چالش های پیش روی پست های دیجیتال در شبکه های انتقال

فرشته حسینی [1]، شاهین شکری [2]، ملیحه منتظریان [3]

[1] سرپرست بخش نرم افزار و پست های دیجیتال، اترک انرژی، تهران
f.hosseini@atrakenergy.com

[2] سرپرست بخش رلیاژ، اترک انرژی، تهران
s.shokri@atrakenergy.com

[3] سرپرست بخش مناقصات، اترک انرژی، تهران
m.montazeryan@atrakenergy.com

چکیده

پست های دیجیتال با جایگزینی کابل‌کشی سنتی مسی با کابل فیبر نوری مزایای زیادی از جمله کاهش هزینه کابل‌کشی، کاهش زمان راه اندازی و پیاده سازی پست و سرعت بالاتر پا سخ به خرابی ها را به همراه دارد. هدف نهایی ا ستاندارد IEC61850 در پست های دیجیتال ، مجهز شدن تمامی تجهیزات موجود در پســـت، اعم از ترانس های ولتاژ و جریان ، کلیدها و ترانس های قدرت به پورت فیبر نوری می باشـــد اما عمده تجهیزات موجود در صنعت هنوز به این ا ستاندارد مجهز نیستند به همین دلیل برای جمع آوری سیگنال های آنالوگ و دیجیتال از محوطه پست و ار سال به اتاق کنترل از تجهیز وا سط Merging Unit ا ستفاده می شود. در سال های اخیر و با روند رو به تو سعه احداث پست های دیجیتال با ا ستفاده از Merging Unit در کشورهای توسعه یافته، به تعداد زیادی از چالش های پیش روی این پست ها در الزامات جدید نسخه 2 پروتکل IEC61850 پرداخته شده است. در این مقاله سعی بر آن است که به این چالش ها و پاسخ متناظر با هر چالش در نسخه 2 پروتکل پاسخ داده شود.

کلمات کلیدی

پست دیجیتال، Process Bus، فیبر نوری، IEC61850-9-2LE، افزونگی شبکه، امنیت سایبری

1- مقدمه

صنعت برق در دهه‌های اخیر شاهد تحولات چشمگیری در حوزه پست‌های انتقال بوده به نحوی که این پست ها با بهره‌گیری از استانداردهای نوین ارتباطی مانند IEC 61850 به سمت پست‌های دیجیتال حرکت کرده‌اند. در پست های دیجیتال با نصب تجهیزی به نام Merging Unit در محوطه پست و جمع اوری داده ها اعم از داده های آنالوگ از ترانسدیوسرهای جریان و ولتاژ و داده های دیجیتال از تجهیزاتی مانند کلید های قدرت، این داده ها با استفاده بستر فیبر نوری مابین Merging Unit و اتاق کنترل بر پایه پروتکل IEC61850-9-2LE انتقال داده می شوند. در سیستم‌های سنتی، حجم زیادی از کابل‌های مسی برای انتقال این سیگنال‌ها از محوطه پست به تابلوهای کنترل و حفاظت استفاده می شد که استفاده از Merging Unit و شبکه فیبر نوری جایگزینی برای کابل‌کشی‌های سنگین و آنالوگ سنتی به شمار می رود و باعث کاهش قابل توجه در هزینه های احداث پست خواهد گردید.

استفاده از شبکه‌های فیبر نوری در سیستم‌های حفاظت پست‌های دیجیتال، با وجود مزایای زیاد مانند کاهش زمان راه اندازی پست، کاهش هزینه‌های احداث پست و یکپارچه سازی بین برند های سازنده مختلف چالش‌هایی نیز به همراه دارد. در ادامه به مهم‌ترین چالش‌هایی استفاده از فیبر نوری در سیستم حفاظت پست دیجیتال پرداخته شده است:

- جلوگیری از از دست رفتن اطلاعات* مورد نیاز سیستم حفاظت در شبکه Process Bus در پست های دیجیتال

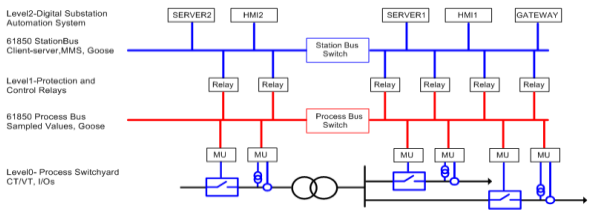
* Zero Packet Lost

- سنکرون زمانی تجهیزات مورد استفاده (اعم از رله ها و Merging Unitها) در شبکه Process Bus پستهای دیجیتال
- امنیت سایبری زیرساخت در شبکه Process Bus پست های دیجیتال
- نحوه تست تجهیزات در پست های دیجیتال

در ادامه این مقاله، به مهم‌ترین پیشرفت‌های پروتکل IEC61850 در Edition2 و نحوه حل چالش‌های پست‌های دیجیتال از جمله مکانیزم‌های افزونگی (مانند PRP/HSR) در این نسخه پرداخته می‌شود.

