

Networked Vessel Systems, 2

More Networking Blog

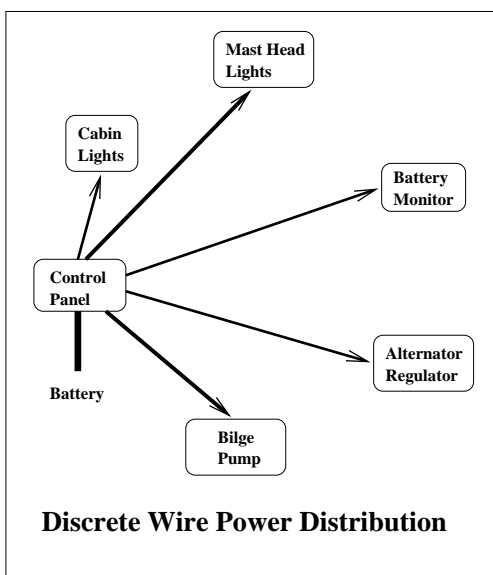
At least some people want to know more about networked systems. Based on the feedback we received, it's not a hot subject, but there is interest. Maybe when some of the horror tales from early adopters begin to appear it will garner more interest.

So who is interested in vessel networking? Those interested in saving the cost of wires, the cost of installing those wires and then verifying that the wires carry out their intended functions. For the most part this group includes people building their own boat, or boat builders looking at ways to cut production costs.

In a discretely wired system, power is fed to a distribution panel where individual circuit breakers are used to switch loads on and off. Each circuit breaker is wired to the load that it controls, and the wire or wires must be sized appropriately for the load current and the length of wire. The greater the distance between the load and the circuit breaker, the larger the wire must be. There is plenty of room for errors here, and a lot of expensive wire can be used.

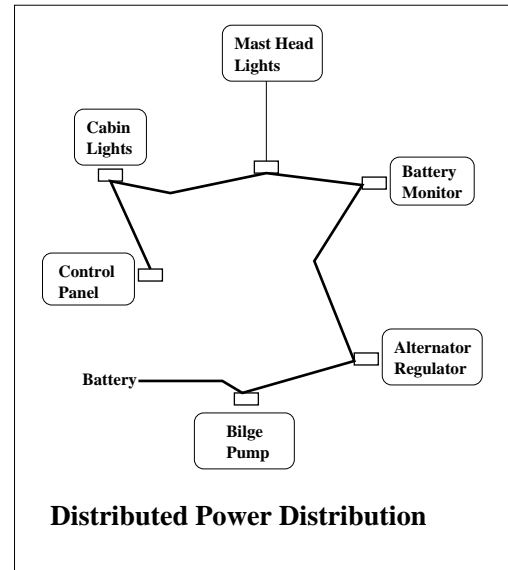
A networked system can reduce the amount of copper wire used, a considerable cost savings in itself. Power is routed in the most efficient way possible and connected to network nodes close to each device. The network nodes control the device based on signals from the control panels rather than directly. One or more control points can easily be incorporated in a networked system, something very difficult to do in a discretely wire one..

Installation and checkout costs are also reduced. In theory the system can be more easily maintained and diagnosed in the event of failures. Will those theoretical arguments for a networked system stand up to practice?



Vocabulary

Every field of human endeavor, from Lindy Hop dancing to electrical systems to neural surgery is surrounded by a vocabulary that one must learn to take part in the discussion. Learning the vocabulary is the price one pays to enter the club.



Here are a few ideas or acronyms about networked systems:

- A man with two watches doesn't know what time it is. While redundancy is good, two watches are unlikely to be exactly synchronized so a resolution procedure is necessary to decide what the correct time is.
- *Single Point Failure*. Two watches are better than one. If your only watch fails, time keeping stops. If system operations depend on knowing the time, then the watch becomes a single point failure mechanism.
- *Failsafe*. Devices in a system which can fail without jeopardizing safety are *failsafe mechanisms*. A car radio is failsafe, while brakes are not.
- *Failover* A *failover mechanism* is one which substitutes for another which has failed. Failover may be a manual operation, more commonly called *switchover*, or the system may use automatic failover procedures.
- *Ping Pong*. A term used for devices which takes turns operating. If you're wearing a watch on each wrist, and one time you read the time from you left wrist and the next time from your right wrist, then the watches are *ping ponging*. (Aren't technical terms wonderful.)
- *Inherent fail safe design*. This is the holy grail of systems. A failure cannot create an unsafe circumstance.
- *Failure Point Analysis*. The process of examining all points in a system to determine how they might fail, and what the consequences would be if that point fails.

The Perfect Network

If there is a perfect network topology it has yet to be discovered. Likewise, the perfect way to manage a network, has been elusive.

The result is a proliferation of networks with various claims about performance. It would seem there should be a method of separating networks into simple good/bad buckets. One thing that stands in the way of that is politics. By that term we don't mean national

politics, but the information and mis-information disseminated by organizations that have something to be gained by public acceptance of their position.

