تعیین‌شده اجرا می‌شود.
3	درصورتی‌که فرآیند Startup موفقیت‌آمیز باشد، ماژول Master (CPU 0) به مد standalone سوئیچ می‌کند. ماژول Master برنامه کاربر را به‌تنهایی (Solo) اجرا می‌کند. توجه شود که در زمان انتقال به وضعیت سیستمی LINK-UP نمی‌توان بلاک‌ها را مانیتور کرد و هیچ جدول تگی فعال نیست.

4	با درخواست LINK-UP از سوی ماژول Standby، هر دو ماژول master و standby برنامه خود را مقایسه کرده و در صورت وجود هرگونه اختلاف، ماژول master برنامه ماژول Standby را به‌روزآوری می‌کند.
5	بعد از موفقیت‌آمیز بودن مرحله LINK-UP، ماژول master داده دینامیکی ماژول Standby را به‌روزآوری می‌کند. داده‌های دینامیک شامل ورودی‌ها، خروجی‌ها، تایمرها، شمارنده‌ها و حافظه‌های بیتی و بلاک‌های داده DB می‌باشد. به دنبال اجرای update، محتوای حافظه هر دو CPU یکسان می‌باشد.
6	بعد از update هر دو CPU در مد RUN هستند. هر دو CPU برنامه را در مد سنکرون پردازش می‌کنند. توجه شود که وضعیت ریداندانت فقط با ماژول‌های CPU با نسخه سیستم‌عامل یکسان پشتیبانی می‌شود.

11.1.1 CPU Self Test

درصورتی‌که سیستم H برای اولین بار پس از مونتاژ سیستم و روشن کردن تغذیه، روشن می‌شود، بعد از روشن کردن CPU چراغ Stop روی CPUها به رنگ زرد و چشمک‌زن می‌شود و تا زمانی که چراغ زرد Stop به‌صورت چشمک‌زن بوده و قطع نشده است، نمی‌توان با CPUها ارتباط داشت و آن‌ها را برنامه‌ریزی کرد. در این حالت CPU در مد اجرای «خود آزمون» (Self Test) می‌باشد. در این آزمون که معمولاً مدت‌زمان آن حدود ۱۰ الی ۱۵ دقیقه می‌باشد، تمام قسمت‌های مختلف CPU چک می‌شود.

بعدازاینکه سیستم یک‌بار تست شد و به‌عبارت‌دیگر «خود آزمون» را انجام داد. در دفعات بعد که برق قطع و وصل شود، اگر باتری روی ماژول تغذیه (PS) موجود بوده و سالم باشد، عمل «خود آزمون» کوتاه خواهد بود. ولی اگر باتری وجود نداشته باشد و یا سوئیچ مربوطه در وضعیت خاموش باشد، با قطع و وصل شدن برق، روند «خود آزمون» مجدداً تکرار می‌شود. لذا باتری نقش مهمی را در سیستم‌های S7400H بازی می‌کند.

همچنین اگر باتری وجود داشته باشد و عمل «خود آزمون» یک‌بار انجام‌شده باشد. با جدا شدن ماژول CPU از رک و نصب دوباره آن، عمل «خود آزمون» مجدداً تکرار خواهد شد. بعد از اتمام «خود آزمون» حالت چشمک‌زن در نشانگر Stop متوقف‌شده و به‌صورت ثابت با رنگ زرد روشن می‌ماند.

برای اطلاعات بیشتر در خصوص مدهای کاری سیستم H به صفحه ۱۲۳ از سند مرجع زیر مراجعه شود.

“SIMATIC Fault-tolerant systems S7-400H system manual, S7_400_h_en_en-US-2014.pdf

- chapter 11.3 : The operating states of the CPUs

11.1.2 LINK-UP and UPDATE Modes

قبل از اینکه سیستم H در مد ریداندانت قرار گیرد، ماژول master، محتوای حافظه CPU رزرو را بررسی و آن را به‌روزآوری می‌کند. این کار در دو مرحله متوالی اجرا می‌شود. که عبارت است از: Link-up و Update. در طی فازهای Link-up و Update، پردازنده master همیشه در مد RUN است و CPU رزرو در مد Link-up یا Update است. دو فاز Link-up و Update برای ایجاد مد ریداندانت در سیستم S7-400H انجام می‌شود.