2- تشریح کلی سیستم پست دیجیتال

در معماری پست‌های دیجیتال مبتنی بر پروتکل IEC61850 ، Station Bus و Process Bus دو بستر کلیدی برای انتقال اطلاعات بین تجهیزات هستند. هر دوی این باس های اطلاعاتی از سوییچ های صنعتی تشکیل شده اند که مهم ترین تفاوت های آن در جدول 1 نشان داده شده است.



شکل 1: معماری پست های دیجیتال مبتنی بر پروتکل IEC61850

Station Bus وظیفه ارتباط بین IEDها (اعم از رله های حفاظتی، BCU، AVR و دستگاه های اندازه گیری) و سیستم‌های کنترل و مانیتورینگ پست (SAS[1]) را برعهده دارد و عمدتا برای جابه جایی پیام های IEC61850-8-1 (MMS) به منظور باز و بسته کردن کلیدها، کنترل بریکرها و نظارت بر وضعیت تجهیزات پست استفاده می شود.

Process Bus به انتقال داده‌های نمونه برداری شده بین ترانسدیوسرهای جریان و ولتاژ نوری یا Merging Unitها و و رله های حفاظتی می‌پردازد. این باس جایگزین کابل‌های مسی سنتی شده و ارتباطات دیجیتال را در سطح تجهیزات محوطه پست فراهم می‌کند. داده‌های نمونه برداری شده توسط Merging Unit از طریق Process Bus به رله‌های حفاظتی ارسال می‌شوند تا وضعیت لحظه‌ای جریان و ولتاژ را تشخیص دهند. این اطلاعات به رله‌ها کمک می‌کند که در شرایط بحرانی واکنش نشان دهند. از آنجاییکه رله های حفاظتی در پست دیجیتال فاقد کارت های آنالوگ و دیجیتال می باشند، تریپ های حفاظتی را از طریق شبکه Process Bus و پروتکل Goose به Merging Unitها ارسال کرده و خروجی های دیجیتال موجود در Merging Unit، تریپ ها را به کلید های قدرت ارسال می نمایند.

ویژگی	Process Bus	Station Bus
کاربرد اصلی	ارتباط بین Merging Unit با سیستم‌های کنترلی و حفاظتی	ارتباط بین سیستم‌های کنترلی و حفاظتی با سیستم اتوماسیون پست
پروتکل‌های استفاده‌شده	Sampled Values و Goose های Critical	MMS و Goose های Non Critical
پیام ها	مقادیر ولتاژ و جریان مورد استفاده در سیستم حفاظت پست	پیام های کنترلی و نظارت از سیستم اتوماسیون پست
رسانه انتقال	فیبر نوری	اترنت یا فیبر نوری
هدف	حفاظت بلادرنگ و نمونه‌برداری از داده‌ها	کنترل و مانیتورینگ
وابستگی به تأخیر کم	بسیار مهم	مهم اما بحرانی نیست

جدول1 : تفاوت های Process Bus و Station Bus

هرگونه تأخیر یا از دست رفتن این داده‌های نمونه برداری شده از ولتاژ و جریان در Process Bus باعث می شود که سیستم‌های حفاظتی دیر عمل کرده یا به‌طور اشتباه فرمان صادر کنند، که نتیجه آن می‌تواند خاموشی گسترده یا خسارت به تجهیزات باشد. به همین دلیل، شبکه Process Bus در پست‌های دیجیتال باید به مکانیزمی مجهز شوند تا از دسترسی مداوم و بدون وقفه به داده‌های حیاتی نمونه برداری شده اطمینان حاصل شود.

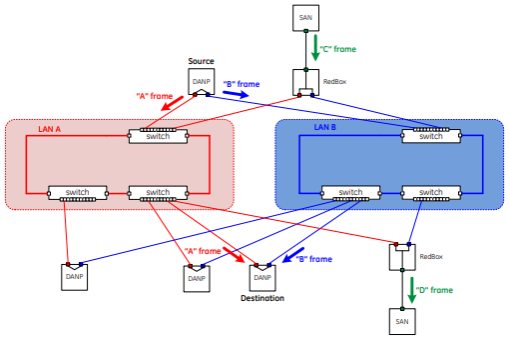
2-1- پروتکل های افزونگی در شبکه Process Bus

در نسخه 2 پروتکل IEC61850 بر لزوم استفاده از پروتکل های PRP[2] و HSR[3] به عنوان پروتکل های افزونگی[4] در شبکه Process Bus در پست های دیجیتال تاکید شده است. این پروتکل ها با فراهم آوردن دو مسیر مجزا برای انتقال اطلاعات به بهبود قابلیت اطمینان و پایداری شبکه کمک می‌کنند و با ارسال داده ها در این دو مسیر مجزا امکان از دست رفتن اطلاعات را با فرض خرابی هر کدام از این مسیرهای شبکه به صفر می رساند.

