مروری بر امنیت سایبری سیستم‌های الکترونیک قدرت

1-1- مقدمه

امنیت سایبری صنعتی به مجموعه‌ای از راهکارها و فرایندهای حفاظتی اطلاق می‌شود که با هدف صیانت از سامانه‌های کنترل صنعتی(ICS) ، شبکه‌های عملیاتی (OT) و زیرساخت‌های حیاتی در برابر تهدیدات سایبری طراحی شده‌اند. با گسترش روزافزون اتوماسیون صنعتی و اتصال تجهیزات صنعتی به شبکه‌های دیجیتال، ضرورت تأمین امنیت در محیط‌های صنعتی بیش از گذشته احساس می‌شود. حملات سایبری به تأسیسات حیاتی مانند نیروگاه‌ها، پالایشگاه‌ها، کارخانه‌ها و سامانه‌های حمل‌ونقل مثل کشتی‌ها می‌تواند پیامدهای فاجعه‌باری در پی داشته باشد؛ ازاین‌رو، امنیت سایبری به یکی از ارکان اصلی پایداری و ایمنی در صنعت مدرن تبدیل شده است.

1-2- حملات سایبری به زیرساخت‌های صنعتی

سیستم‌های صنعتی پیشرفته که از قابلیت‌های سایبری نیز بهره‌مند هستند(معروف به سیستم‌های سایبر-فیزیکی (CPS)) نقش محوری در ارائه خدمات حیاتی، افزایش بهره‌وری، و بهینه‌سازی فرآیندها در حوزه‌های گوناگون صنعتی ایفا می‌کنند. این سیستم‌ها با ادغام سطوح فیزیکی، محاسباتی و ارتباطی، به سنگ‌بنای زیرساخت‌های صنعتی مدرن تبدیل شده‌اند.

با این حال، پیچیدگی و اتصال فزاینده این سیستم‌ها نه‌تنها کارایی را افزایش می‌دهد، بلکه آن‌ها را در برابر تهدیدات و آسیب‌پذیری‌های سایبری نیز آسیب‌پذیرتر می‌سازد. به‌ویژه، تعامل دائم میان اجزای فیزیکی و سایبری، زمینه را برای بروز حملات هماهنگ و گسترده فراهم می‌کند؛ حملاتی که می‌توانند با صدور یک فرمان اشتباه یا تغییر یک متغیر حساس، منجر به خرابی‌های فیزیکی شدید، توقف تولید یا حتی فجایع ایمنی شوند.

در سال‌های اخیر، پژوهش‌های متعددی در زمینه تحلیل آسیب‌پذیری سیستم‌های سایبر-فیزیکی انجام شده است که هدف آن‌ها شناسایی نقاط ضعف بالقوه پیش از وقوع حمله یا آسیب واقعی است. این تحقیقات نشان داده‌اند که هرچه درهم‌تنیدگی و ارتباط بین اجزای CPS بیشتر شود، احتمال یافتن مسیرهای نفوذ و بهره‌برداری از آسیب‌پذیری‌ها توسط مهاجمان نیز افزایش می‌یابد. بنابراین، طراحی ایمن، تحلیل تهدیدات و پیاده‌سازی مکانیسم‌های دفاعی چندلایه، برای حفظ پایداری و ایمنی این سیستم‌های حیاتی امری ضروری است

از جمله مهم‌ترین حملات سایبری انجام‌شده، حمله به زیرساخت شبکه قدرت اوکراین [17] و استاکس‌نت [17,18] است.

1-3- امنیت سایبری در الکترونیک قدرت

در یک سیستم قدرت نوین، مبدل‌های متصل به شبکه معمولاً از راه دور توسط سیستم کنترل و از طریق خطوط ارتباطی مانند Zigbee، G3 (cellular) و G4 (LTE) کنترل می‌شوند.[19] این ظرفیت‌های ارتباطی و

کنترلی، رویارویی با حملات سایبری را به صورت اجتناب‌ناپذیری گسترش می دهند. بنابراین، حساسیت این سیستم به حملات سایبر-فیزیکی زیاد می شود. ساختار سایبر-فیزیکی این سیستم‌ها شامل دو لایه اصلی است:)در شکل ۱ نشان داده شده است.

