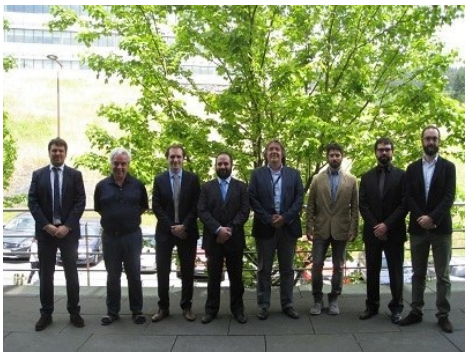
Escuela Politécnica Superior

Noticias

Lecturas de la tesis de Mikel Iturbe



24/05/2017

Presidente*:* Dr. D. Fco. Javier López Muñoz (Universidad de Málaga)

Vocal: Dr. D. José Camacho Páez (Universidad de Granada)

Vocal: Dr. D. Josu Bilbao (IKERLAN)

Vocal: Dr. D. Jorge Ricardo Cuéllar Jaramillo (Siemens AG)

Secretario: Dr. D. Iñaki Garitano Garitano (Mondragon Unibertsitatea)

Desde el desarrollo de los primeros Controladores Lógicos Programables (PLC) en la década de 1960, los sistemas de control industrial (SCI) han evolucionado considerablemente. Desde las instalaciones aisladas primitivas, los SCI están mas conectados entre sí, hasta formar los entornos interconectados complejos conocidos como redes industriales (RIs) de hoy en día. Los SCI son responsables de un gran número de procesos físicos, incluyendo aquellos que pertenecen a infraestructuras críticas (ICs). Por ello, la protección de este tipo de redes es vital para el bienestar de sociedades modernas. De los muchos avances en este campo, los sistemas de detección de anomalías (SDAs) tienen un rol importante. Estos sistemas monitorizan el comportamiento de las RI y/o SCI para detectar eventos anómalos, sean conocidos o desconocidos. Sin embargo, al volverse las RIs cada vez más complejas, su monitorización para el descubrimiento de se ha convertido en un problema Big Data. Dicho de otra forma, los datos creados en las INs se han convertido en demasiado complejos para ser procesados por los medios habituales, dada su gran escala, variedad y velocidad de creación. No obstante, los SDAs diseñados para tragajar en RIs no han evolucionado igualmente, y las propuestas recientes no estan diseñadas para abordar esta complejidad de los datos, ya que no escalan correctamente o no analizan la mayoría de los tipos de datos creados en RIs. Esta tesis aspira a llenar ese vacío mediante dos propuestas principales: (i) un sistema visual de monitorización de red y (ii) un SDA multivariante, capaz de trabajar a gran escala y con datos heterogéneos. Para la monitorización de flujos, proponemos un sistema que crea visualizaciones de seguridad en base al estado actualizado de la red, representando los flujos de red activos y destacando aquellos que son anómalos. Para el SDA multivariante, analizamos en primer lugar la eficacia del Control Estadístico Multivariante de Procesos (CEMP) para la detección y diagnosis de anomalías. Después, presentamos un SDA basado en CEMP capaz de trabajar en entornos Big Data, que monitoriza tanto los datos a nivel de red como a nivel de proceso para la detección de anomalías. Estas dos propuestas se validan experimentalmente, construyendo RIs en entornos de prueba y analizando los datos creados. Para responder a esta necesidad de un entorno de pruebas donde realizar investigación de forma rigurosa y reproducible, presentamos un banco de pruebas que cumple con ese propósito.