در حین کار اگر standby عمل Link-up درخواست کند، پردازنده‌های master و standby برنامه خود را (user program) با یکدیگر مقایسه می‌کنند. در صورت مشاهده هرگونه اختلاف، پردازنده master، پردازنده standby را به‌روز می‌کند.

برای اطلاعات بیشتر در این خصوص به فصل ۱۲ صفحه ۱۳۵ از سند مرجع زیر مراجعه شود.

SIMATIC Fault-tolerant systems S7-400H system manual, chapter 12 Link-up and update

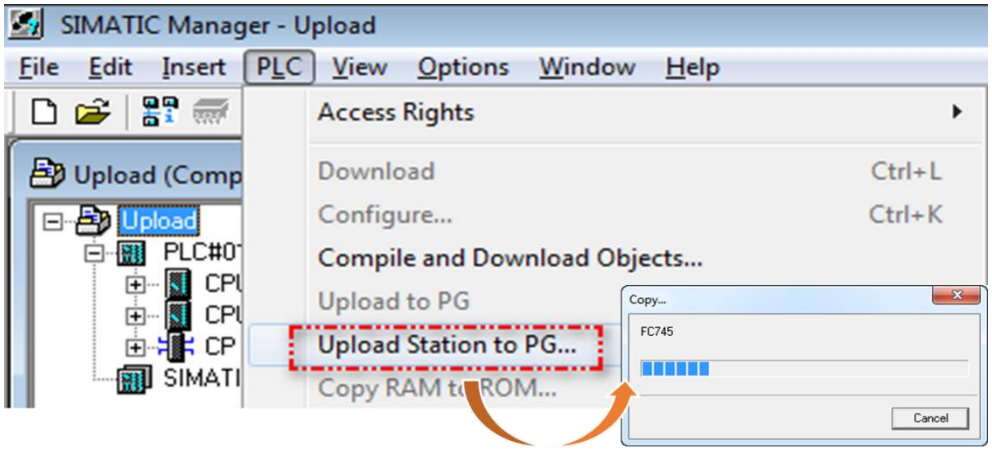
11.2 Ensuring Availability

برای اطمینان از قرار گرفتن سیستم 400H در مد ریداندانت یعنی در دسترس بودن سیستم کنترل در زمان بهره‌برداری، همواره باید تدابیری را اتخاذ نمود. در این خصوص برخی از تدابیر زیر توصیه می‌شود:

- همواره سعی کنید، شرایط مرجع (reference condition) یک پلنت را حفظ کنید. به‌عنوان‌مثال در فواصل زمانی تعریف‌شده عملیات نگهداری مانند تعویض باتری و کالیبراسیون را انجام دهید.
- پلنت را بهینه کرده و از بروز خطا جلوگیری کنید. مانند به‌روزرسانی‌های سیستم‌عامل (firmware)، حذف منابع خطاهای شناخته‌شده.
- زمان خرابی ناشی از فالت‌ها را به حداقل برسانید. به‌طور مثال: با تهیه نسخه پشتیبان.

11.2.1 Data backup

از داده‌های پروژه می‌توان به روش‌های مختلف و برای اهداف مختلف پشتیبان تهیه کرد. به‌عنوان‌مثال آرشیو پروژه، تهیه یک تصویر از کل سیستم (image) کامپیوتر مهندسی. لذا پس



شکل ۱۱-۴۷: اجرای دستور آپلود کل حافظه CPU به داخل کامپیوتر

۳- همانند روش بالا در پنجره بازشده اطلاعات CPU را وارد کرده و بر روی OK کلیک می‌کنیم. با بسته شدن پنجره تنظیم آپلود، برنامه داخل CPU و پیکربندی سخت‌افزار آن در قالب یک Station به پروژه ایجادشده اضافه می‌شود.

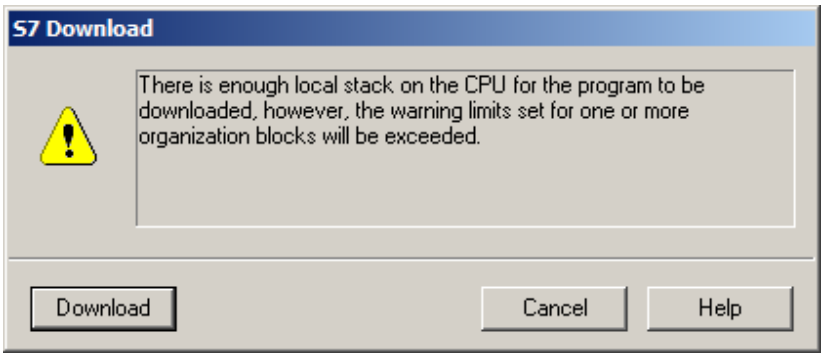
11.10 Some Common Errors in S7-400FH

11.10.1 Download Errors

Exceeding the limit in Local data stack

در بیشتر برنامه‌های مبتنی بر سیستم FH این نوع خطا در زمان دانلود یا کامپایل برنامه CFC ظاهر می‌شود.

