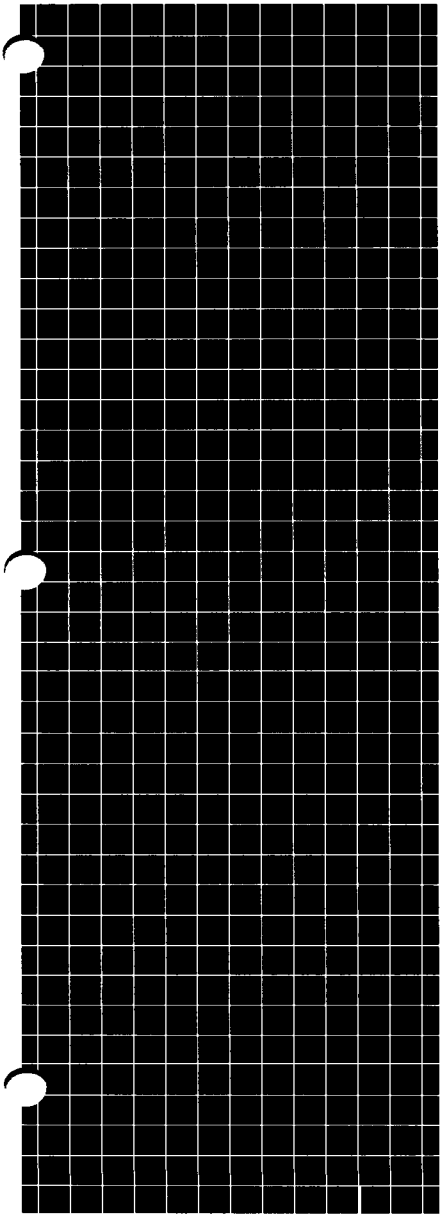

A Comparison Between Buffer Insertion Protocol
(a.k.a. All Masters Protocol)
And
Token Passing Protocols
(a.k.a. Master of the Moment Protocol)
(a k a Rotating Master Protocol)

by
Stephen L Seabury
and
Grant O Provins

Technical Paper

TP87-16

Bailey

A COMPARISON BETWEEN BUFFER INSERTION PROTOCOL (a.k.a. All Masters Protocol) AND TOKEN PASSING PROTOCOLS (a.k.a. Master of the Moment Protocol) (a.k.a. Rotating Master Protocol)

by Stephen I. Seabury and Grant O. Provins

Recently, there have been a number of requests to compare the Network 90 "Buffer Insertion" communication system to "token passing" communication systems such as the IEEE 802.4 in relation to their use in real time process control applications. The following discussion is an attempt to examine the two communication architectures in a common framework of terms and concepts.

TOKEN PASSING PROTOCOL (Rotating Master or Master of the Moment)

The use of "token passing" protocols (whether deterministic or not) in applications which demand "no single point of failure" introduces a number of difficult technological issues. All "token passing" protocols, by definition, fall into a category of communication systems referred to as Master/Slave architectures. In the token passing approach, control of the communication channel is passed from one user to the next by means of a specific message referred to as the token message or simply the "token". Implicit in this protocol, as in all other master/slave protocols, is the fact that there can be only one master of the communication channel for any specific instant. All drops other then this "Master of the moment" are by definition "slaves of the moment". The drop that is in "Master" at any given time is determined by possession of the token.

TOKEN PASSING PROTOCOL (Rotating Master or Master of the Moment) (Continued)

Other potential users of the channel, must be disabled from attempting to use the communication channel at that time. Because of this gyratory movement of the single master, the token becomes a **rotating single point of failure**. Any failure of the drop while it is the master, will result in loss of the token which in turn will climax in a catastrophic failure of the entire communication system. No token always equals no communication.

Because of this inherent single point of failure, additional components must be added to the system in an attempt to forestall the case of the "dropped token" from causing this critical failure. The necessity of having these recovery techniques confirms the single point of failure of the token protocol. One of the most common attempts at preventing the "dropped token" scenario involves placing token timing monitors at one or more drops within the system. These timers are set to produce a new token if the existing token has not been passed in a fixed amount of time. This approach to token recovery is flawed by the potential failure of the token timer at any one of the drops. This type of failure would then cause multiple tokens to be generated on the communication channel. This simultaneous masters scenario will result in complete failure of the communication channel since two drops transmitting data at the same time will result in all data being garbled and unusable. Multiple tokens always equals no communication.