Politics

Once we were listening to a presentation about batteries given by a representative of a major battery supplier. Someone in the audience asked how to determine if their battery was defective. The short answer was, "if it's not one of ours, it's defective".

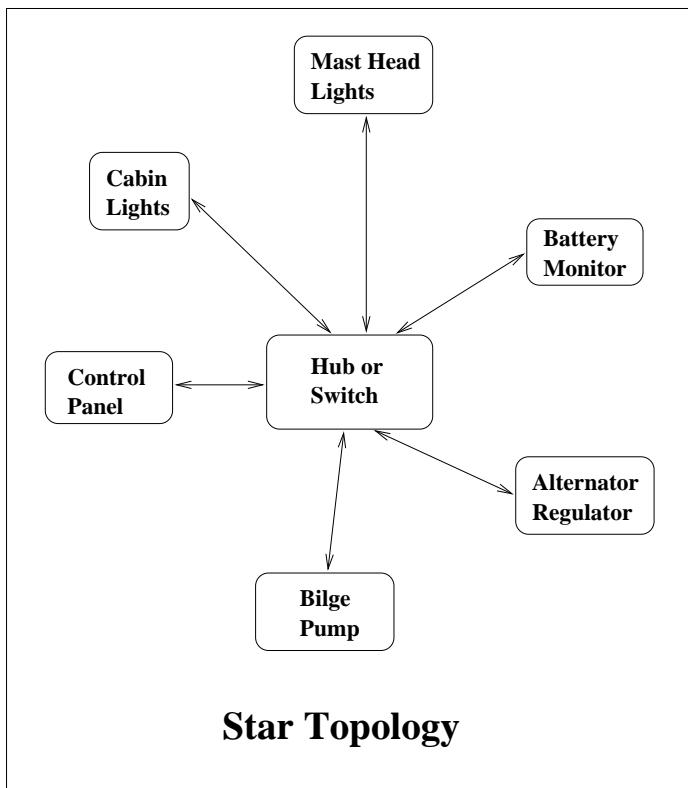
A company with a significant market presence can make those kind of statements because technology most often takes a back seat to market clout.

Manufacturer associations are often based on the idea that there should be compatibility between equipment from each of them, and standards are produced with the apparent intent of fostering compatibility. In reality, the specifications are often written with some minimum requirements and full of exceptions that essentially gut compatibility. Then, a hefty price tag is placed on a copy of the specifications so that only large manufacturers can belong to the club.

Do they have your interests in mind? They argue that if they didn't charge an astronomical price for a copy of the specification and many times more for later qualification testing, you the consumer would end up with products that aren't compatible. Thanks goodness that never happens.

Network Topology

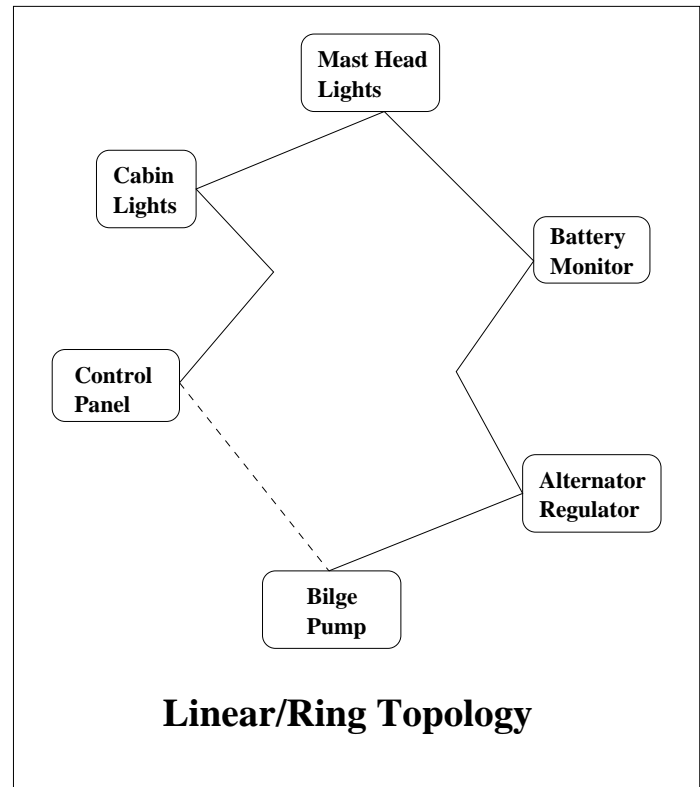
Strictly speaking, a consumer shouldn't care about how a network is wired. But, while networking is good when it works, a network that tends to fail often, and the network is critical to operations, then safety issues must be considered.



The star topology is illustrated above. Devices on the network

communicate over wires routed to a central *hub* or *switch*. Most small offices with networked computers are wired in the star topology.

One disadvantage of the star network is the reliance on the central hub. If it fails then the whole network is down. A second disadvantage is the amount of network cabling required. Two adjacent devices must each be wired to the hub instead of more directly to each other.



A linear network is illustrated above. Each device is connected to the network which runs from one device to the next. The devices could be placed on a straight line, hence the name linear network.