در شبکه PRP ، هر دستگاه به دو شبکه مجزا و مستقل LAN A و LAN B متصل می‌شود و تمام داده های نمونه برداری شده را به‌طور همزمان و موازی در هر دو شبکه ارسال می‌کند. گیرنده (به عنوان مثال رله یا Merging Unit)، اولین نسخه از اطلاعات (داده های ولتاژ و جریان نمونه برداری شده) را که به مقصد برسد پردازش کرده و نسخه دوم را نادیده می‌گیرد.

اگر هر کدام از شبکه‌های LAN A یا LAN B دچار خطا یا قطعی شود، داده‌ها از شبکه دوم بدون تأخیر ارسال می‌شوند. این مکانیزم باعث می‌شود که هیچ زمانی برای بازیابی اطلاعات در شبکه دوم نیاز نباشد و داده‌های

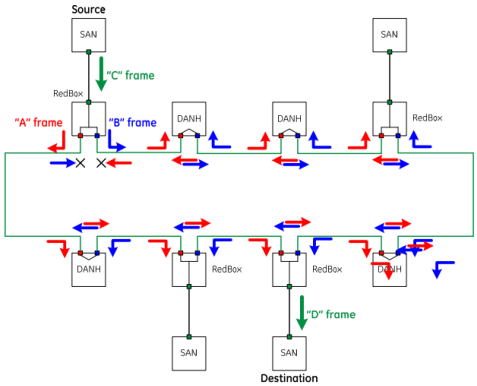
حیاتی مانند مقادیر نمونه برداری شده از ولتاژ و جریان و یا تریپ های حفاظتی مبتنی بر پروتکل GOOSE در صورت بروز خرابی بدون وقفه منتقل شوند.



شکل2: مفهوم پروتکل PRP [1]

پروتکلPRP به دلیل سازگاری کامل با لایه 2 شبکه و استفاده از فریم‌های استاندارد اترنت، می‌تواند بدون نیاز به تغییرات اساسی در زیرساخت شبکه، روی سوییچ های معمولی پیاده‌سازی شود. تنها دستگاه های گیرنده و فرستنده (رله ها و Merging Unit ها در شبکه پست دیجیتال) باید از پروتکل PRP پشتیبانی کنند و با استفاده از دو پورت شبکه به دو شبکه مستقل متشکل از سوییچ های اترنت معمولی متصل شوند.

در شبکه HSR تجهیزات به صورت زنجیره‌ای در یک ساختار حلقه‌ای به یکدیگر متصل می‌شوند و هر تجهیز با دو پورت ارتباطی PortA و PortB به صورت سری به پورت‌های تجهیز بعدی متصل می‌شوند و در نهایت حلقه کامل می‌شود .این حلقه در دو مسیر ارتباطی موازی عمل می‌کند و از ارسال داده های نمونه برداری شده به طور همزمان در هر دو جهت اطمینان حاصل می‌کند. در صورتی که یکی از مسیرها دچار مشکل شود، انتقال داده بدون اختلال در مسیر دیگر حلقه ادامه خواهد یافت.



شکل3: مفهوم پروتکل HSR [1]

در پروتکل PRP ، اطلاعات افزونگی در یک دنباله[5] (Lan Identifier Sequence Number, EtherType) در انتهای پکت های داده اضافه می شود و از دیدگاه سوییچ های شبکه، این دنباله جزیی از خود پکت های داده به شمار می رود. بنابراین در صورتی که دستگاهی که پروتکل PRP را ساپورت نمی کند به این شبکه متصل شود، اختلالی در عملکرد آن به وجود نمی آید و تنها همان دستگاه از قابلیت افزونگی برخوردار نخواهد بود. اما در پروتکل HSR بر خلاف PRP، اطلاعات افزونگی در یک هدر[6] در ابتدای پکت های داده افزوده می شود. به همین علت تمام دستگاه هایی که در شبکه HSR به کار می روند باید با پشتیبانی از پروتکل HSR، قابلیت تفکیک اطلاعات افزونگی از داده های اصلی را داشته باشند. به طور کلی مزایای پروتکل PRP نسبت به HSR عبارتند از:

- در شبکهPRP، نیازی نیست همه تجهیزات از این پروتکل پشتیبانی کنند. دستگاه‌هایی که از PRP پشتیبانی نمی‌کنند، می‌توانند به یکی از دو شبکه فیزیکی متصل شوند و همچنان به درستی عمل کنند. این ویژگی باعث می‌شود که PRP برای شبکه‌هایی که ترکیبی از تجهیزات قدیمی و جدید را شامل می‌شوند، مناسب‌تر باشد.
- شبکه PRP محدودیتی در تعداد تجهیزات ندارد، زیرا دو شبکه فیزیکی جداگانه می‌توانند مشابه شبکه‌های معمولی اترنت به هر میزان گسترش یابند. اما درHSR ، تعداد تجهیزات محدود است زیرا افزایش بیش از حد تعداد دستگاه‌ها می‌تواند باعث تأخیر در انتقال داده در حلقه و کاهش کارایی شبکه شود.
- با توجه به پشتیبانی PRP از دو شبکه فیزیکی کاملاً مجزا ، خطر از دست رفتن داده‌ها در اثر خطاهای شبکه به شدت کاهش می‌یابد زیرا حتی اگر یکی از شبکه‌های فیزیکی به طور کامل دچار خرابی شود، شبکه دیگر می‌تواند بدون هیچ تأثیری بر عملکرد کلی، کار خود را ادامه دهد، اما در شبکه HSR ، به دلیل ساختار حلقه‌ای، ممکن است در صورت بروز مشکلات خاص در شبکه (مانند خرابی همزمان چند لینک)، عملکرد شبکه مختل شود.

این ویژگی‌ها PRP را به گزینه‌ای مناسب‌تر برای محیط‌هایی با نیازهای متنوع و شبکه‌های بزرگ‌تر تبدیل می‌کند، به ویژه در مواردی که شبکه شامل تجهیزات غیر استاندارد یا ترکیبی از دستگاه‌های جدید و قدیمی باشد.

2-2- پروتکل های سنکرون زمانی در شبکه Process Bus

رله‌های حفاظتی در پست دیجیتال، برای انجام تصمیمات صحیح در شرایط خطا به داده‌های نمونه برداری شده از ولتاژ و جریان نیاز دارند. این داده‌ها باید به صورت همزمان و دقیق از نقاط مختلف شبکه توسط Merging Unitها جمع‌آوری شوند تا رله‌ها بتوانند وضعیت سیستم را به درستی تحلیل کنند. برای مثال، اگر نمونه‌برداری‌های جریان و ولتاژ بین رله و Merging Unit حتی به اندازه چند میلی ثانیه اختلاف داشته باشند، این تأخیر می‌تواند باعث اختلاف فاز شود و بر عملکرد صحیح رله‌ها تأثیر بگذارد.

برای محاسبه اختلاف فاز ناشی از 1 میلی‌ثانیه ناهماهنگی در سنکرون‌سازی داده‌های نمونه‌برداری رله‌ها در فرکانس 50 هرتز:

(1) میلی ثانیه T=1/f=1/50=20

یک چرخه کامل در فرکانس 50 هرتز برابر با 20میلی‌ثانیه است.

(2) 0.05 یا 5% =1 ms/20 ms

از آنجا که یک چرخه کامل برابر با 360درجه است، اختلاف فاز ناشی از 1 میلی‌ثانیه ناهماهنگی به صورت زیر محاسبه می‌شود:

(3) درجه360×0.05=18

در یک شبکه با فرکانس 50 هرتز، هر 1 میلی‌ثانیه ناهماهنگی در سنکرون‌سازی بین رله‌ها و Merging Unit باعث ایجاد 18درجه اختلاف فاز در داده‌های نمونه‌برداری می‌شود. بنابراین، دقت در سنکرون‌سازی رله‌ها و Merging Unitها در پست دیجیتال برای اطمینان از دقت بالای داده‌های نمونه برداری به ویژه در کاربردهای حفاظتی که حتی چند درجه اختلاف فاز می‌تواند تأثیر قابل توجهی بر عملکرد سیستم داشته باشد، بسیار حائز اهمیت است.

Time synchronization classes for IED synchronization				
Time performance class	Accuracy (µs)	Phase angle 50 Hz (°)	Phase angle 60 Hz (°)	Fault location (%)
TL	> 10 000	> 180	> 216	NA
T0	10 000	180	216	NA
T1	1 000	18	21.6	7.909
T2	100	1.8	2.2	0.780
T3	25	0.5	0.5	.0.195
T4	4	0.1	0.1	0.031
T5	1	0.02	0.02	0.008

شکل4: دقت زمانی مورد نیاز برای سنکرون تجهیزات در پست دیجیتال [2]

بر اساس استاندارد IEC61850، دقت 1 میکروثانیه در نمونه‌برداری تضمین می‌کند که اختلاف فاز در حدی کوچک باشد که عملکرد سیستم حفاظتی دچار مشکل نشود. دستیابی به این دقت زمانی در پست‌های دیجیتال به منظور هم‌زمانی و هماهنگی دقیق بین رله ها و Merging Unitها ، نیازمند استفاده از تکنیک‌ها و پروتکل های خاصی است.