TOKEN PASSING PROTOCOL (Rotating Master or Master of the Moment) (Continued)

Further complicating this dropped token timer and regeneration solution to one of the failure modes, is the reality that, in a single token system, each user or drop that has this token timer and regenerator, will in fact, increase the potential for the system as a whole, to incur the multiple token type of failure. Furthermore, the use of standard failure mode analysis techniques reveals that the increase in complexity and parts that this or any other regeneration approach must incur, will ultimately yield an even higher probability of failure occurring to of one of these token timer or token regenerators, then even the original "dropped token" scenario. This essentially means that the attempts to remedy the dropped token failure mode will actually increase the potential for the multiple token failure mode. Unfortunately, both the dropped token occasion and the multiple token occurience will result in a complete communication system collapse.

Another concern related to the characteristics of token passing systems has to do with their responsiveness. Since there is only one master at any moment, there is only one drop that can launch a message. Other drops in the system must remain passive, regardless of the urgency of the information they have. In a token passing system two major approaches to determining the "next master" are used. The simplest is to have a fixed order where drop N always passes the token to drop N+1. The technical tradeoff of this approach is that each drop must wait one entire revolution of the token through all the nodes before it can output it's data.

TOKEN PASSING PROTOCOL (Rotating Master or Master of the Moment) (Continued)

The second approach is to use some "deterministic" method of selecting the next drop to become master. In this approach the current master must determine which destination to send the token to. Many schemes have been designed to allow the current master to make this decision. "Quick polling" of all the other drops and time synchronized "windows" of opportunity for other drops to request the token are just two of the methods which have been implemented. Regardless of the method of determining the next "master" the elementary fact remains that under any of these schemes, additional overhead bandwidth of the communication channel and, more critically, additional complexity will be used to make the determination. Additional concern in the use of a deterministic token scheme is that there exists a rather simple case where one node with critical data can be starved off the communication system for some period of time by another node or group of nodes with less critical data. Furthermore, this situation is most likely to occur during a plant wide upset when each node is generating large amounts of critical data. These faults are clearly unacceptable in a real time process control or data acquisition communication system.

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" Token Protocol)

The protocol used in Network 90 Plant Wide Communication Systems is an "All Masters" convention. This method of structuring a communication system permits each user of the data channel to generate a message independently of the any other nodes on the system. The technique is referred to as " Buffer Insertion" protocol

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" - Token Protocol) (Continued)

because each node is able to "insert" a "buffer" of data into the data stream without any interaction or concurrence of the other drops or nodes in the system.

While the Network 90 buffer insertion technique goes well beyond simple token passing systems in many essential and fundamental ways (specifically security and speed of response) it is possible in a limited fashion, to describe the Network 90 communication system's data exchange operation in token-passing terms. In order to make this comparison it is necessary to understand the rules used in buffer insertion protocol to initiate a message from the perspective of an individual node.

RULES FOR BUFFER INSERTION NODE TO TRANSMIT (launch a new message)

1) The node has a new message formatted and ready to send.

2) The incoming message receive buffer of the node is empty or currently filling and does not require immediate transfer to the output transmit buffer.

3) The node is not waiting for the return of a previously transmitted message.

If all three conditions are met, the new message will be sent.

****
Note: All of these tests might be valid simultaneously for every node in the Network. In this extreme case, every node in the Network could simultaneously launch a message. This provides a quantum increase in the responsiveness of the "all master" buffer insertion protocol over any single master protocol.
****

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" Token Protocol) (Continued)

Since each node's transmit and receive functions are asynchronous and isolated from each other, message collisions cannot occur. As each message requires some finite amount of time to fill the incoming receive buffer in the node, there is an assured "window" to permit the node to inject it's own message (buffer insert) into the outbound data stream. In the extreme case noted, all the messages would successfully launched at the same instant. The superiority of the Network 90 system's approach in it's parallel use of available bandwidth is clear when compared to simple token passing. In a similar case, a token passing protocol will require consume a time equal to the circulation lag of the token to each drop in the system (or a greater time if overhead for deterministic mastership is incurred), in order to insure that the values generated at each drop are started on through the communication channel. In addition, the actual passing of the data will consume more time. Effectively, any token passing system has its communication channel throughput divided by the number of nodes being serviced. This weakness is inherent in all single master protocols and results in a diamatic reduction in responsiveness as the size of the system increases. In direct contrast, large system applications of the buffer insertion technique do not suffer this performance degradation because each additional node increases the message handling capacity of the network by one. The cascading effects of the token passing systems reduced node time segment with increasing deterministic overhead are replaced in the buffer insertion technique with a small and predictable linear delay per node characteristic.