1. **لایه فیزیکی** : شامل بار، خطوط انتقال و مبدل‌های الکترونیک قدرت است که برای ادوات آن می‌توان مدل‌های ریاضی تقریبی رفتار دینامیکی آن‌ها را به دست آورد. [21]

2. **لایه سایبری**: شامل واحدهایی مانند کنترل، تشخیص، الگوریتم‌ها و ارتباطات است که توسط سیستم‌های کنترلی و خطوط ارتباطی تشکیل شده‌اند. [22]

نقاط آسیب‌پذیر این ساختار در برابر حملات عبارت‌اند از: [23]

1. **حملات سایبری به سیستم کنترل**: در این نوع حمله، هدف اصلی **واحد کنترل مبدل** و الگوریتم‌های کنترلی آن است. مهاجمان می‌توانند با دسترسی به نرم‌افزار سیستم کنترل، آن را تغییر داده، غیرفعال کرده یا رفتار آن را تخریب کنند. مسیرهای متداول نفوذ شامل:

- نفوذ از طریق ایستگاه‌های مانیتورینگ(HMI)
- بهره‌برداری از پورت‌های باز یا ارتباطات ناایمن بین کنترلر وSCADA
- دسترسی به پلتفرم‌های مبتنی بر Ethernet/IP یا Modbus که اغلب بدون رمزنگاری یا احراز هویت عمل می‌کنند

❖ *نمونه حمله* :تغییر پارامترهای حلقه کنترلی یا ارسال فرمان قطع ناگهانی به سیستم قدرت که می‌تواند موجب خاموشی، نوسانات ولتاژ یا اضافه‌بار شود.

2. **حمله به خود مبدل**: در این حملات، هدف خود سخت‌افزار مبدل است. مبدل‌های متصل به شبکه از اجزای الکترونیکی پیچیده‌ای نظیر:

- DSP (Digital Signal Processor)
- میکروکنترلرهای بلادرنگ
- FPGA/ASICهای هوشمند

تشکیل شده‌اند که هر یک می‌تواند به‌عنوان نقطه ورود یک حمله مورد استفاده قرار گیرد. برخی تهدیدات در این حوزه عبارت‌اند از:

- تزریق بدافزار به حافظه داخلی(firmware attack)

- آلوده‌سازی از طریق به‌روزرسانی‌های نرم‌افزاری آلوده
- اعمال ولتاژ غیرمجاز به ورودی‌های دیجیتال/آنالوگ برای ازکارانداختن سخت‌افزار

❖ *نتیجه* :خرابی فیزیکی، آتش‌سوزی، ازکارافتادن زیرماژول‌ها، یا تغییر رفتار مبدل.

3. **حمله به سیستم مانیتورینگ و شناسایی**: این حملات، اطلاعات حسگرها و سیستم مانیتورینگ را هدف قرار می‌دهند. اهداف رایج شامل:

- **تزریق داده جعلی** (FDI): ارسال مقادیر غیرواقعی به حسگرهای ولتاژ، جریان یا موقعیت موتور
- حملاتReplay : بازپخش داده‌های قبلی برای فریب سیستم‌های تشخیص ناهنجاری
- تزریق پارازیت زمانی یا نویز دیجیتال برای ایجاد تأخیر یا خطا در تفسیر داده‌ها

با رشد استفاده از سنسورهای IoT و شبکه‌های بی‌سیم، سطح حمله به‌طرز قابل توجهی گسترش یافته و مهاجمان می‌توانند از راه دور سیستم مانیتورینگ را فریب دهند.

