

**صفحه عنوان- نمونه پيوست هاي شماره 1، 2، 3**

مهندسي امنيت مبتني بر مدل براي سيستم هاي فيزيکي سايبري

Model-based security engineering for cyber-physical systems

**صفحه سوم: تصويب نامه**

**صفحه چهارم سپاسگذاري**

**صفحه پنجم: حقوق مالکيت**

**صفحه ششم: صحت، اصالت و امانت**

**صفحه هفتم: تقديم اثر**

**صفحه هشتم: فهرست مطالب**

**صفحه نهم: فهرست جدول ها**

**صفحه دهم: فهرست شکل ها**

**صفحه يازدهم: فهرست نمادها**

بخش دوم:

چکيده:

سيستم هاي فيزيکي سايبري (CPS) به نسل بعدي سيستم هاي مهندسي که به اصطلاح انقلاب صنعتي چهارم ناميده مي شود تبديل شده است. CPS ها پيچيده تر، باز (open) و بيشتر مستعد تهديدات امنيتي مي شوند، که مستلزم مهندسي سيستماتيک امنيت در CPS ها است. مهندسی امنیتی مبتنی بر مدل (MBSE) می تواند وسیله ای کلیدی برای مقابله با این چالش از طریق امنیت بوسيله طراحی، انتزاع (abstraction) و اتوماسیون (automation) باشد. هدف ما ارائه يک ارزيابي اوليه از جديدترين MBSE هاي پيشرفته براي CPS ها است. ما يک مطالعه سيستماتيک (SMS) براي استخراج و بررسي مطالعات انجام شده در مورد MBSE4CPS انجام داديم، نتايج SMS نشان مي دهد که در سه سال اخير (2014 تا 2016) تعداد مطالعات اوليه در مورد MBSE4CPS به طور قابل توجهي افرايش يافته است. در مطالعات اوليه محبوبيت استفاده از زبان هاي مدل سازي خاص دامنه (DSL) با زبان مدل سازي استاندارد UML قابل مقايسه است. اکثر مطالعات اولیه به صراحت به نگرانی های امنیتی خاص (مثلا محرمانه بودن، یکپارچگی) نپرداخته اند، بلکه بر روی تجزیه و تحلیل های امنیتی به طور کلی بر تهدیدات، حملات یا آسیب پذیری تمرکز دارند. مطالعات اوليه کمي براي مهندسي کردن راه حل هاي امنيتي براي CPS ها مطرح شده است. بيشتر مطالعات بر روي مراحل اوليه چرخه زندگي (lifecycle) توسعه مانند مهندسي يا تجزيه و تحليل نيازمندي هاي امنيتي تمرکز دارند. SMS نه تنها فقط جديدترين MBSE4CPS ها را ارائه مي کند، بلکه چندين مسئله باز را که مستلزم تحقيقات بيشتر است، از جمله عدم راه حل هاي امنيتي مهندسي براي CPS ها، پشتيباني ابزارهاي محدود، موارد مطالعه صنعتي بسيار کم، و چالش مرتبط ساختن DSL ها به مهندسي امن CPS ها را مورد توجه قرار مي دهد.

واژه هاي کليدي:

Cyber-physical system, Security, Model-based engineering, Security engineering, Model Base Security Engineering For Cyber Physical System

# فصل اول: مقدمه

امروزه، سيستم هاي فيزيکي سايبري (CPS) مي تواند در طيف وسيعي از صنايع (به عنوان مثال، در توليد، انرژي، مراقبت هاي بهداشتي و صنعت خودرو)، زيرساخت ها (به عنوان مثال، حمل و نقل، مدیریت آب، خطوط لوله نفت و گاز، مزارع بادي)، امکانات (به عنوان مثال، فرودگاه ها، ایستگاه های فضایی و ساختمان ها) و در کاربردهاي نظامي (به عنوان مثال، هواپیماهای بدون سرنشین و وسایل نقلیه بدون سرنشین) مورد استفاده قرار گيرد. با توجه به [‎1] "سيستم هاي فيزيکي سايبري (CPS) سيستم هاي فيزيکي و مهندسي هستند که عمليات آنها تحت نظارت، هماهنگي، کنترل و يکپارچه سازي بوسيله يک هسته محاسباتي و ارتباطي انجام مي شود". يک مثال از CPS ها در سيستم هاي شبکه برق پيشرفته مشاهده مي شود. در اين چنین سیستم شبکه هوشمند، فناوری اطلاعات و ارتباطات (ICT) در سراسر شبکه براي پشتيباني ارتباطات جديد و توابع کنترل در ميان منابع فيزيکي مثل مزرعه بادي، مزرعه خورشيدي، دستگاه هاي اندازه گيري هوشمند و سيستم هاي اطلاعات و کنترل يکپارچه شده است. داده ها (مثلا خواندن متر) از سنسورهای منابع فیزیکی جمع آوری شده (به عنوان مثال، مترهای هوشمند) به سیستم اطلاعات و کنترل برای مانیتور و کنترل زنده (به عنوان مثال، قطع ارتباط از راه دور هوشمند) منتقل می شود. محاسبات براساس این ارتباطات دوطرفه، امکان استفاده از منابع تجدیدپذیر و استفاده از سرویسهای هوشمند شبکه را بهینه تر می سازد. انتظار می رود که تکنولوژی CPS تغییری در نحوه ارتباط افراد با سیستم های مهندسی مانند اینترنت داشته باشد تا افراد با اطلاعات ارتباط برقرار کنند.

CPS ها بيشتر جوانب زندگي انسان ها را در بر مي گيرد، مهم تر اينکه اين CPS ها بايد امن باشند. یک مسئله امنیتی در شبکه هوشمند (smart grid) می تواند منجر به قطع کامل برق شهر یا حتی قطع کامل برق يک کشور شود. مطلوب اين است که انجام حملات در مقياس بزرگ به قسمت نرم افزاري سيستم هاي کنترل صنعتي فوق تخصصي بسيار غير محتمل باشد. با اين حال حمله کرم استاکسنت (Stuxnet) در تابستان سال 2010 يک هشدار براي توجه بيشتر به مقوله امنيت در CPS هاي صنعتي بود[‎2]. کرم استاکسنت با ايجاد تداخل در نرم افزاري که دستگاه هاي فيزيکي را در يک نيروگاه هسته اي کنترل مي کرد، توانست دستگاه هاي فيزيکي يا حتي نيروگاه را از بين ببرد. استاکسنت ثابت کرد که حتي CPS هاي صنعتي ايزوله شده مي تواند در معرض خطر باشد، و باعث شود که آنها عمليات غيرمنتظره (فيزيکي)، مانند خود نابودي (self-destruction) داشته باشند. علاوه بر این، بسیاری از CPS های پيشرفته به طور ناگزیر نیاز به اتصال به اینترنت دارند که می تواند چالش های امنیتی بسیار بیشتری را به همراه داشته باشد. امنیت CPS ها از اهمیت اساسی برخوردار است، زیرا در بسیاری موارد امنیت اين سيستم ها می تواند امنیت فیزیکی انسان هايي که در اطراف این سیستم ها زندگي مي کنند را به دنبال داشته باشد. جدا از سيستم هاي صنعتي، يکي از بزرگترين تهديدات امنيت سايبري در سال 2016 مربوط به هک وسايل پزشکي است. با ربودن پمپ های انسولین و ضربان سازهایی که بخشی از CPS ها در حوزه مراقبت های بهداشتی هستند، هکرها توانستند خون بها زندگي بيماران را، همانطور که در [‎3] هشدار داده شده است را بدست بياورند. باز هم این نوع تهدید باعث می شود تا امنیت CPS ها خیلی زود، جدی و منظم در نظر گرفته شود. یک نتيجه مهم که باید از شیوه ای که سیستم های اطلاعاتی در گذشته طراحی شده بايد استنباط شود این است که امنیت اغلب به عنوان یک نتیجه بعد از انجام تهديد مورد توجه قرار می گیرد [‎4]. اگر امنیت در اوايل چرخه عمر توسعه نادیده گرفته شود، تقریبا غیرممکن است که نیازهای امنیتی را به درستی در هر سیستم پیچیده مهندسی کند. یکی از دلایل اصلی این است که نیازهای امنیتی اغلب پراکنده و در سراسر نیازمندي هاي عملکردی سیستم دخيل است. بنابراين، امنيت CPS ها بايد از طريق طراحي در اوايل توسعه CPS ها مهندسي شود. با این حال، CPS ها در بسیاری از موارد بسیار پیچیده هستند و اطمینان از امنیت آنها بسیار چالش برانگيز است. علاوه بر چالش های امنیت سایبری CPS ها، امنیت بخش های فیزیکی CPS ها، که توسط کنترلرهای مبتنی بر نرم افزار بر اساس الگوریتم های محاسباتی کنترل می شود، در واقع یک چالش مهم جدید است. به عنوان مثال، دستگاه های فیزیکی مانند متر هوشمند در سمت client قرار مي گيرند، جایی که هکرها می توانند شانس بیشتری برای دستکاري آنها و نفوذ به شبکه های هوشمند داشته باشند. نرم افزار روح CPS ها است. بنابراين، متدلوژي هاي مهندسي امنيت نرم افزار نوآورانه و امن براي پيدا کردن و حل چالش هاي امنيت CPS ها مورد استفاده قرار مي گيرد. برخي از محققان، مهندسي مبتني بر مدل (MBE) يا مهندسي Model Driven (MDE) را یکی از راه حل های کلیدی برای مدیریت سیستم های پیچیده [‎5]، از جمله CPS ها [‎6] می دانند. یکی از ایده های اصلی MBE / MDE مهندسی در سطح مدل، که يک سطح انتزاعي و بالاتر از سطح کد است. اين امر به مهندسي امنيت و سيستم بهتر کمک مي کند و همچنین پایه های برای تایید (نیمه) خودکار (رسمی) یا اعتبار امنیت سیستم های پیچیده را فراهم می کند. در واقع، روش هاي MDE به صورت فعال براي مهندسي امنيت سيستم هاي نرم افزاري پيچيده در اوايل و در سراسر چرخه عمر توسعه همانطور که در [‎7] مورد بررسي قرار گرفته توسعه يافته است. در یک مطالعه اخیر که وضعیت هنر و وضعیت عمل در تأیید و اعتبارسنجی CPS ها را ارزیابی می کند، نویسندگان نشان می دهند که "استفاده از رویکردهای مبتنی بر مدل (model-based) به صورت صعودي رو به افزايش است و اين مورد که روش های مبتنی بر مدل می تواند برای CPS های همه منظوره استفاده می شود امري اجتناب ناپذير است."[‎8]. بوسيله ي مهندسی سیستم ها از طریق مدل های قابل فهم توسط کامپيوتر، تکنیک های مهندسی امنیت مبتنی بر مدل (MBSE) می توانند راه حل هایی را برای حل چالش های امنیتی CPS ارائه دهند. ما رهيافت هاي MBSE را که به طور خاص براي CPS ها طراحي شده را MBSE4CPS مي ناميم. با این حال، موضوع چگونگي توسعه رويکردهاي MBSE4CPS به عنوان یک سوال بزرگ همچنان باقی مانده است. در اين مقاله ما به دنبال پاسخ اين سوال هستيم. بعد از انجام يک بررسي هاي آزمايشي در رابطه با موضوع MBSE4CPS، دريافتيم که اين يک حوزه تحقيقاتي ميان رشته اي که مربوط به چندين رشته تحقيقاتي مختلف مانند مهندسي نرم افزار (سيستم)، مهندسي امنيت (نرم افزار) و مهندسي برق/سيستم مي شود است. بنابراین، یک مطالعه نگاشت سیستماتیک (SMS) برای ارائه تصویری از تحقیقات MBSE4CPS تا به امروز، به نفع محققان و متخصصان در زمینه های تحقیقاتی که در بالا ذکر شد خواهد بود. ما از آخرين دستورالعمل ها در [‎9] براي انجام SMS در مورد مطالعات اوليه MBSE4CPS موجود استفاده مي کنيم. هزاران مقاله مرتبط به طور سيستماتيک از چهار پايگاه داده انتشار آنلاين استخراج شد، و يک فرآيند snowballing بزرگ [‎10] در نهايت مجموعه اي از 48 مطالعه MBSE4CPS اوليه را بدست آورد. ما داده ها را از مطالعات اوليه MBSE4CPS استخراج و سنتز کرديم تا سوالات تحقيقاتي ما را پاسخ دهند. در نهایت، مشارکت کلیدی این کار پاسخ ما به سوالات تحقیق زیر (و سوالات زیر در بخش 5) است:

* سئوال تحقيق1: آمار نشر مطالعات اولیه MBSE4CPS در ادبیات چیست؟
* سوال تحقيق 2: مطالعات اولیه MBSE4CPS موجود و ویژگی های آنها چیست؟
* سوال تحقيق 3: مسائل باز تحقیقات MBSE4CPS چیست؟

علاوه بر این، مهم است که توجه داشته باشیم که در سیستم های پیچیده مانند CPS، عدم اطمینان به احتمال زیاد اتفاق می افتد و باید مورد استفاده قرار گیرد [‎11]. از دیدگاه امنیت، عدم قطعیت در CPS ها می تواند منجر به مسائل امنیتی جدی شود. به عنوان مثال، برخی از عدم اطمینان در عملکرد CPS ها ممکن است منجر به آسیب پذیری شود که توسط دشمن، مهاجم یا کاربر مخرب مورد سوء استفاده قرار می گیرد. برعکس، هر عدم قطعیت در مشخصات، پیاده سازی و تکامل مکانیزم های امنیتی ممکن است باعث عدم اطمینان هاي دیگري در عملکرد CPS ها شود، مثلا کنترل دسترسی نادرست می تواند برخی از فرایندهای فیزیکی را غیرفعال کند، به ویژه که نیازهای real-time آن بسیار مهم است. از سوی دیگر، حملات امنیتی همچنین می تواند باعث عدم اطمینان در عملکرد CPS ها شود. بنابراین، هنگام انجام این SMS، ما در نظر داشتیم که بررسي کنيم هر مطالعه MBSE4CPS به طور صريح با عدم اطمینان در ارتباط باشد. مرور ساختار کلي مقاله

# فصل دوم: زمينه موضوع و مرور منابع علمي

## مهندسي امنيت مبتني بر مدل (Model-based security engineering):

### مهندسي مبتني بر مدل (Model-based Engineering، MBE) و Model Driven Engineering (MDE)

MBE می تواند مفهومي کلیدی برای مهندسی سیستم های پیچیده، از جمله CPS ها و امنیت آنها باشد. با مدل سازی سیستم مورد نظر و دستکاری مدل، سطح انتزاع بالاتر از سطح کد است که مزایای زیادی را به همراه دارد، به خصوص در مورد مهندسی امنیت.

اول، نگرانی های امنیتی (مانند محرمانهگي، جامعيت، در دسترس بودن) می تواند خیلی زود با منطق کسب و کار (و دیگر ویژگی های کیفی مانند عملکرد) ترکيب شود، که در مهندسی سیستم های امنیتی اهمیت زيادي دارد. همانطور که در [‎12] بيان شده است، زبان هاي خاص دامنه (domain-specific languages، DSL) به طور معمول توسعه يافته است و در مهندسی امنیت به دلیل توانایی بیان آنها برای به دست آوردن مکانیزم های امنیتی مورد استفاده قرار می گیرند. به عبارت دیگر، یک DSL که برای تعیین یک جنبه امنیتی خاص (مانند کنترل دسترسی) طراحی شده است، رساتر از یک زبان مدلسازی عمومی مانند UML باشد. اگرچه، مکانيسم پروفايل UML مي تواند براي تعريف DSL هاي امنيت گرا (security-oriented) همانطور که در [‎12] اشاره شده است مورد استفاده قرار گيرد. علاوه بر اين پروفايل هاي UML، برخی از رویکردهای دیگر مورد بررسی در [‎12] DSL های مبتنی بر غیر UML را معرفی کرد.

دوم، استدلال در مورد سیستم های مورد نظر در سطح مدل می تواند روش های تصديق و اعتبار سنجی مبتنی بر مدل با پشتیبانی ابزار را فرآهم کند کند، که برای تجزیه و تحلیل امنیتی مهم هستند. اگر تبدیل مدل های امنیتی به ورودی های احتمالی برای روش های رسمی (و ابزارهای موجود، مانند Alloy [‎13]) امکان پذیر باشد، روش های رسمی (formal methods) مانند چک کردن مدل برای تایید ویژگی های امنیتی استفاده می شود. روش های آزمون امنیت مبتنی بر مدل می تواند برای اعتبارسنجي نتیجه سیستم های امن (به ویژه در مواردی که روش های رسمی قابل استفاده نیستند) استفاده شود. سوم، مهندسی در سطح مدل، اتوماسیون را فراهم می کند که بوسیله مدل های تبدیل مدل به مدل (MMT) و تبدیل مدل به متن (MTTs) فرآهم مي شود. MMT ها می توانند بخشي از مراحل اصلی فرایند مهندسی، برای مثال برای ساختن مدل های امنیتی از مدل های تجاری و یا تبدیل مدل ها بین DSL های مختلف باشند. MTT ها می توانند برای تولید کد، از جمله مکانیسم های امنیتی، مانند يک مکانیسم کنترل دسترسی پیکربندی شده استفاده شوند. خودکار سازی فرآیند توسعه را از لحاظ کمي سرعت مي بخشد و با کیفیت بالاتری نسبت به یک فرآیند توسعه کدهای دستی انجام میشود [‎14]. براي تعيين دامنه چيزي که مي تواند به عنوان يک رويکرد MBSE (و سپس MBSE4CPS) در نظر گرفته شود، ما از مفاهيم MBE، MDE و Model-Driven Development (MDD) در [‎15] استفاده مي کنيم. با توجه به [‎15] مدل هاي رويکردهاي MBE ممکن است لزوما عناصر مرکزي در چرخه عمر توسعه نباشند. به عنوان مثال، مدل ها در یک روش MBE ممکن است برای هر یک از اهداف مستندسازي (documentation) یا تأیید (verification) مورد استفاده قرار گیرد، اما ممکن است لزوما یا شاید برای اجرا (implementation) آن مورد استفاده قرار نگیرد. از سوي ديگر، مدل ها در رويکرد MDE مصنوعات اوليه اي هستند که به توسعه (development)، تکامل (evolution) يا کارهاي مهاجرت (migration tasks) ختم مي شوند[‎15]. اگر یک رویکرد MDE تنها بر توسعه تمرکز کند، MDD نامیده می شود. بنابراین، MDD یک زیر مجموعه از MDE است. به همین ترتیب، MDE یک زیرمجموعه از MBE است که در [‎15] مورد بحث قرار گرفته است، زیرا مدل های MDE باید "هدايت" مصنوعات اوليه باشد و فقط براي اهداف مستندسازي يا هر هدف مهندسي واحد همانند محدوده MBE نباشد.

