

## 1 . معرفی و کلیات سیستم S7-1200

### 1.1 هدف و مخاطبین دفترچه راهنمای Easy Book

دفترچه راهنمای SIMATIC S7-1200 Easy Book به عنوان یک منبع آموزشی و مرجع سریع برای آشنایی با خانواده کنترلرهای فشرده S7-1200 طراحی شده است. این دفترچه به طور خاص برای مهندسان، برنامه‌نویسان، نصاب‌ها و تکنسین‌های برقی که دانش پایه‌ای در زمینه کنترلرهای منطقی قابل برنامه‌ریزی (PLC) دارند، در نظر گرفته شده است. هدف اصلی این کتابچه ارائه یک مرور کلی از قابلیت‌ها و ویژگی‌های این خانواده از کنترلرهاست، بدون آنکه به جزئیات فنی بسیار پیچیده بپردازد. به عنوان مثال، در نسخه‌های اولیه این دفترچه، مانند نسخه 2009/05، تاکید بر معرفی S7-1200 به عنوان یک کنترلر ماژولار و کم‌حجم برای سیستم‌های اتوماسیون کوچک بوده که می‌توانند نیازهایی از ساده تا پیشرفته در زمینه‌های منطق، رابط انسان-ماشین (HMI) و شبکه‌سازی را برآورده کنند. همچنین، در نسخه‌های جدیدتر مانند نسخه 2015/01، این دفترچه همچنان به عنوان یک راهنمای مقدماتی برای محصولات S7-1200 و نرم‌افزار STEP 7 V11 Basic و Professional شناخته می‌شود. مخاطبین این دفترچه، افرادی هستند که به دنبال درک کلی از ساختار، توانایی‌ها و نحوه استفاده از این کنترلرها در پروژه‌های خود هستند و برای اطلاعات فنی دقیق‌تر به دفترچه راهنمای سیستم (System Manual) ارجاع داده می‌شوند.

### 1.2 . ویژگی‌های کلیدی و قابلیت‌های سیستم

#### 1.2.1 . طراحی فشرده و مقرون به صرفه

یکی از مهم‌ترین ویژگی‌های برجسته خانواده کنترلرهای SIMATIC S7-1200، طراحی فشرده و ابعاد کوچک آنهاست که باعث صرفه‌جویی در فضای تابلو برق می‌شود. این طراحی به گونه‌ای است که نصب آنها هم بر روی ریل DIN استاندارد و هم بر روی پنل امکان‌پذیر است. ابعاد دقیق این کنترلرها بسته به مدل CPU متفاوت است. برای مثال، CPU 1211C و CPU 1212C عرضی برابر با 90 میلی‌متر دارند، در حالی که CPU 1214C

عریض تر بوده و 110 میلی متر عرض دارد. این طراحی فشرده نه تنها در CPU ها بلکه در ماژول های توسعه ای نیز دیده می شود، به طوری که ماژول های سیگنال (SM) و ماژول های ارتباطی (CM) عرضی برابر با 30 میلی متر دارند. این ویژگی در کنار هزینه پایین، S7-1200 را به یک راه حل اقتصادی و کارآمد برای کنترل طیف وسیعی از برنامه های کاربردی کوچک و متوسط تبدیل کرده است. در نسل دوم این کنترلرها (S7-1200 G2)، این طراحی فشرده حتی بیشتر بهینه سازی شده و ردپای فیزیکی آن ها به طور قابل توجهی کاهش یافته است.

### 1.2.2. پشتیبانی از شبکه PROFINET

تمامی کنترلرهای S7-1200 به صورت استاندارد دارای یک رابط PROFINET داخلی هستند که امکان ارتباط سریع و قابل اعتماد در شبکه های صنعتی را فراهم می کند. این رابط در بالای CPU قرار دارد و در برخی مدل ها دارای دو پورت برای ایجاد توپولوژی های خطی و زنجیره ای است PROFINET. یک استاندارد ارتباطی صنعتی مبتنی بر اترنت است که امکان تبادل داده های زمان بندی شده و غیرزمان بندی شده را بین دستگاه های مختلف اتوماسیون مانند PLC، HMI، درایوها و سنسورها فراهم می کند. وجود این رابط داخلی باعث کاهش نیاز به ماژول های ارتباطی اضافی و در نتیجه کاهش هزینه و پیچیدگی سیستم می شود. از طریق این رابط، می توان برنامه نویسی، عیب یابی و تبادل داده با سایر دستگاه های هوشمند را انجام داد. این ویژگی به S7-1200 اجازه می دهد تا به عنوان یک جزء یکپارچه در سیستم های "اتوماسیون کاملاً یکپارچه (TIA)" شرکت زیمنس عمل کند.

