# Hacia un conjunto estándar de ataques contra sistemas de control para la evaluación de contramedidas

Mikel Iturbe, Iñaki Garitano, Ignacio Arenaza-Nuño, Urko Zurutuza

Departamento de Electrónica e Informática
Escuela Politécnica Superior
Mondragon Unibertsitatea
Goiru 2, E-20500 Arrasate-Mondragón
Email: {miturbe,igaritano,iarenaza,uzurutuza}@mondragon.edu

***Resumen*—La generación de datos mediante simulación es una aproximación muy utilizada a la hora de evaluar propuestas de ciberseguridad de los sistemas de control, particularmente los sistemas de detección de intrusiones (SDIs). En este sentido, el proceso Tennessee-Eastman (TE) juega una función relevante, convirtiendose en un estándar. Sin embargo, aún utilizando el mismo proceso, la falta de un conjunto de ataques estandarizado dificulta la evaluación entre diferentes propuestas. Por ello, en este trabajo presentamos cinco ataques sobre el proceso TE con los objetivos de *(i)* dañar el equipamiento y *(ii)* causar pérdidas económicas. Estos ataques cumplen sus objetivos y pueden servir como medida de evaluación de diferentes propuestas, además de servir de base para el desarrollo futuro de ataques más sofisticados.**

***Index Terms*—sistemas de control, tennessee-eastman, ataques**

**Tipo de contribución:** *Investigación en desarrollo*

## I. Introducción

Los conjuntos de datos para la evaluación de sistemas de detección de intrusiones (SDIs), tales como los conocidos KDD99Cup [1] o VAST2012 [2], siguen siendo un recurso muy utilizado a la hora de evaluar diferentes propuestas con un mismo criterio. Sin embargo, dadas las particularidades de las redes industriales, estos conjuntos de datos no son extensibles para la evaluación de mecanismos de seguridad en este tipo de redes. Frente a esta carencia, la comunidad científica ha optado mayoritariamente por la generación de datos *ad hoc* para la evaluación las propuestas [3].

Así, el célebre proceso Tennessee-Eastman (TE), presentado por Downs y Vogel [4] se ha convertido en un estándar *de facto* para la investigación en cibereseguridad que atañe a procesos industriales. Aunque el proceso TE es un proceso químico inicialmente diseñado para la evaluación de diferentes algoritmos de control, su uso se ha extendido a diversos campos de la ciberseguridad, como la detección de anomalías [5], [6] o el análisis de riesgos [7]. Esto se debe principalmente a su naturaleza real y la existencia de una versión de código abierto, DVCP-TE [1], específicamente diseñada para la experimentación en este campo.

Sin embargo, a la hora de evaluar propuestas de detección de anomalías, los autores han evaluado sus propuestas con diferentes implementaciones de ataques. La diversa naturaleza de los ataques posibilita que algunos tipos de ataques, más evidentes, sean más detectables frente a los diseñados con el objetivo de pasar desapercibidos. Por ello, la utilización de ataques y escenarios propios dificulta la comparación de resultados entre diferentes propuestas, ya que contemplan casos de uso diferentes. Para facilitar esta comparación, en este trabajo presentamos una aproximación preliminar sobre ataques al proceso TE, como parte del objetivo de construir un marco estándar para evaluar diferentes propuestas.

[1] https://github.com/satejnik/DVCP-TE

## II. Ataques contra el proceso TE

El proceso TE tiene en total 41 variables medibles (XMEAS) que corresponden a las lecturas de sensores del proceso simulado, y 12 señales de salida (XMV), que corresponden a los actuadores. Para una descripción completa del proceso, sus reacciones, variables medidas y actuadores, pueden referirse a la publicación original [4]. El modelo DVCP-TE tiene implementados varios ataques sobre estas señales de entrada y salida, en las que el atacante tiene capacidad de comprometer las comunicaciones entre los controladores y los dispositivos de campo (actuadores y sensores).

Krotofil y Cárdenas [8] analizaron la resiliencia del proceso ante diferentes ataques y aunque no propusieron un conjunto de ataques, sí que definieron dos grandes tipos de ataques con los objetivos de (i) dañar físicamene el equipamiento del proceso y (ii) causar perjuicio económico, bien mediante un aumento de los costes de operación, o rebajando la pureza –y por tanto, el precio– del producto final.

Estudiando el proceso, identificamos una serie de variables que pueden afectar tanto a la operación segura de la planta, como aquellas en las que su manipulación conlleva un mayor coste de operación. Mientras que estudios previos se han centrado en los sensores [8], analizamos también las válvulas.

A continuación presentamos un listado de cinco variables cuya manipulación puede tener consecuencias en la operación normal del proceso.

- XMV(6) es la válvula que controla el flujo de la purga. Si se abre más de lo debido, se desecharán más componentes químicos, y por lo tanto aumentará el coste de operación. Sin embargo, si se abriese demasiado,

la presión del reactor sería demasiado baja para seguir operando.

- XMV(9) es la válvula de entrada del flujo del vapor que se utiliza en la columna de fraccionamiento. El vapor tiene un coste asociado, por lo que si se aumenta su uso, también lo hacen los costes.
- XMV(10) es la válvula que controla la entrada del agua de refrigeración al reactor. Como tal, es la variable más crítica de todo el proceso ya que es la forma de regular las altas temperaturas que se alcanzan en el reactor. Si se cierra la válvula, la presión del reactor aumentaría peligrosamente, pudiendo llegar a estallar.
- XMEAS(7) es el sensor de presión del reactor. Como en el caso de XMV(10), una lectura errónea podría ocasionar una presión demasiado elevada en el reactor.
- XMEAS(10) es el sensor del flujo de purga. De forma similar a XMV(6), una lectura errónea podría ocasionar pérdidas económicas.

