Mensajes de alarma en redes industriales basadas en Ethernet TCP /IP

Gustavo Jiménez-Placer[1], Fabiana Ferreira[2], Amado Osvaldo Vitali[1]
[1] Instituto de Industria – Universidad Nacional de General Sarmiento.
J.M. Gutierrez 1150. Los Polvorines 1613), gplacer@ungs.edu.ar
[2] Dpto. de Ciencia y Tecnología – Universidad Nacional de Quilmes.
Roque Saenz Peña, Bernal 352 (1876), fferreira@unq.edu.ar

Resumen: La utilización de redes Ethernet TCP- IP como buses de campo en las aplicaciones de control industrial se está difundiendo rápidamente. Sin embargo las Ethernet industriales disponibles en el mercado producen los mensajes de alarma de diferentes maneras. Los motivos por los que la forma de producir estos mensajes no esta estandarizada no están bien delimitados. Está pendiente el estudio de los sistemas que utilizan redes basadas en Ethernet cuando pasan al estado de alarma. El objetivo de este trabajo es realizar una propuesta preliminar para la realización de este tipo de estudios en redes industriales basadas en Ethernet.
Se presentan experimentos desarrollados sobre un banco de simulación para comparar el comportamiento de una aplicación industrial, en estado normal y en estado de alarma.

Palabras Clave. Ethernet. TCP-IP. Acceso al Medio. Mensajes de alarma.

1. Introducción

La arquitectura de los sistemas de automatización industrial ha evolucionado desde los primeros sistemas cableados a sistemas con equipos conectados a través de redes de comunicación. En los sistemas cableados las estaciones de supervisión se conectaban también punto a punto, pero el incremento en la complejidad de las aplicaciones de control industrial hizo necesario desarrollar redes LAN específicas (buses de campo o fieldbus) para conectar los dispositivos de campo, los controladores y las estaciones de supervisión en una única arquitectura. Hoy en día gran parte de las aplicaciones de control industrial incorporan algún bus de campo (además de alguna otra red de comunicación tal como Ethernet o inalámbricas) por lo que los sistemas de automatización industrial pasaron a denominarse sistemas de control en red (NCS: Network Control System) [1].

Uno de los desafíos que se plantearon en el desarrollo de las redes industriales fue el de tratar de conseguir un único protocolo que permitiera conectar entre sí equipos

de los más diversos fabricantes y características. Sin embargo, la evolución tecnológica y las características del mercado hicieron que fueran apareciendo diferentes redes o buses de campo [2], adaptados a diferentes tipos de procesos industriales y con poca o escasa interoperabilidad entre sí [3]. La situación fue tan conflictiva que se llegó a darle el nombre de "guerra de los buses"[4]. En el momento más álgido de este conflicto se pensaba que la adopción de redes basadas en Ethernet resolvería todos los problemas de heterogeneidad. Incluso hubo quienes pronosticaron que para el 2006 el mercado de control iba a ser 100% Ethernet [5]. Hoy en día, por diversos motivos [6] la utilización de estas redes en el piso de planta está muy lejos de ser masiva [7] y coexiste con los buses de campo tradicionales. Una de las explicaciones para esto es que han surgido en el mercado de automatización una diversidad de redes industriales basadas en Ethernet aunque incompatibles entre sí [8] generando confusión en los usuarios finales respecto a la confiabilidad de su utilización en entornos industriales de automatización. Estas "Ethernet Industriales" adaptan de distintas formas los protocolos tradicionales de Ethernet y TCP/IP [9].

La incorporación de Ethernet como red de comunicación industrial involucra cambios en las prestaciones de las aplicaciones, principalmente retardos en los tiempos de respuesta del sistema. La magnitud y consecuencias de estas demoras dependen del tipo de aplicación, del tipo de señales y de las características de los dispositivos utilizados.

Para lo estudios temporales de los NCS se utiliza una clasificación bien establecida de los mensajes, de acuerdo a la forma en que son enviados a la red [10] en periódicos y aperiódicos. En los sistemas de control industrial basados en Ethernet se intercambian mensajes de muy diferentes orígenes con distintos requerimientos temporales y de seguridad. En el estado de funcionamiento normal de una aplicación la mayoría de los mensajes corresponden a la ejecución de lazos de control y por ende son periódicos. Por este motivo, los trabajos que analizan la performance de alguna red en particular utilizan en las aplicaciones testigo sólo mensajes periódicos. Sigue pendiente el estudio de los sistemas que utilizan redes basadas en Ethernet cuando la aplicación industrial pasa al estado de alarma. El objetivo de este trabajo es realizar una propuesta preliminar para la realización de este tipo de estudios en redes industriales basadas en Ethernet.

