When control failure is just not an option

David G. Tyas IKON AVS Ltd, 238 Ikon Estate, Hartlebury, Worcs.. DY10 4EU
www.ikonavs.com

1. Introduction

Whilst we all expect the technology we use to operate flawlessly, alas it's not always the case. Sometimes it's just the choice of inappropriate equipment for the function or it may be the result of inept or sloppy configuration or programming. There are however some critical situations when the failure to function correctly is not only annoying but also potentially catastrophic.

2. Basic Example

Taking a couple of examples of what in our industry are often referred to as basic AV systems, if we have a simple panel controlling a projector in a school classroom, well if it fails to operate the most likely outcome is only likely to be frustration or embarrassment of the user.

Move this same scenario into a Boardroom environment where it is the Chief Executive who experiences the frustration or embarrassment, and you could easily find the AV technician clutching their P45 as they look for another job.

Now clearly in both these cases, whilst a failure to operate correctly is undesirable it can hardly be classed as critical.

3. Typical Systems Introduction

So how do we define a critical system? During the course of this seminar I will look at the implementation of three real scenarios:-

Prison Lighting

Whilst lighting control is not normally considered a critical system, except this is in a high security prison and we are controlling the perimeter and yard lighting.

Nuclear Facility

The second follows the use of AV technology as part of the voice alarm system in a nuclear facility.

Command and Control

The final example is a 24/7 Strategic command and control room.

Perhaps a little more modern than the one shown here.

Due to limited time available I am only giving an overview of these three systems but using elements of them to draw up a number of useful guidelines for the design of critical systems. More in-depth technical descriptions are available from;-

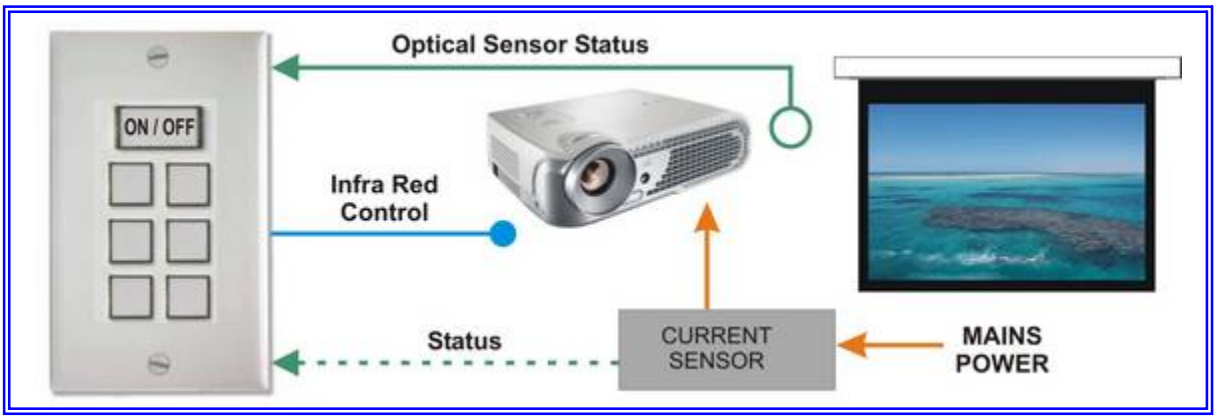
www.ikonavs.com/whitepapers

But before launching into these, lets cover a few basic everyday do's and don'ts for creating a reliable and stable system and on the way start to set down a few guidelines.

4. Reliable Display Control

Probably the most basic control function is display control.

All to often control panels fitted for projectors and other displays are the simple 'send and hope' types. Once the command, be it IR or RS232 has been sent, its assumed that the device received it and responds correctly. With IR you haven't much of an option as it's a one-way communication, that's unless you add sensors to detect the status of the display and integrate this into the control program. In general though, these types of control panels have been chosen for cost so even if it's possible, it just doesn't happen.



With systems that only transmit RS232 it's the same story so it always best to use a bi-directional RS232 port and configure the system to interrogate the display as to its status and communicate accordingly to ensure its not only on but ready for use.