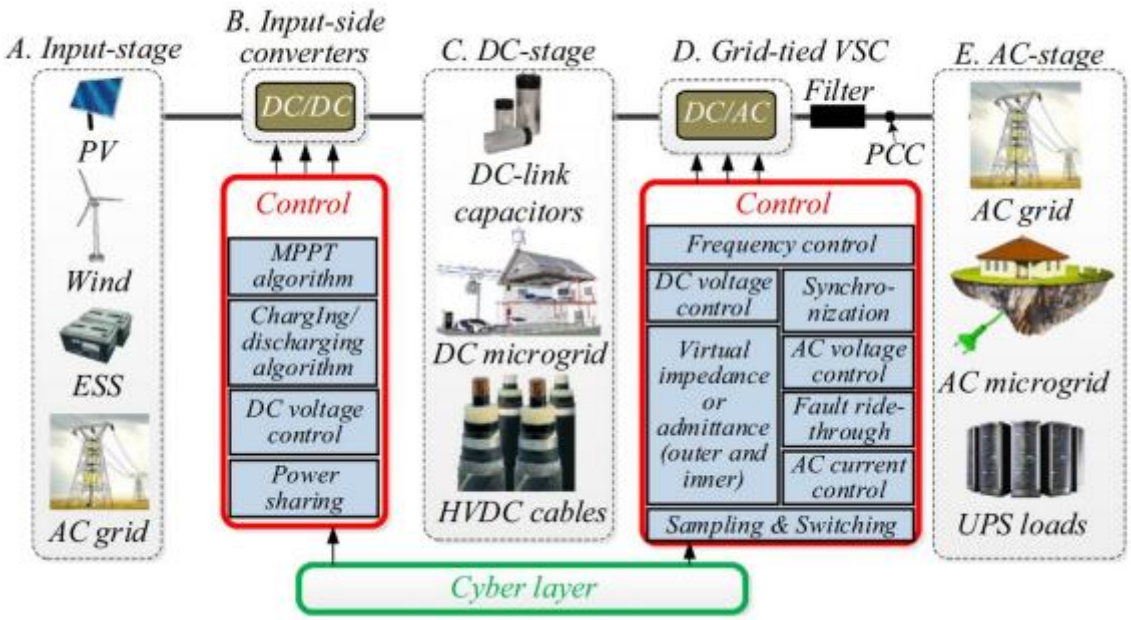
❖ *نتیجه* :تصمیم‌گیری اشتباه توسط سیستم حفاظتی یا کنترلی و وارد شدن آسیب به بار یا مبدل.

4. **حمله به شبکه**: در این نوع، هدف حمله شبکه ارتباطی بین اجزای سیستم است. این حملات می‌توانند شامل موارد زیر باشند:

- جعل پیام‌های کنترلی (مانند تغییر سطح تقاضای انرژی)
- قطع ارتباط بین نیروگاه و شبکه از طریق حملات DoS یا خاموش‌سازی کلیدهای حفاظتی
- تحریک مبدل برای جداسازی از شبکه با تزریق ولتاژهای غیرعادی (مثلاً شبیه‌سازی شرایط ولتاژ پایین یا ولتاژ صفر)

❖ *نتیجه*: خارج شدن مبدل از سرویس، ناپایداری شبکه، یا توقف کامل فرآیندهای حیاتی صنعتی.

درمجموع، آسیب‌پذیری لایه‌های فیزیکی و سایبری این سیستم‌ها در برابر طیف گسترده‌ای از حملات فیزیکی و سایبری، نیاز به توجه ویژه به امنیت این سیستم‌ها را ضروری می‌سازد.