Para esto se comienza por caracterizar los estados de alarma y los mensajes en este estado, comparándolos con los mensajes en otros estados. Se proponen estrategias para su tratamiento. Se analizan en general las restricciones de los protocolos Ethernet TCP/IP para su utilización industrial y se obtienen requisitos específicos para los estados de alarma. Finalmente se analizan las consecuencias que la utilización de este tipo de redes puede tener sobre el tiempo de respuesta de la aplicación en alarma.

2. Caracterización de los Mensajes y de los estados de alarma

2.1 Clasificación de mensajes

Los mensajes que se transmiten por las redes de comunicación industrial pueden clasificarse según diferentes criterios. El criterio mayormente adoptado es por la

modalidad con la que deben ser intercambiados [10]. Los mensajes suelen clasificarse en:
- Lanzados por tiempo (time-triggered): Corresponde a los mensajes periódicos o sincrónicos que son enviados a la red una vez por período.
- Lanzados por eventos (time-triggered): corresponde a los mensajes aperiódicos que son enviados sólo en el instante indicado por su tiempo de lanzamiento.

Esta clasificación no tiene en cuenta la finalidad con la que los mensajes son generados por la aplicación aunque se suelen asociar los mensajes periódicos al control de la aplicación y los aperiódicos a las alarmas.

La gran mayoría de los buses de campo existentes implementan diferentes mecanismos de comunicación para cada uno de estos tipos de mensajes, estando algunos buses mejor adaptados a algún tipo de mensajes que a otro. En general esta adecuación depende de los mecanismos de acceso al medio. Las redes con mecanismos de acceso al medio aleatorios (CSMA, tales como Ethernet) están mejor adaptadas a los mensajes aperiódicos mientras que las determinísticas (por ejemplo las que tienen arbitrador de bus, tal como Foundation Fieldbus) manejan mejor los mensajes periódicos.

Se propone, por lo tanto, una clasificación complementaria según la finalidad de los mensajes:
- Mensajes de control: corresponden a las variables sensadas en el proceso y necesarias para ejecutar los lazos de control, que deben ser enviadas y recibidas periódicamente. Un retardo en su recepción provoca demoras en la respuesta física del sistema que a su vez pueden producir una pérdida de control de la aplicación.
- Mensajes de interfase hombre máquina (HMI): corresponden al monitoreo de variables (en cuyo caso se intercambian en forma periódica) o a comandos por eventos. Si una señal de monitoreo se retrasa o incluso se pierde no hay consecuencias graves para el control de la aplicación. Las señales de comando son enviadas una sola vez. Si se retrasan no tienen efectos tan críticos como las alarmas aunque no puede permitirse que se pierdan ni que arriben en orden distinto al de origen.
- Mensajes de alarma: surgen cuando hay una falla en el proceso o en el sistema de control. Su demora puede impedir que la falla sea reconocida y corregida a tiempo llevando a un agravamiento del estado de falla. Es fundamental que arriben a destino en el orden en que se han producido para que pueda identificarse la causa de la falla. La aparición de las señales de alarma puede introducir demoras en la transferencia de otras señales.

2.2 Estado del sistema y tipo de mensajes intercambiados

Existen muchos estados posibles de funcionamiento de un sistema de control que se han detallado en la guía GEMMA (Guía de estudio de modos de marcha y parada). Estos estados se pueden agrupar en tres modos principales: procesos de parada y puesta en marcha, procesos en falla y procesos en funcionamiento.
- En funcionamiento normal se intercambian mensajes de control y mensajes HMI (tanto periódicos como aperiódicos).
- En los procesos de parada y puesta en marcha hay una sobrecarga de los mensajes de comando.