Error: There is enough local stack on the CPU for the program to be downloaded, however, the warning limits set for one or more organization blocks will be exceeded.

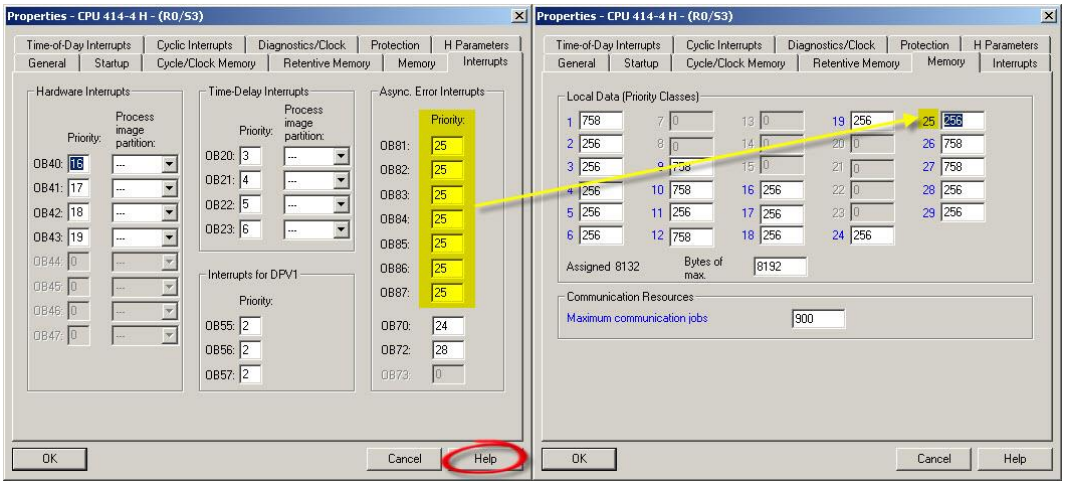


شکل ۱۱-۴۸: خطای عدم حافظه کافی در Statck

برای رفع این نوع خطا به دو روش می‌توان اقدام کرد.

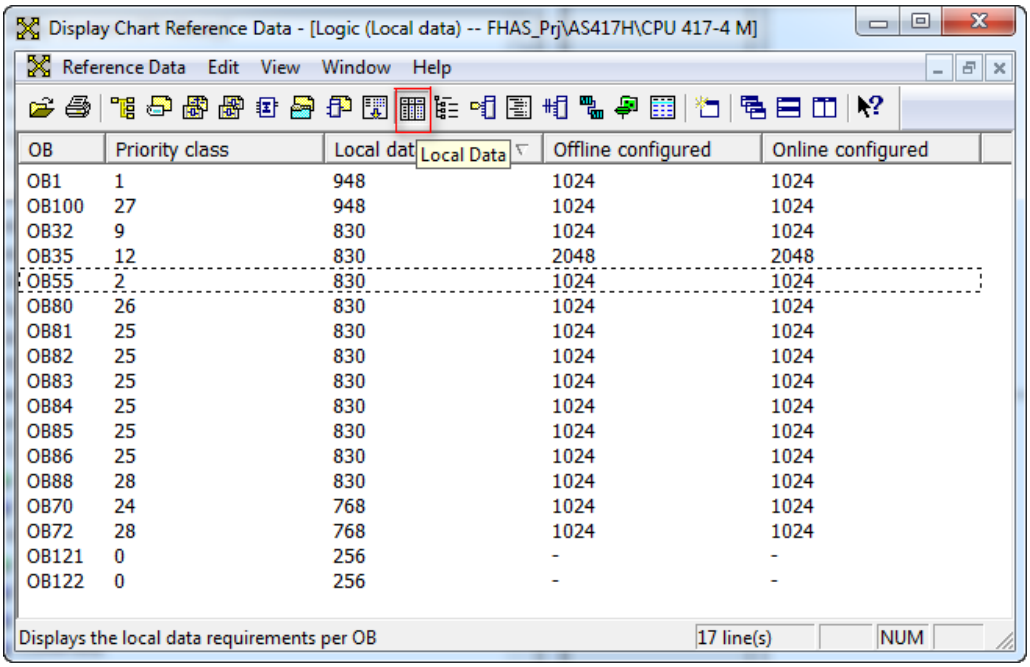
- تعدادی متغیرهای TEMP را برای بلاک‌هایی که در OBها فراخوانی شده‌اند، را کاهش دهید.