For reliable operation you also need a method of letting users know all is operating OK, otherwise the instinctive panic reaction is to keep pressing all buttons to incite a response. This is particularly a problem if the display is remote, so some user feedback is preferable. This could take the form of a flashing and steady indicator on push button panels or a 'Please Wait' message on a touch screen, and this brings us to the first of the guidelines for designing critical systems: -

Design point 1. 'Keep the user informed of the system status at all time'

Now of course this is a very simple closed loop situation;

Send Command – if after X seconds no reply resend --- on reply next operation

A number of control systems manufacturers either supply or allow the creation of macros to achieve just this. The problem is that they often don't allow for error handling and what to do if it fails to operate correctly. And so we have a second guideline in designing critical systems: -

Design point 2. 'Include a mechanism for error handling'

Lets take a quick look at an example of this.

I was recently called to look at the operation of a system installed in a prestigious boardroom in central London. It had been installed a couple of years earlier and had operated on the whole as expected. More recently though it was prone to operational failures where the screen would lower but the projector failed to operate and then the screen would retract whilst the projector came on, along with other similar faults.

After examination it was apparent that the ON command was being continually sent to the projector whilst the system waited for an acknowledgement that it had been received, only then was the screen lowered. Whilst this appeared an initially sensible arrangement, as the projector aged and the lamp started taking longer to strike, as there was no user feedback as to what was happening, and, as no control lockouts had been coded into the system, the touch screen buttons remained active. With no information (remember design point 1) users keep pressing the ON button toggling it between ON and OFF so that when the projector was on the screen lowered, but by

then it had been told to turn off. A very undesirable situation that was virtually impossible to escape from.

Now if consideration had been given to design points 1 and 2, not only would the users have been kept informed and not panicked but also error handling would have taken over and corrected the situation or at least returned it to a known stable condition.

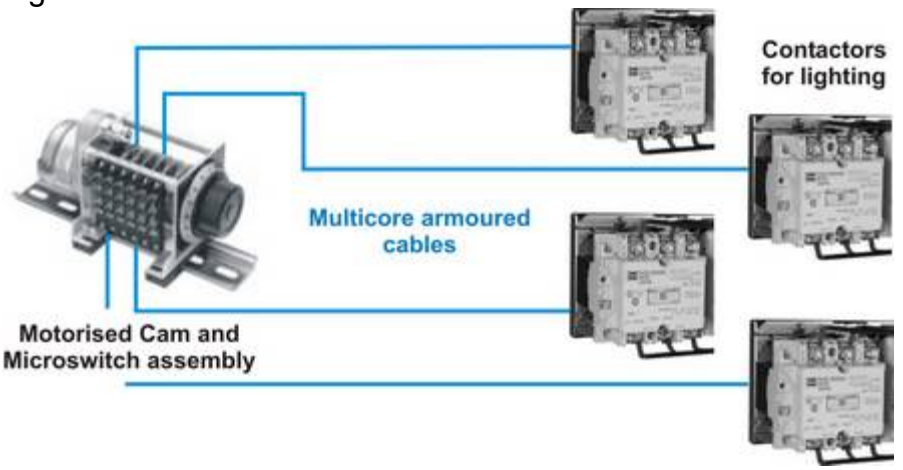
This simple example shows that even with suitable hardware, not only is it important to know how the system should operate but also to understand what can cause problems and how to deal with them. This is the very essence of designing critical systems.

Lets now look at the first critical system, prison lighting control.

5. Prison Lighting Control

Old or new prison, on the surface the control of yard and perimeter lighting should be a simple matter of operating a switch and the lights come on. Well not exactly if the lights are spread out over a several acre site and fed from separate, remotely located power feeds, each with its own backup generator. Whilst CCTV is available to look at if the lights are on and off, during an incident these are unavailable so reliable remote operation is essential.

In each remote plant room a set of latching contactors control the high current feeds to the lights. These contactors have separate ON and OFF 24V DC coils with these controlled centrally by a cam and microswitch arrangement to turn areas on in sequence to minimise the instantaneous load requirements. I did say it was an old arrangement and whilst it has worked reliably for 30 years, it's reached end of life and need replacing.