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" Token Protocol) (Continued)

One of the subtle implications inherent in rule number 3 shown above, will permit a more direct comparison between buffer insertion and token passing systems. Rule 3 states that when a node launches a message it cannot generate another message until it's first message returns. (A node can, however, always receive data from another node or pass other nodes messages through to the next node on the loop); The rule 3 constraint only applies to generation of new messages from a node that has a message outstanding.) This rule can be interpreted in the following manner:

Each message generated by a node acts as a token for that node, and each node in the system passes it's token around the loop to its self.

One transit of the loop will normally insure that the data values contained in the message will have been received at the multiple destinations, individual value transaction acknowledged. This means that the originating node normally can remove the message from the loop after only one rotation. Receipt of the acknowledged message by the source node returns that node to the status of ready to transmit a new message. Thus, the Network 90 system can be viewed as an "N token" system where N is the number of messages capable of circulating at any given time. The maximum number of messages that can be in transit at any instant, is the equal to the number of nodes or drops in that system. As the number of nodes or drops increases, the message handling capacity and network bandwidth efficiency INCREASES!

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" Token Protocol) (Continued)

Another superiority of N-token technology over a single token system is that the loss of a token (message) affects only one node and one message. All other messages continue on the Loop unaffected by the loss. The node whose message has been lost can easily detect the condition by counting the number of messages that pass till the original message returns. If the number of messages passing the originator since the message was launched exceeds the number of possible drops plus one, then the original message must have been lost or corrupted and removed. Even more advantageous to system fault tolerance is the fact that the recovery from this scenario is easily accomplished by means of re launching the message in a routine, non catastrophic way.

The other possible transmission errors can also be corrected in a non destructive and routine manner. The occurience of multiple or repetitive messages if it were to occur, is non catastrophic since the originating node is easily programmed to handle this case by simple removal of any message that carries the nodes source address and does not match the currently circulating message.

Should a message have have been corrupted to contain a false source address (such as a node not in the system) an embedded count within the message will cause the corrupted message's removal. This circulation counter which is a field within the message itself, is incremented by each drop as the message is passed along. The drop that adds the final count to cause the total to exceed the maximum will remove the message by simply not passing it on to it's output buffer.

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" Token Protocol) (Continued)

All of the non destructive recovery modes of the buffer insert (N token) protocol are in sharp contrast to the fault modes of the single token protocols. A single token system **always** reacts catastrophically to a token loss or to multiple tokens; all communications ceases. A N token system reacts to either of these same problems in a very non catastrophic almost routine manner. If some new and reliable means is invented to insure that only one new token is generated and is attempted on a single token system, a significant period of "scrambling" will be required while each node tests for mastership, or attempts to determine which drop is the proper node to regenerate the token. As all of these decisions can not occur instantaneously, and the token passing communication channel cannot be used during this time. At best, a temporary communication blackout condition will occur for some period of time dependent on the number of drops competing to be the token regenerator.

Another major difference between the N token Network 90 technique and any single token approach is elimination of condition called "Token Choke". This "Token choke" condition occurs any time that the amount of data being generated at a specific drop exceeds the bandwidth/time segmert for that drop. For a number of reasons, some of which have been previously presented, (token timing monitor, deterministic widow synchronization, etc.) the amount of time that an individual drop has possession of the token is normally restricted. As the number of drops within the system increases either the time segment allowed for

each drop must be decreased or the system data throughput requirements reduced (in reality, a somewhat rare occurrence). In either case, the individual drop will only have a finite amount of time to transmit its backlog of data before it must surrender the token. If the data being generated from an individual drop exceeds the rate at which the data can be exported from that drop before it must pass the token, then a continuously increasing "backlog" of data in the drop will start to build. This "token choke off" condition will continue to build the export data backlog. Because of the rules for passing the token in the deterministic systems, token choke in one drop may actually induce sympathetic choke conditions in other drops (by hoarding the token at one drop or the reoccurring overhead of the deterministic decision) the possibility will increases that other drops will have their data rate exceed their reduced transmit time segments. This condition can continue to proliferate until the entire communication system bandwidth is absorbed in overhead or dedicated to one drop. In either of these cases the resultant effects on the controlled process may be disastrous.