### MBSE و MDS

در [‎12]، يک تعريف مشخص و محدوده از MDS ارائه شده است. به طور کلی، MDS یک زیرمجموعه از MDE است که در آن سیستم های امنیتی تمرکز مهندسی است. به طور مشابه، MBSE یک زیر مجموعه از MBE است. از آنجا که CPSs نسل جدیدی از سیستم های مهندسی هستند، رویکردهای مهندسی امنیت مبتنی بر مدل ها يک مفهوم نوظهور است. در این مقاله، ما علاقه مند به درک گسترده ای از روش های مهندسی امنیت بر اساس مدل ها، به عنوان مثال MBSE هستيم. در توسعه سیستم های امن، MBSE می تواند نقش مهمی ایفا کند، مثلا در تأیید و اعتبارسنجي سیستم های امنیتی راجع به خواص امنیتی آن. مدل ها در رویکرد MBSE ممکن است برای اهداف طراحی یا پیاده سازی مورد استفاده قرار گیرند، اما همچنین ممکن است فقط برای تحلیل امنیت یا اهداف اعتبارسنجي و تایید نيز مورد استفاده قرار گيرد. رویکردهای MBSE که به طور خاص برای CPS طراحی شده است MBSE4CPS نامیده می شود. MBSE4CPS می تواند برای درک دیدگاه امنیت با طراحی، همانطور که در [‎16] اشاره شده، برای یکی از محبوبترین مثال های CPS: به عنوان مثال شبکه هوشمند استفاده شود.

## سيستم هاي فيزيکي سايبري (Cyber-physical systems) و امنيت

### سيستم هاي فيزيکي سايبري (CPS)

"سیستم های فیزیکی سایبري (CPS) سیستم های مهندسی هستند که از ادغام یکپارچه و بدون درز الگوریتم های محاسباتی و اجزای فیزیکی ساخته شده و به آن بستگي دارد" [‎17]. با توجه به [68]، "CPS ها سیستم های فیزیکی و مهندسی هستند که عملیات آنها نظارت، هماهنگ، کنترل و یکپارچه سازی با یک هسته محاسباتی و ارتباطی" می باشد. ما از این تعاریف برای جستجوی نشریات در حوزه های کاربردی CPS ها و دامنه های مرتبط مانند سیستم های تعبيه شده و سیستم های سیستم (system of systems) استفاده کردیم. به طور خاص، ما همچنین سیستم های تعبيه شده یا سیستم های سیستم (systems of systems) که ویژگی های CPS را دارند، مورد توجه قرار داديم.

بر اساس تعاریف CPS فوق، بسیاری از سیستم های مدرن در حوزه های مختلف می توانند به عنوان CPS طبقه بندی شوند. در [36] دامنه های کاربردی محبوب CPS مورد بررسی قرار گرفته و به شرح زیر ذکر شده است: سیستم های وسايل نقليه و حمل و نقل (به عنوان مثال، ماشین های هوشمند)؛ سیستم های مراقبت بهداشتی و پزشکی؛ خانه های هوشمند و ساختمان ها؛ شبکه اجتماعی و بازی؛ مديريت برق و گرما؛ مراکز داده (برای حفظ هزینه های انرژی برای محاسبات و خنک سازی حداقل شبيه CPS ها عمل مي کند)؛ شبکه برق الکتريکي و سیستم های انرژی (به عنوان مثال شبکه هوشمند)؛ سیستم های شبکه؛ نظارت.

توسعه CPS ها در مقیاس بزرگ به عنوان زیرساخت های حیاتی اغلب نیاز به کار استاندارد سازی برای ایجاد قابلیت همکاری اجزای مختلف از فروشندگان (Vendor) مختلف دارد. به عنوان مثال، برای توسعه شبکه های هوشمند، به اصطلاح Smart Grid Architecture Model (SGAM) از مجوز M/490 کمسیون اروپایی [12] منشا شده است. SGAM نه تنها از جنبه های قابلیت همکاری پشتیبانی می کند، بلکه راه را برای رسمیت بخشیدن به جنبه های عملکردی و همچنین جنبه های امنیتی در توسعه شبکه های هوشمند را فراهم می کند. دستورالعملهای NIST IR 7628 برای امنيت سايبري شبکه هاي هوشمند[75] یکی دیگر از کارهای مهم سازمان های استاندارد است که استانداردهای مشترک را برای امنیت شبکه هوشمند تعیین کرده است. این سند تعاریف نگرانی های امنیتی سنتی (اهداف) را برای امنیت CPS، به عنوان مثال امنیت شبکه هوشمند، اتخاذ کرده است. ما بيشتر درباره [75] در بخش زير بحث خواهيم کرد.

### امنيت CPS ها

اکثر (اما نه همه) CPS ها سیستم های امنیتی بحرانی هستند. نگرانیها (اهداف) امنیتی سطح بالا CPS ها با نگرانیهای امنیتی مرسوم در امنیت رایانه، مانند محرمانه بودن، یکپارچگی، دسترسی پذيري (CIA) و حسابرسي (accountability)، متفاوت نیست. اين اهداف امنيت عمومي در دستور العمل هاي (Guidelines) NIST IR 7628 براي امنيت سايبري شبکه هاي هوشمند [75] براي مستندسازي استانداردهاي امنيتي مشترک براي شبکه هاي هوشمند استفاده مي شود. فقط این که جزئیات هر یک از نگرانی های امنیتی باید در زمينه CPS ها، به عنوان مثال همانطور که در [13] یا [61]، آمده است تفسیر شود، که چالش هاي امنيتي جديدي، به عنوان مثال در حفاظت (کنترل کننده هاي) دستگاه هاي فيزيکي مطرح مي شود. در این مقاله، ما اصطلاحات امنيتي شرح داده شده در [46] مانند تهدیدات امنیتی، آسیب پذیری ها، حملات و راه حل های امنیتی را به عنوان جنبه های مختلف (جنبه های امنیتی) که باید در حین مهندسی امنیت در نظر گرفته شود اشاره مي کنيم. از سوي ديگر نگراني هاي امنيتي به اهداف امنيتي (به عنوان مثال، CIA و حسابرسي) و مکانيسم ها (مانند احراز اصالت، مجازشناسي و رمزگذاري) اشاره مي کند. راه حل های امنیتی ترکیبی از مکانیزم های امنیتی با توجه به اهداف امنیتی برای کاهش آسیب پذیری های امنیتی است. ما بعضي از تعاريف نگراني هاي امنيتي عمومي را از [10, 46] اخذ مي کنيم و موارد خاص CPS را طبق [13, 75] مطابق زير مي پذيريم.

"محرمانه بودن پنهان سازی اطلاعات یا منابع است" [10]. "از دست دادن محرمانه بودن - افشای اطلاعات غیرمجاز است" [75]. مانع آگاهي افراد غير مجاز به اطلاعات يا منابع، حتي آگاهي از وجود آنها مي شود. در CPS ها، وضعیت سیستم فیزیکی باید از افراد غیر مجاز محرمانه نگه داشته شود، به عنوان مثال، مکانیسم های امنیتی کافی، باید از استراق سمع در کانال های ارتباطی، به عنوان مثال، بین سنسور و یک کنترلر، و بین یک کنترلر و یک محرک (actuator) جلوگیری کند. علاوه بر این، برخی از CPS هایی که حاوي اطلاعات کاربري حساس است، این داده ها باید از دسترسی غیر مجاز محافظت شود.

"جامعيت به اعتبار داده ها (trustworthiness) یا منابع اشاره دارد و معمولا در اصطلاح به معني جلوگیری از تغییر نامناسب یا غیر مجاز است" [10]. "از دست دادن جامعيت - تغییر غیر مجاز یا تخریب اطلاعات است" [75]. جامعيت در CPS ها می تواند به عنوان توانایی برای حفظ اهداف عملیاتی با جلوگیری، شناسایی و یا وجود حملات فریب (deception attacks) در اطلاعات ارسال شده و دریافت شده توسط سنسورها، کنترلرها و محرک ها مشاهده شود. اگر یکپارچگی تضمین نشود، ممکن است فریب خوردن (deception) رخ دهد، به عنوان مثال، "وقتي که یک شخص مجاز دریافت داده های دروغین را دريافت مي کند و باور داشته باشد که درست است" [13]. "دسترس پذيري به توانایی استفاده از اطلاعات یا منابع مورد نظر" اشاره دارد [10]. "خسارت دسترس پذيري - اختلال دسترسی به یا استفاده از اطلاعات یا یک سیستم اطلاعاتی" [75]. عدم دسترس پذيري ممکن است منجر به انکار سرویس (DoS) شود. يک حمله DoS بوسيله ي يک تلاش صريح براي "جلوگيري از استفاده هاي مشروع به يک سرويس" توصيف مي شود [45]. بنابراين هدف دسترس پذيري در CPS ها، حفظ اهداف عملياتي از طريق جلوگيري يا انجام حملات DoS براي اطلاعات جمع آوری شده توسط شبکه های حسگر، دستورات داده شده توسط کنترلرها و اقدامات فیزیکی گرفته شده توسط محرک ها است. چالش های جدیدی برای اطمینان از دسترس بودن در بسیاری از CPS ها وجود دارد که محدودیت های realtime آن ها بحرانی است.

حسابرسي: علاوه بر CIA، حسابرسي یکی دیگر از نگرانی های امنیتی است که در بسیاری از برنامه های کاربردی نیز مهم است. حسابرسي به توانایی پیگیری اينکه چه کسی چه کاري و در چه زمانی انجام داده اشاره مي کند. در هر CPS، کنترل موثر بر روي برخي فرآيندهاي فيزيکي، هدف اصلي است. بنابراین، براي جامعيت اطلاعات و در دسترس پذيري حصول اطمینان از این که یک وضعيت کنترل (control state) از نزديک وضعيت سيستم فيزيکي را به صورت آينه اي منعکس کند (mirrors) ضروري است. رمزنگاری، کنترل دسترسی و احراز هویت، برخی از مکانیسم های امنیتی هستند که می توانند جامعيت را در سیستم ها فرآهم کنند. نگرانی ها / اهداف امنیتی مهم تر، کاملا به یک CPS خاص بستگی دارد و اينکه ما راجع به چه بخش هایی از آن CPS صحبت می کنیم. به عنوان مثال، شبکه هوشمند یکی از محبوب ترین نمونه های CPS است. در شبکه هوشمند، اگر ما انتقال انرژی را در نظر بگيريم، آنگاه در دسترس بودن مهم است. اما اگر ما زیرساخت اندازه گیری پیشرفته (Advanced Metering Infrastructure- AMI) شبکه هوشمند را در نظر بگیریم، آنگاه محرمانگي و جامعيت از اهمیت کمتری نسبت به در دسترس پذيري برخوردار نیستند. به عبارت ديگر، در حالي که از دسترس پذيري سرويس انرژي اطمينان حاصل مي کنيم، AMI بايد محرمانگي و جامعيت داده هاي مبادله شده بين مترهاي هوشمند و نقطه پايان (head-end) AMI را در نظر بگيرد. به این معنا، امنیت CPS هنوز اهداف عمومی عمومی را از امنیت سایبری / امنیت رایانه ای، به عنوان مثال CIA، به ارث می برد. توجه داشته باشید که اهداف امنیتی باید در کل حفظ شود [58]. یک راه حل برای حل یک نگرانی امنیتی خاص، اغلب به راه حل های دیگر مربوط به سایر نگرانی های امنیتی بستگی دارد. یک راه حل برای حل یک نگرانی امنیتی خاص، اغلب به راه حل های دیگر مربوط به سایر نگرانی های امنیتی بستگی دارد.

با اين حال، هر مکانيزم امنيتي که استفاده مي شود همچنين بايد دسترس پذيري کافي را فرآهم کند. این محدودیت اغلب استفاده از مکانیزم های امنیتی را محدود می کند زیرا ممکن است دسترسی به یک عملکرد بحرانی را رد کند [76]. تعامل ناکافی بین مکانیزم های امنیتی و عملیات CPS ها می تواند باعث عدم اطمینان در CPS ها شود. براي مثال يک مکانيزم کنترل دسترسي نامساعد مي تواند دسترسي به يک دستگاه فيزيکي که نيازمندي هاي real-time آن بحراني است را مسدود يا کم کند.

### عدم قطعيت CPS ها و امنيت

ما از تعریف عدم قطعیت در [95] استفاده می کنیم: "عدم اطمینان یک حالت CPS است که غیر قابل پیش بینی است، نتیجه بعدي وضعيت ممکن است تعیین نشود، یا احتمال بیشتر از یک نتیجه از وضعيت وجود دارد". عدم اطمینان و امنیت یکی از ویژگی های اساسی اصلی CPS است که چالش های بزرگی را که باید در تحقیق مورد توجه قرار گیرد، بررسي مي کند [30]. عدم اطمینان و امنیت CPS ها می تواند به روش های مختلف به هم مربوط شود. یک حادثه امنیتی (مثلا، ناشی حمله مهاجمان) یا اشتباه ممکن است منجر به عدم قطعيت شود. در عوض، عدم قطعیت ممکن است منجر به آسیب پذیری های امنیتی شود که توسط مهاجمان مورد سوء استفاده قرار می گیرد. این عدم اطمینان مربوط به امنیت می تواند در CPS به دلايل 1) نيازمندي هاي امنیتی مبهم یا کشف نشده؛ فرضیه امنيتي نادرست؛ اهداف امنیتی نادرست؛ 2) پيکربندي نادرست امنيت، پیاده سازی نادرست یا سیاست امنیتی اشتباه که می تواند از انجام اعمال به طور قطع در CPS جلوگیری کند؛ و 3) آسیب پذیری های احتمالی امنیتی یا پيکربندي هاي نادرست CPS می تواند به حملات امنیتی موفق منجر شود؛ حملات امنيتي غیر قابل پیش بینی با هدف رسيدن به CPS.

# فصل سوم:روش تحقيق

رويکرد مطالعه نگاشت سيستماتيک (Systematic Mapping Study- SMS)

ما SMS خودمان را با پیروی از آخرین دستورالعمل های (guideline) مطالعه نگاشت سیستماتیک [66] و همچنین به عنوان مثال، بررسي سایر دستورالعمل هاي مربوطه و مطالعات گزارش شده در [9،37،89] و [38] انجام دادیم. ما بر اساس سوالات تحقیقاتی (بخش 3.1)، اصطلاحات جستجو (بخش 3.2) را شناسایی کردیم و یک استراتژی جستجو (بخش 3.4) را برای یافتن مطالعات اولیه که می تواند به سوالات تحقیقاتي ما پاسخ دهد، طراحی کرديم. همچنین مهم است که معیارهای حذف و اضافه کردن (بخش 3.3) را برای کاهش ضعف هاي احتمالی در روند انتخاب (بخش 3.4) توضيح دهيم. فرایند استخراج داده ها و ترکيب مطالعات اولیه بر اساس مجموعه ای از معیارهای ارزیابی (بخش 4) خواهد بود.

## سوالات تحقيقاتي

برای پاسخ دادن به سوالات تحقیقاتي عمومی که در بخش 1 مطرح کرديم، ما جزئيات آنها را در زيرسوالات زير بررسي مي کنيم. همانطور که در [38] بحث شده است، سوالات تحقیقاتي SMS معمولا عمومی هستند و مربوط به خاص روند تحقیق مي شوند، به عنوان مثال، برای پیدا کردن چه محققاني، چه فعالیت هايي و غیره. براي مشخص شدن بيشتر آمار انتشاري که ما مي خواهيم پيدا کنيم، سوال تحقيقاتي 1 (RQ1) به 4 سوال زير تقسيم مي شود.

اول، ما علاقه مند به روند (trend) مطالعات اوليه MBSE4CPS (primary MBSE4CPS study) منتشر شده در طول سال هستيم. RQ1.1- در چه سال هايي مطالعات اوليه MBSE4CPS منتشر شد و تعدا انتشارات سالانه چيست؟ جواب دادن به سوال RQ1.1 به ما اجازه کشف زماني که اولين مطالعه اوليه MBSE4CPS منتشر شد و فرکانس انتشار مطالعات اوليه MBSE4CPS را مي دهد. ما می توانیم از این یافته ها برآورد کنیم که آیا این موضوع تحقیق براي جامعه تحقیق (research community) توجه بیشتری دارد یا نه.

دوم، مي خواهيم در مورد مکان انتشار مطالعات اوليه MBSE4CPS بدانيم، به عنوان مثال محل نشر يک روزنامه (journal)، کنفرانس يا کارگاه (workshop) است. مطالعات اوليه MBSE4CPS رهيافت هايي است که تکنيک هاي مهندسي امنيت نرم افزار مبتني بر مدل را براي CPS ها توسعه يا بهبود مي بخشد. بنابراین، این مطالعات می تواند در مکان های مختلف مانند محل های مهندسی نرم افزار، مراکز امنیتی مهندسی و یا مکان های مهندسی سیستم منتشر شود. RQ1.2 - در کدام مکان های هدف (مثلا محل هاي مهندسي نرم افزار، محل هاي مهندسي امنيت) و نوع محل هايي (مانند کنفرانس، مجله، کارگاه) اولین مطالعات MBSE4CPS منتشر شد؟ توجه داشته باشيد که هنوز نشريات يا کنفرانس هاي اختصاصي MBSE4CPS وجود ندارد. جواب سوال RQ1.2 وسيله ي دانستن اينکه چه مکان هایی به عنوان هدف براي انتشار مطالعات اولیه MBSE4CPS انتخاب شده اند را فرآهم مي کند. نوع محل نیز می تواند برخی نکات مربوط به اعتبار مطالعات اولیه MBSE4CPS را ارائه دهد، به عنوان مثال، مقالاتی که در نشریات منتشر مي شود، فرض بر اين است که از اعتبار بالاتري نسبت به مقالات منتشر شده در کنفرانس ها و کارگاه های آموزشی برخوردار هستند.