- اندازه حافظه پیش‌فرض تعریف‌شده برای داده‌های محلی (Local data) کلاس OB مربوطه را تغییر دهید. برای انجام این کار، در HWConfig بر روی CPU دو بار کلیک کرده و سپس در پنجره پراپرتی بازشده در سربرگ Memory اندازه Local data را برای کلاس اولویت OB موردنظر را تنظیم کنید.



شکل ۱۱-۴۹: تغیر اندازه حافظه Local data برای بلاک‌های OB

قبل از تغییر مقدار Local data ابتدا بایستی چک شود که کدام‌یک از کلاس‌های اولویت OB نیاز به افزایش مقدار حافظه Local data دارد. برای این منظور یک چارت CFC را بازکرده و ازآنجا پنجره Chart Referenceرا (Tools > Chart Reference Data) باز می‌کنیم. با باز شدن پنجره Chart Reference با کلیک بر روی آیکون مربوط به Local data مقادیر حافظه مصرف‌شده برای هر یک از OBها را می‌توان مشاهده کرد.



OB	Priority class	Local dat	Offline configured	Online configured
OB1	1	948	1024	1024
OB100	27	948	1024	1024
OB32	9	830	1024	1024
OB35	12	830	2048	2048
OB55	2	830	1024	1024
OB80	26	830	1024	1024
OB81	25	830	1024	1024
OB82	25	830	1024	1024
OB83	25	830	1024	1024
OB84	25	830	1024	1024
OB85	25	830	1024	1024
OB86	25	830	1024	1024
OB88	28	830	1024	1024
OB70	24	768	1024	1024
OB72	28	768	1024	1024
OB121	0	256	-	-
OB122	0	256	-	-

شکل ۱۱-۵۰: مشاهده مقدار حافظه استفاده‌شده برای Local data در هر بلاک OB

11.10.2 Download safety Program from CFC Editor to Flash EPROM

درصورتی‌که به جای حافظه RAM از کارت‌های حافظه فلش در یک سیستم FH استفاده شود، با دانلود برنامه F از ویرایشگر CFC، پیغام خطایی مبنی بر عدم امکان دانلود نمایش داده شود. نمونه این پیام‌ها به‌صورت زیر می‌باشد. توجه شود که این نوع خطا در دانلود به PLCSIM نمایش داده نمی‌شود.

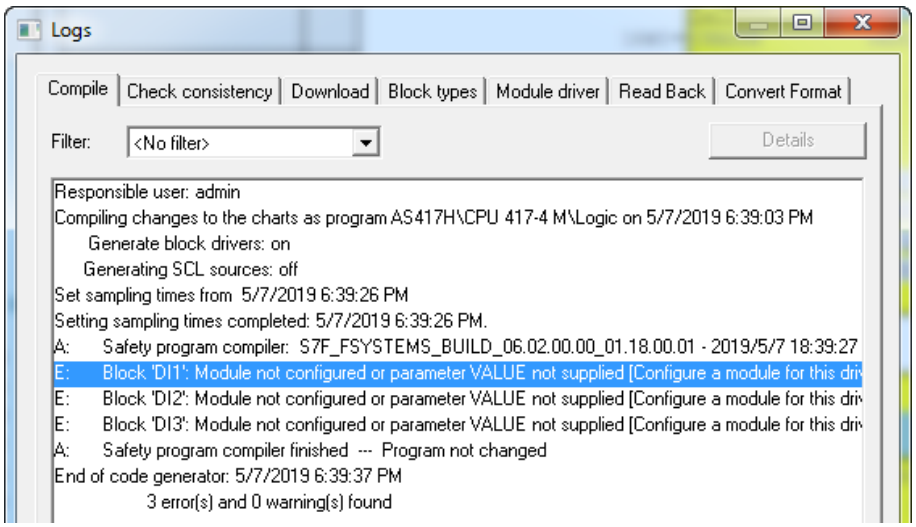
- “For modules with memory cards, the safety-related program in the work memory cannot be changed. For this reason no blocks can be reloaded." and the download stops.
- “For module with memory cards, the safety related program cannot be reloaded”