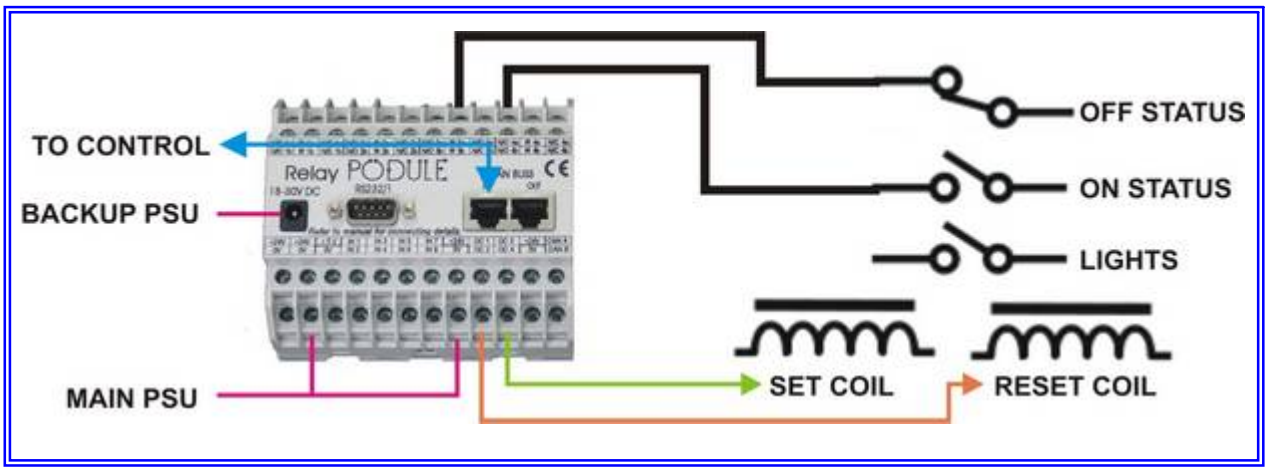


As the coils all operated at 24V, the original system used separate armoured multicore cables from the central control room to the remote plant rooms but over time these cables had deteriorated due to water ingress or had been damaged by building works.

A major requirement was that the replacement system had to allow operation and monitoring from more that one location and even if control was lost, each area should have a suitable default condition. There must also be no single point of failure within the control system, as was the situation with the motorised cams and microswitches. In practise it is almost impossible to totally remove the chance of a single point of failure but provided a suitable risk assessment is carried out the chance of this occurring can be minimised. And so we have a third guideline in designing critical systems: -

Design point 3. 'Carry out a risk assessment to define which parts of the systems are critical and which are not.'

Starting with the remote switch room, lets look at the design adopted and expand on why it was done this way.



The Relay Podule from iKON AVS is a self-contained controller with internal power relays and its own processor and whilst it will operate in isolation, it is normally linked by a propriety network to control panels and other processors.

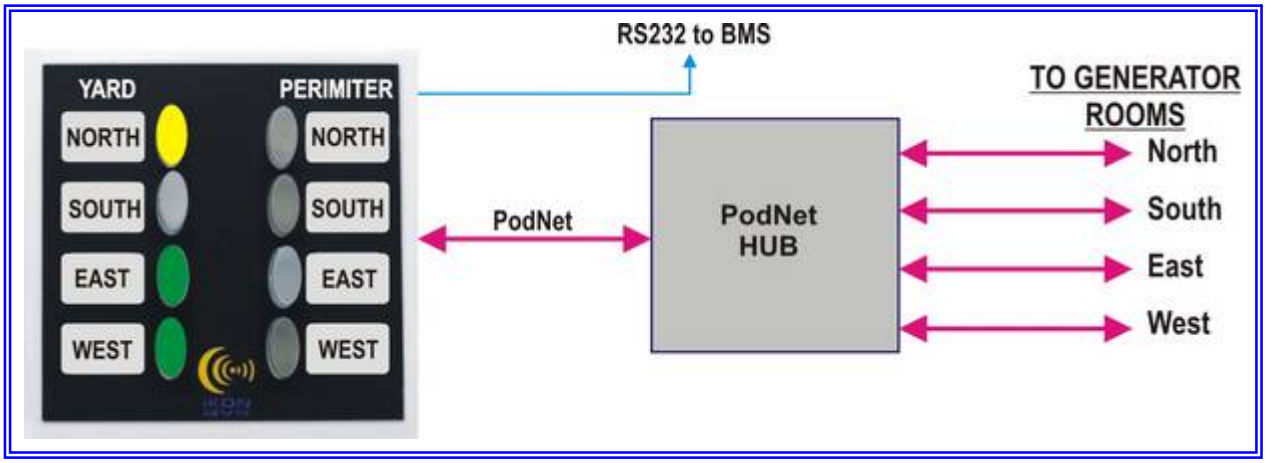
Here we see the internal power relays used to control the Set and Reset coils of the main lighting control contactors. Now its fortunate that these contactors have an auxiliary contact that's closed when it is on with this previously being used to illuminate the push button in the old control switches. But this is only half the story as we also need to know when it is Off. Now the obvious reaction is 'well if its not on then it must be off' but what if the cable is broken, you just wont know until you fail to get an on conformation, and by then it's to late. And so we have a fourth guideline in designing critical systems: -