شکل1- ساختار فیزیکی-سایبری سیستم قدرت مبتنی بر منابع انرژی تجدیدپذیر

1-4- معرفی حملات متداول

حملات سایبری به سیستم‌های قدرت مبتنی بر مبدل‌های الکترونیک قدرت، می‌تواند شامل موارد زیر باشد:

1. **خودداری از خدمات(DoS)** : حمله DoS یکی از رایج‌ترین و مخرب‌ترین تهدیدات سایبری است که هدف آن، مختل کردن دسترسی کاربران مجاز به منابع و خدمات سیستم است. در این نوع حمله، مهاجم با ایجاد بار اضافی و مصرف بیش‌ازحد منابع حیاتی سیستم (مانند پهنای باند شبکه، توان پردازشی، یا ظرفیت ذخیره‌سازی) عملاً عملکرد طبیعی سامانه را فلج می‌کند. در شبکه‌های صنعتی و سامانه‌های سایبر-فیزیکی نظیر مبدل‌های قدرت و محرکه‌های الکتریکی، بروز یک حمله DoS می‌تواند تبعات بسیار خطرناکی به همراه داشته باشد. برای مثال، مهاجم با تزریق حجم عظیمی از ترافیک به شبکه صنعتی، باعث ایجاد ازدحام ارتباطی شده و ارتباط میان اجزای حیاتی سیستم (از جمله مبدل‌ها، واحدهای کنترل‌کننده، سیستم مانیتورینگ و محرکه‌های الکتریکی) مختل می‌شود. در چنین شرایطی، فرمان‌های کنترلی به‌درستی منتقل نمی‌شوند، پاسخ سنسورها با تأخیر یا گمراهی مواجه می‌شود، و حلقه‌های کنترلی دچار اختلال می‌گردند. این وضعیت می‌تواند منجر به رفتار ناپایدار در سامانه قدرت، بروز خطا در عملکرد مبدل‌ها، یا حتی ایجاد حوادث فیزیکی خطرناک در محیط صنعتی شود. به همین دلیل، تشخیص زودهنگام حملات DoS و پیاده‌سازی راهکارهای دفاعی مانند سامانه‌های تشخیص نفوذ(IDS) ، تخصیص پهنای باند تطبیقی، و فیلترهای ترافیکی صنعتی در شبکه‌های OT از اهمیت ویژه‌ای برخوردار است.

2. **تزریق اطلاعات غلط (FDI[2])**

حمله FDI یکی از تهدیدات پیشرفته و هدفمند در سامانه‌های سایبر-فیزیکی است که با دست‌کاری داده‌های تبادلی میان اجزای سیستم، عملکرد سامانه کنترلی را به‌طور مستقیم تحت تأثیر قرار می‌دهد. در این نوع حمله، مهاجم با قرار گرفتن در موقعیت مرد میانی (Man-in-the-Middle) یا با نفوذ به گره‌های میانی شبکه، پیام‌هایی را که بین حسگرها، کنترلرها و واحدهای اجرایی تبادل می‌شوند، دست‌کاری یا جعل می‌کند. تمرکز اصلی این حملات معمولاً بر داده‌های خروجی حسگرها است؛ زیرا حسگرها نقش حیاتی در درک وضعیت سیستم برای تصمیم‌گیری کنترلی دارند. با ارسال مقادیر نادرست (مانند دمای کمتر از حد واقعی، جریان اشتباه، یا موقعیت غلط)، مهاجم سیستم کنترل را فریب داده و باعث می‌شود فرمان‌های اشتباهی به اجزای فیزیکی داده شود. این موضوع ممکن است منجر به: عملکرد نادرست مبدل‌ها و محرکه‌ها بروز نوسانات خطرناک در شبکه قدرت توقف فرآیندهای حیاتی وارد آمدن آسیب‌های مکانیکی یا الکتریکی به تجهیزات برخلاف حملات DoS که با قطع ارتباط موجب توقف سیستم می‌شوند، حملات FDI با ارائه اطلاعات قانع‌کننده اما نادرست، سیستم را به انجام رفتارهای مخرب ولی ظاهراً معتبر وادار می‌کنند. این امر تشخیص آن‌ها را بسیار دشوار می‌سازد و خطرات پنهانی به‌مراتب بیشتری به همراه دارد.