سوم، مشارکت صنعت در مطالعات MBSE4CPS نشان دهنده علاقه صنعتی به موضوع MBSE4CPS و همکاری پژوهشی بین صنعت و دانشگاه است. بنابراین، ما می خواهیم بدانیم که نویسندگان مطالعات اوليه MBSE4CPS در دانشگاه یا صنعت کار می کنند. يک مقاله دانشگاهي طبقه بندي مي شود اگر همه نويسندگان آن دانشگاهي (دانشگاه يا موسسه تحقيقاتي)، صنعت، اگر همه نويسندگان آن از يک شرکت و هر دو (دانشگاه و صنعت) اگر نويسندگان به صورت ترکيبي از صنعت و دانشگاه باشند. RQ1.3 - توزیع نشریات از نظر وابستگی تحصیلی و صنعتی چیست؟

چهارم، ما می خواهیم بدانیم که در کدام کشور مطالعات تحقيقاتي اولیه MBSE4CPS انجام شده است. RQ1.4 - توزیع جغرافیایی تحقیقات در مورد MBSE4CPS چیست؟ پاسخ به RQ1.4 به ما اجازه ي شناسایی اينکه کدام کشورها (یا قاره ها) از نظر انتشارات تحقیقاتی در این حوزه پيشتاز هستند را مي دهد. یافته های این تحقیق می تواند مربوط به تحقیقات بر روی CPS ها باشد که توسط بسیاری از کشورها مانند ایالات متحده و اتحادیه اروپا (اتحادیه اروپا) ترویج شده است [27].

برای وضوح بيشتر اینکه چه خصوصیاتی از مطالعات اولیه MBSE4CPS را می خواهیم بررسی کنیم، RQ2 به 7 سوال زیر تقسیم می شود.

دانستن اينکه چه نگرانی های امنیتی در هر مطالعه اولیه MBSE4CPS مورد توجه قرار گرفته مهم است. از دیدگاه مهندسی امنیت، رویکردهای امنیتی باید از نگرانی های امنیتی خاص (concrete security concerns) جدا شوند. RQ2.1 – چه نگرانی های امنیتی (مانند محرمانه گي، جامعيت، دسترس پذيري) در مطالعات اولیه MBSE4CPS مورد توجه قرار گرفته است؟ هر رویکرد مهندسی امنیت می تواند به صورت واحد یا ترکیبی از جنبه های مختلف امنیتی مانند حملات، تهدیدات، آسیب پذیری ها یا راه حل ها باشد. برای هر مطالعه اولیه MBSE4CPS، ما می خواهیم دقیقا بدانیم که کدام جنبه ها عمدتا مورد بررسي قرار گرفته است. RQ2.2 – روي چه جوانب امنیتی (مثلا حمله، تهدید، آسیب پذیری، راه حل) تمرکز شده است؟

در هر مطالعه اولیه MBSE4CPS، جنبه های امنیتی باید مدل سازی یا مشخص شود. سپس این مدل ها در فرآيندهاي توسعه CPS ها مهندسي و / يا تبديل مي شوند. RQ2.3 - جنبه های امنیتی مدل سازی شده (مشخص شده) و مهندسی شده (تبدیل شده) چیست؟

همانند هر روش مهندسی نرم افزار، هر مطالعه اولیه MBSE4CPS می تواند بر پشتیبانی از مراحل خاص مهندسی در چرخه عمر توسعه تمرکز کند. RQ2.4 - مطالعات اولیه MBSE4CPS روی کدام مراحل مهندسي تمرکز یا پشتیبانی کرده اند، مانند مهندسی نيازمندي ها، طراحی و آزمایش؟ آیا رویکرد ابزار گزارش را می دهد؟

مشابه به هر روش مهندسی نرم افزار، می توانیم از انواع مشارکت پژوهشی و تحقیقاتی که در [68] بحث شده، برای تحلیل مطالعات MBSE4CPS اولیه استفاده شود. RQ2.5 - مطالعات اولیه MBSE4CPS از چه نوع مشارکت (به عنوان مثال، فرایند، ابزار، روش (method)) و چه نوع ريزدانگي تحقیقاتی (مثلا نظر (opinion) ، مفهومی، راه حل، اعتبار سنجی، ارزیابی) استفاده مي کنند؟

از دیدگاه CPS ها، ما می خواهیم بدانیم چه نوع CPS هایی مطالعات اولیه MBSE4CPS روي آنها انجام شده است و آیا موارد واقعي است؟ RQ2.6 – در چه CPS هايي این مطالعات اولیه MBSE4CPS مورد استفاده قرار گرفته است؟ چه نوع مطالعات موردی (دانشگاهی یا صنعتی) برای ارزیابی رویکردها مورد استفاده قرار گرفته است؟

همانطور که در مقدمه ذکر شد، عدم اطمینان باید به طور خاص برای CPS مورد توجه قرار گیرد. ما می خواهیم بررسی کنیم که آیا هر مطالعه اولیه MBSE4CPS برای حل عدم قطعیت پیشنهاد شده است. RQ2.7 - آیا هر مطالعه اولیه MBSE4CPS با عدم قطعیت برخورد کرد؟ RQ3 به دو سوال تقسیم می شود. بر اساس ویژگی های مطالعات اولیه MBSE4CPS، ما می خواهیم مسائل باز را بیاموزیم که شايسته تحقيق بيشتر در آینده است و مسيرهاي بالقوه ای برای مقابله با این مسائل داشته باشيم. RQ3.1 - مسائل باز تحقیقات MBSE4CPS چیست؟ RQ3.2 - چه مسیرهای تحقیقاتی می تواند برای مقابله با مسائل باز توصیه شود؟

## رشته هاي جستجو

از سوالات تحقیقاتی، واژه های جستجو را شناسایی کرده و آنها را به چهار گروه تقسیم کردیم: جمعیت (population)، مداخله (intervention)، مقایسه (comparison) و نتیجه (outcome) (PICO) [37].

اصطلاحات جمعيت کلمات کليدي هستند که دامنه CPS را نشان مي دهند. ما از کلمات کلیدی برخی از دامنه های کاربردی محبوب CPS، به عنوان مثال شبکه هوشمند استفاده کرديم.

* جمعيت (Population): ("سیستم هاي فیزیکی سایبري (cyber-physical system)" یا CPS یا "شبکه هوشمند (smart grid)" یا "شبکه برق (power grid)" یا "ماشین هوشمند (smart car)" یا "سیستم هاي فیزیکی سایبري خودرو (automotive cyber-physical system)" یا سیستم "سیستم مراقبت های بهداشتی فراگیر (pervasive healthcare system)" یا "سیستم هواپیماهای بدون سرنشین (unmanned aircraft system)")

شرایط مداخله کلمات کلیدی هستند که تکنیک های MBE را نشان می دهند.

* مداخله (Intervention): (مدل يا مدل سازي يا مبتني بر مدل يا modeldriven)

شرایط مقایسه بیانگر نگرانی ها يا جنبه های امنیتی است. این ها اصطلاحات کلیدی در مهندسی امنیتی است که در [49] ارائه شده است. علاوه بر اصطلاحات امنیتی، ما همچنین یک کلمه کلیدی خاص تحت عنوان "عدم اطمینان" را اضافه کرديم.

* مقايسه (Comparison): (امنیت یا محرمانه بودن یا یکپارچگی يا دسترس پذيري يا پاسخگو بودن يا احراز هویت يا مجازشماري يا "کنترل دسترسی" یا حمله يا تهدید يا آسیب پذیری یا عدم قطعیت)

اصطلاحات نتیجه نشان دهنده اهداف فرایند مهندسی هستند.

* نتيجه: (معماری یا طراحی يا تأیید يا اعتبار سنجی يا آزمون يا تجزیه و تحلیل)

برای تشکیل رشته جستجو، ما از ترکیب گروه های اصطلاحات فوق استفاده کرد، یعنی جمعیت و مداخله و مقایسه و نتایج. رشته جستجو ورودی فرآیند جستجوی پایگاه داده ما است که در بخش 3.4 توضیح داده شده است.

## معيارهاي حذف و اضافه کردن

هدف ما در این SMS شناسایی و طبقه بندی مقالات مربوط به رویکردهای MBSE برای CPS ها است. معيارهاي اضافه کردن (inclusion criteria- IC) عبارتند از:

* (IC1) مقاله باید حاوي محتواي MBSE باشد. این به این معنی است که مدل (ها) باید در بعضی فرآیندهای مهندسی امنیت مورد استفاده قرار گیرند.
* (IC2) مقاله باید مربوط به امنیت سایبری باشد.
* (IC3) مقاله باید مربوط به اهداف CPS ها باشد، چه به طور کلي يا در يک دامنه کاربرد خاص CPS ها مانند شبکه هوشمند.

ما مقالاتی را که ملاک هر یک از معیارهای حذف زیر را داشتند حذف کردیم:

* (EC1) مقاله هایی که حاوي امنیت سایبری نبودند، حذف می شوند.
* (EC2) مقالاتی که رهيافت هاي MBE را مطرح نکردند، حذف می شوند.
* (EC3) مقالاتی که مربوط به CPS نبودند، حذف می شوند.
* مقالاتي که به زبان هاي غير انگليسي بودند، حذف مي شوند.
* (EC5) مقالات غیررسمی بررسی شده، سخنرانی ها، گزارش هاي کارگاه، کتاب ها، پایان نامه ها و پایان نامه ها، حذف می شوند.
* (EC6) هر نسخه منسوخ یا قدیمی نشريات، حذف مي شود.

به عنوان مثال، ما برخی از گزارش هاي کارگاهي (workshop) یا مقالات کنفرانسي (conference) را هنگامی که ما نسخه ی مجله اي (journal) توسعه يافته این مقالات را پیدا کردیم، حذف کردیم.

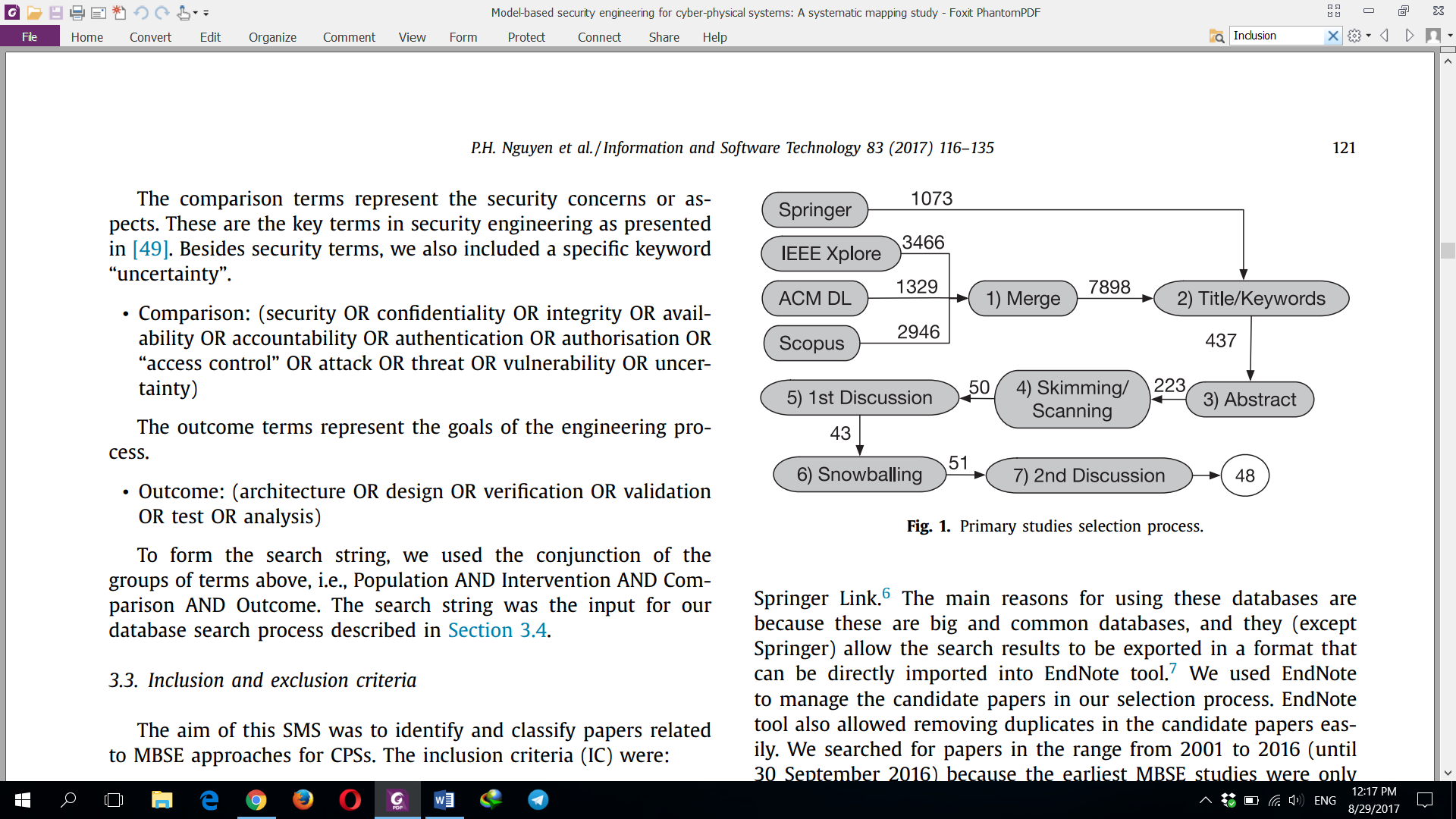
## استراتژی جستجو و فرآیند انتخاب

با توجه به [66]، جستجوهای پایگاه داده از طریق پایگاه داده های آنلاین مانند IEEE Xplore رایج ترین روش برای پیدا کردن مطالعات اولیه برای SMS یا SLR است. علاوه بر این، با جستجو در پایگاه های داده های مختلف، می توانیم شانس بیشتری برای پیدا کردن مقالات مربوط به MBSE4CPS از جوامع مختلف تحقیقاتی داشته باشیم. انتظار داریم محققانی که در حوزه CPS ها و امنیت کار می کنند از زمینه های مختلف تحقیقاتی مانند مهندسی برق، مهندسی نرم افزار و مهندسی امنیت باشند. علاوه بر این، برای غلبه بر برخی محدودیت های جستجوی پایگاه داده، همانطور که توسط [90] اشاره شده، ما از استراتژي snowballing [89] براي کامل کردن مجموعه مطالعات اوليه اي که از جستجوي پايگاه داده به دست آمده است استفاده مي کنيم. بنابراین، روند جستجوی و انتخاب ما به شرح زیر است.

### جستجوي پايگاه داده ها

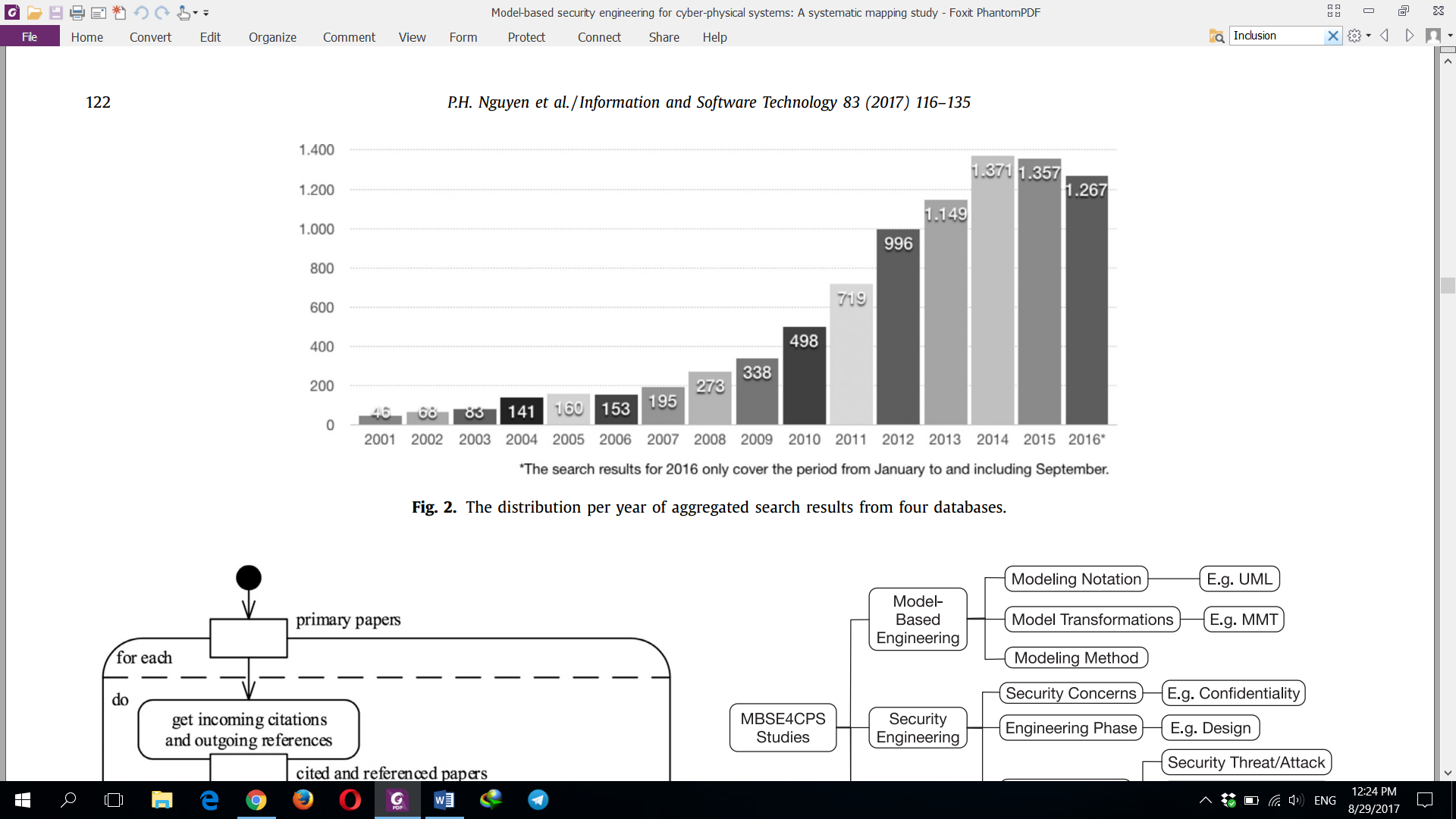
ما رشته هاي مورد جستجو که قبلا عنوان شد را در چهار پايگاه داده آنلاين: IEEE Xplore[[1]](#footnote-1)، ACM DL[[2]](#footnote-2)، Scopus [[3]](#footnote-3)و Springer Link[[4]](#footnote-4) جستجو کرديم. دلایل اصلی استفاده از این پایگاه های داده به این دلیل است که این پایگاه های بزرگ و مشترک هستند و آنها (به استثنای Springer) اجازه استخراج نتایج جستجو را در یک فرمت که می تواند به طور مستقیم به ابزار EndNote [[5]](#footnote-5)وارد شود، را مي دهند. ما از EndNote برای مدیریت مقاله هاي داوطلب در روند انتخاب استفاده کردیم. ابزار EndNote همچنین به راحتی حذف مقاله هاي داوطلب تکراري را امکان پذیر می سازد. ما مقالات را در محدوده سال هاي 2001 تا 2016 (تا تاریخ 30 سپتامبر 2016) جستجو کردیم زیرا اولین مطالعات MBSE فقط در اوایل قرن بیست و یکم صورت گرفته اس[43].