استفاده از پروتکل PTP [۷] به منظور سنکرون زمانی با ساختار Master-Slave که در آن یک یا چند دستگاه به عنوان Master (منبع زمان) و سایر دستگاه‌ها به عنوان Slave (دریافت‌کننده زمان) عمل می‌کنند باعث می شود که دستگاه Master زمان دقیق را به دستگاه‌های Slave منتقل کند. PTP برای محاسبه تأخیر در انتقال داده های نمونه برداری شده از Delay Request و Delay Response استفاده می‌کند. این فرایند به تجهیزات (اعم از رله ها و Merging Unitها) اجازه می‌دهد تا تأخیر بین Master (به عنوان مثال MasterClock) و خودش را محاسبه کرده و آن را در تنظیمات زمان خود جبران کند .

این جبران‌سازی، تأثیر شبکه به عنوان مثال سوئیچ‌ها را کاهش داده و دقت سنکرون زمانی را افزایش می‌دهد. در ادامه به برخی دیگر از روش های ممکن برای افزایش سرعت و کاهش تاخیر در پست های دیجیتال اشاره می‌شود:

- طراحی شبکه با توپولوژی مناسب : طراحی شبکه پست دیجیتال باید به گونه‌ای انجام شود که حداقل تجهیز واسط اعم از سوییچ مابین Merging Unitها و رله‌ها وجود داشته باشد. به عبارتی بهتر است رله ها و Merging Unitهای هر فیدر در کنار هم به یک سوییچ یا حداکثر دو سوییچ کنار هم متصل شوند.
- مدیریت ترافیک شبکه : بهینه‌سازی ترافیک شبکه و اطمینان از عدم ازدحام داده ها می‌تواند تأثیر مستقیمی بر زمان‌بندی و کاهش تأخیر در انتقال داده‌ها داشته باشد. برای این منظور استفاده از سرویس های VLAN و QoS در سوییچ های شبکه می تواند به نحو قابل توجهی ترافیک شبکه در Process Bus را کاهش دهد. با استفاده ازQoS ، می‌توان ترافیک Goose و SMV را در سطح بالاتری از اولویت قرار داد. به این معنی که داده های Goose و SMV به سرعت و قبل از سایر انواع ترافیک (مانند داده‌های معمولی و غیره) پردازش و ارسال می‌شوند.
- جداسازی فیزیکی شبکه Process Bus و Station Bus: سوییچ‌های Process به طور خاص برای انتقال سریع و مطمئن داده‌های سریع مانند Goose و SMV طراحی شده‌اند. در حالی که سوییچ‌های Station ممکن است شامل ترافیک‌های کند و حجیم مانند داده های MMS یا حتی پروتکل های دیگر مانند Modbus یا داده های پیکره بندی تجهیزات باشند. جداسازی این دو شبکه می‌تواند باعث کاهش تأخیر در ارسال بسته‌های داده‌های سریع شود.

3- امنیت در شبکه پست دیجیتال

امنیت تجهیزات کنترلی پست های برق به دلیل پیوستگی آن با شبکه داخلی پست ، با مخاطرات زیادی روبرو است. برای جلوگیری از این تهدیدات، ارائه راهکاری مناسب و جامع با توجه به پروتکلها و استانداردهای ارتباطی این تجهیزات، امری ضروری است. ازنقطه نظر فنی، ارتقای پارامترهای امنیتی سیستم میتواند نقش مهمی در اطمینان پذیری از صحت عملکرد سیستم ها داشته باشد. لذا امنیت شبکه های ارتباطی و سیستمهای موجود در پستهای برق از دیدگاههای متفاوت نرم افزاری، سخت افزاری و شبکه میتواند اولین و مهمترین اولویت صنعت برق در حوزه فناوری اطلاعات باشد.[3]

در پست‌های دیجیتال مبتنی بر IEC 61850-9-2LE، داده‌های مهم مورد استفاده در رله های حفاظتی مانند اندازه‌گیری جریان و ولتاژ به صورت

نمونه‌های دیجیتال شده بین تجهیزات مختلف پست با استفاده از شبکه انتقال می‌یابد و پیام‌های Goose و SMV برای انتقال این اطلاعات به کار می‌روند. این داده‌ها برای عملکرد صحیح و به‌موقع تجهیزات حفاظتی و کنترلی در پست‌های دیجیتال بسیار مهم هستند. هرگونه تغییر یا دستکاری در این داده‌ها می‌تواند باعث اختلالات شدید، عملکرد نادرست تجهیزات، یا حتی خرابی‌های گسترده در شبکه برق شود. درنتیجه باید شبکه ارتباطی پست دیجیتال امن و مطمئن باشد.