از جمله روش‌های مقابله با حمله FDI می‌توان به موارد زیر اشاره کرد:

- ❖ استفاده از ناظرهای مقاوم (Robust Observers) مانند Kalman Filter مقاوم در برابر خطا
- ❖ طراحی سامانه‌های تشخیص ناهنجاری مبتنی بر مدل یا داده‌محور
- ❖ رمزنگاری و احراز هویت در لایه‌های ارتباطی برای جلوگیری از دست‌کاری بسته‌ها

بنابراین، امنیت داده‌های حسگری و کنترل، نقشی حیاتی در حفظ عملکرد ایمن و پایدار سیستم‌های صنعتی مدرن ایفا می‌کند.

3. **درج بدافزار** : در حمله درج بدافزار، مهاجم با بهره‌گیری از آسیب‌پذیری‌های نرم‌افزاری یا ضعف‌های امنیتی موجود در سیستم، اقدام به وارد کردن کد یا نرم‌افزار مخرب به محیط کنترل یا مانیتورینگ می‌نماید. این نوع حمله می‌تواند از طریق مسیرهای مختلفی انجام شود، از جمله:

- اتصال دستگاه‌های آلوده) مانندUSB ، لپ‌تاپ تعمیرکار(
- به‌روزرسانی‌های نرم‌افزاری ناسالم
- نفوذ از طریق شبکه ناامن(IT/OT)

[2] False Data Injection

- بهره‌برداری از سرویس‌های باز یا بدون احراز هویت در سیستم‌های SCADA وPLC

کد مخرب تزریق‌شده ممکن است عملکردهای گوناگونی داشته باشد، از جمله:

- **تغییر رفتار کنترلی مبدل‌ها یا محرکه‌ها**
- **خاموش‌سازی یا راه‌اندازی مکرر اجزا**
- **جمع‌آوری و ارسال اطلاعات حساس به مهاجم (جاسوسی صنعتی)**
- **باز کردن در پشتی (Backdoor) برای حملات بعدی**
- **تخریب تدریجی عملکرد سیستم(Sabotage)**

برخلاف حملاتی که صرفاً داده یا ارتباطات را هدف قرار می‌دهند، بدافزارها می‌توانند **در درازمدت، بدون جلب توجه، در ساختار سیستم باقی بمانند** و حتی به‌صورت زمان‌بندی‌شده یا شرطی فعال شوند. نمونه‌های معروف مانند **Stuxnet** و **Triton** نشان داده‌اند که حملات بدافزار به سیستم‌های صنعتی می‌توانند صدمات جدی به تجهیزات فیزیکی وارد کرده و فرآیندهای حیاتی را مختل کنند.

4. **حمله تأخیری** : حمله تأخیری یکی از انواع حملات زمان‌بندی‌شده در سامانه‌های سایبر-فیزیکی و شبکه‌های صنعتی است که هدف آن برهم زدن هماهنگی و زمان‌بندی دقیق اجزای سیستم کنترلی از طریق وارد کردن تأخیر مصنوعی در تبادل داده‌ها است. در این نوع حمله، مهاجم با قرار گرفتن در مسیر ارتباطی بین اجزای مختلف سیستم (مانند سنسورها، کنترلرها، مبدل‌ها و سیستم مانیتورینگ)، بسته‌های اطلاعاتی را با تأخیر غیرعادی ارسال یا دریافت می‌کند. اگرچه محتویات داده‌ها ممکن است تغییر نکند، اما تاخیر در زمان تحویل آن‌ها می‌تواند موجب اختلال در عملکرد حلقه‌های کنترلی بلادرنگ شود.