- En los procesos de falla aparecen gran cantidad de mensajes de alarma que se superponen (hasta que se reconoce la falla por parte de los operadores del sistema) con los mensajes de control. También es frecuente que se generen una cantidad importante de mensajes de comando tanto provenientes de la intervención de operadores como generados automáticamente por la aplicación. Por lo tanto, el análisis de estos casos es muy diferente al de los sistemas basados en Ethernet en funcionamiento normal y son el objetivo de este trabajo.

2.3 Estrategias para la modalidad de intercambio de los mensajes de alarma

Otros de los problemas que han sido escasamente estudiados en la bibliografía es la modalidad de intercambio de los mensajes de alarma. Esta modalidad es decidida por el programa aplicación (residente en el sensor o el controlador) que genera la alarma y por lo tanto depende de la implementación por parte de los programadores o los fabricantes del dispositivo. Se pueden implementar alguna de las siguientes estrategias:

- Periódica: los mensajes de alarma se intercambian en forma periódica durante toda la vida útil de la aplicación. Para asegurar la prioridad de los mensajes de alarma sobre los mensajes de control se podría asignar una mejor prioridad a los mensajes de alarma (lo que no es posible en Ethernet TCP/IP por la escasa cantidad de prioridades) o utilizar para los mensajes de alarma un período más corto que para los mensajes de control. Esta estrategia parece ser "segura" porque garantiza que los mensajes de alarma lleguen a destino, a costa de la mayor ocupación del ancho de banda del canal.
- Aperiódica: los mensajes de alarma son lanzados a la red sólo cuando se produce la alarma. En este caso puede haber dos situaciones distintas
- Por eventos: los mensajes se envían sólo una vez y se queda a la espera del ACK del mensaje. Se establece una ventana de tiempo y si el ACK no ha llegado en esa ventana se repite el mensaje. Este mecanismo es posible en TCP configurando el tamaño de la ventana.
- En ráfaga: cuando aparece la alarma se comienzan a enviar mensajes en forma continua (puede considerárselos como periódicos de período muy corto) hasta que la alarma es reconocida por el operador.

2.4 Retardos en la transmisión de mensajes

Un dato que debe ser transmitido a través de una red de comunicación industrial sufre retardos en cada uno de los nodos por donde pasa y en la red. En la Figura 1 se presentan los procesos que intervienen desde que el dato es producido en el campo hasta que llega al controlador. El retardo total puede calcularse como:

$$Tadq = Tsen + Tapi + Tcpi + Tacc + Ttrans + Tcpc \quad (1)$$

Donde:

Tadq es el tiempo que transcurre desde que la señal se ha producido en el campo hasta que está en condiciones de ser procesada en el controlador
Tsen es la demora física en la adquisición del dato o el tiempo transcurrido desde que se produce el cambio físico en el campo hasta que el dispositivo de campo lo comienza a procesar
Tapi es la demora en el proceso aplicación del emisor.
Tcpi es la demora en el proceso de comunicación del emisor.
Tacc es lo que demoran los mensajes, una vez lanzados a la red, en poder acceder al medio.
Ttrans es el tiempo de la transmisión de los mensajes por la red

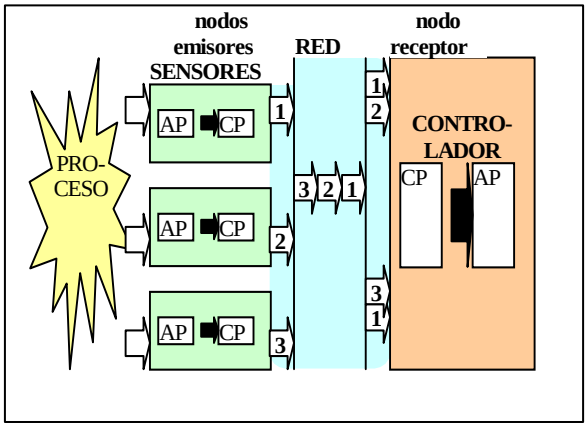

Figura 1. Tareas necesarias para llevar una señal desde el campo al controlador

A los fines de este trabajo, se deben realizar las siguientes consideraciones:
- El tiempo de sensado *Tsen* no se considera pues es idéntico tanto en estado de alarma como en estado de funcionamiento normal.
- Las demoras en los procesos de comunicación *Tcpc* y *Tcpi* son despreciables frente a otras demoras [1].
- El tiempo de transmisión de un mensaje *Ttrans* depende de la longitud de los mensajes y la velocidad de la red, por ende de la aplicación y del perfil de red utilizado.
- El tiempo de espera en el acceso al medio *Tacc* ha sido identificado como el causante de las mayores demoras en los sistemas de control en red [2], por ende será el más crítico para el análisis de los efectos en los mensajes de alarma. Además se diferencia de las otras demoras por su carácter aleatorio. Depende del tipo de protocolo de acceso al medio y de los mensajes que intercambie la aplicación.