علاوه بر آن پروتکل‌هایی مانندIEC 60870-5-104 ، DNP3 و IEC61850 که در سیستم‌های اتوماسیون و زیرساخت‌های حیاتی استفاده می‌شدند، زمانی طراحی شدند که امنیت سایبری دغدغه‌ی اصلی نبود و در آن زمان، تمرکز اصلی بر کارایی و عملکرد سیستم‌ها بود، و تهدیدات سایبری در سطحی که امروز وجود دارد، چندان مطرح نبودند. در نتیجه این پروتکل‌ها معمولاً بدون مکانیزم‌های امنیتی داخلی طراحی شده بودند، به این معنی که هیچ تضمینی برای محرمانگی، یکپارچگی، یا احراز هویت پیام‌ها وجود نداشت. در نتیجه، سیستم‌های مبتنی بر این پروتکل‌ها در برابر حملاتی مانند شنود (Eavesdropping) ، دستکاری داده‌ها (Data Tampering) و تزریق پیام‌های جعلی (Spoofing) آسیب‌پذیر هستند.

به همین علت استفاده از پروتکل امنیتی IEC62351 (به عنوان پروتکل امنیتی مکمل پروتکل های داده پست) سیستم‌های شبکه‌های برق علی الخصوص در شبکه پست دیجیتال به دلیل نقش مهمی که در حفاظت از پروتکل های Goose و SMV ایفا می‌کند، بسیار محبوب شده است. این پروتکل امنیتی به طور خاص برای رفع مشکلات و کمبودهایی طراحی شده است که در پروتکل‌های قدیمی‌تر اتوماسیون و شبکه داده وجود داشت. پروتکل‌های Goose و SMV از پروتکل‌های لایه 2 (Data Link) در مدل OSIهستند. پروتکل های لایه 2 از آدرس های MAC برای مسیریابی داده ها استفاده می کنند و به همین دلیل معمولاً بسیار سریع و کارآمد هستند. این بدان معناست که داده‌ها در یک دامنه محدود انتقال می‌یابند و نیاز به پردازش‌های مسیریابی پیچیده، مانند آنچه در لایه 3 (IP) اتفاق می‌افتد، ندارند. در لایه 3 پکت‌ها باید به آدرس‌های IP پردازش و برای ارسال به شبکه‌های مختلف مسیریابی شوند، که این فرآیند زمان بر است. به دلیل ساختار ساده و کارآمد لایه 2، انتقال داده‌ها با حداقل تأخیر و حداکثر سرعت انجام می‌شود که باعث می شود برای پروتکل هایی مانند Goose و SMV که سریع هستند ایده‌آل باشد. اما مکانیزم‌های امنیتی مانند رمزنگاری و احراز هویت در لایه 2 قابل پیاده‌سازی نیستند. در نتیجه، داده‌ها می‌توانند به راحتی توسط مهاجمان شنود، دستکاری داده یا بازپخش (replay attack) شوند.

استاندارد IEC62351-6 یکی از بخش‌های کلیدی استاندارد امنیتی IEC62351 است که به طور خاص برای حفاظت از پروتکل‌هایGoose و SMV مورد استفاده در پست های دیجیتال طراحی شده است و مکانیزم‌هایی را فراهم می‌کند که امنیت پیام‌های Goose و SMV را در برابر تهدیدات سایبری تقویت می‌کنند. روش‌های امنیتی اصلی که توسط این استاندارد ارائه می‌شوند به شرح زیر هستند:

- احراز هویت: پروتکل IEC62351-6 از امضای دیجیتال برای احراز هویت استفاده می‌کند. هر پیام Goose یا SMV با استفاده از یک کلید خصوصی که منحصراً در اختیار فرستنده است، امضا می‌شود. گیرنده پیام می‌تواند با استفاده از کلید عمومی فرستنده، صحت امضا را بررسی کرده و تأیید کند که پیام واقعاً از یک منبع معتبر و مجاز ارسال شده است و در طول مسیر تغییر نکرده است.
- بررسی یکپارچگی: استفاده از امضای دیجیتال همچنین به تضمین یکپارچگی پیام کمک می‌کند. امضای دیجیتال شامل Hash پیام است که اگر کوچک‌ترین تغییری در محتوای پیام رخ دهد، امضای دیجیتال نامعتبر می‌شود و گیرنده می‌تواند بلافاصله تغییرات غیرمجاز را تشخیص دهد.
- رمزنگاری: در حال حاضر، IEC 62351-6 عمدتاً بر روی احراز هویت و یکپارچگی متمرکز است و رمزنگاری کامل محتوای پیام را پیشنهاد نمی‌دهد، زیرا پیام‌هایGoose و SMV نیاز به انتقال سریع دارند و اضافه کردن رمزنگاری می‌تواند باعث افزایش تأخیر شود. با این حال، برای مواردی که امنیت بیشتری نیاز است، می‌توان از رمزنگاری لایه‌های پایین‌تر استفاده کرد.