Design point 4. 'You must monitor not only that the system has operated but that it will operate when so instructed.'

Returning to our diagram, here you will see that both the existing ON and new Off auxiliary contacts are fed into the controller for monitoring, with this information conveyed by the network to the main control room. I will come onto the network shortly but before leaving this diagram I should point out the use of dual power supplies. If the main contactors DC supply fails, then the contactors wont operate, but we need to let main control know this, hence the second supply. Similarly if the link to main control is lost, the system is programmed to activate the lights automatically.

Main Control

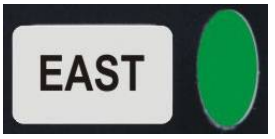
Whilst a touch screen would be swish, it's not really necessary for relatively simple control functions.



In this case a number of simple eight button panels where used but with bi-colour buttons. Remember that this system is for use by multiple prison officers and they have quite enough to do without fighting technology.

If the indicator is off, the lights are off.

If the indicator is Yellow, the command has been sent but its not yet confirmed that the circuit has operated.



If the indicators Green than the lights are active.

If the indicator is flashing yellow then the command has failed to operate the circuit – there is a faulty that need investigating.

If the indicator is flashing alternate yellow and green – there is a network failure.

Of course the officers only need to know that if it's flashing there a fault and they need to report it to maintenance. From the diagram you will note that the panel has a serial port that is used to send information to the building management system to allow faults to be automatically logged.

6. VA System Control

This particular site, not the one shown above, had an existing, if rather old, evacuation system. The new requirements were two fold, to provide a replacement system with dual graphical user interfaces offering a greater degree of control and user information and also to link this to a site wide independent monitoring system that would provide users with real time information on the system and its remote zones. The system also had to operate from either of two control points without compromise should one station still be linked but unusable. A further requirement was that the system had to operate over existing fibre optic cables.

As the site has an extensive computer network one easy solution would be to offer IP / Ethernet based control, but this was rejected as unfortunately to many products offer limited 'browser' type access for pre-defined control, so unless you are very skilled in writing Ethernet drivers and have access to the relevant information from the manufacture of the equipment you wish to use, you have in general insufficient control for a critical situation. It also goes further as some manufactures include a disclaimed with the licensing agreement leaving the onus on the installer if anything goes wrong. Now of course there are always exceptions and please let me know of any you find as they are few and far between.

A more major issue though is the network itself, as most existing networks are not designed for the robustness required for a critical system. If you have to use an existing network you will at minimum need to set up a VPN and assign subnets. You will also need to configure network switches to prioritise traffic, not something most network administrators will be happy with. Also, whose responsibility is it if the network goes down?

A short glitch or access delay, as can occur re-routing traffic via a spanning tree, is a relatively minor problem if you are just transferring a document, who can put their hand on their heart and say they have never had a computer lock up on them whilst waiting for the network? It's a different matter if you are waiting conformation of a critical condition prior to sounding the evacuation message.

And so we have a fifth guideline in designing critical systems: -

Design point 5. 'Unless you control the network, you can't rely on it for critical applications.'

Returning to the system design, there are three main elements to the control of a system of this type.