### 1.2.3. ورودی/خروجی های پرسرعت (High-Speed I/O)

کنترلرهای S7-1200 مجهز به ورودی ها و خروجی های پرسرعت (High-Speed I/O) هستند که برای کاربردهای خاص مانند کنترل حرکت، شمارش سریع پالس ها و تولید پالس های دقیق طراحی شده اند. این ویژگی در دفترچه راهنمای Easy Book به عنوان یکی از قابلیت های کلیدی کنترلرهای S7-1200 معرفی شده است. این I/O های پرسرعت امکان پاسخ گویی سریع به رویدادهای خارجی را فراهم می کنند که برای بسیاری از فرآیندهای صنعتی حیاتی است. برای مثال، در سیستم های بسته بندی یا ماشین آلاتی که نیاز به همگام سازی دقیق با قطعات متحرک دارند، این ورودی ها می توانند سیگنال های سنسورهای نوری یا انکودرها را با سرعت بالا ثبت کنند. همچنین، خروجی های پرسرعت می توانند پالس هایی با فرکانس بالا تولید کنند که برای کنترل سروو درایوها یا استپر موتورها استفاده می شود. این قابلیت باعث می شود که S7-1200 بدون نیاز به ماژول های تخصصی گران قیمت، بتواند کاربردهای پیچیده تری را نسبت به کنترلرهای سطح پایین بازار پوشش دهد.

#### 1.2.4 . ورودی‌های آنالوگ داخلی (Onboard Analog Inputs)

برخی از مدل‌های CPU در خانواده S7-1200 دارای ورودی‌های آنالوگ داخلی (Onboard Analog Inputs) هستند که امکان اتصال مستقیم سنسورهای آنالوگ مانند سنسورهای دما، فشار یا سطح را بدون نیاز به ماژول‌های ورودی آنالوگ اضافی فراهم می‌کند. این ویژگی به طور قابل توجهی فضای مورد نیاز در تابلو برق را کاهش می‌دهد و هزینه‌های سیستم را پایین می‌آورد. در دفترچه راهنمای Easy Book، این ویژگی به عنوان یکی از نقاط قوت طراحی فشرده S7-1200 ذکر شده است. تعداد این ورودی‌های آنالوگ داخلی بسته به مدل CPU متفاوت است. این ورودی‌ها معمولاً قادر به دریافت سیگنال‌های ولتاژ (مانند 0-10V) یا جریان (مانند 4-20mA) هستند و توسط نرم‌افزار STEP 7 قابل پیکربندی می‌باشند. وجود این ورودی‌ها باعث می‌شود که S7-1200 برای برنامه‌های کاربردی ساده که نیاز به اندازه‌گیری چند پارامتر آنالوگ دارند، یک راه‌حل بسیار مناسب و اقتصادی باشد.

#### 2 . اجزای اصلی سخت‌افزار

##### 2.1 . واحد پردازش مرکزی (CPU)

###### 2.1.1 . نقش و عملکرد CPU در سیستم

واحد پردازش مرکزی (CPU) قلب تپنده کنترلر S7-1200 است و تمام عملیات کنترل و نظارت بر فرآیند یا ماشین را انجام می‌دهد. CPU ترکیبی از یک میکروپروسسور، منبع تغذیه یکپارچه، مدارهای ورودی و خروجی، رابط PROFINET داخلی، شمارنده‌های پرسرعت و قابلیت‌های کنترل حرکت را در یک محفظه فشرده جای داده است. پس از بارگذاری برنامه کاربر، CPU منطق لازم برای نظارت بر دستگاه‌ها و تغییر خروجی‌ها را طبق منطق برنامه ذخیره‌شده در حافظه خود اجرا می‌کند. این منطق می‌تواند شامل عملیات بولی، شمارش، زمان‌بندی، محاسبات ریاضی پیچیده، کنترل حرکت و ارتباط با سایر دستگاه‌های هوشمند باشد. CPU به طور مداوم ورودی‌ها را اسکن می‌کند، برنامه را اجرا می‌کند و سپس خروجی‌ها را به‌روزرسانی می‌کند. این چرخه به طور مداوم تکرار می‌شود. همچنین، CPU وظیفه مدیریت حافظه، برقراری ارتباط از طریق شبکه و پاسخ به درخواست‌های عیب‌یابی را نیز بر عهده دارد.

## 2.1.2 . انواع CPU های استاندارد S7-1200

خانواده S7-1200 شامل چندین مدل CPU استاندارد با قابلیت‌ها و ظرفیت‌های مختلف است که انتخاب را بر اساس نیازهای خاص برنامه کاربردی آسان می‌کند. این مدل‌ها شامل CPU 1211C، CPU 1212C، CPU 1214C، CPU 1215C و CPU 1217C هستند. تفاوت اصلی بین این مدل‌ها در تعداد ورودی/خروجی‌های دیجیتال و آنالوگ داخلی، حافظه کاربر و پشتیبانی از ویژگی‌های پیشرفته مانند کنترل حرکت است. برای مثال، CPU 1211C و CPU 1212 دارای ابعاد کوچک‌تری هستند (عرض 90 میلی‌متر) در حالی که CPU 1214C عریض‌تر است (عرض 110 میلی‌متر). همچنین، تعداد نقاط I/O داخلی در این CPU ها متفاوت است. برای مثال، برخی مدل‌ها دارای 6 تا 14 ورودی دیجیتال و 4 تا 10 خروجی دیجیتال داخلی هستند. انتخاب CPU مناسب به عواملی مانند تعداد I/O مورد نیاز، حجم برنامه، پیچیدگی کنترل و الزامات ارتباطی بستگی دارد.