این استاندارد به گونه‌ای طراحی شده است که ویژگی‌های خاص پیام های Goose و SMV را در نظر بگیرد. از آنجا که این پروتکل ها برای انتقال پیام‌های بسیار سریع و حساس به زمان طراحی شده است، استاندارد تلاش می‌کند تا امنیت را بدون تأثیر چشمگیر بر کارایی پیام‌ها پیاده‌سازی کند.

3-1- استفاده از سیستم های IDS[۸] در پست های دیجیتال

سیستم‌های تشخیص نفوذ برای شناسایی فعالیت‌های غیرمجاز در شبکه استفاده می‌شوند. در پست‌های دیجیتال، IDS با نظارت بر ترافیک شبکه در Process Bus، رفتارهای غیرعادی و تهدیدهای سایبری بالقوه را شناسایی می کند. IDSها در پست دیجیتال به دو صورت عمل میکنند:

- Signature-based IDS: این سیستم‌ها بر اساس پایگاه داده‌ای از الگوهای شناخته‌شده حملات کار می‌کنند. زمانی که ترافیک شبکه Process Bus با یکی از این الگوها مطابقت داشته باشد، IDS هشدار می‌دهد.
- Anomaly-based IDS: این سیستم‌ها به جای تطبیق الگوهای ثابت، به شناسایی رفتارهای غیرعادی در شبکه

Process Bus می‌پردازند. به عنوان مثال، اگر یک رله رفتار غیرعادی از خود نشان دهد (مانند ارسال حجم زیادی از پیام‌های غیرمنتظره Goose)، IDSمی‌تواند این فعالیت را شناسایی کند و هشدار دهد. این نوع سیستم ها برای شناسایی حملات جدید و ناشناخته مؤثرتر است.

از جمله کاربرد های اصلی IDS در شبکه Process Bus پست دیجیتال می توان به محافظت از پیام های Goose و SMV در برابر دستکاری، شناسایی تغییرات در الگوهای ترافیک شبکه Process Bus و جلوگیری از حمله بازپخش (Replay Attack) اشاره کرد.

4- تست تجهیزات در پست دیجیتال

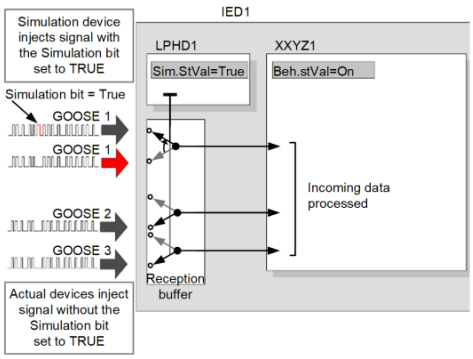
5- برای تست و نظارت بر پست‌های دیجیتال به جای استفاده از دستگاه های روتین مانند Multi-meter، از ابزارهای خاصی مانند Analyzersو Protocol Testers استفاده می‌شود که قادر به تست و ارزیابی پروتکل‌های دیجیتال و ارتباطات شبکه هستند. این ابزارها باید توانایی بررسی و تحلیل داده‌های Goose و SMV را داشته باشند.

در پست های سنتی یا اتوماسیون معمولی، تست تجهیزات از طریق تزریق ولتاژ و جریان توسط دستگاه تست به سمت ثانویه تجهیزات انجام می شود. اما در پست دیجیتال برای تست تجهیزات از یک دستگاه تست مدرن که قابلیت انتشار پیام Goose و SMV بر مبنای شبکه را دارد استفاده می شود.

پروتکل IEC61850 در نسخه 2، از دو ویژگی مهم زیر برای تست تجهیزات در پست های دیجیتال استفاده می کند:

- ارسال و دریافت پیام های Goose با Simulation Tag
- قرار دادن هر یک از Logical Nodeهای تعریف شده در IEC61850 به صورت جداگانه در حالت Test, Block, Test/Bock, On, Off

در روش اول تست تجهیزات، به عنوان مثال رله ها با تغییر Sim.StVal به حالت True موظف می شوند فقط به پیام های Goose با Simulation Bit=True پاسخ دهند. به این ترتیب دستگاه تست مدرن می تواند با شبیه سازی خود به جای رله یا Merging Unit پیام های Goose را شبیه سازی کرده و پاسخ های مناسب در شرایط مختلف را دریافت کند.