مرحله 1. پيش پردازش (Preprocessing): بر اساس نتایج موتورهای جستجو، ما آنها را با پشتيباني ابزار EndNote (مرحله 1 در *شکل 1*) براي حذف موارد تکراري ادغام کردیم. ما همچنین به صورت دستي کتابها، مقالات سفید، فهرست محتويات و غیره را حذف کردیم.



*شکل 1: فرآيند انتخاب مطالعات اوليه*

شکل 2 توزیع نتایج جستجو جمع آوري شده از چهار پایگاه داده را در سال را نشان می دهد. همان طور که در شکل 2 مشاهده می شود، تعداد مقالات مرتبط با موتورهای جستجو از سال 2001 تا 2016 به طور چشمگیری افزایش یافته است.



شکل 2: توزيع نتايج جستجو جمع آوري شده از 4 پايگاه داده در سال

مراحل 2، 3، 4. بررسی چند سطحی محتوا: از مجموعه مقالات داوطلب، مقالات MBSE4CPS با توجه به معیارهای حذف / اضافه از پیش تعریف شده فیلتر شده است. فرایند انتخاب ما بر اساس بررسي چند سطح بود: عنوان، چکيده، مرور سطحي، بواسطه مرور اجمالي محتوای اصلی هر مقاله داوطلب. براي مشخص شدن بيشتر، براي هر مقاله داوطلب ما اول عنوان مقاله، کلمات کليدي را مي خوانيم تا ببينيم آيا مي توان آن را در معيارهاي حذف و يا اضافه دسته بندي کرد. اگر عنوان و کلمات کلیدی براي تصمیم گيري راجع به حذف یا اضافه کردن آن کافي نباشد، ما در مرحله بعد چکيده مقاله را بررسی می کنیم. اگر ما هنوز نتوانستيم تصميمي راجع به حذف يا اضافه کردن مقاله بر مبناي چکيده بگيريم، ما در مرحله بعد محتواي کامل مقاله را به صورت سطحي بررسي مي کنيم. علاوه بر EndNote، ما از ابزار Mendeley [[6]](#footnote-6)برای مدیریت مقالاتي که محتویات دقیق آنها نیاز به مرور (با استفاده از skimming و scanning) داشت استفاده کرديم. توجه داشته باشید که ما بیشتر از هر زمان دیگری برای چک کردن مقاله هاي کاندید شک و تردید داریم. در نهایت، ما هنوز مجبور بودیم مناظره اي میان منتقدين ترتیب دهیم تا مقاله هايي که هنوز تصميم نهايي راجع به آن ها صورت نگرفته بررسي مجدد شود و تصمیم نهایی در مورد حذف يا اضافه کردن آنها گرفته شود.

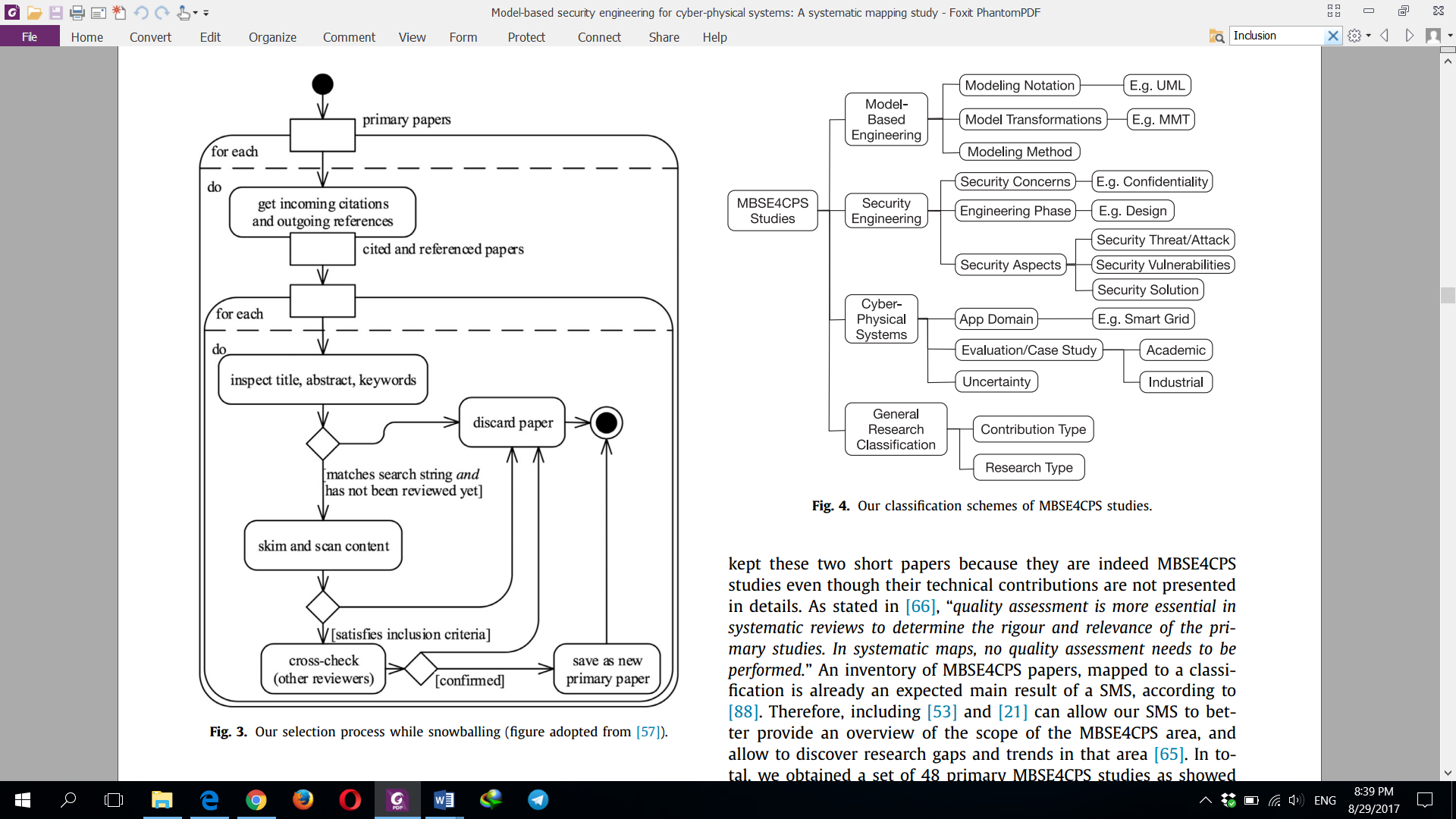
مرحله 5. بررسي مجدد و مناظره رو به رو (face to face): 1: مقالات مرزی در میان نویسندگان این مقاله برای دستیابی به تصمیم گیری در مورد حذف / اضافه مورد بحث قرار گرفت. در انتهای مرحله 5، يک مجموعه از 43 مقاله اولیه از جستجوی پایگاه داده ها به دست آمد که در *شکل 1* نشان داده شده است.

### جستجوي Snowballing

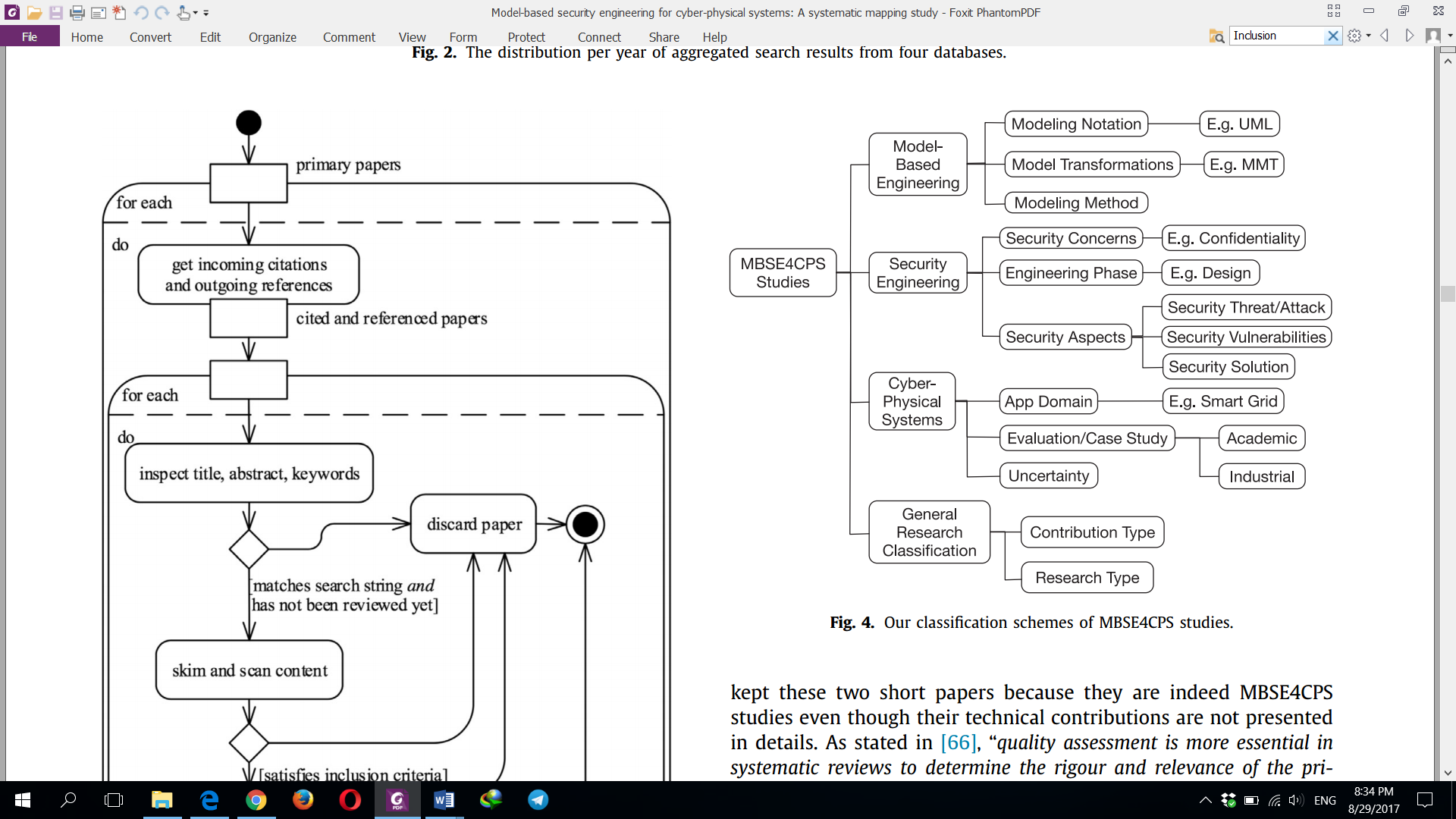
همانطور که در [90] اشاره شد و براساس تجربه شخصی ما از [57]، ما یک فرایند جستجوی ثانویه برای غلبه بر محدودیت جستجو پایگاه داده با استفاده از استراتژی snowballing [89] در مقالات اولیه انتخاب شده بعد از جستجوی پایگاه داده انجام دادیم.

مرحله ششم Snowballing: این به این معنی است که ما لیستی از مراجع و نقل قولهاي (را از Google Scholar) هر مقاله اولیه استخراج شده را پس از جستجوی پایگاه داده را برای یافتن مقالات اولیه جديد بررسي مي کنيم (به شکل 3 نگاه کنيد).

شکل 3: فرآيند انتخاب ما حين Snowballing (شکل برگرفته شده از [57])



شکل 4: طرح هاي طبقه بندي مطالعات MBSE4CPS



برای هر مقاله در مجموعه مقالات ذکر شده و ارجاع شده از 43 مقاله اولیه بالا، فرآیند انتخاب ما دوباره بر اساس چند سطح چک کردن: عنوان، چکيده و مرور سطحي محتوای اصلی است. فرآيند snowballing همچنين به طور بازگشتي به مقالات اوليه که اخيرا پيدا مي شود اعمال مي شود. ما هشت مقاله دیگر را از فرآيند snowballing پیدا کردیم.

مرحله 7. بررسي مجدد و بحث رو به رو (face to face) 2: بعد از بحث در مورد مقالات مرزي ما 3 مقاله از 8 مقاله استخراج شده از فرآيند Snowballing را حذف کرديم. براساس بحث، ما همچنين تصميم گرفتيم که دو مقاله کوتاه را نگه داريم (يک مقاله راجع به نسخه آزمايشي ابزار [53] و يک مقاله کوتاه راجع به الگوهاي امنيتي [21]). ما این دو مقاله کوتاه را حفظ کردیم زيرا آنها مطالعات MBSE4CPS هستند با وجود اينکه مشارکت هاي فني (technical contributions) آنها با جزئيات ارائه نشده است. همانطور که در [66] بیان شده است، "ارزیابی کیفی در بررسی سیستماتیک برای تعیین سختی و ارتباط مطالعات اولیه ضروری است. در نقشه های سیستماتیک هیچ ارزیابی کیفی لازم نیست انجام شود. "فهرستی از مقالات MBSE4CPS که از قبل به يک طبقه بندي (classification) نگاشت شده، نتيجه اصلي مورد انتظار SMS، طبق [88] است. بنابراين، با توجه به [53] و [21] مي توانيم به SMS مان اجازه دهيم تا يک مرور کلي بهتر از حوزه ي محدوده MBSE4CPS را فرآهم کند، و اجازه کشف شکاف هاي (gap) پژوهشي و گرايشات را در آن محدوده مي دهد [65]. در کل، ما يک مجموعه ای از 48 مطالعات اولیه MBSE4CPS که در شکل 1 نشان داده شده، برای استخراج داده در جهت پاسخ به سوالات تحقیقاتی خود بدست آورديم.

# فصل چهارم يافته هاي تحقيق

برای تجزیه و تحلیل مطالعات اولیه MBSE4CPS درجهت پاسخ دادن به سؤالات تحقیق ما چهار دسته از معیارهای طبقه بندی را تعریف کردیم. همانگونه که در شکل 4 دیده می شود، طرح های طبقه بندی ما بر اساس مصنوعات (artefacts) اصلی MBE، مهندسی امنیت، و CPS ها، بعلاوه چندين مصنوعات طبقه بندی عمومي برای نشریات پژوهشی است. به طور خاص، طرح هاي طبقه بندي ما شامل مصنوعات کليدي (key artefacts) که از طبقه بندي ارزيابي MDS در [57] انتخاب شده، از مفاهيم امنيتي کليدي در [46]، از چرخه توسعه امن مايکروسافت (Microsoft Security Development Lifecycle (SDL)) [47]، و دامنه هاي کاربرد CPS ها در [36] مي شود. علاوه بر اين، ما همچنين از برخي مصنوعات طبقه بندي کلي در اصطلاحات نوع مشارکت پژوهش (research contribution type) و نوع پژوهش (research type) همانطور که در [66] براي طبقه بندي (classify) مطالعات اوليه MBSE4CPS بحث شده استفاده مي کنيم.

**از دیدگاه MBE**، ما می خواهیم بدانیم کدام **نشانه گذاری مدل سازی (ها) (modelling notation)** در مطالعات اولیه MBSE4CPS مورد استفاده قرار گرفته است. نشانه گذاري مدل سازی برای تعیین و ثبت دامنه دانش برای اهداف مهندسی مهم است. نشانه گذاري مدلسازي مبتني بر UML (UML-base modelling notation) استاندارد است، اما زبان هاي خاص (مدل سازي) دامنه براي مهندسي سيستم هاي امن ارائه شده است [57]. جدا از نشانه گذاري مدل سازي، **روش مدل سازي (modelling methodology)** نيز نقش مهمي در MBSE ايفا مي کند. روش مدل سازي معيارگرا (Aspect-oriented modelling methodology (AOM)) [26,86] فرض بر اين است که مزايايي در تعيين ويژگي هاي متقابل سيستم هايي مانند امنيت ارائه مي دهد. ما می خواهیم حداکثر مزيت AOM در MBSE4CPS را بررسي کنيم. علاوه بر این، چگونگي جنبه های امنیتی و عناصر سیستم CPS، بسته به **انواع مدل** در مطالعات اولیه MBSE4CPS، به عنوان مثال مدل های ساختاری مبتنی بر UML (مانند، نمودارهای کلاس (class diagrams)، نمودار ساختار مرکب (composite structure diagrams))، مدل های رفتاري مبتنی بر UML (به عنوان مثال، نمودارهای توالی (sequence diagrams)، نمودارهای حالت(state diagrams)) و یا مدل های اختصاصی دامنه (domain-specific models) (DSM هاي ایجاد شده توسط DSL ها، مانند، Security Analysis Language [20]) مشخص مي شود. یکی دیگر از مهمترین نتايج MBE، **تبديلات مدل (model transformations)** است که می تواند به عنوان قلب و روح توسعه نرم افزار مبتنی بر مدل (model-driven) محسوب شود [74]. در طی فرآیندهای مهندسی مبتنی بر مدل (model-base)، تبديلات مدل به مدل (MMTs) می تواند برای اهداف مختلف مهندسی مانند ساخت مدل های امنیتی با مدل های سیستم و یا تبدیل مدل های طراحی امن به برخی از مدل هایی که برای تحلیل امنیت مورد استفاده قرار مي گیرد استفاده مي شود. MMT ها همچنین می توانند به عنوان MMT های درونی (بین مدل های بیان شده در همان زبان) یا MMT های خارجی (بین مدل های بیان شده با استفاده از زبان های مختلف) طبقه بندی شوند. از سوی دیگر، تبديلات مدل به متن (MTTs یا تکنیک های تولید کد) می تواند برای تولید کد پیاده سازی، از جمله تنظیمات امنیتی استفاده شود.