While this potential condition exists at all times in a token passing system it is even more likely to occur during the high traffic conditions of an upset. Because this condition is actually a case sensitive result of dynamic system conditions as opposed to an indisputable communication system "bug" it is difficult to authenticate or duplicate. When it is encountered it is frequently unresolved and considered coincidental until it's next appearance.

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" - Token Protocol) (Continued)

The Network 90 system's approach to data burst response is to have all drops continuously capable of exporting data, and to alter the number of values and destinations per message as data rate requirements increase. The inherent queuing/de-queuing nature of this variable message packet approach, together with the parallel use of the available bandwidth means that the data burst capabilities of the Buffer Insert protocol will far exceed those of a token passing system using the same speed communication channel. Furthermore, should this enhanced capacity be exceeded, the internal queuing of export data at each drop would result in a linear degradation in communication throughput performance not a catastrophic disintegration of all communication function, as exhibited in the single token passing approach.

Simply stated, all single master systems are using a time division multiplexing of the communication channel. Use of this approach, means that the bandwidth (data carrying ability) of the channel can only be equal to the bandwidth of the channel after subtraction of the overhead (deterministic windows etc.) and the result **divided** by the number of nodes or drops. The burst throughput requirements of each node must not be greater then the nodes maximum time segment of channel bandwidth or a choke condition will occur and data will be lost. Since token passing systems are always at their load saturation point it is obvious that as the number of drops is increased the vulnerability to data burst mode token choke will increase.

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" Token Protocol) (Continued)

In contrast, N token buffer insertion type communication systems do not divide their bandwidth by node count. Instead, they pass data in a parallel manner simultaneously on each node to node segment. Additionally, the support of buffer insertion by any drop when the drop is ready to send the message, and the inclusion of multiple values in a message with multiple destinations, effectively eliminates the susceptibility to burst mode choke for the Network 90 N Token system.

Buffer insertion or N token passing communication systems when used for Distributed Control Systems (DCS) and Distributed Processing Systems (DPS), observes the generally accepted requirement of not having any single point of failure. The Network 90 communication systems can be referenced using a token passing conventions, but in doing so, it is important to remember that buffer insertion corrects the inherent deficiencies and many of the inefficiencies of conventional token passers. Not expressly evident in this type of comparison, is the fact that the Network 90 N token approach utilizes the available channel bandwidth in a multiple access, parallel segment method which maximizes the responsiveness to each node and it's ability to send and receive data.

Bailey Network 90 Buffer Insertion Protocol (All Masters" or "N" Token Protocol) (Continued)

In summary, The Network 90 buffer insertion communication system eliminates the catastrophic single point of failure which is inherent in all token passing protocols. Buffer insertion protocol meets and exceeds the requirements for both fault tolerance and security of plant wide communication systems. Token passing approaches are shown to be viable for passing files between computers for non critical data exchanges operations such as "electronic mail" and office type systems where loss of data results only in an inconvenience. Token passing protocols can not be recommended for large real time process control applications because they do not provide the necessary degree of responsiveness. Additionally, the catastrophic failure modes of the dropped or multiple token add potential risk to both personnel and equipment when these types of failure occur in a token passing system.

Because of the possible danger to personnel or potential damage to equipment that can result from catastrophic failure modes of the token passing communication systems in a process control environment token passing protocols do not provide the necessary degree of communication security or the responsiveness required for real-time process control applications.

For additional copies contact

Bailey Controls Company

29801 Euclid Avenue Wickliffe Ohio 44092 U S A • (216) 585 8500
Telex 980621 • Telefax (216) 585 8756 or (216) 943 4609

Lithon U S A 1987