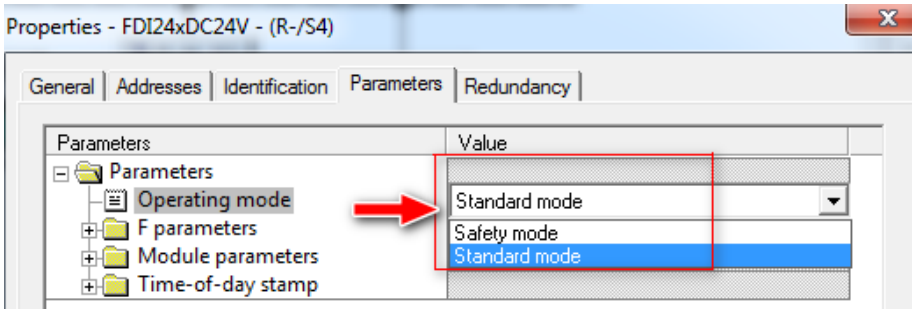
توصیه می‌شود که برای رفع این مشکل از حافظه‌های RAM استفاده شود.

11.10.3 Compile Errors

Block 'DI1': Module not configured or parameter VALUE not supplied

فرض کنید که در یک برنامه از یک بلاک درایور ورودی دیجیتال استفاده‌شده است که در آن اسم بلاک درایور DI1 نام‌گذاری شده است. سیگنال ورودی با آدرس درست تعریف‌شده و به‌درستی به بلاک متصل شده است. ولی ازآنجایی‌که در پنجره تنظیم پارامترهای ماژول ورودی دیجیتال، مد عملیاتی کارت به‌جای Safety به مد Standard تنظیم‌شده است، این خطا رخ می‌دهد.





شکل ۱۱-۵۱: خطای مربوط به عدم تنظیم مد Safety برای کانال‌های F

11.10.4 All leds flashing

در برخي موارد در CPUهای سری S7 اتفاق می‌افتد که تمام چراغ‌هاي روي CPU چشمك زن مي‌شود. منشأ اين مشكل به‌صورت كلی يا فيزيكی و يا به دليل خراب شدن سيستم‌عامل می‌باشد. منشأ فيزيكي و محيطي خاص شامل شوك ولتاژي، حرارت بالا، رطوبت و غيره می‌باشد. درصورتی‌كه منشأ مشكل، فيزيكی نباشد، با بالا بردن نسخه Firmare و سپس مجدداً با برگرداندن آن به نسخه اوليه ممكن است مشكل برطرف شود.

11.11 References

[1] System Software for S7-300/400 System and Standard Functions Volume 1/2, Reference Manual 2017

[2] SIMATIC Fault-tolerant systems System manual, 03/2012

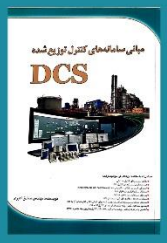
[3] S7 F/FH Systems, Configuring and Programming, Programming and Operating Manual, 2016, A5E37822367

درباره ناشر

شـرکت آدلی کنترل باور یک شـرکت مهندسی فعال در زمینه تامین، طراحی مهندسی، پیاده‌سازی و اجرای پـروژه های جدید، بهینه سـازی، ارتقاء، افزایش ظرفیت و آموزش تخصصی سیسـتم‌های کنترل صنعتی PLC ,DCS,PCS,ESD,F&G می‌باشـد. که دارای مجوز رسـمی نشر دیجـیتال کتـــاب و محتوای آموزشـی می‌باشـد. خدمات این شـرکت در حوزه تولید و نشـر محتوای آموزش اتوماسیون صنعتی به شرح زیر می‌باشد

- تولید و نشـر کتاب به صورت دیجیتال
- نشـر آموزش ویدیویی در زمینه اتوماسیون صنعتی

سایر کتاب ها



تهران – شـهرک گلستان – بلوار هاشم زاده
بلوارافاقیـا – پلاک ۳۰ – طبقه همکف

۰۲۱۴۴۷۳۲۹۸۱ – ۰۹۱۲۳۱۸۲۷۳۴

ACTRAIN
Training for Industry

Adli Control bavar

تامین کالا ، خدمات مهنـــدسی و آموزش اتوماسیون صنعتی

SIEMENS