**از دیدگاه مهندسی امنیت،** ما مي خواهيم بررسي کنيم که کدام **نگراني هاي امنيتي** بر روي محرمانگي، جامعيت، دسترس پذيري، حسابرسي، احراز هويت و مجازشناسي (CIAAAA) متمرکز شده است. علاوه بر این، رویکردهای مهندسی امنیت (security-engineering approaches) بر برخی از **جنبه های امنیتی** (security aspects) خاص، مانند حملات، تهدیدها، آسیب پذیری ها یا راه حل ها تمرکز می کنند. برخی از تعاریف طبق [46] به صورت زیر است: "**تهدید** یک نقض بالقوه امنیت است. **حمله** یک اقدام است که می تواند موجب رخداد نقض امنیت شود. **آسیب پذیری** ضعف یک دارایی (asset) یا کنترل است، که ممکن است توسط يک تهدید مورد سوء استفاده قرار گیرد." **راه حل های امنیتی** موجب کاهش آسیب پذیری های امنیتی مي شود. برای هر مطالعه اولیه MBSE4CPS، ما علاقه مند به دانستن فازهاي مهندسي امنيت که رهيافت بر آنها متمرکز بوده هستيم. براي داشتن يک ديد يکپارچه از فازهاي مهندسي امنيت، طبقه بندي ما بر مبناي مراحل اصلي SDL [47]، يعني، نيازمندي ها، طراحي، پياده سازي، تاييد (verification)، انتشار (release) و پاسخ (response) است. می بینیم که SDL تقريبا شبیه به چرخه زندگی توسعه نرم افزار (software development life cycles) است. همانطور که در RQ 2.4 بیان شد، ما می خواهیم رهيافت هايي را بررسی کنیم که از ابزارها براي فازهاي مهندسي امنيت پشتيباني مي کنند (**tool support**). برای هر رهيافت، پشتیبانی ابزار (tool support) می تواند به عنوان یک ابزار جدید توسعه یافته، استفاده از ابزار موجود و یا بدون پشتیبانی ابزار طبقه بندی شود. برای هر ابزار، ما پلت فرم ابزار، ورودی و خروجی ابزار را بررسی می کنیم.

از ديدگاه CPS ها، ما مي خواهيم بدانيم کدام انواع CPS ها و امنيت آنها متمرکز بر مطالعات اوليه MBSE4CPS است. این اطلاعات به دامنه هاي کاربردی CPS ها که توجه جامعه تحقیقاتی MBSE4CPS را جلب کرده است، اشاره می کند. ما دامنه های کاربرد CPS ها را که در [36] بررسي شده را مي پذيريم. برای ارزیابی مشارکت صنعت (از طریق مطالعات موردی واقعی) در این حوزه تحقیقاتی، ما می خواهیم بدانیم اگر CPS ها به عنوان **مطالعات موردی (case studies)** در مطالعات اولیه MBSE4CPS استفاده شده اند بواسطه صنعت یا دانشگاه بوده است. علاوه بر این، به علت علاقه ما به عدم اطمینان (uncertainty) در CPS ها، همانطور که قبلا ذکر شد، در حین انجام SMS، ما همچنین در نظر داشتیم آيا مطالعات اوليه MBSE4CPS به صراحت با عدم اطمینان در ارتباط است.

از طبقه بندی پژوهش عمومي، علاوه بر مصنوعات خاص MBSE4CPS، ما همچنین از مصنوعات طبقه بندی عمومي در عبارات نوع مشارکت پژوهشي (research contribution type) و نوع پژوهش (research type) همانطور که در [66] بحث شده براي طبقه بندي مطالعات استفاده کرديم. انواع مشارکت هاي پژوهشي عبارتند از: روش (تکنیک ها / رهيافت ها)، مدل، معیارها (metrics)، ابزارها (tools) و موارد باز (مسائل شناسایی شده که باید مورد توجه قرار گیرد). طبقه بندي انواع پژوهشي با توجه به [88] در جدول 1 آمده است.

# نتايج

نویسنده اول از صفحه گسترده مایکروسافت اکسل برای ثبت داده های استخراج شده از مطالعات اولیه MBSE4CPS استفاده کرده است. بعد از آن چندين بازبيني از صفحات گسترده انجام شد که استخراج داده ها براي پشتيباني بهتر از فرآيند استخراج و قابليت مقايسه بين مطالعات را فرآهم مي کند. پس از تهیه داده ها، ما به پرسش های تحقیقاتی در بخش های 5.1-5.3، پاسخ مي دهيم.

## در مورد انتشار مطالعات MBSE4CPS

در این بخش، ما نتایج خود را برای پاسخ به RQ1 و زیر سوالات آن ارائه می کنیم.

### گرايشات انتشارات (Publication trends)

پاسخ ما به RQ1.1 در شکل 5 یافت مي شود که تعداد مطالعات اولیه MBSE4CPS منتشر شده در سال را نشان مي دهد. ما قبلا در شکل 2 شاهد افزایش شدید مقالات مرتبط با نتایج جستجوی جمع شده هستیم. ما قبلا در شکل 2 شاهد افزایش شدید مقالات مرتبط با نتایج جستجوی جمع آوري شده هستیم. با این حال، شکل 5 به بررسی مطالعات اولیه MBSE4CPS می پردازد. به طور خاص، مطالعات اولیه MBSE4CPS تا قبل از سال 2007 پيدا نشده است. اولین تحقیق اوليه MBSE4CPS در سال 2007 و به دنبال آن یکی دیگر در سال 2008 بود. بيشتر مطالعات اولیه MBSE4CPS در سه سال اخیر صورت گرفته است. در سال 2014، با 13 مطالعه اولیه بيشترين تعداد مطالعه ثبت شده است. در سال 2015، ده مطالعات اولیه منتشر شده است. در سال 2016، ما فقط برای مطالعه اولیه MBSE4CPS در دوره ژانویه تا آخر سپتامبر را (فقط تا قبل از اتمام مقاله) جستجو کردیم. با توجه به اينکه سال 2016 تمام نشده بود، ما یازده مطالعه ابتدایی را برای این دوره پيدا کردیم. به طور متوسط، از سال 2007 تا آخر سپتامبر سال 2016، حدود پنج مطالعات اولیه سالانه منتشر شده است. اخیرا، در دوره 2014-2016 به طور متوسط بیش از 11 مطالعه اولیه به صورت سالانه منتشر شده است. ما در [96] بر اين باوريم که رویکردهای مبتنی بر مدل برای CPS ها در حال افزایش چشمگير هستند. ما به آساني مي توانيم يک افزايش چشمگي در تعداد مطالعات اوليه MBSE4CPS را در سه سال اخير مشاهده کنيم. اين افزايش مي تواند نشانه گرايش باشد، که در آن بيشتر تکنيک هاي MBSE توسعه يافته یا محبوبیت استفاده از CPS ها به سرعت در حال افزايش است. توجه داشته باشید که تعداد این نشریات در هر سال بر اساس تاریخ رسمی نشریات ثبت شده توسط Google Scholar است، که اغلب بر مبناي تاریخ هاي مقالات چاپ شده است. با اين حال، مقاله اي که تقريبا در پايان سال پذيرفته شود، اغلب در همان سال به صورت آنلاين منتشر مي شود، نه در سال بعد همانطور که به طور رسمي توسط Google Scholar ثبت شده است. اگر ما نگاهی دقیق تر به مطالعات اولیه که در سال 2014 به صورت رسمي منتشر شده است بيندازيم، دو مقاله [81،94] براي اولين بار در سال 2013 به صورت آنلاین منتشر شده، وجود دارد. بنابراین، اعداد در شکل 5 به صورت مطلق درست نيستند. به طور کلی، هنوز می توانیم روند انتشار افزايشي مطالعات اولیه MBSE4CPS را در دوره مورد بررسی به وضوح مشاهده کنیم.

### مکان هاي انتشار (Publication venues)

نمودار ميله اي در شکل 6 توزیع مطالعات اولیه MBSE4CPS را در هر مکان نشان می دهد که می تواند پاسخ هاي ما به RQ1.2 باشد. از لحاظ محل نشر، بسیاری از مطالعات اولیه MBSE4CPS در کنفرانس ها (29 در مجموع) به نسبت مجلات (یازده) و یا کارگاه های آموزشی (هشت) منتشر شده است. این امر برای یک جهت تحقیق جدید مانند MBSE4CPS قابل فهم است که در آن ایده ها باید در کنفرانس ها بهتر از قبل مبادله شوند. اين براي يک مسير پژوهشي جديد مانند MBSE4CPS که فرض بر اين است که ايده ها بهتر در کنفرانس ها مبادله مي شود قابل درک است. علاوه بر اين بسياري از آثار ممکن است به اندازه کافي بزرگ (extensive) يا کامل (mature) براي انتشار در مقاله نباشند.

شکل 7 به صورت دقیق تر توزیع انواع نشریات را در سال نشان مي دهد. دوره چهار ساله (2007-2010) تنها شامل سه مقاله کنفرانس مطالعات اولیه MBSE4CPS مي شود. مقالات مجله اي (Journal) از سال 2011 شروع شده و تعداد مقالات مجله اي همچنين به نظر می رسد به طور کلي همراه با تعداد مقالات کنفرانسي و مقالات کارگاهي به طور کلی افزايش يابد.

اگر به نوع محل در ستون آخر شکل 6 نگاه کنیم، تعداد بسیار کمی از مطالعات اولیه (در مجموع هفت مکان) از مکان ها مرتبط با مهندسی نرم افزار است. مراکز انتشاراتی بیشتر مربوط به مهندسی امنیت و مهندسی برق / سیستم هستند به ترتیب 17 و 24 مطالعه اوليه MBSE4CPS را به خود اختصاص داده اند. ما دریافتیم که کمی تعداد مطالعات اولیه در محل های مهندسی نرم افزار، قابل توجیه است زیرا CPS ها دامنه ي تحقیقاتی جدیدی برای جامعه تحقیقاتی مهندسی نرم افزار است. مسائل امنیتی برای CPS ها تمرکز اصلی در مطالعات اولیه MBSE4CPS هستند، در حالیکه تکنیک های MBE موجود نهايت استفاده آنها پشتيباني از مشارکت ها (contributions) است. این امر می تواند دلیل آن باشد که محل های نزدیک به مهندسی امنیت و مهندسی برق / سیستم مقالات بیشتری را به خود اختصاص مي دهند. همچنین لازم به ذکر است که طبقه بندی ما از مکان های انتشار همانطور که در بخش 6 بحث شده، به صورت مطلق درست نیست.

### دانشگاهي در برابر صنعتي

برای پاسخ به RQ1.3، نمودار دايره اي در شکل 8 بيانگر اين است که 91٪ (41 مقاله) از مطالعات اولیه MBSE4CPS تنها به نویسندگان دانشگاهي اختصتص دارد. کارهاي اشتراکي میان دانشگاه ها و صنعت تنها سه مقاله (7٪) را به خود اختصاص داده است. تنها یک مقاله [61] (2٪) وابسته به صنعت است، به عنوان مثال، Roll Royce. بنابراین، در مجموع، تنها 9٪ از مطالعات اولیه MBSE4CPS با صنعت در ارتباط است.

### توزیع جغرافیایی

برای پاسخ دادن به RQ1.4، ما در نظر مي گيريم یک مطالعه اولیه در يک کشور انجام شده است اگر حداقل يک نویسند از مطالعه اولیه وابستگي به اين کشور داشته باشد. به عنوان مثال، در یک مطالعه اولیه که دارای سه نویسنده از سوئد و یک نویسنده از ایالات متحده آمریکا است، ما فرض را بر اين مي گيريم که مطالعه در هر دو کشور سوئد و ایالات متحده انجام شده است. شکل 9 نشان می دهد که محققان مستقر در ایالات متحده آمریکا (USA) تاکنون در بیشترین تعداد مطالعات اولیه MBSE4CPS با 18 مورد شرکت داشته اند و به دنبال آن محققان مستقر در فرانسه (FR) با هفت نشریه، سنگاپور (SG) با شش نشریه، و اتریش (AT) با پنج نشریه به ترتيب بيشترين تعداد را داشته اند. محققان مستقر در کانادا (کالیفرنیا) و United Kingdoms (UK) چهار نشریه اشتراکي برای هر کشور داشتند. محققان مستقر در امارات متحده عربی (AE)، آلمان (DE) و سوئد (SE) دارای سه نشریه در هر کشور هستند. محققان بلژیک (BE)، اسپانیا (ES)، ایتالیا (IT)، ایران (IR) و چین (CN) دو نشریه در هر کشور دارند. محققان مجارستان (HU)، لوکزامبورگ (LU)، نروژ (NO)، روسیه (RU)، کره جنوبی (KR) یک نشریه را در هر کشور دارند. پژوهش هاي صورت گرفته در رابطه با تعداد مطالعات اولیه MBSE4CPS در کشورهای پیشرو مانند ایالات متحده آمریکا و کشورهای اتحادیه اروپا به تحقیقات بر روی CPS هایی که در این کشورها و مناطق توسعه یافته، کاملا مرتبط است [27].

## ويژگي هاي مطالعات MBSE4CPS

اين بخش نتايج اصلي براي پاسخ به RQ2 و سوالات مشتق شده از آن توضيح مي دهد.

### نگراني هاي امنيتي (Security concerns) و جوانب امنيتي (security aspects)

پاسخ سوالات RQ2.1 و RQ2.2 را می توان در شکل 10a پیدا کرد.

از دیدگاه امنیتی، ما می خواهیم بدانیم چه نگرانی های امنیتی در مطالعات اولیه MBSE4CPS مورد توجه قرار گرفته است. در شکل 10a مشخص است که اکثر رویکردها (67٪، 32 مقاله) به تمام يا چندين نگرانی امنیتي کلیدی (به عنوان مثال، CIAAAA) مربوط می شود. این به این معنی است که فعالیتهای مهندسی امنیت (به عنوان مثال، تجزیه و تحلیل امنیت(security analysis)) باید از عهده همه یا چندین نگرانی امنیتی کلیدی (به صورت ضمنی یا صریح) برآيد و آنها را حل کند. تقریبا یک سوم (33٪، 16 مقاله) مطالعات MBSE4CPS اولیه مربوط به برخی نگرانی های امنیتی خاص، اما نه همه ي نگرانی های اصلی (مانند محرمانه گي و جامعيت، اما عدم دسترس پذيري (not availability)) است.

در شکل 11a، می بینیم که بیشتر مطالعات MBSE4CPS اولیه در حالت کلي به جاي تمرکز بر روی تحلیل امنیت (security analysis) بر روي تهدیدات امنیتی، حملات و یا آسیب پذیری ها (77٪) متمرکز شده اند. فقط حدود 13٪ (شش مقاله) از مطالعات صرفا راهکارهای امنیتی را مطرح کرده و 10٪ (پنج مقاله) راه حل های امنیتی را همراه با تجزيه و تحليل تهديد/ حمله/ آسيب پذيري مطرح کرده اند. تجزیه و تحلیل دقیق تر این آمار در پاسخ های ما به سوالات تحقیق باقی مانده به شرح زیر است.

### نشانه گذاری مدل سازی (Modelling notation) و روش مدل سازی (modelling methodology)

در جواب به سوال RQ2.3، شکل 11b نشان مي دهد که درصد مطالعات اوليه MBSE4CPS که از نشانه گذاري مدل سازي UML (54%) استفاده نکرده است کمي بيشتر از درصد مطالعات اوليه MBSE4CPS است که از نشانه گذاري مدل سازي UML استفاده کرده است (46%). زبان های مدل سازی در مطالعات اولیه MBSE4CPS، که از نشانه گذاري مدل سازی UML استفاده نمی کنند، اغلب در قالب DSL ها است. توجه داشته باشيد غير معمول نيست که شاهد استفاده گسترده از DSL ها در مقايسه با زبان مدل سازي استاندارد، مانند UML در بعضي از حوزه هاي پژوهشي مهندسي نرم افزار، همانطور که در [17] گزارش شده است باشيم. محبوبیت استفاده از DSL ها در مدل سازی (جنبه های امنیتی) CPS ها که با استفاده از UML استاندارد قابل مقایسه است، ماهیت ناهمگون (heterogeneous nature) CPS را منعکس می کند. يک تجزیه و تحلیل در [51] نشان می دهد که رهيافت هاي DSL ها برای مدل سازی CPS ها می تواند در زمینه های مختلف طراحی مانند مهندسی نرم افزار، مهندسی مکانیک، مهندسی برق و مهندسی الکترونیک (و همچنین مهندسی امنیت در مورد MBSE4CPS) استفاده شود. در واقع، اکثر مطالعات اوليه MBSE4CPS که بر روي تجزيه و تحليل تهديد/ حمله/ آسيب پذيري تمرکز دارند (شکل 11a) از حداکثر مزاياي DSL ها براي مدلسازي تهديد/ حمله/ آسيب پذيري CPS ها استفاده کرده اند. علاوه بر اين، استفاده از نشانه گذاري غير UML در تقریبا نیمی از مطالعات اولیه MBSE4CPS نشانه افزایش قابل توجهی در استفاده از نشانه گذاري هاي مدل سازی غیر UML در مهندسی امنیت را نشان می دهد. استفاده از نشانه گذاري مدل سازی غیر UML در رهيافت هاي MDS همانطور که در مطالعه اخیر مربوطه [57] نشان داده شده به طور کلی تنها 13٪ است (87٪ از نشانه مدلسازی UML استفاده شده است).