2.5 Efectos de los retardos en la aplicación

Los efectos para la aplicación son diferentes según el tipo del mensaje demorado.

Una demora en un mensaje de alarma puede impedir que las acciones correctivas se realicen a tiempo de solucionar la falla y por lo tanto producir consecuencias materiales tanto para la aplicación como para el proceso controlado. La situación puede agravarse si diferentes alarmas resultan con diferentes demoras y por lo tanto las alarmas son procesadas en un orden distinto al de su aparición en el proceso. En este caso una demora puede inducir a un diagnóstico erróneo del origen de la falla, y por ende a acciones correctivas erróneas que agraven el estado de falla.

Para los mensajes aperiódicos el tiempo de vida no está limitado por el período, sino por consideraciones relacionadas con la aplicación. Supongamos que el mensaje aperiódico a_k se generó en el instante ti_k y el siguiente mensaje aperiódico a_{k+1} se generó en el instante $ti_{k+1} = ti_k + \Delta ti_k$. El mensaje a_k sufre una demora Δtd_k y el a_{k+1} una demora Δtd_{k+1} .La diferencia en el tiempo de recepción de ambos mensajes Δto_k se puede calcular como:

$$\Delta to_k = \Delta ti_k + (\Delta td_{k+1} - \Delta td_k) \qquad (2)$$

Pueden resultar tres casos:

- $\Delta to_k > 0$: El mensaje a_k llega antes del mensaje a_{k+1} . No se presentan mayores problemas desde el punto de vista de la aplicación, mientras Δto_k no sea muy diferente a Δti_k.
- $\Delta to_k < 0$: El mensaje a_{k+1} llega antes del mensaje a_k . Este caso es crítico.
- $\Delta to_k = 0$: El mensaje a_{k+1} llega al mismo tiempo que el mensaje a_k . Este caso es crítico pues, por ejemplo, se podrían estar dando dos ordenes distintas (e incluso contradictorias) en forma simultánea

3. Restricciones en la utilización de los protocolos de redes ethernet tcp/ip

3.1 Análisis de prestaciones de los protocolos

En las redes industriales se suele utilizar como referencia el modelo OSI [11], implementándose generalmente las capas 1, 2 y 7 de este modelo. La capa aplicación suele ser propietaria de cada red industrial y por ende no se analiza en este trabajo. Para este análisis se adopta como capa enlace lo propuesto por IEEE 802.3 [12]. Para las capas superiores se adopta IP y TCP. A continuación se analizan las restricciones capa por capa.

Capa Física. En las aplicaciones industriales la longitud de los datos suele ser pequeña, entre 4 y 8 bytes son suficientes para la mayoría de las aplicaciones. El tamaño mínimo de la trama de IEEE 802.3 es mucho mayor, por lo que se debe rellenar. Una solución que suele proponerse es empaquetar las informaciones lo que implica dejar datos en espera en los dispositivos. Para los mensajes de alarma esto no es admisible pues deben ser enviados en tiempo real. Por lo tanto, una aplicación en

estado de alarma producirá una cantidad excesiva de mensajes, ocupando gran parte del ancho de banda y pudiendo producir la saturación del sistema y el incremento en la cantidad de colisiones. Desde este punto de vista el protocolo Ethernet no parece demasiado adecuado para aplicaciones en alarma, por lo que debería realizarse una aplicación específica para el manejo de alarmas.

Mecanismo de acceso al medio. El problema del acceso al medio CSMA- CD es su aleatoriedad pues se pueden producir colisiones con las subsecuentes demoras en el arribo de los mensajes. El riesgo de colisión aumenta en los estados de alarma generalizados, pues varios nodos intentan enviar sus alarmas simultáneamente. Si la alarma queda restringida y la respuesta es rápida no habría problemas de colisiones. Los mensajes de alarma demorados en el estado generalizado pueden hacer que los datos lleguen a destino desordenados, con lo que se puede interpretar mal la alarma y realizar una serie de operaciones de corrección en una secuencia errónea, agravando el estado del sistema.