آثار و نتایج احتمالی حمله تأخیری:

- نوسانات ناخواسته در ولتاژ یا جریان به‌دلیل واکنش دیرهنگام سیستم کنترل
- اختلال در هماهنگی بین مبدل‌ها و واحدهای محرکه
- فروپاشی پایداری سیستم به‌ویژه در شرایط گذرا یا بار متغیر
- تشخیص نادرست وضعیت سیستم در الگوریتم‌های مانیتورینگ
- فعال‌سازی اشتباه حفاظت‌ها یا خاموشی ناخواسته تجهیزات

نمونه‌های کاربردی:

در مبدل‌های MMC یا سیستم‌های کنترل ولتاژ در شبکه‌هایHVDC ، ورود تأخیر حتی در حد چند میلی‌ثانیه می‌تواند باعث ناهماهنگی در کلیدزنی زیرماژول‌ها، نوسانات خازنی، و در نهایت آسیب به بار یا مبدل شود

5. **حمله پارازیت** : حمله پارازیتی نوعی از حملات فیزیکی-سایبری است که در آن مهاجم با ارسال سیگنال‌های مخرب و مزاحم (پارازیت) در باندهای فرکانسی مورد استفاده توسط سیستم، باعث ایجاد اختلال در ارتباطات بی‌سیم یا عملکرد حسگرهای الکترونیکی می‌شود. این حمله به‌ویژه در سیستم‌هایی که به شبکه‌های ارتباطی بی‌سیم (Wireless ICS/SCADA) یا سنسورهای IoT وابسته هستند، بسیار خطرناک و مؤثر است.

مهاجم با استفاده از تجهیزات ساده‌ای مانند فرستنده‌های رادیویی یا امواج RF تنظیم‌شده، فرکانس کاری شبکه یا حسگر را هدف قرار داده و با تزریق نویز در آن باند، مانع از دریافت صحیح سیگنال‌های واقعی توسط گیرنده می‌شود. این نویز می‌تواند:

- ارتباط بین حسگر و کنترلر را قطع کند
- موجب از دست رفتن بسته‌های داده یا تکرار ارسال شود
- تاخیر و خطا در تصمیم‌گیری سیستم به‌وجود آورد
- سامانه را به اشتباه در حالت خطا یا خطر تشخیص دهد و اقدامات نامناسب انجام دهد

کاربرد در سیستم‌های صنعتی:

در سامانه‌هایی نظیر کنترل مبدل‌هایMMC ، پیشرانه‌های الکتریکی یا سیستم‌های مانیتورینگ مبتنی بر حسگر بی‌سیم، حمله پارازیتی می‌تواند منجر به اختلال در حلقه کنترلی بلادرنگ، فعال شدن بی‌مورد حفاظت‌ها، یا حتی خاموشی کامل سیستم شود.

پیامدها:

- از بین رفتن هماهنگی بین اجزای کنترل و فرمان
- عملکرد ناپایدار سیستم
- افزایش تلفات و کاهش بهره‌وری

- خرابی تجهیزات به‌دلیل پاسخ اشتباه به شرایط غیرواقعی

به‌طورکلی، حملات خودداری از خدمات (DoS) و تزریق اطلاعات غلط، دو نوع حمله‌ای هستند که به‌طور منظم در این حوزه مشاهده می‌شوند و مخرب بودن آن‌ها برای طیف گسترده‌ای از عناصر سیستم قدرت هوشمند، به اثبات رسیده است. توجه به این تهدیدات و درک عمیق‌تر از آن‌ها، برای تقویت امنیت سایبری سیستم‌های قدرت و جلوگیری از وقوع حملات ضروری است.

مراجع

[1] IEEE Standard 1662-2008, Guide for the Design and Application of Power Electronics in Electrical Power Systems on Ships, is published by the IEEE (E-ISBN: 978-0-7381-5840-2, ISBN: 978-0-7381-5841-9, and Digital Identifier: 10.1109/ IEEESTD.2009.4804134).

[2] IEEE Spectrum, "The Increasing Importance of Cybersecurity in the Power Industry," 2019

[3] J. Wang, H. Li, and Y. Zhang, *Modular Multilevel Converters: Analysis, Control, and Applications*. Hoboken, NJ, USA: Wiley, 2014.