### مشخصات فنی CPU های استاندارد S7-1200

ویژگی	CPU 1211C	CPU 1212C	CPU 1214C	CPU 1215C	CPU 1217C
اندازه فیزیکی (mm)	75×100×90	75×100×90	75×100×110	75×100×130	75×100×150
حافظه کاربر (Work)	Kbytes 30	Kbytes 50	Kbytes 75	Kbytes 100	Kbytes 125
حافظه بار (Load)	Mbyte 1	Mbyte 1	Mbytes 4	Mbytes 4	Mbytes 4
حافظه ماندگار	Kbytes 10	Kbytes 10	Kbytes 10	Kbytes 10	Kbytes 10
I/O دیجیتال داخلی	6 ورودی / 4 خروجی	8 ورودی / 6 خروجی	14 ورودی / 10 خروجی	14 ورودی / 10 خروجی	14 ورودی / 10 خروجی
I/O آنالوگ داخلی	2 ورودی	2 ورودی	2 ورودی	2 ورودی / 2 خروجی	2 ورودی / 2 خروجی
توسعه ماژول سیگنال	هیچ	2	8	8	8
پورت‌های PROFINET	1	1	1	2	2

منبع: صفحه 14 دفترچه راهنمای SIMATIC S7-1200 Easy Book

## 2.2 . ماژول‌های ورودی/خروجی (I/O Modules)

### 2.2.1 . ماژول‌های سیگنال (Signal Modules) - صفحه 16

ماژول‌های سیگنال (Signal Modules یا SMS) برای افزایش تعداد نقاط ورودی/خروجی کنترلر S7-1200 استفاده می‌شوند. این ماژول‌ها به سمت راست CPU متصل می‌شوند و سیستم را قادر می‌سازند تا تعداد بیشتری سیگنال دیجیتال یا آنالوگ را پردازش کند. در دفترچه راهنمای Easy Book، این ماژول‌ها به عنوان یکی از اجزای اصلی برای گسترش سیستم معرفی شده‌اند. ماژول‌های سیگنال در انواع مختلفی موجود هستند، از جمله ماژول‌های ورودی دیجیتال، خروجی دیجیتال، ورودی آنالوگ، خروجی آنالوگ و ماژول‌های ترکیبی. برای مثال، ماژول‌های دیجیتال در نسخه‌های 8 یا 16 نقطه‌ای و ماژول‌های آنالوگ در نسخه‌های 2، 4 یا 8 کاناله عرضه می‌شوند. این ماژول‌ها به راحتی بر روی ریل DIN نصب می‌شوند و از طریق باس داخلی با CPU ارتباط برقرار می‌کنند. استفاده از این ماژول‌ها انعطاف‌پذیری زیادی در طراحی سیستم ایجاد می‌کند و امکان سفارشی‌سازی تعداد و نوع I/O ها را بر اساس نیازهای خاص هر برنامه کاربردی فراهم می‌کند.

### 2.2.2 . ماژول‌های دیجیتال (Digital Modules)

ماژول‌های دیجیتال برای اتصال سنسورها و اکچویتورهای دیجیتال (ON/OFF) به سیستم S7-1200 استفاده می‌شوند. این ماژول‌ها در دو نوع اصلی ورودی دیجیتال (DI) و خروجی دیجیتال (DO) وجود دارند. ماژول‌های ورودی دیجیتال سیگنال‌های DC 24 ولت یا 230/120 ولت AC را از سنسورها دریافت می‌کنند، در حالی که ماژول‌های خروجی دیجیتال سیگنال‌های DC 24 ولت یا رله‌ای را برای کنترل اکچویتورها مانند شیرهای برقی، کنتاکتورها و چراغ‌های هشدار ارسال می‌کنند. همچنین، ماژول‌های ترکیبی (DI/DO) نیز در دسترس هستند که هر دو نوع ورودی و خروجی را در یک ماژول فراهم می‌کنند. این ماژول‌ها به صورت ماژول‌های سیگنال (SM) به CPU متصل می‌شوند و تعداد نقاط I/O دیجیتال سیستم را به میزان قابل توجهی افزایش می‌دهند.

### 2.2.3 . ماژول‌های آنالوگ (Analog Modules)

ماژول‌های آنالوگ برای اتصال سنسورها و اکچویتورهای آنالوگ (سیگنال پیوسته) به سیستم S7-1200 استفاده می‌شوند. این ماژول‌ها در انواع ورودی آنالوگ (AI)، خروجی آنالوگ (AO) و ترکیبی (AI/AO) موجود هستند.

ماژول‌های ورودی آنالوگ سیگنال‌های ولتاژ (مانند  $V_{10\pm}$ ,  $V_{0-10}$ ) یا جریان (مانند  $4-20\text{ mA}$ ,  $0-20\text{ mA}$ ) را از سنسورهای مانند سنسورهای دما، فشار یا سطح دریافت می‌کنند و آن‌ها را به مقادیر دیجیتال تبدیل می‌کنند. ماژول‌های خروجی آنالوگ نیز مقادیر دیجیتال را به سیگنال‌های ولتاژ یا جریان آنالوگ تبدیل کرده و برای کنترل درایوهای سرعت متغیر، شیرهای کنترلی یا سایر دستگاه‌هایی که به سیگنال آنالوگ پاسخ می‌دهند، استفاده می‌شوند. این ماژول‌ها معمولاً دارای رزولوشن 12 یا 16 بیت هستند که دقت بالایی را برای کنترل فرآیندهای پیوسته فراهم می‌کنند.