Se han realizado varios trabajos respecto a la utilización en aplicaciones industriales de switches para dividir la red en dominios de colisión [13]. Se concluye que para garantizar el arribo de todos los datos en tiempo real es necesario modificar alguno de los protocolos del stack Ethernet TCP/IP o adoptar switches con gestión. Es necesario tener en cuenta que estos switchs pueden introducir demoras adicionales inadmisibles para las alarmas.

El tema de las colisiones sigue siendo el más crítico en las redes industriales basadas en Ethernet: la única forma de solucionarlo es evitar las colisiones con un adecuado algoritmo de schedulling en la red y por ende complicando la capa aplicación o el programa usuario. Por lo tanto, si se quiere garantizar que no haya colisiones, es necesario utilizar otro protocolo MAC (por ejemplo CSMA-AMP) para lo que es necesario modificar el stack.

Capa Transporte. TCP, por ser un protocolo con conexión orientado a transmisiones punto a punto, impide que varios nodos adquieran un dato simultáneamente. Una alarma debe ser difundida en modo broadcast o multicast, lo que TCP no puede hacer, por lo tanto será necesario utilizar UDP.

Otra de las razones para no usar TCP, es que su mecanismo de conexión produce demoras inadmisibles. Si un nodo debe transmitir una alarma, deberá primero conectarse con lo que la alarma resulta demorada. UDP evita esta demora pero no posee mecanismos para garantizar la llegada correcta de la alarma.

3.2 Ejemplo de aplicación

A los fines de ejemplificar lo analizado se presenta una experiencia realizada para comparar el comportamiento de una aplicación industrial, en estado normal y en estado de alarma.

Descripción del experimento. Se implementó un banco de pruebas (figura 2) en el que el comportamiento de los dispositivos desde el punto de vista de la red se simula en PCs conectadas entre sí a través de una red Ethernet 10BaseT. Las simulaciones en cada una de las PCs se implementaron con Labview. Una de las PCs se utiliza como instrumental de medición y análisis, y las restantes computadoras se encargan de simular los dispositivos industriales. Los ensayos son realizados sin interacción con softwares que puedan causar accesos a Ethernet indeseados o que provoquen demoras en los procesos simulados. Los sistemas de seguridad convencional en redes de datos, tales como firewall o antivirus fueron anulados.

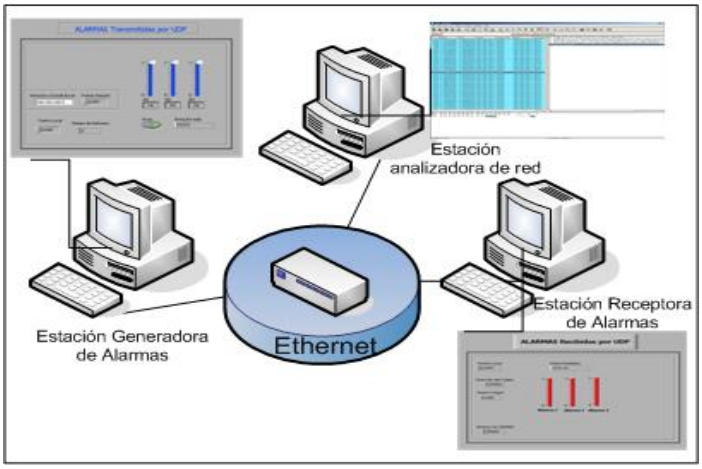

Figura 2. Banco de prueba

La aplicación simulada consiste en el control de posición de una herramienta que corta en un perfil triangular una plancha continua colocada debajo de ella y avanzado a alta velocidad sobre un eje *x* (sobre una cinta de transporte). Para lograr el perfil, la máquina de corte se desplaza sobre dos ejes perpendiculares *x* e *y*. Si el desplazamiento de la máquina de corte no es el adecuado a la velocidad y posición del material sobre la cinta, el corte es erróneo y la plancha se descarta con el consecuente desperdicio de material. La máquina de corte debe entonces ser capaz de interpretar las coordenadas *(x,y)* que le envía el controlador a través de una red Ethernet. La figura 3 muestra como debe ser en forma ideal la acción de control en función del tiempo para cada ciclo del proceso de fabricación.