شکل5: رله تحت تست که فقط به دستگاه تست یا MU با Simulation Tag=True پاسخ می دهد. [4]

در روش های سنتی تست تجهیزات با استفاده از Test Block از سایر قسمت های سیستم ایزوله می شوند به نحوی که در زمان Test تریپ های رله به قسمت های در سرویس منتقل نشود. در نسخه جدید پروتکل IEC61850 این Test Block به صورت مجازی و با استفاده از قابلیت های Mode و Behavior شبیه سازی می شود. به نحوی که با قرار دادن این قسمت از رله روی حالت های Test، Block یا Test/Block تریپ های رله به خروجی های دیجیتال منتقل نمی شوند و فرآیند ایزولاسیون فرامین رله از قسمت های تحت سرویس به صورت مجازی انجام می شود.

Mode and Behavior	Value
ON (enabled) Function active Outputs (to process) generated Reporting (to client) Control services (from client) accepted Functional (process related) data visible Configuration (capability) data visible (Normal state)	1
BLOCKED Function active No outputs (to process) generated No reporting Control services (from client) rejected Functional (process related) data visible Configuration (capability) data visible (Process is passively supervised)	2
TEST Function active Outputs (to process) generated Reporting (to client) flagged as test Control services (from client) accepted Functional (process related) data visible Configuration (capability) data visible (Function is operated but results are indicated as test results)	3
TEST/BLOCKED Function active No outputs (to process) generated Reporting (to client) flagged as test Control services (from client) accepted Functional (process related) data visible Configuration (capability) data visible (Function is operated in Test Mode but with no impact to the process)	4
OFF (disabled) Function not active No outputs (to process) generated No reporting (to client) Control services (from client) rejected Functional (process related) data not visible	5

شکل6: حالت های مختلف برای Mode در رله ها [4]

همانطور که در شکل بالا معلوم است با قراردادن رله ها در حالت Test/Blocked فرامین تریپ به خروجی های دیجیتال منتقل نمیشوند.

5- نتیجه گیری

کاهش هزینه‌ها در پست‌های دیجیتال به‌ویژه در مقایسه با پست‌های سنتی به دلایل زیر از مزایای قابل توجه و اصلی این فناوری به شمار می‌آید.

- کاهش قابل توجه در هزینه های کابل کشی پست به دلیل جایگزینی با شبکه فیبر نوری
- کاهش قابل توجه در هزینه های عمرانی پست به دلیل حذف ساختمان های BCR پست و کاهش حجم کانال های کابل پست
- کاهش قابل توجه در هزینه و تعداد تابلو های پست به دلیل حدف رله های کمکی TCS، CCS و Lockout و در نتیجه کاهش ابعاد ساختمان اتاق کنترل
- کاهش قابل توجه در زمان راه اندازی پست به دلیل عدم نیاز به چک کردن سر سیم ها
- کاهش قابل توجه در زمان خاموشی مورد نیاز در پست های در حال توسعه

با وجود مزایای قابل توجه کاهش هزینه‌ها در پست‌های دیجیتال،برای این که یک پست دیجیتال به‌طور مؤثر و کارآمد عمل کند، نیاز است که در زمان طراحی پست به چالش‌های مطرح شده توجه شود و به هر قسمت با توجه به الزامات مطرح شده در استاندارد پاسخ داده شود.

مراجع

[1] Rich Hunt, Bogdan Popescu, "Comparison of PRP and HSR Networks for Protection and Control Applications," Presented at the Western Protective Relay Conference, Spokane, WA, October 20-22, 2015

[2] Marcel Geor, , Alex Lippitt, and Hayden Alves, Full digital substation with Process Bus - time synchronization best practice, , June, 2020

[3] رضا ابراهیمی آتانی، محدثه اسماعیلی، فاطمه فکوری، مسعود ایمانی، فرزان دستیار بررسی حملات سایبری روی سامانه های کنترل صنعتی شبکه فوق توزیع برق،چهارمین کنفرانس بین المللی ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات29 و 30 آبان 1398

[4] Edson Hernández, Tovah Whitesell, and Karen Leggett Wyszczelski, "A Practical Guide to Substation Testing Using IEC 61850 Mode and Behavior", Presented at the Power and Energy Automation Conference Seattle, Washington March 3–4, 2020

[1] Substation Automation System
[2] Parallel Redundancy Protocol
[3] High Availability Seamless Redundancy
[4] Redundancy

[5] Trailer
[6] Header
[7] Precision Time Protocol
[8] Intrusion Detection System