### 2.3. ماژول‌های ارتباطی (Communication Modules)

ماژول‌های ارتباطی (Communication Modules - CM) برای افزودن پروتکل‌های ارتباطی دیگر به کنترلر S7-1200 استفاده می‌شوند. این ماژول‌ها به سمت چپ CPU متصل می‌شوند و امکان ارتباط با دستگاه‌هایی که از PROFINET پشتیبانی نمی‌کنند را فراهم می‌کنند. انواع مختلفی از ماژول‌های ارتباطی وجود دارد، از جمله CM 1241 RS232 و CM 1241 RS485 برای ارتباطات نقطه‌به‌نقطه سریال، و CM 1242-5 و CM 1243-5 برای اتصال به شبکه‌های PROFIBUS. این ماژول‌ها به سیستم اجازه می‌دهند تا به عنوان یک gateway عمل کند و داده‌ها را بین شبکه‌های مختلف تبادل کند. استفاده از این ماژول‌ها انعطاف‌پذیری سیستم را در معماری‌های شبکه پیچیده افزایش می‌دهد.

### 2.4. ماژول‌های جانبی و توسعه‌دهنده

#### 2.4.1. بردهای سیگنال (Signal Boards) - صفحه 16

بردهای سیگنال (Signal Boards یا SBs) یکی دیگر از راه‌های افزایش توانایی‌های I/O کنترلر S7-1200 هستند. برخلاف ماژول‌های سیگنال که به کنار CPU متصل می‌شوند، این بردها به جلوی CPU نصب می‌شوند و فضای بسیار کمی اشغال می‌کنند. این ویژگی آن‌ها را برای مواردی که فضای تابلو برق محدود است، بسیار مناسب می‌کند. در دفترچه راهنمای Easy Book، این بردها به عنوان یک نوآوری در طراحی S7-1200 معرفی شده‌اند که امکان افزودن I/O اضافی بدون افزایش ابعاد کلی سیستم را فراهم می‌کنند. بردهای سیگنال معمولاً برای افزودن تعداد کمی ورودی یا خروجی دیجیتال/آنالوگ یا رابط‌های ارتباطی خاص (مانند RS232/485) (

استفاده می‌شوند. برای مثال، می‌توان یک برد سیگنال با یک خروجی آنالوگ (SB 1232) به CPU اضافه کرد تا یک سیگنال کنترلی آنالوگ تولید شود. این بردها به راحتی در یک اسلات اختصاصی در جلوی CPU قرار می‌گیرند و پیکربندی آن‌ها در نرم‌افزار STEP 7 انجام می‌شود.

## 2.4.2 . کارت‌های حافظه (Memory Cards)

کارت‌های حافظه (Memory Cards یا MCs) برای افزایش حافظه داخلی CPU و همچنین برای انتقال برنامه‌ها و داده‌ها استفاده می‌شوند. این کارت‌ها در یک اسلات اختصاصی در جلوی CPU قرار می‌گیرند که پشت درب پوشانده شده است. استفاده از کارت حافظه چندین مزیت دارد. اولاً، می‌توان از آن به عنوان حافظه خارجی برای ذخیره‌سازی داده‌های بیشتر استفاده کرد. ثانیاً، می‌توان برنامه کاربر را روی کارت حافظه ذخیره کرد و سپس آن را به راحتی به CPU دیگری منتقل کرد، که این برای تولید انبوه ماشین‌های یکسان بسیار مفید است. همچنین، می‌توان از کارت حافظه برای بروزرسانی CPU firmware استفاده کرد. در برخی موارد، کارت حافظه می‌تواند به عنوان یک حافظه پشتیبان عمل کند و در صورت بروز مشکل در CPU، برنامه را بازیابی کند. این کارت‌ها معمولاً از نوع SIMATIC Memory Card هستند که استاندارد اختصاصی شرکت زیمنس می‌باشد.

## 3 . ویژگی‌های پیشرفته سخت‌افزار

### 3.1 . سیستم شمارش پرسرعت (High-Speed Counters)

#### 3.1.1 . تعداد و ظرفیت شمارنده‌ها - صفحه 82

کنترلرهای S7-1200 دارای شمارنده‌های پرسرعت (High-Speed Counters یا HSCs) داخلی هستند که امکان شمارش پالس‌هایی با فرکانس بسیار بالا را فراهم می‌کنند. در دفترچه راهنمای Easy Book، این ویژگی در صفحه 82 مورد بحث قرار گرفته است. تعداد این شمارنده‌ها بسته به مدل CPU متفاوت است و می‌تواند تا 6 شمارنده پرسرعت باشد. این شمارنده‌ها می‌توانند پالس‌هایی با فرکانس تا چند صد کیلوهرتز را پردازش کنند، که برای کاربردهایی مانند اندازه‌گیری سرعت، طول یا موقعیت بسیار مناسب است. شمارنده‌های پرسرعت می‌توانند در چندین حالت مختلف کار کنند، از جمله حالت شمارش ساده (up/down counting)، حالت اندازه‌گیری دوره (period measurement) و حالت اندازه‌گیری فرکانس (frequency).

measurement). این شمارنده‌ها به ورودی‌های دیجیتال خاصی از CPU متصل می‌شوند که برای کار در فرکانس‌های بالا بهینه‌سازی شده‌اند. استفاده از این شمارنده‌ها باعث می‌شود که نیاز به ماژول‌های شمارنده خارجی گران‌قیمت در بسیاری از برنامه‌های کاربردی حذف شود.