[4] M. A. S. Masoum, M. F. Conlon, and K. A. M. H. Al-Mansoori, "Modular Multilevel Converter Topologies Suitable for Smart Grid Applications," *IEEE Transactions on Power Electronics*, vol. 30, no. 1, pp. 82-95, Jan. 2015.

[5] M. Hagiwara, R. Maeda, and H. Akagi, "Modular Multilevel Converter: An Overview of Its Control and Modulation Techniques," *IEEE Transactions on Power Electronics*, vol. 30, no. 1, pp. 37-53, Jan. 2015.

[6] Du, S., Dekka, A., Wu, B., & Zargari, N. (2018). *Modular Multilevel Converters: Analysis, Control, and Applications*. Wiley. ISBN: 978-1-119-36630-0.

[7] H. Akagi, E. H. Watanabe, and M. Aredes, *Instantaneous Power Theory and Applications to Power Conditioning*. Hoboken, NJ, USA: Wiley, 2007.

[8] P. M. Curtis, *Maintaining Mission Critical Systems in a 24/7 Environment*. Hoboken, NJ, USA: Wiley, 2013.

[9] C. C. Davidson and D. R. Trainer, "Innovative Concepts for Hybrid Multi-Level Converters for HVDC Power Transmission," 2010.

[10] B. JACobson, P. Karlsson, G. Asplund, L. Harnefors, T. Jonsson, VSCHVDC Transmission with Cascaded Two-Level Converters, in: CIGR´E B4-110, 2010.

[11] S. Rohner, M. Hiller, and R. Sommer, "A New Highly Modular Medium Voltage Converter Topology for Industrial Drive Application," in *Power Electronics and Applications*, 2009, pp. 1-6.

[12] S. Zhou, H. Zhang, and Y. Liu, "Capacitance Reduction of the Hybrid Modular Multilevel Converter by Decreasing Average Capacitor Voltage in Variable-Speed Drives," *IEEE Transactions on Power Electronics*, vol. 34, no. 2, pp. 1580-1594, Feb. 2018.

[13] B. Gemmell, A. H. M. A. Rahman, and J. R. R. G. M. de Almeida, "Prospects of Multilevel VSC Technologies for Power Transmission," in *2008 IEEE/PES Transmission and Distribution Conference and Exposition*, Chicago, IL, USA, 2008, pp. 1-6.

[14] Du, Sixing, and Jinjun Liu. "A study on DC voltage control for chopper-cellbased modular multilevel converters in D-STATCOM application." IEEE TransACtions on Power Delivery28.4 (2013): 2030-2038.

[15] H. Zhu, S. Du, and J. Liu, "Design of Power Electronic Transformer Based on Modular Multilevel Converter," in *2012 Asia-Pacific Power and Energy Engineering Conference*, Shanghai, China, 2012, pp. 1-6.

[16] D. Iannuzzi, L. Piegari, and P. Tricoli, "A Novel PV-Modular Multilevel Converter for Building Integrated Photovoltaics," in *2013 Eighth International Conference and Exhibition on Ecological Vehicles and Renewable Energies (EVER)*, Monte Carlo, Monaco, 2013, pp. 1-6

[17] M. G. Angle, S. Madnick, J. L. Kirtley and S. Khan, "Identifying and Anticipating Cyberattacks That Could Cause Physical Damage to Industrial Control Systems," in IEEE Power and Energy Technology Systems Journal, vol. 6, no. 4, pp. 172-182, Dec. 2019, doi: 10.1109/JPETS.2019.2923970.

[18] Erno Pentzin, " Protecting an Industrial AC Drive Application against Cyber Sabotage," M.S. thesis, school of electrical engineering, aalto university, 2013. [Online]. Available: https://aaltodoc.aalto.fi/bitstream/handle/123456789/8780/master_Pentzin_Erno_2013.pdf?sequence=1&isAllowed=y

[19] V. C. Gungor et al., "Smart grid technologies: Communication technologies and standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529-539, 2011.