جدول 2 مطالعات اولیه MBSE4CPS را بر مبناي UML (UML-based) یا برمبناي رهيافت هاي ديگر مدل سازي طبقه بندی می کند. جزئیات رهيافت هایی که از نشانه گذاری هاي مبتني بر UML استفاده می کنند و از نشانه گذاري هاي مبتنی بر UML استفاده نمی کنند، در جداول A.1 و A.2 در ضمیمه A آمده است. علاوه بر این، ما همچنین می توانیم ببینیم که تنها یک روش MBSE4CPS [86] استفاده از AOM استفاده کرده است. استفاده محدود از AOM در MBSE4CPS تا کنون قابل درک است زیرا AOM نیز در 15٪ از مطالعات اولیه MDS که در [57] مرور شد مورد بررسی قرار گرفته است.

اجازه دهید به رویکردهای مدل سازی در مطالعات اولیه MBSE4CPS دقيق تر نگاه کنیم. شکل 12 نشان می دهد که استفاده از مدل های ساختاری یا رفتاری برای تعیین تهدید / حمله یا آسیب پذیری امنیتی کمتر از انواع دیگر مدل ها برای این منظور استفاده مي شود. انواع دیگر مدل ها اغلب در قالب DSM ها مانند مدل درخت حمله (attack tree) و یا انواع خاصی از مدل ها هستند که می توانند توسط ابزار تجزیه و تحلیل (امنیتی) استفاده شوند. در مجموع در بين يازده مطالعه اوليه (23%، شکل 11) که راه حل هاي امنيتي را ارائه کرده اند، مدل هاي ساختاري (8 مورد) از مدل هاي رفتاري (4 مورد) و ساير انواع (4 مورد) بيشتر مورد استفاده قرار گرفته اند. به عنوان مثال، برخی از رهيافت ها الگوهای امنیتی را برای CPS ارائه می دهند که معمولا در مدل های ساختاری بیان می شود. با این حال، همانطور که در شکل 12 دیده می شود، تعداد مدل های مورد استفاده برای تعیین راه حل های امنیتی بسیار کمتر از تعداد مدل ها برای مشخص کردن تهدیدات / حملات و آسیب پذیری ها است. دلیل این امر این است که تنها 23 درصد از مطالعات اولیه راه حل های امنیتی را مطرح کرده است در مقایسه با اينکه 77 درصد از مطالعات اولیه فقط تجزیه و تحلیل تهدید / حمله / آسیب پذیری را مطرح کرده است (شکل 11).

شکل 13 نشان می دهد که MMT ها در چندین مطالعه اولیه، به عنوان مثال، تهدید / حمله (9 مطالعه)، آسیب پذیری (6 مطالعه)، و راه حل امنیتی (3 مطالعه)، قابل استفاده است. در مجموع، تعداد مطالعات اولیه برای استفاده از MMT ها اشاره شده ده تا است، و مجموع مطالعات اولیه که دارای MTT ها هستند، چهار عدد است. این تعداد در مقایسه با 48 مقاله از مطالعات اولیه MBSE4CPS بسیار کم است. علاوه بر این، تنها دو مطالعه اولیه (پیشنهاد راه حل های امنیتی همراه با تجزیه و تحلیل تهدید / حمله) برخی از اطلاعات پیاده سازی MMT را ارائه کرده اند [20،72]. همچنین در شکل 13 می بینیم که از میان نه مطالعات اولیه که از MMT ها استفاده مي کنند، بیشتر آنها (هشت) MMT خارجی (exogenous MMTs) هستند که مدل های امنیتی/ سیستم را به چند DSM ديگر که می تواند بوسيله ابزارهاي تحلیل (امنیت) استفاده شود تبديل مي کند (به عنوان مثال [20،63]). تنها یک MMT به صورت داخلي برای ساختن جنبه های امنیتی (security aspects) در مدل سیستم استفاده شده است [72]. هیچ رویکردی وجود ندارد که تجزیه و تحلیل امنیتی خودکار را به طور مستقیم بر روی مدل های امنیتی/ سیستم (در مرحله تأیید) ارائه دهد؛ زیرا تجزیه و تحلیل های رسمی (امنیتی) مبتنی بر مدل نیاز به روش های تحلیل تخصصی با ورودی های تخصصی مدل دارد. بنابراین، MMT های خارجی در چندين مطالعه اولیه برای پرکردن شکاف توسعه یافته اند. به عبارت دیگر، MMT های خارجی می توانند برای تبدیل مدل های امنیتی/ سیستم به مدل های تخصصی که به ورودی هاي روش های تأیید/ تجزیه و تحلیل و/ یا ابزارها نزدیک تر است کمک کند.

### مراحل (فازهاي) مهندسي امنيت و پشتيباني ابزارها

تمرکز مطالعات اوليه MBSE4CPS راجع به تجزيه و تحليل امنيت همچنين مي تواند وقتي که ما دقيق تر مرحله يا مراحل SDL را که مطالعات اوليه MBSE4CPS روي آن انجام شده را بدانيم توضيح داده شود. در پاسخ به سوال RQ2.4، شکل 14 توزیع مطالعات اولیه MBSE4CPS را با توجه به مراحل اصلی نشان مي دهد: تجزیه و تحلیل نيازمندي ها/ دامنه، معماری/ طراحی و ساير موارد (پیاده سازی، تایید، انتشار، پاسخ). 100٪ مطالعات اولیه MBSE4CPS بر روی تجزیه و تحلیل نيازمندي ها / دامنه یا معماری/ طراحی یا هر دو مرحله انجام شده است. تقریبا نیمی از مطالعات (48٪) فقط به مرحله نيازمندي ها تمرکز داشتند. 14٪ از مطالعات اولیه عمدتا در مرحله طراحی قرار داشت و در مجموع 40٪ در مرحله طراحی قرار داشتند. فقط 4%، به طور نسبي رهيافت های توسعه امن تر از تجزيه و تحليل نيازمندي ها/ دامنه به معماري/ طراحي و سپس به مراحل بعدي را مطرح کردند. تجزیه و تحلیل دقیق تر مطالعات MBSE4CPS با توجه به مراحل اصلی SDL بعدا در شکل 22 ارائه می شود.

از نظر پشتیبانی ابزار (به عنوان مثال، برای مدلسازی، تحلیل امنیت)، 11 مطالعه اولیه (23٪) براي پشتيباني از ابزارها ذکر شده، که فقط چهار مطالعه یک ابزار جدید و نسخه توسعه يافته آن را، به عنوان مثال، [31،53،83] ارائه کرده است. هفت مطالعات اولیه براساس توسعه ابزارهاي موجود است. 37 مطالعه اولیه (76٪) از هیچ پشتیبانی ابزاري پشتيباني نمي کنند (شکل 15a).

پلت فرم ابزار. با در نظر گرفتن فقط ابزارها، يک ترکيب مشترک از ابزارهاي مدل سازي مبتني بر UML با ابزارهاي تجزيه و تحليل براي ايجاد يک پلت فرم ابزار در 5 مقاله از آنها يافت مي شود. به صورت دقيق تر، ابزارهاي مدل سازي مبتني بر UML مانند Papyrus در [6] و MagicDraw در [81] ترکيبي از ابزارهاي تحليل (رسمي (formal)) مانند ProVerif در [63] و Diversity در [6] است. بعضی از ابزارها ابزارهاي شبیه سازی مانند [53] هستند. بقیه ابزارها به صورت وضوح توضیح داده نشده اند. درصد مقاله هایی که از ابزار پشتیبانی استفاده نمی کنند، می تواند برای زمینه مطالعه بسیار زیاد باشد. به خصوص در زمینه مهندسی امنیت، پشتیبانی ابزار بسیار مهم است. برای مثال، برای مهندسان امنیت، به منظور استفاده بهتر از DSL های امنیتی جهت تعیین مدل های امنیتی، ابزار لازم است. برخلاف مدل سازي هاي مبتني بر UML که از طيف وسيعي از ابزارها (به عنوان مثال، Papyrus و MagicDraw) پشتيباني مي کند، DSL ها اغلب از ابتدا طراحي و توسعه مي يابد. بدون پشتيباني ابزار، کاربران نهايي DSL ها قادر به استفاده درست از DSL ها براي تعيين مدل هاي امنيتي نخواهند بود. ابزارها همچنين براي پشتيباني تاييد و اعتبارسنجي خودکار امنيت ضروري هستند. انجام تأیید و اعتبارسنجي امنيت به صورت دستی می تواند بسیار مستعد خطا باشد زیرا پیاده سازی های امنیتی اغلب پراکنده و با کل سیستم ترکيب شده است.

ورودي ابزار (Tool input). تعداد کل مطالعات اولیه با استفاده از نشانه گذاري هاي مبتني بر UML به عنوان ورودی هفت (64٪ از مقالات يک ابزار را گزارش مي دهند، شکل 15b) عدد است. چهار مطالعات اولیه با پشتیبانی ابزار (به عنوان مثال، [20]) از DSM های مبتنی بر غیر مبتنی بر UML (non-UML-based) به عنوان ورودی ابزار استفاده می کنند. بنابراین، تعداد رهيافت هاي مبتنی بر UML با پشتیبانی ابزار، بيشتر از تعداد رويکردهاي غیر UML با پشتیبانی ابزار است. این قابل درک است زیرا پشتیبانی ابزار برای UML ارتقاء يافته و صنعتی شده است. خروجی ابزار (Tool output). خروجی های ابزار در قالب نتایج تجزیه و تحلیل امنیت مانند اثبات هاي امنیتي، خطرات امنیتی (آسیب پذیری ها) و نيازمندي هاي امنیتی برمبناي برآورد ریسک (risk estimation) است. انواع خروجی ابزار با توجه به این که اکثر مطالعات اولیه MBSE4CPS به طور عمده برای تجزیه و تحلیل تهدید، حمله یا آسیب پذیری مطابقت دارد (شکل 11a).

### مشارکت و نوع تحقيق

شکل 16 و 21 مي تواند به ما در پاسخ دادن به سوال RQ2.5 کمک کند. شکل 16 نشان مي دهد که روش (به عنوان مثال، روش تجزيه و تحليل امنيت) مهم ترين اصل در مشارکت تحقيق در همه مطالعات اوليه MBSE4CPS است. در میان مطالعات اولیه، 67٪ تنها به معرفي روش ها (method)، 20٪ روش ها را همراه با پشتیبانی ابزار ، 9٪ روش ها را همراه با معيار يا معيارهاي (امنیتی) و 4٪ روش ها، ابزار و معیارها را در يک مطالعه واحد معرفی کرده اند. ما در شکل 19 درصد مطالعات اولیه MBSE4CPS که مدل ها به عنوان بخشی از مشارکت تحقيق است را نشان نمي دهيم زيرا از معيارهاي انتخاب ما واضح است که همه مطالعات اوليه MBSE4CPS بايد مدل يا مدل هايي در مشارکت هاي تحقيقاتي خود داشته باشند. با توجه به انواع تحقيق دقيق، شکل 17 نشان مي دهد که 88% مطالعات اوليه MBSE4CPS از نوع پيشنهادهاي راه حل هستند در حاليکه فقط 2% (يک مقاله) از نوع مقالات معتبر [78] است. 10٪ از مطالعات فقط از نوع پیشنهادات مفهومی است. هيچ مطالعه اي از انواع نظريه ها (opinion)، ارزيابي (evaluation) يا گزارش تجربي پيدا نشد. برای اطلاعات دقیق تر، ما توزیع مقالات را در بين جنبه های تحليل مختلف (various analysis aspects)، تجزيه و تحلیل می کنیم. شکل 18 نشان مي دهد که بيشتر مطالعات اوليه MBSE4CPS نوع مشارکت پژوهشي آنها به عنوان روش هاي (method) (به عنوان مثال براي تحليل امنيت) مرتبط با تهديد/ حمله يا آسيب پذيري (به ترتيب 41 و 24 مقاله دارند) با تعداد ابزارهاي کم (تعداد 8 و 9 عدد) معرفي شده است. فقط حدود یک چهارم از مطالعات MBSE4CPS اولیه (یعنی یازده مقاله در شکل 21) به عنوان روش (method) برای راه حل امنیتی مشارکت پژوهشی (research contribution) دارند و تنها دو مورد از ابزار (tool) پشتیبانی می کند.

در شکل 19 می توانیم ببینیم که بیشتر مطالعات MBSE4CPS اولیه نوع تحقيق آنها پیشنهاد راه حل هاي (solution proposal) (به عنوان مثال برای تحلیل امنیت) مربوط به تهدید/ حمله یا آسیب پذیری (به ترتیب 36 و 21 مقاله) است. کمتر از یک چهارم از مطالعات اولیه MBSE4CPS (نه عدد) نوع تحقيق آنها پيشنهاد راه حل هاي حاوي راه حل هاي امنيتي (security solution) است. به طور مشابه، شکل 20 نشان می دهد که بسیاری از مطالعات اولیه MBSE4CPS مشارکت های تحقیقاتی از نوع "روش (method)" را در مراحل اولیه مانند تجزیه و تحلیل نیازمندي ها/ دامنه یا طراحی (37 و 22 مقاله)، همچنین با چند ابزار مشابه (9 و 6 عدد) دارند. روش های بسیار کمی از مراحل بعد SDL مانند پياده سازي- implementation (پنج)، تأیید- verification (هفت) و منتشر کردن- release (دو)، را با کمترین (یک یا دو ابزار) یا هیچ ابزار پشتیبانی، پشتیبانی کرده است.

مرحله ي تأیید و اعتبارسنجي برای ارائه مدارک و ارزیابی امنیت CPS بسیار مهم است. از آنجائیکه همان طور که قبلا مورد بحث قرار گرفت، امنیت CPS ها، حیاتی است، مرحله تأیید و تأیید امنیتی باید یک بخش حیاتی از SDL باشد. با این حال تنها چند رهيافت (به عنوان مثال، [20،63]) تایید رسمی را ارائه دادند، و هيچ مطالعه اي رهيافت تست امنيت بر مبناي مدل (model-based security testing approach) را براي CPS ها مطرح نکرده است. در دو مقاله برخی از موارد/ مسائل باز، به عنوان مثال، چگونگی ترکيب تجزیه و تحلیل امنیت با کلاس های مختلف DSL (برای مشخص کردن تهدید/ حمله/ آسیب پذیری)، مانند موارد برمبناي جریان کنترل (control flow) [20]، يا چالش هاي اتصال فاصله هاي (gap) پياده سازي از نيازمندي ها تا طراحي و سپس به پياده سازي هاي واقعي (hardware based) براي امنيت CPS ها در سطح کد [3] را مطرح شده است.

در شکل 21 می بینیم که بیشتر مطالعات اولیه MBSE4CPS نوع تحقیق "پیشنهاد راه حل" را برای مهندسی در مراحل اولیه مانند تجزیه و تحلیل نيازمندي ها/ دامنه (32 مقاله) و طراحی (19 مقاله) دارد. تعداد بسيار کمي از مطالعات اوليه MBSE4CPS راه حل هاي پشتيباني از مراحل بعدي SDL را (تعداد 5 عدد مربوط به مرحله پياده سازي (implementation)، 7 عدد براي تاييد (verification) و فقط يک عدد مربوط به انتشار (release)) مطرح کرده است. شکل 21 همچنين نشان مي دهد فقط که تنها يک مقاله [78] از نوع تحقيق اعتبارسنجي ( validation research) است که عمدتا در مورد ارزيابي يک رهيافت براي مهندسي نيازمندي هاي امنيتي بوسيله يک مطالعه موردي دانشگاهي راجع به شبکه هوشمند (smart grid) (با توجه به تهديد/ حمله/ آسيب پذيري) است. ما هیچ تحقیق ارزیابی (evaluation research) یا گزارش تجربي یا یک مقاله معتبر (opinion paper) را پیدا نکرده ایم.

### دامنه هاي کاربرد و عدم قطعيت (Application domains and uncertainty)

در پاسخ به RQ2.6، شکل 22a نشان می دهد که تقریبا نیمی از مطالعات اولیه MBSE4CPS (44٪) از شبکه های انرژی هوشمند (smart energy grids) به عنوان مطالعات موردي یا دامنه های کاربردی استفاده می کنند. این قابل درک است، زیرا شبکه هوشمند (the next-generation power system) می تواند محبوب ترین نمونه CPS ها باشد که اولویت های ملی را در بسیاری از کشورهای توسعه یافته مانند ایالات متحده آمریکا و اتحادیه اروپا دریافت می کند [27]. نظرسنجی اخیر همچنین نشان می دهد که بیشتر تکنیک های تشخیص نفوذ برای CPS تاکنون برای امنیت ابزار هوشمند (عمدتا شبکه انرژي هوشمند) پیشنهاد شده است [49]. علاوه بر این، برای تحقق بخشیدن به بسیاری از ویژگی های پیشرفته، شبکه هوشمند به شدت به شبکه های اطلاعاتی (باز) بستگی دارد که به ناچار آن را آسیب پذیرتر نسبت به تهدیدات امنیتی می کند [85]. در شبکه های هوشمند، فناوری اطلاعات و ارتباطات (ICT) به طور فزاینده ای در سراسر شبکه برای حمایت از ارتباطات جدید (novel communication) و توابع کنترل (control functions) يکپارچه شده است، اما در عین حال بسیاری از چالش های امنیتی ICT را به ارمغان می آورد. دامنه های مطالعات اوليه MBSE4CPS شامل 30 درصد از جمله خودرو، CPS هاي حمل و نقل (transportation)، مراقبت های بهداشتی (healthcare) و سیستم های تصفیه آب (water treatment) بود. حدود یک چهارم از مطالعات اولیه MBSE4CPS (26٪) به CPS ها در حالت کلی اختصاص داده شده، به عنوان مثال، یک زبان عمومی برای توصیف حملات به CPS ها است [92].