### 3.1.2. کاربرد در پروژه‌های مختلف

شمارنده‌های پرسرعت در طیف وسیعی از کاربردهای صنعتی استفاده می‌شوند. یکی از رایج‌ترین کاربردها، اتصال به انکودرهای چرخشی برای اندازه‌گیری موقعیت یا سرعت یک محور است. برای مثال، در یک سیستم جابجایی مواد، می‌توان از HSC برای شمارش پالس‌های تولید شده توسط یک انکودر برای تعیین موقعیت دقیق یک نوار نقاله یا یک بازوی رباتیک استفاده کرد. همچنین، در کاربردهای بسته‌بندی، HSC می‌تواند برای شمارش سریع محصولات عبوری از یک سنسور نوری استفاده شود. در حالت اندازه‌گیری فرکانس، HSC می‌تواند برای نظارت بر سرعت چرخش یک توربین یا یک موتور استفاده شود. این قابلیت‌ها باعث می‌شوند که S7-1200 برای کاربردهایی که نیاز به پاسخ‌گویی سریع و دقیق به رویدادهای خارجی دارند، بسیار مناسب باشد.

### 3.2. ژنراتورهای پالس (Pulse Generators)

#### 3.2.1. تعداد و کاربرد در کنترل موقعیت - صفحه 84

کنترلرهای S7-1200 مجهز به ژنراتورهای پالس (Pulse Generators یا PTOs) هستند که می‌توانند پالس‌هایی با فرکانس و تعداد مشخص تولید کنند. در دفترچه راهنمای Easy Book، این ویژگی در صفحه 84 مورد بحث قرار گرفته است. این ژنراتورها معمولاً برای کنترل موقعیت استپر موتورها یا سروو درایوهای ساده استفاده می‌شوند. تعداد این ژنراتورها در CPUهای S7-1200 معمولاً 2 عدد است. با استفاده از این ژنراتورها، می‌توان حرکت‌های دقیق و کنترل‌شده‌ای را در ماشین‌آلات ایجاد کرد. برای مثال، می‌توان یک میز کار را به یک موقعیت دقیق حرکت داد یا یک بازوی رباتیک را برای انجام یک عملیات خاص کنترل کرد. این ژنراتورها توسط دستورالعمل‌های کنترل حرکت در نرم‌افزار STEP 7 کنترل می‌شوند و می‌توانند پروفایل‌های حرکتی پیچیده‌ای را اجرا کنند.



### 3.2.2 . کاربرد در کنترل عرض پالس (PWM)

علاوه بر حالت PTO، ژنراتورهای پالس S7-1200 می‌توانند در حالت مدولاسیون عرض پالس (Pulse Width Modulation – PWM) نیز کار کنند. در این حالت، ژنراتور یک سیگنال با فرکانس ثابت ولی با عرض پالس متغیر تولید می‌کند. این قابلیت برای کنترل میانگین توان تحویل داده شده به یک بار بسیار مفید است. برای مثال، می‌توان از PWM برای کنترل سرعت یک موتور DC یا کنترل روشنایی یک لامپ LED استفاده کرد. با تغییر عرض پالس (Duty Cycle)، می‌توان میزان توان تحویل داده شده را به صورت پیوسته تغییر داد. این ویژگی یک راه‌حل مقرون‌به‌صرفه برای کنترل فرآیندهای آنالوگ با استفاده از خروجی‌های دیجیتال فراهم می‌کند.

### 3.3 . قابلیت کنترل حرکت (Motion Control)

#### 3.3.1 . پشتیبانی از I/O پرسرعت برای کنترل حرکت - صفحه 86

کنترلرهای S7-1200 دارای قابلیت‌های کنترل حرکت (Motion Control) داخلی هستند که امکان کنترل ساده تا پیشرفته محورهای حرکتی را فراهم می‌کنند. در دفترچه راهنمای Easy Book، این ویژگی در صفحه 86 مورد بحث قرار گرفته است. این قابلیت از طریق ترکیب شمارنده‌های پرسرعت (HSCs) برای بازخورد موقعیت و ژنراتورهای پالس (PTOs) برای فرمان حرکت به دست می‌آید. نرم‌افزار STEP 7 دارای توابع و دستورالعمل‌های آماده‌ای برای کنترل حرکت است که استفاده از این ویژگی را آسان می‌کند. با استفاده از این قابلیت، می‌توان حرکت‌های نقطه‌به‌نقطه (point-to-point)، حرکت‌های با پروفیل (profiled motion) و همچنین همگام‌سازی چند محور را انجام داد. این ویژگی باعث می‌شود که S7-1200 برای کاربردهایی مانند ماشین‌های بسته‌بندی، سیستم‌های جابجایی مواد و ماشین‌آلات CNC کوچک بسیار مناسب باشد.