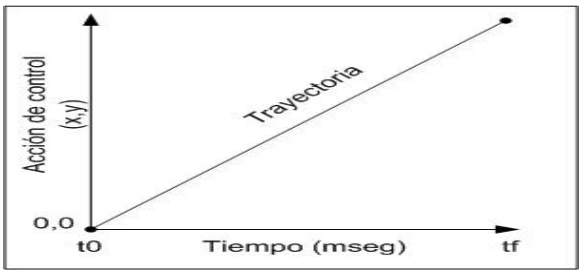

Figura 3. Acción de control ideal

Para lograr un corte parejo y continuo, la velocidad de acción del dispositivo de corte debe ser más rápida que el desplazamiento de la plancha, por lo que estará limitada por la velocidad de llegada de los paquetes de información provenientes del controlador a través de la red Ethernet.

El comportamiento del controlador desde el punto de vista de la red se simula en una PC que actúa como estación transmisora encargada del envío de las coordenadas *(x,y)* y de la orden de encendido/apagado a la máquina de corte. La estación receptora (máquina de corte) se simula en una segunda computadora personal. El control implementado es a lazo abierto. Las variables transmitidas *x* e *y* son de un octeto cada una y se envía un tercer octeto para encendido o apagado del dispositivo de corte.

Los resultados del ensayo con la red dedicada únicamente al control de este proceso se presentan en la pantalla de la estación receptora (figura 4) donde se observa el perfil obtenido en la máquina de corte.

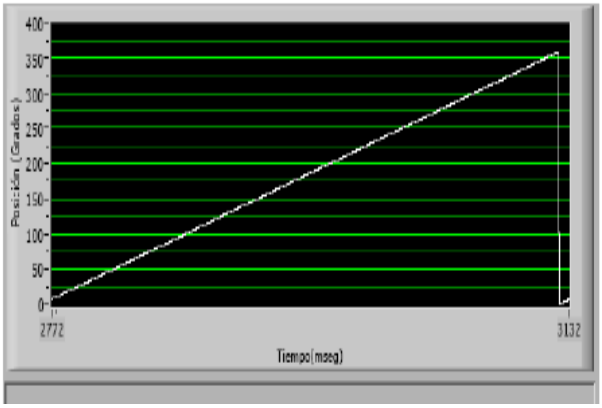

Figura 4. Perfil obtenido con la red dedicada

Se puede observar que este perfil es coincidente con el ideal por lo cual la utilización de la red Ethernet no ha introducido errores en la ejecución del proceso, con la aplicación en estado normal.

En la misma red se introduce ahora una estación generando gran cantidad de mensajes (que podrían corresponder por ejemplo a aplicaciones de video o de datos, o a otros dispositivos transmitiendo sobre la misma red). En este caso la red tiene gran parte de su ancho de banda ocupado. El perfil obtenido se presenta en la figura 5.

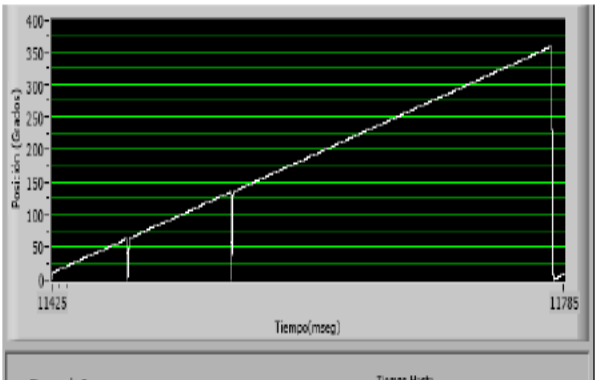

Figura 5. Perfil obtenido con el proceso en estado de alarma

Se puede observar que, en por lo menos dos puntos, la herramienta de corte no pudo realizar el trabajo indicado. En un proceso real cada una de estas ocasiones hubiera generado una parada del proceso, el descarte de la producción en curso y hubiera obligado a operaciones para despejar la máquina y reiniciar nuevamente.