شکل 22b نشان می دهد که بیشتر مطالعات اولیه MBSE4CPS (88٪) فقط موارد مطالعات دانشگاهي ارزيابي شده است (به عنوان مثال بيشتر موارد مطالعات دانشگاهي در مورد در شبکه های هوشمند است) در حالی که تعداد بسیار کمی از مطالعات ابتدایی (12٪) موارد مطالعات صنعتی بود. برای پاسخ دادن به RQ2.7، در حالی که ما مطالعات اوليه MBSE4CPS را مرور مي کنيم همچنين هر مطالعه ي مربوط به امنيت CPS ها که عدم قطعيت در آن به صراحت مد نظر قرار گرفته باشد را بررسي مي کنيم. با این حال، ما هیچ مطالعه اولیه MBSE4CPS را که به صراحت مسئله عدم قطعیت CPS ها در آن مورد بررسي قرار گرفته باشد پیدا نکردیم. این بدان معنا نیست که مطالعات موجود از عدم اطمینان CPS ها آگاه نيستند. آنها ممکن است به طور صريح يا رسمي عدم اطمينان در آن بررسي نشده باشد. برخی از روشهای اوليه MBSE4CPS (به عنوان مثال [7،15،31،71]) به طور غیرمستقیم یا به طور جزئی مشکل عدم قطعیت را در تجزیه و تحلیل ريسک امنیتی خود برای CPS ها بررسي مي کنند. اما در واقع، ما هیچ رهيافت MBSE4CPS را پیدا نکرده ایم که به طور صریح یا رسمی به عدم قطعیت CPS ها بپردازد. به عنوان یکی از دلایل این امر همانطور که در ابتدا در این مقاله اشاره شد، می توان به این مورد اشاره کرد که رهيافت هاي MBSE4CPS فقط چند سال پیش به وجود آمده است. به عنوان بهترين دانش ما، تا کنون تنها یک پروژه تحقیقاتی، تحت عنوان U-Test[[7]](#footnote-7)، به صراحت به عدم قطعیت CPS ها با استفاده از مهندسی مبتنی بر مدل پرداخته است. علاوه بر این، U-Test به طور خاص روشهای MBSE4CPS را مطرح نمی کند. به عبارت دیگر، تعامل بین عدم اطمینان و امنیت CPS ها، حداقل در رهيافت هاي MBSE4CPS که ما بررسی کردیم، هنوز مورد مطالعه و بررسي قرار نگرفته است.

## مسائل باز و برنامه هاي تحقیقاتي پیشنهاد شده

بر اساس یافته های ما برای پرسش های تحقیق RQ1 و RQ2، ما می خواهیم مسائل باز کنونی پژوهش هاي MBSE4CPS را برای پاسخ به RQ3.1 و RQ3.2 مشخص کنیم. برای هر مسئله باز، پیشنهاداتي (جهت تحقیق) جهت ارائه آن را پیشنهاد می کنیم.

### نگراني ها/ اهداف امنيتي ضمني (Implicit)

در بخش 5.2، پاسخ ما به RQ2.1 بیان می کند که کمی بیش از نیمی از مطالعات اولیه MBSE4CPS در مطالعات خود به صراحت اين که کدام نگرانی های امنیتی خاص (مثلا CIA) مورد توجه است را بیان نمی کنند، بلکه به طور ضمنی بيان مي کنند. از دیدگاه مهندسی امنیت، رهيافت هاي امنیتی باید از نگرانی های امنیتی جدا شود. وقتي نگراني هاي امنيتي مورد توجه به صراحت ذکر شود، مطالعات اوليه MBSE4CPS مي تواند با اين نگراني ها سيستماتيک تر و قانع کننده تر کنار بيايد. بنابراین، ما پیشنهاد می کنیم نگرانی های امنیتی به طور صریح در هر مطالعه اولیه MBSE4CPS اشاره شود. این ممکن است که در حال حاضر، یک درک مشترک از امنیت و CPS با هم نامفهوم باشد. یکی از راه های دستیابی به این هدف، ایجاد یک مدل مفهومی است که بتواند هر دو جنبه را با هم پوشش دهد.

### راه حل هاي مهندسي شده خيلي کم

همانطور که در پاسخ ما برای RQ2.2 اشاره شد، بیشتر مطالعات اولیه بر پشتيباني از تحلیل های امنیتی بر اساس تهدیدات امنیتی، حملات و آسیب پذیریها متمرکز شده بودند و روي مهندسي راه حل های امنیتی متمرکز نبودند. این را به عنوان یک زمینه نسبتا جدید می توان درک کرد، پژوهش هاي MBSE4CPS تا کنون عمدتا بر نیازمندي ها و تحلیل هاي دامنه متمرکز بوده است. بنابراین، راه حل های امنیتی برای CPS هنوز کمياب است. علاوه بر این، انواع تهدیدات امنیتی جدید، حملات بسیار متفاوت از موارد سنتی در بسیاری از دامنه های برنامه های CPS ها مانند تهدید امنیتی جدید به بخش هاي فیزیکی CPS ها می باشد. راه حل های امنیتی برای این نوع تهدیدات جدید هنوز در حال توسعه است. در آینده، رهيافت هاي جدید MBSE4CPS باید برای راه حل های امنیتی مهندسی برای توسعه CPS ها پیشنهاد شود.

### اتوماسیون محدود در تجزیه و تحلیل امنیتی صوري

همانطور که در بخش 5.2 مورد بحث قرار گرفت، هیچ مطالعه اولیه MBSE4CPS که تجزیه و تحلیل را مستقیما بر روی مدل های امنیتی/ سیستم در مرحله تأیید انجام دهد وجود نداشت. بعضی مقالات (مثلا [20،63]) در مورد ترجمه کردن مدلها به فرمالیسمهای دیگر برای فعال کردن تحلیلهای خودکار را مطرح کردند. تبدیل به فرمالیسم دیگر برای تجزیه و تحلیل، هزینه اضافی ترجمه را به دنبال دارد که ممکن است به طور کامل امکان پذیر و کاملا به طور خودکار نباشد. با این حال، این روش تحول دسترسی به ابزارهاي تجزیه و تحلیل کامل را فراهم می کند، مانند ابزارهاي بر مبناي Alloy [48]. استفاده از تغییرات مدل در مطالعات اوليه MBSE4CPS بسیار محدود بود و می تواند بیشترین مزايا را به دنبال داشته باشد. با این وجود، تبديلات مدل می تواند به عنوان قلب و روح توسعه نرم افزار مبتنی بر مدل (model-driven) به طور کلی در نظر گرفته شود [74]. تبديلات مدل به طور گسترده ای مورد استفاده قرار می گیرد، به عنوان مثال، برای فعال کردن تجزیه و تحلیل خودکار از آنچه در حال حاضر در چند مطالعه اولیه MBSE4CPS استفاده می شود. بر اساس یافته های ما، ما معتقدیم که ادبیات MBSE4CPS فعلی از لحاظ ارائه تجزیه و تحلیل رسمی (formal) خودکار در مرحله تأیید به حد کافي رشد و پيشرفت نداشته است. این محدودیت همچنین می تواند از لحاظ پشتیبانی ابزار بسیار محدود در این مرحله توسط مطالعات اولیه MBSE4CPS موجود مطرح شود. همانطور که در نتایج این تحقیق بحث شده است، در میان چندین مطالعه اولیه که پیشنهاد پشتیبانی ابزارها را می دهند، بسیار معمول است که ابزارهاي مدل سازی مبتنی بر UML با ابزارهاي تجزيه و تحليل (analysis)/ تصديق (verification) (رسمي (formal)) ترکيب شده است. ترکيب ابزارهاي مدل سازي مبتني بر DSL (DSL-based) با ابزارهاي تجزيه و تحليل (analysis) حتي در ميان برخي از مطالعات اوليه MBSE4CPS با پشتيباني ابزار بسيار نادر است.

### کار محدود (Limited work) در مراحل بعدي SDL

از آنجا که محدوده تحقیقات امنیتی در CPS ها هنوز خيلي پيشرفت نکرده، بیشتر مطالعات اولیه به تجزیه و تحلیل در مراحل اولیه SDL (یعنی نیاز، طراحی) همانطور که در بخش 5.2 مورد بحث قرار گرفت متمرکز شده اند. ما معتقدیم همچنانکه رشته تکامل مي يابد، انتظار می رود پشتیبانی بیشتری از مهندسی امنیت در مراحل بعدی SDL مانند پياده سازي، تأیید (مثلا تست امنیت مبتنی بر مدل، تأیید رسمی (formal) مبتنی بر مدل)، انتشار (release) و پاسخ (response) ارائه شود. مرحله تأیید (verification stage) برای بازبيني کردن امنیت CPS ها بسیار مهم است. در پاسخ ما به RQ2.5، اشاره کردیم که فقط چند مطالعه اولیه، تأیید رسمی (formal verification) را ارائه دادند، و هیچ مطالعه اولیه اي، رهيافت تست امنیت مبتنی بر مدل (MBST) را برای CPS ها ارائه نداد. MBST یک مسیر بالقوه برای شرکت در اعتبارسنجي امنیت CPS ها خواهد بود.

### کار محدود در مطالعات اعتبارسنجي و ارزيابي

همانطور که در بخش 5.2 توضیح داده شد، ما نتوانستيم هیچ مطالعه اولیه ای از انواع، نظر (opinion)، ارزيابي (evaluation) يا گزارش تجربي (experience report) پیدا کنیم. بسیاری از مطالعات MBSE4CPS اولیه از نوع پیشنهاد راه حل (solution proposals) هستند در حالی که فقط یک مقاله از نوع تحقیق اعتبار سنجی (validation research) است، اما بیشتر مقالات برای مهندسی نیازمندي هاي MBSE4CPS [78] است. یک بار دیگر، اين به طور وضوح بيانگر عدم توسعه رشته MBSE4CPS است.

### همکاری محدود با صنعت

همانطور که در بخش های 5.1 و 5.2 نشان داده شد، بیشتر مطالعات اولیه MBSE4CPS درحوزه مطالعات موردی دانشگاهی مورد ارزیابی قرار گرفت، در حالی که تعداد بسیار کمی از مطالعات اولیه (حدود 10٪) بر اساس مطالعات موردی واقعی صنعتی بود. با توجه به گرايش CPS ها به سمت و سويي که باصطلاح انقلاب صنعتي چهارم ناميده مي شود، ارزيابي ها در مورد مطالعات صنعتي واقعي بايد به صورت جدي مورد نياز باشد. علاوه بر این، بيشتر نویسندگان مطالعات اولیه تنها قشر دانشگاهی هستند، که دلالت بر عدم همکاری هاي پژوهشي MBSE4CPS بین دانشگاه و صنعت است. بنابراین، بايد همکاری هاي بیشتر بين دانشگاه و صنعت برای پژوهش هاي MBSE4CPS ارتقا یابد.

### نياز به رسيدگي به عدم اطمينان

عدم اطمینان در CPS ها به دلیل پیچیدگی CPS ها و ماهیت چند رشته ای است، به عنوان مثال، در ترکيب فن آوری های مختلف در محاسبات (computing)، شبکه (networking) و کنترل برای نظارت و کنترل، نه تنها کنترل اطلاعات بلکه کنترل فرآیندهای فیزیکی [32] ذاتی است. علاوه بر این، مسائل امنیتی در زمينه CPS ها می تواند یکی از عوامل شرکت کننده کلیدی برای معرفی عدم قطعیت در CPS ها باشد که ممکن است منجر به عملیات غیرقابل اعتماد (unreliable) یا حتی ناامن (unsafe) شود. تعامل محکم (tight) بین بخش هاي (part) سایبري و فیزیکی CPS ها و همچنین وابستگی شدید به شبکه هاي ارتباطي (Communication network) (شبکه باز) باعث ايجاد CPS ها مي شود، مخصوصا فرآیندهای فیزیکی آن، آسیب پذیر ترين آسيب پذيري هاي امنيتي در بخش سایبري است [84]. از سوی دیگر، محدودیتهای امنیتی نامناسب (مثلا کنترل دسترسی) ممکن است باعث عدم موفقيت (fail) برخی از فرایندهای فیزیکی را که نيازمند يک زمان واقعی بحرانی (critical real-time) هستند شود. عدم اطمینان به طور کلی در زمينه CPS ها مورد بررسي قرار نگرفته است و در نتیجه، عدم اطمینان به علت مسائل مربوط به امنیت به هیچ وجه مورد مطالعه قرار نگرفته است که توسط SMS ما نشان داده شده است. جامعه تحقیقاتی MBSE4CPS باید تلاش بیشتری برای مقابله با مشکلات عدم اطمينان/ عدم قطعيت برای CPS ها بخصوص برای امنیت این سیستم های مهم انجام دهد.

### مدل سازی و چالش های یکپارچه سازی

در حال حاظر استفاده حدود نيمي از مطالعات اوليه MBSE4CPS از نشانه گذاري هاي مدل سازي غير UML (nonUML) تمايل استفاده از زبان هاي خاص دامنه را در مهندسي (امنيت) CPS ها نشان مي دهد. مدل سازی یک CPS خود به دلیل ماهیت چند رشته ای آن که نیاز به تخصص در نرم افزار، سخت افزار و پدیده های فیزیکی دارد، چالش برانگیز است. (DSL های مبتنی بر غیر مبتنی بر UML) ارزش دارند که در مطالعات MBSE4CPS مورد بررسی قرار گیرند زیرا هر DSL معمولا سبک وزن (lightweight) است (در مقایسه با زبان های مدل سازی عمومی) و برای مهندسی يک دامنه مشکل خاص در نرم افزار یا سخت افزار یا امنیت CPS ها طراحی شده است. بعلاوه، توسعه پروفایل های UML به عنوان DSL ها همچنين براي رویکردهایی که بر مبناي نشانه گذاري مدل سازی UML است همانطور که در [57] مورد بررسی قرار گرفته امکان پذير است. در واقع، برخی از مطالعات اولیه MBSE4CPS (به عنوان مثال، [3،40]) توسعه زبانهای مدل سازی سیستم مبتنی بر UML مانند SysML و MARTE را پيشنهاد کرده اند.

يکي ديگر از چالش هاي جدي ترکيب کلاس هاي مختلف DSL ها (براي تعيين جنبه هاي امنيتي) با تحليل امنيت (همانطور که در [20] اشاره شده) است. تبديلات مدل می تواند فاصله بين کلاس هاي مختلف DSL و تحليل امنيت را از بين ببرد، اما باید در این زمینه بررسي هاي بيشتري صورت گيرد. ترکیب مدل سازی (modelling) و تجزیه و تحلیل نگرانی های امنیتی در CPS ها حتی چالشي تر است. در اغلب موارد نگرانی های امنیتی نگرانی های متقابل هستند که چالش های مدل سازی اضافی را ایجاد می کنند. در اغلب موارد نگرانی های امنیتی نگرانی های متقابل (crosscutting concerns) هستند که چالش های مدل سازی اضافی را ایجاد می کنند. يک نمونه مدل سازي اميدوار کننده (promising modelling paradigm) براي حل اين چالش AOM است. تا کنون تنها یک مطالعه اولیه MBSE4CPS [86] برای استفاده از AOM پیشنهاد شده است و این مسير واقعا جاي کار دارد.

# تهديدات اعتبار (Threats to validity)

ضروري است به طور صريح محدوديت هاي SLR را در در کنار ارائه نتايج آن ضروري بدانيم [19]. حتی اگر یک SMS تجزیه و تحلیلي عمیق تر از SLR داشته باشد، هنوز برخی از تهدیدات اعتبار مطالعه ما به شرح زیر است.

# کارهاي مرتبط

امنیت CPS ها در واقع یک موضوع داغ است. تقریبا در همان زمان با مطالعه ما، یکی دیگر از مطالعه هاي اخير تحت فريم ورک SMS در مورد امنیت CPS ها در [44] گزارش شده است. نویسندگان [44] همچنین دستورالعمل های معمول پذیرفته شده در [66] و [37] را برای انجام SMS خود استفاده کردند. تفاوت اساسی بین مطالعه ما و [44] در دامنه مورد بررسي است. همانطور که در [44] گزارش شده، دامنه SMS آنها امنیت به طور عمومی در CPS ها است. مطالعه ما در این مقاله گزارش شده است، به صورت تخصصي متمرکز بر روش های MBSE برای CPS ها است. بسیار جالب است، اما جای تعجب نیست، [44] و مطالعه ما برخی از یافته های کلیدی را به اشتراک می گذارد. هر دو تحقیق گزارش مشابهی را در مورد افزایش شدید علاقه علمی اخیر به امنیت عمومی CPS ها ([44]) و بخصوص MBSE4CPS (این مطالعه) گزارش کرده اند. علاوه بر این، برتري شبکه های برق با نگرانی های امنیتی آن به عنوان محبوب ترین حوزه کاربرد CPS در نتایج مطالعه ما و همچنین در [44] مورد تاييد قرار گرفته است است. در مطالعه ما، مطالعات MBSE4CPS اولیه از دیدگاه حوزه های مختلف (MBE، مهندسی امنیت و CPS) و از زوایای مختلف مانند مراحل مهندسی (SDL)، مشارکت های پژوهشی (به عنوان مثال، روش- method، ابزار- tool، متریک- metric) و انواع تحقیق (به عنوان مثال، پیشنهاد راه حل- solution proposal ، تحقیق اعتبار سنجی- validation research) مورد بررسي قرار مي گيرد. مطالعه ما و [44] جنبه های طبقه بندی مشابهی را در محدوده امنیت به اشتراک می گذارند. با این حال، مطالعه ما بیشتر به صورت تخصصي در حوزه MBE است. در حالی که، [44] تحلیلی عمیق تر از حوزه CPS نظیر جنبه های کنترل کننده (controller) و ارتباطات (communication) ارائه می کند.

[56] و [57]، توسعه model-driven سیستم های امن در حالت کلي است، و به طور خاص برای CPS ها، به طور گسترده مورد بازبینی قرار نگرفته است. تمرکز بر توسعه model-driven بود نه در يک محدوده وسيع تر به عنوان مهندسي model-based. به عبارت دیگر، این مطالعات رهيافت هاي امنيت Model-Driven طبقه بندي شده به عنوان توسعه Model-Driven را در [11] که مدل ها در آن فرآيند توسعه را "هدايت (drive)" مي کند بررسي کرده است. اين مطالعه SMS رهيافت هاي MBSE (خاص CPS ها) طبقه بندي شده به عنوان MBE در [11] را بررسي کرده است، که در آن مدل ها مي تواند در هر مرحله اي به طور واحد در چرخه عمر توسعه (development life cycle) مهندسي شده، و الزام به هدايت کل فرآيند توسعه نيست. یک مطالعه اولیه وجود دارد (به عنوان مثال [20]) که در میان این SMS مشترک است [56] و [57].