## 4 . امنیت و محافظت

### 4.1 . سطوح مختلف محافظت

سیستم S7-1200 دارای چندین لایه امنیتی برای محافظت از دسترسی غیرمجاز به CPU و برنامه کنترل است. این ویژگی‌ها برای حفاظت از سرمایه‌گذاری توسعه‌دهندگان نرم‌افزار و جلوگیری از دستکاری غیرمجاز در فرآیند تولید طراحی شده‌اند. این سطوح مختلف محافظت عبارتند از:

#### 4.1.1 . محافظت با رمز عبور (Password Protection)

تمامی CPU های S7-1200 دارای قابلیت محافظت با رمز عبور هستند که به کاربر اجازه می‌دهد تا سطوح مختلف دسترسی به توابع CPU را پیکربندی کند. برای مثال، می‌توان یک رمز عبور برای دسترسی کامل (Read/Write) و یک رمز عبور دیگر برای دسترسی فقط خواندنی (Read-Only) تعریف کرد. این ویژگی از دسترسی افراد غیرمجاز به برنامه و پیکربندی سیستم جلوگیری می‌کند. در صورت فراموشی رمز عبور، بازیابی آن تقریباً غیرممکن است و ممکن است نیاز به بازنشانی کامل CPU باشد. بنابراین، نگهداری ایمن رمز عبور بسیار مهم است.

#### 4.1.2 . محافظت از دانش فنی (Know-how Protection)

ویژگی "محافظت از دانش فنی (Know-how Protection)" امکان مخفی کردن کد منبع (Source Code) یک بلوک خاص (مانند یک Function یا Function Block) را فراهم می‌کند. هنگامی که این ویژگی برای یک بلوک فعال می‌شود، محتوای آن بلوک برای کاربرانی که رمز عبور لازم را ندارند، قابل مشاهده یا ویرایش نخواهد بود. این قابلیت برای محافظت از الگوریتم‌های خاص، فرمول‌ها یا منطق کنترل پیچیده که توسط یک توسعه‌دهنده ایجاد شده‌اند، بسیار مفید است. این ویژگی به توسعه‌دهندگان اجازه می‌دهد تا کتابخانه‌های توابع خود را با دیگران به اشتراک بگذارند بدون اینکه نگران کپی یا بررسی منطق داخلی آن باشند.

#### 4.1.3 . محافظت در برابر کپی (Copy Protection)

قابلیت "محافظت در برابر کپی" (Copy Protection) امکان اتصال یک برنامه کاربر به یک کارت حافظه (Memory Card) یا CPU خاص را فراهم می‌کند. هنگامی که این ویژگی فعال می‌شود، برنامه تنها در صورتی اجرا می‌شود که کارت حافظه یا CPU خاصی که در پیکربندی تعیین شده‌اند، در دسترس باشند. این ویژگی یکی از قوی‌ترین روش‌های محافظت از برنامه در برابر کپی غیرمجاز است. این قابلیت برای تولیدکنندگان ماشین‌آلات (OEMs) بسیار مفید است که می‌خواهند برنامه کنترل خود را به فروش برسانند ولی از کپی شدن آن توسط مشتریان جلوگیری کنند.

## 4.2 . اهمیت امنیت در زیرساخت‌های فنی

در دنیای امروز صنعتی، امنیت سیستم‌های کنترل صنعتی (ICS) و زیرساخت‌های فنی بیش از هر زمان دیگری اهمیت دارد. سیستم‌هایی مانند S7-1200 که در قلب بسیاری از فرآیندهای تولیدی و زیرساختی قرار دارند، در برابر تهدیدات سایبری آسیب‌پذیر هستند. یک حمله موفق می‌تواند منجر به توقف تولید، آسیب به تجهیزات، نقض ایمنی کارکنان و خسارات مالی قابل توجهی شود. بنابراین، استفاده از ویژگی‌های امنیتی داخلی مانند محافظت با رمز عبور، محافظت از دانش فنی و محافظت در برابر کپی، نه تنها برای حفاظت از سرمایه‌گذاری معنوی توسعه‌دهندگان، بلکه برای اطمینان از یکپارچگی، در دسترس بودن و محرمانگی کل سیستم اتوماسیون ضروری است. این ویژگی‌ها به عنوان یک خط دفاعی اولیه عمل می‌کنند و باید به عنوان بخشی جدایی‌ناپذیر از هر طراحی سیستم در نظر گرفته شوند.

## 5 . منابع و مستندات تکمیلی

### 5.1 . مرجع اصلی: دفترچه راهنمای Easy Book

دفترچه راهنمای SIMATIC S7-1200 Easy Book که با شماره سند 39710145 در وبسایت پشتیبانی صنعتی زیمنس در دسترس است، منبع اصلی این گزارش بوده است. این دفترچه به عنوان یک راهنمای مقدماتی و مرور کلی بر قابلیت‌های کنترلرهای S7-1200 طراحی شده است. همان‌طور که در مقدمه این دفترچه ذکر شده، هدف آن ارائه یک مرور کلی از ویژگی‌ها و توانایی‌های دستگاه‌ها است. این دفترچه برای افرادی که به تازگی با این خانواده از کنترلرها آشنا می‌شوند یا به دنبال درک کلی از ساختار و عملکرد آن هستند، بسیار مفید است. با این حال، برای اطلاعات فنی دقیق‌تر و جزئیات کامل‌تر در مورد نصب، برنامه‌نویسی و مشخصات فنی، باید به مستندات تکمیلی مراجعه شود.