En esta experiencia se puede observar que, si bien Ethernet resultó adecuada como red industrial en estado de funcionamiento normal del sistema, cuando se produjo una alarma generalizada, no pudo mantenerse el control del proceso.

4. Conclusiones

De los análisis realizados y de los resultados expuestos se puede concluir que las redes basadas en Ethernet TCP-IP pueden utilizarse en aplicaciones industriales en estado de alarma, solo si se contienen las alarmas. Si el estado de alarma se generaliza la red puede dejar de responder adecuadamente. Por lo tanto es necesario implementar alguna modificación en el sistema de automatización, en la arquitectura de la red o en el stack de protocolos.

La primera recomendación que surge es reemplazar TCP por UDP para evitar mayores demoras en la llegada de los mensajes de alarma. Con esto se pierde la posibilidad de tener ACK a nivel de protocolo, por lo que se debería implementar a nivel del programa de aplicación.

Otro de los problemas es la abundancia de colisiones en estado de alarma generalizado el mecanismo de acceso al medio. La división en dominios de colisión acarrea el problema de las demoras en los switches que deberían ser con gestión. Otra solución es implementar un protocolo de capa aplicación que gestione prioridades y

algoritmos de schedulling de las alarmas. También podría implementarse sincronismo y/o un mecanismo de time stamp.

Las soluciones que proponen los estándares de Ethernet industrial implementan alguna de estas alternativas.

Debido a la generalización de Ethernet industrial será necesario establecer formalmente los requisitos para su utilización en estados de alarma.

Agradecimientos. Este trabajo ha sido parcialmente financiado por:

- Proyecto de Investigación "Desarrollo de un sistema de supervisión, control y adquisición de datos orientado a PYMES" de la UNGS.
- Proyecto de Investigación "Arquitecturas de sistemas de control industrial distribuido para aplicaciones en microautomatización" de la UNGS.
- Proyecto de investigación "Vinculación con la Universidad Nacional de Quilmes para el desarrollo de proyectos de investigación conjuntos en el área de automatización industrial" de la UNGS.

Referencias

1. Lian F., Moyne J.,. Tilbury D., "Network Design Considerations for Distributed Control Systems", IEEE Transactions on Control Systems Technology, **Vol. 10,** Nº 2, pp 297-307, (2002).
2. Chavez M.L., Thomesse J.P., "Fieldbuses and real time MAC Protocols", 4th IFAC International Symposium SICICA 2000, Buenos Aires, (2000).
3. IEC Standard IEC 61158, "Digital Data communications for measurement and control-Fieldbus for use in industrial control Systems" (Part 3-o 6), International Electrothecnical Comission, (2000).
4. Felser, M.; Sauter, T.;"Standardization of industrial Ethernet: the next battlefield?", IEEE International Workshop on Factory Communication Systems, 22-24 Sept. 2004, Page(s):413 – 420, (2004).
5. Kaplan, G., "Ethernet's winning ways", Spectrum, IEEE. , **Volume 38**, Issue 1, Jan. 2001 Page(s):113 - 115
6. Fondl M.; "Ethernet on the Floor: There is a proper time and place for industrial communications deployment", Intech ,November 2006, http://www.isa.org/, (2006)
7. Neumann P., "Communication in industrial automation. What is going on? ", Control Engineering Practice, December 2006.
8. IAONA Handbook, "Industrial Ethernet", 3d Edition, Maddeburg, July 2005.
9. Decotignie, J.-D.; "Ethernet-based real-time and industrial communications", Proceedings of the IEEE, Volume 93, Issue 6, June 2005 Page(s):1102 – 1117.
10. Kopetz H, "Event-triggered versus time-triggered real time systems", Operating Systems of the 90s and Beyond International Workshop, pp 87-101. ,(1991).
11. ISO/IEC Std 7498: 1, "Information Processing Systems—Open Systems Interconnection—Basic Reference Model: The Basic Model, 1996.
12. IEEE, Standards for Local Area Networks: Carrier Sense MultipleAccess With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, ANSI/IEEE Std. 802.3-1985.
13. Lee, K.C.; Lee, S.; Lee, M.H.;"Worst Case Communication Delay of Real-Time Industrial Switched Ethernet With MultipleLevels", IEEE Transactions on Industrial Electronics, Vol. 53, Issue 5, Oct. 2006 Page(s):1669 - 1676