تکنیک های مبتنی بر مدل (Model-based) برای مهندسی سیستم ها (SoS) در [59] مورد بررسی قرار گرفته است. به طور خاص، نویسندگان روشهای مبتنی بر مدل را برای توصیف، شبیه سازی، آزمایش و تأیید SoS مورد بررسی قرار دادند. تمرکز [59] SOS بود که دامنه وسیعتری نسبت به CPS ها دارد. تعدادي از CPS ها مي تواند در زيرمجموعه SoS ها قرار گيرد. علاوه بر این، [59] به طور خاص امنیت SoS ها را مورد بررسي قرار نمي دهد. علاوه بر این، مقالات مورد بررسی در [59] تنها بر اساس آگاهی شخصی نویسندگان، نه از طریق یک جستجوي سيستماتيک و فرآيند انتخاب، همانند SMS ما انتخاب شده است. هیچ مطالعه اولیه MBSE4CPS در [59] مورد بررسی قرار نگرفته است.

در [96]، نویسندگان وضعیت هنر (state of the art) و وضعیت عمل (state of the practice) در تأیید و اعتبارسنجي CPS ها را ارزیابی کردند. روش تحقیق آنها دوگانه است: بررسی آثار مهم و برجسته ي تأیید و اعتبارسنجي CPS ها؛ و یک بررسي (survey) ساخت یافته on-line به علاوه مصاحبه هاي (interview) نیمه ساخت یافته. MBE برای تأیید و اعتبارسنجي CPS ها یکی از گروه ها در بخش بررسی آثار مهم و برجسته است. مطالعه آنها در مورد امنیت CPS ها نیست. همچنین هیچ مطالعه اولیه MBSE4CPS در [96] مورد بحث قرار نگرفته است.

رهيافت هاي تست کردن (testing approaches) خاص CPS ها، اخیرا در [4] مورد بررسی قرار گرفته است. چند رهيافت آزمون مبتنی بر مدل (model-base) برای CPS ها مورد بررسي قرار گرفته است. اگرچه، هیچ یک از روش های تست در بررسي خود امنیت سیستم های CPS را بررسي نکرده است.

# نتيجه گيري و کارهاي آينده

## نتيجه گيري ها

در اين مقاله نتايج، يک مطالعه نگاشت سيستماتک (systematic mapping study) روي مطالعات مهندسي امنيت مبتني بر مدل (model-based) براي سيستم هاي فيزيکي سايبري (MBSE4CPS) ارائه شده است. اين نتايج مي تواند باعث وضوح زمينه هاي تحقيقاتي، بين رشته اي ميان حوزه هاي پژوهشي در حال پيدايش مثل مهندسي سيستم، مهندسي نرم افزار و مهندسي امنيت شود. به طور خاص، مطالعه ما بر اساس یک پروتکل دقیق اس ام اس برای شناسایی مجموعه ای از مطالعات اولیه MBSE4CPS طراحی شده و بر اساس سه سوال عمومی تحقیق و سوالات متداول مربوطه مطرح شده است. سهم اصلي اين مقاله پاسخ به اين سوالات و سوالات مشتق شده است، که به صورت زير خلاصه مي شود:

*RQ1. آمار نشر مطالعات اولیه در حوزه MBSE4CPS چگونه است؟*

(در جواب به RQ1.1) اولین مطالعه اولیه MBSE4CPS در سال 2007 منتشر شده است. به طور متوسط، از سال 2007 تا 2016، حدود پنج مطالعات اولیه سالانه منتشر شده است. تعداد مطالعات اولیه MBSE4CPS طی سه سال اخير (2014-2016) به میزان قابل توجهی افزایش یافته است (بیش از یازده تا به طور ميانگين)، که به اين معني است که این حوزه تحقیقاتی در حال گسترش است. (RQ1.2) از لحاظ محل نشر، بيشتر مطالعات اوليه MBSE4CPS در کنفرانس ها نسبت به ژورنال ها (journal) يا کارگاه هاي آموزشي (workshop) منتشر شده است. (RQ1.3) اغلب نويسندگان مطالعات اوليه MBSE4CPS فقط قشر دانشگاهي است. مشارکت صنعت در مطالعات اوليه خيلي کمي مشاهده مي شود. (RQ1.4) تا کنون محققان ایالات متحده آمریکا و به دنبال آن محققان مستقر در فرانسه، سنگاپور، اتریش، کانادا و عمدتا کشورهاي اروپايي ديگر بيشترين مطالعات اولیه MBSE4CPS را ارائه کرده اند. کشورهای پیشرو در رابطه با تعداد مطالعات اولیه MBSE4CPS مانند ایالات متحده آمریکا و کشورهای اتحادیه اروپا به تحقیقات بر روی CPS هایی که در این کشورها ارتقا یافته اند، کاملا مرتبط هستند.

*RQ2. مطالعات اولیه MBSE4CPS موجود و ویژگی های آنها چیست؟*

(RQ2.1) بیشتر مطالعات اولیه به چندین نگرانی امنیتی کلیدی اشاره کرده است. با این حال، تقریبا نیمی از مطالعات اولیه در بررسي هاي خود به صراحت نگرانی های امنیتی خاص خود را که مورد توجه قرار گرفته است را بيان نکردند، بلکه به طور ضمنی. (RQ2.2) در واقع، بيشتر مطالعات اوليه متمرکز شده روي تحليل امنيت (security analysis) در حالت کلي بر مبناي تهديدهاي امنيتي، حملات يا آسيب پذيري ها است. فقط حدود یک دهم (13٪) از مطالعات اولیه صرفا راه حل های امنیتی (security solution) و یک دهم پیشنهادات امنیتی را همراه با تجزیه و تحلیل تهدید / حمله / آسیب پذیری ارائه کرده است. (RQ2.3) استفاده از زبانهای دامنه خاص (DSLs) در مطالعات اولیه MBSE4CPS با استفاده از UML استاندارد قابل مقایسه است. استفاده از مدل های ساختاری یا رفتاری برای تعیین تهدید / حمله یا آسیب پذیری امنیتی، کمی کمتر از استفاده از انواع دیگر مدل ها (به عنوان مثال ایجاد شده در DSL ها) برای این منظور است. تعداد مدل های مورد استفاده برای تعیین راه حل های امنیتی (security solution) بسیار کمتر از تعداد مدل ها برای تعیین تهدیدات / حملات و آسیب پذیری ها است. تبديلات مدل به مدل (Model-to-model transformations (MMTs)) در تعداد بسيار کمي از مطالعات اوليه MBSE4CPS استفاده شده است. تعداد کمي از اطلاعات پياده سازي MMT ها ارائه شده است. (RQ2.4) به عنوان يک گرايش يا زمينه نوظهور پژوهش هاي MBSE4CPS تاکنون روي مراحل اوليه چرخه عمر توسعه امنيت (security development lifecycle- SDL) مانند مهندسي نيازمندي ها و تجزيه و تحليل (analysis) متمرکز بوده اند. تمام مطالعات اوليه MBSE4CPS روي تجزيه و تحليل دامنه/ نيازمندي ها يا معماري/ طراحي يا هر دو مرحله انجام شده است. تقریبا نیمی از مطالعات اولیه صرفا بر روی مرحله ي نيازمندي ها متمرکز شده است. خيلي کم رهيافت هاي توسعه امنيت کامل تري از تجزيه و تحليل دامنه/ نيازمندي ها به معماري/ طراحي، و سپس به مراحل بعدي ارائه شده است. از نظر پشتيباني از ابزار (tool)، کمتر از يک سوم (23%) مطالعات اوليه MBSE4CPS از ابزارها پشتيباني کرده اند. (RQ2.5) روش (method) (به عنوان مثال، یک روش تجزیه و تحلیل امنیت)، نوع اصلی مشارکت پژوهش (research contribution) در تمام مطالعات MBSE4CPS اولیه است. در میان مطالعات اولیه، اغلب تنها روش (method) ارائه شده است. روش هاي کمي همراه با پشتيباني ابزار، يا معيارها (metric) معرفي شده است. کمتر روش ها (method)، ابزار (tool) و معيارها (metric) در همان مطالعه معرفي شده است. بيشتر مطالعات اوليه از نوع ارائه راه حل (solution proposal) است، در حالي که فقط يک مورد از نوع تحقيق اعتبارسنجي (validation research) است. حدود یک دهم مطالعات اولیه تنها از نوع ارائه مفهومی (conceptual proposal) است و هیچ يک از انواع مطالعات نظرات (opinions)، ارزیابی (evaluation) یا گزارش تجربه ای پيدا نشد. روش های بسیار کمی از مراحل بعد SDL مانند پياده سازي، تایید و انتشار پشتیبانی می کنند. (RQ2.6) تقریبا نیمی از مطالعات MBSE4CPS اولیه از شبکه های هوشمند انرژی (smart energy grid) به عنوان مطالعه موردی یا دامنه های کاربرد استفاده کرده اند. دامنه هاي کاربردي ديگر مطالعات اوليه MBSE4CPS شامل تقريبا يک سوم براي هر کدام از جمله CPS هاي خودرو (automotive CPS)، مراقبت هاي بهداشتي (healthcare) و حمل و نقل (transportation) به شمار مي آيد. بسیاری از مطالعات اولیه MBSE4CPS فقط مطالعات موردی دانشگاهي ارزيابي شده است، در حالی که تعداد بسیار کمی از مطالعات اولیه مطالعات موردی صنعتی بوده است. (RQ2.7) ما در نظر داشتیم تا جنبه عدم اطمينان را در CPS ها بررسي کنيم اما هيچ مطالعه اي که جنبه عدم اطمينان را در CPS ها بررسي کرده باشد پيدا نکرديم.

*RQ3. مسائل باز پژوهش هاي MBSE4CPS چيست؟*

اولا، کمی بیش از نیمی از مطالعات اولیه MBSE4CPS در مطالعات خود به صراحت بیان نکرده اند که کدام نگرانی های امنیتی خاص (مثلا CIA) مورد ارزيابي قرار گرفته است. یک راه برای رسیدن به این هدف، ایجاد یک مدل مفهومی است که می تواند هر دو جنبه را با هم پوشش (cover) دهد. دوم، بیشتر مطالعات اولیه بر پشتيباني کردن از تحلیل های امنیتی بر اساس تهدیدات امنیتی، حملات یا آسیب پذیری ها تمرکز کرده و بر راه حل های امنیتی مهندسی متمرکز نشده اند. بيشتر مطالعات MBSE4CPS بايد با راه حل هاي امنيتي در مراحل بعدي SDL مثل پياده سازي (implementation) و تاييد (verification) پيشنهاد شود. سوم، هیچ مطالعه اولیه MBSE4CPS که تجزيه و تحليل ها را به صورت مستقيم در مدل های امنیتی/ سیستم در مرحله تایید (verification) پشتيباني کند وجود ندارد. مقالات برتر MBSE4CPS در حال حاظر از لحاظ ارائه تجزیه و تحلیل هاي رسمی(formal) خودکار در مرحله تأیید (verification) به طور کامل توسعه نيافته است. این محدودیت همچنین می تواند از لحاظ پشتيباني ابزار خيلي محدود که توسط مطالعات اولیه MBSE4CPS ارائه شده است، دیده شود. چهارم، ما همچنین دریافتیم که همکاری میان دانشگاه و صنعت و همچنین دخالت صنعت در زمینه تحقیق تا کنون بسیار محدود بوده است. علاوه بر اين، عدم توجه به عدم اطمينان (uncertainty) ارزش توجه دارد زيرا عدم اطمينان مي تواند در CPS هاي دنياي واقعي اجتناب ناپذير باشد و امنيت شان را پيچيده مي کند. پنجم، مدل سازی CPS ها به دلیل ماهیت چند رشته ای آن چالش برانگیز است. DSL ها مي تواند يک بخش کليدي در مهندسي CPS ها با توجه به ماهيت چند رشته اي شان باشد. اگرچه، یک چالش باز یکپارچه سازی DSL های مختلف است، به عنوان مثال، استفاده از تبديلات مدل براي حداکثر مزايا.

## کارهاي آينده

پروتکل SMS ما و مجموعه مطالعات اوليه MBSE4CPS می تواند در یک SMS پیگیری شود که گزارش کند بیشتر نتایج به روز (up-to-date) را بر اساس مطالعات اولیه MBSE4CPS گزارش شده در این مقاله به همراه مقالات اولیه MBSE4CPS کشف شده در آینده را گزارش کند. کيفيت مجموعه مقالات اولیه MBSE4CPS می تواند به سه روش افزايش يابد و به روز رساني شود. اول، مطالعات MBSE4CPS جديد مي تواند از جستجوهاي پايگاه هاي جديد که بازه بعد از اين SMS را پوشش مي دهد، به عنوان مثال، از اکتبر 2016 به بعد. دوم ما انتظار مطالعات MBSE4CPS بيشتري را در آينده، همچنين مکان هاي اختصاصي يا انتشارات اختصاصي براي انتشار مقالات MBSE4CPS را داريم. اگر فرآهم شود، می توان یک جستجوی دستی در این مکان ها را برای پیدا کردن مطالعات اولیه MBSE4CPS انجام داد. سوم، يکي مي تواند snowballing ديگري را به طور بازگشتي انجام دهد، مخصوصا snowballing پيشرو (forward snowballing) (بوسيله بررسي کردن نقل قول ها(citations))، بر روي مجموعه مطالعات اوليه MBSE4CPS شامل موارد تازه پيدا شده. بعد از اينکه مجموعه ای از مطالعات MBSE4CPS اولیه به روز شد، پروتکل ما می تواند دوباره برای استخراج ، ترکیب داده ها و گزارش نتایج به روز شده دوباره استفاده و اتخاذ شود.

از سوی دیگر، ما طرح انجام یک مرور سيستماتيک را به صورت عميق تر نسبت به رهيافت هاي ارزيابي (validation) و تاييد (verification) امنيت مبتني بر مدل براي CPS ها (MBSVV4CPS) با پيگيري از اين SMS داريم. مجموعه مقالات اولیه MBSE4CPS را می توان به صورت زیر بررسی کرد و تمام مطالعات MBSVV4CPS (زیر مجموعه ای از MBSE4CPS) می تواند فيلتر شده و با جزئيات بررسي شود. علاوه بر اين، به دليل اينکه جنبه هاي عدم اطمينان CPS ها هنوز حل نشه است، ما يک رهيافت تست امنيت model-base را براي CPS هايي که در يک وضعيت عدم اطمينان قرار دارند را توسعه مي دهيم.

**ضميمه A:**

جدول A.1 همه مطالعات اوليه اي را که

مراجع:

1. R.R. Rajkumar, I. Lee, L. Sha, J. Stankovic, Cyber-physical systems: the next computing revolution, in: Proceedings of the 47th Design Automation Conference, ACM, pp. 731–736.
2. S. Karnouskos, Stuxnet worm impact on industrial cyber-physical system security, in: IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society, IEEE, pp. 4490–4494.
3. Forrester, Predictions 2016: Cybersecurity Swings To Prevention, Report, Forrester, 2015.
4. J. Cysneiros L.M. Sampaio do Prado Leite, Non-functional requirements: from elicitation to modelling languages, in: Proceedings of the 24th International Conference on Software Engineering, 2002. ICSE 2002, 2002, pp. 699–700.
5. J. Bézivin, Model Driven Engineering: An Emerging Technical Space, Springer, pp. 36–64.
6. B. Balaji, A. Faruque, M. Abdullah, N. Dutt, R. Gupta, Y. Agarwal, Models, abstractions, and architectures: the missing links in cyber-physical systems, in: Proceedings of the 52nd Annual Design Automation Conference, ACM, p. 82.
7. P.H. Nguyen, M.E. Kramer, J. Klein, Y. Le Traon, An extensive systematic review on the model-driven development of secure systems, Inf. Softw. Technol. 68 (2015) 62–81.
8. X. Zheng, C. Julien, M. Kim, S. Khurshid, On the state of the art in verification and validation in cyber physical systems, Technical Report TR-ARiSE-2014-001, The University of Texas at Austin, The Center for Advanced Research in Software Engineering, 2014.
9. K. Petersen, S. Vakkalanka, L. Kuzniarz, Guidelines for conducting systematicmapping studies in software engineering: an update, Inf. Softw. Technol. 64 (2015) 1–18.
10. C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, ACM, p. 38.
11. M. Zhang, B. Selic, S. Ali, T. Yue, O. Okariz, R. Norgren, Understanding uncertainty in cyber-physical systems: A conceptual model, in: 12th European Conference on Modelling Foundations and Applications (ECMFA 2016), Springer, 2016, pp. 247–264.
12. P.H. Nguyen, M.E. Kramer, J. Klein, Y. Le Traon, An extensive systematic review on the model-driven development of secure systems, Inf. Softw. Technol. 68 (2015) 62–81.
13. MIT, Alloy analyzer, <http://alloy.mit.edu>.
14. T. Weigert, F. Weil, Practical experiences in using model-driven engineeringto develop trustworthy computing systems, in: Sensor Networks, Ubiquitous, and Trustworthy Computing, in: IEEE International Conference on, vol. 1, IEEE, 2006, p. 8.
15. M. Brambilla, J. Cabot, M. Wimmer, Model-Driven Software Engineering in Practice, Morgan & Claypool Publishers, 2012.
16. C. Neureiter, D. Engel, M. Uslar, Domain specific and model based systems engineering in the smart grid as prerequesite for security by design, Electronics 5 (2) (2016) 24.
17. NSF, Cyber-physical systems (cps) program solicitation, 2016 http://www.nsf. gov/pubs/2016/nsf16549/nsf16549.html.

1. IEEE Xplore, <http://ieeexplore.ieee.org/> [↑](#footnote-ref-1)
2. ACM Digital Library, http://dl.acm.org [↑](#footnote-ref-2)
3. Scopus, http://www.scopus.com [↑](#footnote-ref-3)
4. Springer Link, http://link.springer.com [↑](#footnote-ref-4)
5. Endnote, http://endnote.com. [↑](#footnote-ref-5)
6. Mendeley, http://mendeley.com [↑](#footnote-ref-6)
7. تست سيستم هاي فيزيکي سايبري تحت شرايط نامشخص: سيستماتيک، قابل توسعه و متدولوژي هاي تست مبتني بر مدل و مبتني بر جستجو قابل تنظيم (Configurable Model-based and Search-based Testing Methodologies) (http://u-test.Eu). [↑](#footnote-ref-7)