### 5.2 . مستندات تکمیلی: دفترچه راهنمای سیستم (System Manual)

در چندین بخش از دفترچه راهنمای Easy Book، به دفترچه راهنمای سیستم (System Manual) به عنوان منبع اصلی برای اطلاعات تکمیلی اشاره شده است. این دفترچه حاوی اطلاعات دقیق در مورد عملکرد، برنامه‌نویسی و مشخصات فنی کامل خانواده محصولات S7-1200 است. برای مثال، در مورد الزامات نصب و فاصله‌گذاری حرارتی، Easy Book به System Manual ارجاع می‌دهد. همچنین، برای اطلاعات مربوط به استانداردهای UL و FM، برچسب CE و سایر استانداردها، باید به مشخصات فنی در System Manual مراجعه شود. بنابراین، برای یک پروژه واقعی و پیاده‌سازی عملی، مطالعه دفترچه راهنمای سیستم S7-1200 ضروری است. این دفترچه به صورت الکترونیکی (PDF) در وبسایت پشتیبانی صنعتی زیمنس قابل دانلود است و همچنین در دیسک همراه هر CPU S7-1200 نیز وجود دارد.

\*\*\*\*\*

## 1 معرفی کلی محصول (صفحه 27)

S7-1200 یک کنترلر منطقی برنامه‌پذیر (PLC) کامپکت و مقرون‌به‌صرفه است که برای طیف وسیعی از کاربردهای اتوماسیون صنعتی طراحی شده است. این PLC ترکیبی از پردازنده، منبع تغذیه داخلی، مدارهای ورودی/خروجی، پورت PROFINET داخلی و قابلیت‌های کنترل حرکت است.

## 2 معماری سخت‌افزار

### 2.1 واحد پردازش مرکزی (CPU) (صفحه 28)

CPUهای S7-1200 در مدل‌های زیر ارائه می‌شوند:

مدل CPU	حافظه کاری	حافظه بارگیری	O/ادیدجیتال	O/آنالوگ	تعداد ماژول‌های توسعه
CPU 1211C	50 KB	1 MB	6DI/4DQ	2AI	0 SM

تعداد ماژول‌های توسعه	I/O آنالوگ	I/O دیجیتال	حافظه بارگیری	حافظه کاری	مدل CPU
2 SM	2AI	8DI/6DQ	2 MB	75 KB	CPU 1212C
8 SM	2AI	14DI/10DQ	4 MB	100 KB	CPU 1214C
8 SM	2AI/2AQ	14DI/10DQ	4 MB	125 KB	CPU 1215C
8 SM	2AI/2AQ	14DI/10DQ	4 MB	150 KB	CPU 1217C

## 2.2. قابلیت‌های توسعه (صفحه 31)

سیستم S7-1200 از طریق ماژول‌های مختلف قابل توسعه است:

- **Signal Board (SB)** : ماژول‌های کوچک که مستقیماً روی CPU نصب می‌شوند و I/O یا پورت ارتباطی اضافه می‌کنند.
- **Signal Module (SM)** : ماژول‌های استاندارد که در سمت راست CPU نصب می‌شوند و شامل:
  - ماژول‌های دیجیتال و آنالوگ
  - ماژول‌های ترموکوپل و RTD
  - ماژول‌های تخصصی مانند IO-Link Master

- Communication Module (CM) / Communication Processor (CP) : ماژول‌های ارتباطی که در سمت چپ CPU نصب می‌شوند و پروتکل‌هایی مانند PROFIBUS ، RS232/485 ، AS Interface – و ارتباطات سلولی (GPRS/LTE) را اضافه می‌کنند.

### 2.3 . حافظه و ذخیره‌سازی (صفحه 88)

- حافظه بارگیری (Load Memory) : غیرفرار، برای ذخیره پروژه، داده‌ها و پیکربندی. در کارت حافظه یا داخلی CPU قرار دارد.
- حافظه کاری (Work Memory) : فرار، برای اجرای برنامه.
- حافظه پایدار (Retentive Memory) : برای ذخیره مقادیر خاص در هنگام قطع برق.

### 2.4 . تایمر و کانتر (صفحه 30)

- تایمرها و کانترها از نوع IEC هستند.
- تعداد آن‌ها تنها توسط اندازه حافظه محدود می‌شود.
- هر تایمر 16 بایت و هر کانتر بسته به نوع آن 3، 6 یا 12 بایت فضا اشغال می‌کند.

## 3 . پردازش و اجرای برنامه (صفحه 65)

### 3.1 . چرخه اسکن (Scan Cycle)

برنامه کاربر به صورت چرخه‌ای اجرا می‌شود. هر چرخه شامل:

- به‌روزرسانی خروجی‌ها
- خواندن ورودی‌ها
- اجرای برنامه کاربر
- پردازش پس‌زمینه و ارتباطات

### 3.2 . بلوک‌های برنامه (صفحه 65 و 72)

- OB (Organization Block) : بلوک‌های سازمانی که ساختار برنامه را تعریف می‌کنند.

- FC (Function) : توابع بدون حافظه داخلی.
- FB (Function Block) : بلوک‌های تابعی با حافظه داخلی (Instance DB).
- DB (Data Block) : بلوک‌های داده برای ذخیره‌سازی.

### 3.3. مدهای عملیاتی CPU (صفحه 68)

- STOP : برنامه اجرا نمی‌شود.
- STARTUP : بلوک‌های راه‌اندازی اجرا می‌شوند.
- RUN : برنامه به صورت چرخه‌ای اجرا می‌شود.