On the linear diagram is a dashed line. If the two ends of a linear network are connected, it becomes a *ring* network. There are some subtle electrical differences between linear and ring. Some ring networks may use special couplers at each device that effectively disconnect the device's transmit driver unless that device has the *token* that lets it talk. (More about this later)

If the network medium, (wires or optical cable), is broken in a linear network then devices will be *islanded*. That is, able to communicate within their island, but not outside. If the network is shorted, devices can no longer communicate. Depending on termination methods, a ring network may be able to survive and an open circuit, but cannot tolerate a shorted network.

Industrial networks commonly use optical cable made with plastic. Optical networks are immune from electrical noise, and their bandwidth can be very high. Because of cost, and the power to operate them, optical networks are less applicable to vessels.

What About Wireless?

The cost of wireless technology and power consumption have fallen so low that wireless networks can now be considered.

Wireless may be an alternative to wired networks in some cases, however, obstructions in the signal path may disrupt communications unexpectedly. Storing a new piece of gear in a locker may interrupt a signal pathway or create a signal reflection. If the interruption is intermittent then finding it becomes a first class nightmare.

There is also possibility of interference from nearby vessels. That is, signals from their control panel operate devices on your vessel. While encryption can be used to limit such interference, the cost of networks and power consumption both increase.

Once we were visiting some friends at an RV campground. Vehicles were parked quite closely. One of the neighbors was watching TV, which my friend noticed when he opened the door to let us in.

He grabbed his remote control and the neighbor was suddenly watching a different channel. The neighbor clicked it back, but then it got changed again. The channel swapping went back and forth for a few more cycles. We can only imagine what frustrations would occur if two neighboring vessels interfered with each other's control system.

Network Control Protocols

Once several devices are interconnected a controlling protocol is necessary before communications can be successful. Various protocols are in use, some of which will be discussed below.

- Master/Slave
- Token Passing
- Peer to Peer, Retry, (CSMA/CD)
- Peer to Peer, Priority, (CSMA/CR)

A common protocol that is easy to implement is called *master/slave*. This network can be compared to a group of people who must get permission from a moderator before they can speak. There is a difference, however. In the case of a master/slave network, the master asks each slave in turn if they have anything to say. That is, the slave doesn't "raise its hand" to ask to talk, but must wait silently until the master *polls* him.

The problem with the master/slave control protocol is the reliance it places on the master. If the master fails, the whole network is down.

Another control protocol is known as token passing. Imagine a group of people with a flag, (token), they pass from one to another. Only the person with the flag can speak. Once done speaking, the flag is passed to the next person in a specified order. Suppose that you are instructed to pass the flag to Joe when you are finished, but Joe has decided to take a break. Without some other rule, you must hang onto the flag until Joe comes back ... the network is down.

Suppose the person with the flag decides to take a break? The flag is essentially *lost*.

To get around broken masters or lost tokens, peer-to-peer networks are used. This protocol is more like a party where anyone that

wants to speak does. Of course it works best if you listen before speaking instead of interrupting someone presently talking.

Even with diligent listening, two people can still begin to talk at the same time ... a collision. When that happens both people may hesitate and both may again collide when they restart. This might go on forever unless some protocol is followed to prevent it.

Ethernet operates around this principle. Devices can talk when they need to, but they have to detect a collision and retry if one occurs. Each device waits for a random length of time before retrying. This form of network protocol is called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Sensing *carrier* is the same as sensing that someone else is speaking.

Time, or network bandwidth is wasted when collisions occur. The more traffic there is on a network, the more collisions there are.

A second type of peer-to-peer protocol is called CSMA/CR, which stands for Carrier Sense Multiple Access/Collision Resolution. Under this protocol, collisions are detected, but there is a priority established such that one message can proceed without retry, while other messages must stop being sent. Consider the case of two people starting to talk at once. One begins by asking, "have you heard this joke", and the other begins by announcing, "there's a fire in the hallway and we must evacuate immediately".

Some overhead must be added to each message to establish its priority. Message transmission begins with its priority. For the protocol to work, each message must have a unique priority which is its identifier. Identifiers should be handed out with the most important message getting the highest priority.

Peer-to-peer protocols with collision resolution have been used for a number of years. The presently popular form of that is known as the CAN bus, where CAN stands for Controller Area Network. There are quite a few networks that use the underlying CAN protocol, NMEA2000 being one of them. More on this later.

To be continued ...

In the next installment we'll discuss how signals are actually transmitted over the network. Subjects like single ended and differential levels will be presented, and why one is chosen over another.

How a network is expanded with new devices, and what happens when a device is removed, are questions that have to be answered to determine the suitability of any network for a given application. And yet to be discussed is how information, (not signals), is exchanged over a network. Information is something humans understand, and a network should transport information with a minimum of rules which are only published outside the network itself. That is, a network should be as self-descriptive as possible.

Stay tuned.

If you'd like to be notified when the next installment is released, send us an email. The subject should read *Network Blog*. See the image below for the email address.

smead@amplepower.com