## III. Resultados preliminares

Esta sección presenta los resultados de la realización de ataques de integridad sobre las variables mencionadas anteriormente, en los que el atacante reemplaza el valor original de una variable por un valor arbitrario antes de la llegada a su destino. Las tablas I y II muestran estos resultados, que han sido obtenidos utilizando DVCP-TE.

Tabla I
Ataques con el objetivo de dañar el equipamiento

| Variable atacada | Valor de reemplazo | Tiempo a parada |
|---|---|---|
| XMV(10) | 0 | 2m 24s |
| XMEAS(7) | 0 | 8h 19m |

La tabla I contiene los resultados correspondientes a los ataques contra el equipamiento del proceso. En este tipo de ataques, el objetivo del atacante es dañar los componentes físicos que posibilitan el proceso. En el caso del proceso TE, el reactor es el componente más crítico y como tal, puede ser considerado el objetivo principal de los atacantes que quieran dañar equipamiento.

En DVCP-TE no es posible evaluar los daños físicos directamente, pero sí es posible comprobar si el proceso ha excedido los límites para su operación segura. Por lo tanto, se puede definir una métrica que corresponde al tiempo que transcurre desde el inicio del ataque hasta la parada del proceso debido a que alcanza estos límites. En tiempos menores, el efecto sería más pronunciado y por lo tanto, habría mayor probabilidad para dañar el equipamiento si no existiesen mecanismos de seguridad adicionales.

Como muestra la tabla I, el ataque a XMV(10), que cierra la válvula de refrigeración, es la más efectiva, ya que consigue aumentar la presión del reactor hasta límites peligrosos en poco menos de dos minutos y medio.

La tabla II muestra los resultados correspondientes a los ataques con impacto económico. En este caso, el objetivo del atacante es limitar la competitividad de la planta aumentando sus costes operativos, sin tratar de parar la producción. DVCP-TE calcula los gastos de operación en tiempo real que, bajo condiciones normales, es, de media, de 113,98 $/h. Esta vez, utilizamos el sobrecoste medio como métrica de la efectividad del ataque. Los resultados muestran que los ataques correspondientes a los actuadores tienen entre 3,8 % y 5,8 % de sobrecoste al comparar con los costes operativos normales. Sin embargo, es cuando se manipula la señal del sensor de purga, XMEAS(10), cuando se producen los mayores efectos, con casi un 100 % de aumento en los gastos operativos.

Tabla II
Ataques con impacto económico

| Variable atacada | Valor de reemplazo | Sobrecoste medio ($/h) |
|---|---|---|
| XMV(9) | 100 | 4,36 |
| XMV(6) | 28 | 5,97 |
| XMEAS(10) | 0 | 112,84 |

## IV. Conclusiones y Líneas Futuras

Hemos evaluado la efectividad de cinco ataques sobre el proceso TE con dos objetivos: causar daños físicos en el proceso y aumentar los gastos de producción. Los ataques presentados cumplen el fin para el que fueron diseñados y pueden servir para evaluar propuestas de detección de intrusiones. Sin embargo, es necesario seguir trabajando para desarrollar un mayor número de ataques sofisticados. En el caso de los procesos químicos, son especialmente interesantes aquellos ataques camuflados que causen una calidad menor del producto. Para otros dominios, la publicación de otros modelos de procesos puede llevar a implementar ataques sobre otros casos de uso.

## Agradecimientos

Este trabajo ha sido desarrollado por el grupo de Sistemas Inteligentes para Sistemas Industriales, financiado por el Departamento de Educación, Política Lingüística y Cultura del Gobierno Vasco.

## Referencias

[1] "Kdd-cup99," disponible en: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[2] K. Cook, G. Grinstein, M. Whiting, M. Cooper, P. Havig, K. Liggett, B. Nebesh, and C. L. Paul, "VAST challenge 2012: Visual analytics for big data," in *Visual Analytics Science and Technology (VAST), 2012 IEEE Conference on*. IEEE, 2012, pp. 251–255.

[3] B. Genge, I. Kiss, P. Haller, and C. Siaterlis, "Generating high quality data for the protection of modern critical infrastructures," in *Digital Forensic and Security (ISDFS), 2016 4th International Symposium on*. IEEE, 2016, pp. 53–58.

[4] J. J. Downs and E. F. Vogel, "A plant-wide industrial process control problem," *Computers & Chemical Engineering*, vol. 17, no. 3, pp. 245–255, 1993.

[5] M. Krotofil, J. Larson, and D. Gollmann, "The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '15. ACM, 2015, pp. 133–144.

[6] M. Iturbe, J. Camacho, I. Garitano, U. Zurutuza, and R. Uribeetxeberria, "On the feasibility of distinguishing between process disturbances and intrusions in process control systems using multivariate statistical process control," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*. Toulouse, France: IEEE, Jun. 2016, pp. 155–160.

[7] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the 6th ACM symposium on information, computer and communications security*. ACM, 2011, pp. 355–366.

[8] M. Krotofil and A. A. Cárdenas, "Resilience of process control systems to cyber-physical attacks," in *Nordic Conference on Secure IT Systems*. Springer, 2013, pp. 166–182.