### 4. ورودی/خروجی (I/O) و آدرس‌دهی (صفحه 94)

- Process Image (I/Q) : ناحیه حافظه برای نگهداری snapshot ورودی/خروجی.
- آدرس‌دهی فیزیکی (P): : دسترسی مستقیم به نقطه فیزیکی I/O (مثال %I0.0:P :).
- آدرس‌دهی سمبلیک: استفاده از نام‌های معنادار به جای آدرس‌های مستقیم.

### 5. ویژگی‌های ایمنی و امنیتی (صفحه 28 و 149)

- محافظت با رمز عبور برای دسترسی به CPU.
- محافظت از دانش فنی (Know-How Protection) برای مخفی کردن کد.
- محافظت از کپی (Copy Protection) برای جلوگیری از کپی غیرمجاز برنامه.
- امنیت ارتباطات با استفاده از پروتکل‌های امن مانند TLS.

### 6. ماژول‌های توسعه (صفحه 1257 به بعد)

- ماژول‌های دیجیتال (SM 1221, 1222, 1223)
- ماژول‌های آنالوگ (SM 1231, 1232, 1234)
- ماژول‌های دمایی ( ترموکوپل و RTD )
- ماژول‌های ارتباطی (CM/CP)
- کارت حافظه (SIMATIC Memory Card) برای بارگیری برنامه، آپدیت فرمور و انتقال داده.

## 7. ساعت زمان‌سنج (RTC) صفحه 92–93

- پشتیبانی از Real-Time Clock
- پشتیبانی از NTP برای همگام‌سازی شبکه‌ای
- ذخیره‌سازی زمان در خاموشی با خازن SuperCap (تا 20 روز)

## 8. پردازش آنالوگ صفحه 99

دقت و بازه ورودی/خروجی

نوع	بازه	دقت
ولتاژ	$\pm 10V$ , $\pm 5V$ , $\pm 2.5V$	16-bit (0–27648)
جریان	0–20mA	16-bit (0–27648)

تبدیل به واحد مهندسی

- استفاده از دستورات NORM\_X و SCALE\_X برای تبدیل به واحدهای واقعی (مثلاً دما، فشار)



## 9. امنیت سخت‌افزاری صفحه 149–157

محافظت از برنامه

- Know-how protection : رمزگذاری روی بلاک‌ها
- Copy protection : قفل برنامه به سریال CPU یا Memory Card
- Protection of confidential PLC configuration data : رمزگذاری فایل‌های پیکربندی

سطوح دسترسی CPU

توضیح	سطح دسترسی
بدون رمز	Full access
فقط خواندن	Read access
فقط HMI	HMI access
کاملاً قفل	No access

## 10. ارتباطات و شبکه صفحه 555–580

پروتکل‌های پشتیبانی شده

- PROFINET (TCP/IP, ISO-on-TCP, UDP)
- PROFIBUS (DP Master/Slave)
- AS-i

- Modbus TCP/RTU
- USS ( برای درایوهای سینوسی )
- GPRS/LTE ( با CP 1242-7 )

#### پیگر بندی شبکه

- IP Address باید دستی تنظیم شود
- NTP Server برای همگام سازی زمان
- X.509 Certificates ، Security: TLS 1.3

#### 11. ابعاد و نصب صفحه 46-47

مدل CPU	عرض (mm)	ارتفاع (mm)	عمق (mm)
1211C	90	100	75
1212C	110	100	75
1214C	130	100	75
1215C	150	100	75
1217C	150	100	75

- نصب: روی DIN Rail یا پنل
- فاصله برای تهویه: حداقل 25 mm بالا و پایین
- نصب عمودی کاهش 10 درجه ای دمای محیط را می طلبد

## 12. ماژول‌های خاص صفحه 511–550

### High-Speed Counter (HSC)

- تعداد: تا 6 کانتر در CPU
- فرکانس: تا 1 MHz ( بسته به CPU و نوع ورودی )

### Pulse Train Output (PTO)

- تعداد: تا 4 خروجی پالس
- فرکانس: تا 1 MHz برای کنترل سروو درایوها

### PID Control

- ماژول‌های PID : PID\_Compact ، PID\_3Step ، PID\_Temp
- قابل استفاده در ماژول‌های آنالوگ

## 13. ماژول‌های جانبی و لوازم صفحه 1360–1362

کاربرد	نام ماژول
منبع تغذیه V/2.5A24	PM 1207
سوئیچ شبکه 4 پورت	CSM 1277
ارتباط CANopen	CM CANopen

کاربرد	نام ماژول
ماژول RFID	RF120C
ماژول کنتور انرژی (Energy Meter)	SM 1238

#### 14. جمع‌بندی ساختار سخت‌افزاری S7-1200

صفحه	منطق عملکرد	بخش
27–30	واحد مرکزی با پردازنده، حافظه، I/O، و ارتباطات	CPU
31–32	افزودن I/O یا ارتباطات جدید به CPU	ماژول‌ها
88–90	ذخیره برنامه، داده‌ها، و بازیابی پس از خاموشی	Memory
92–93	زمان‌سنج دقیق با پشتیبانی NTP	RTC
149–157	رمزگذاری، محافظت از برنامه و داده‌ها	Security
555–580	پشتیبانی از PROFINET, PROFIBUS, Modbus, GPRS	Communication
46–47	نصب آسان، تهویه مناسب، ابعاد کوچک	Installation