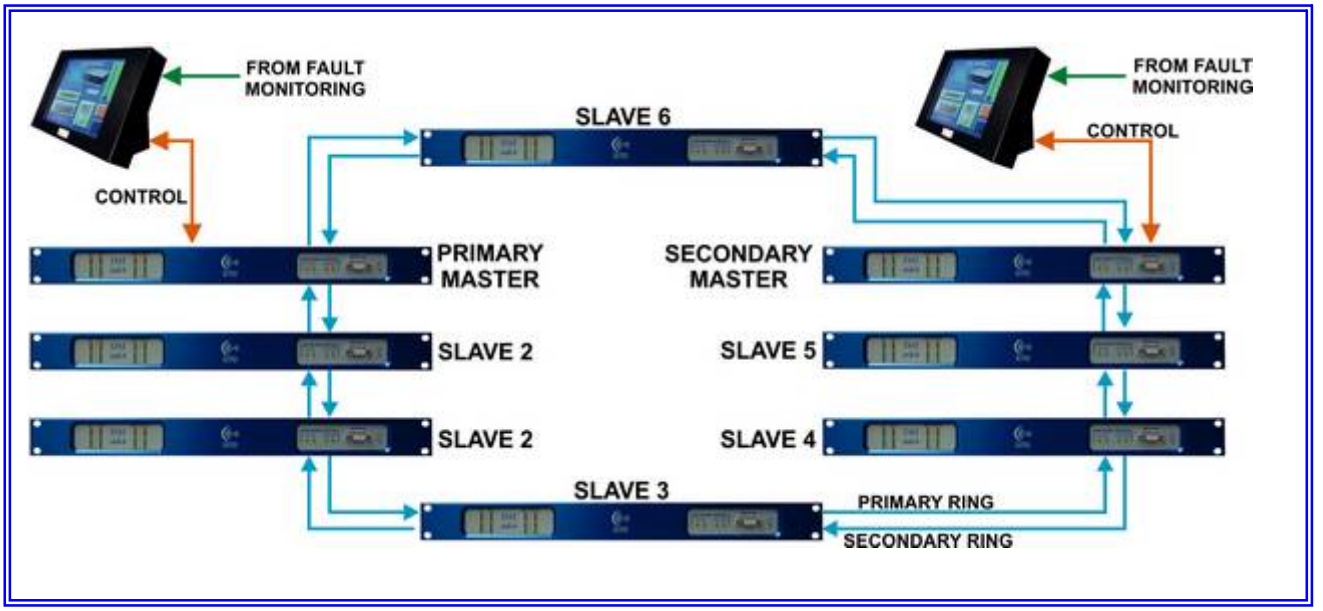
1. The graphical user interface (GUI) that is what the operators see and use. It needs not only to give a clear method of controlling the system but also accurate conformation that commands have been executed and not just that 'the button was pushed'.
   This is also the interface between the system and users for fault indication and a good method of checking the effectiveness of the GUI is to create an interactive demo and let the operators try it WITHOUT any instruction, this soon confirms if it is easy to use or not. We now have a sixth guideline in designing critical systems: -

Design point 6. 'Keep any GUI clear, uncluttered and intuitive to operate, at least for the critical tasks.'

2. Some audio signal processors incorporate the GUI as an integral part of the system. Whilst this creates a simple user interface, if the associated audio processor fails, then so does the GUI leaving users blind as to what has happened.
   Using a separate GUI removes this potential single point of failure. Of course you do need to set up a watchdog or handshaking to monitor the connection.

3. Whilst fault monitoring and reporting is mandatory for the actual audio circuits, the relevant standards are not as clear regarding the control and leave this to the designer and installer to carry out a risk assessment.
On a large distributed system, as per this example, the use of a secondary network for monitoring and reporting pays a dividend in providing a quick and easy method for faultfinding.
This was made abundantly clear on this site as with the previous system, a full system test and diagnostics took two to three days whilst with the new system it is completed and logged within a couple of hours.

OK, having covered the basics, lets delve into the system itself.



The above diagram shows a simplified version of the audio distribution system. The units selected use two independent fibre rings with both carrying audio and embedded control simultaneously. Each unit is configured to monitor the unit preceding it on both primary and secondary circuits and report any network faults to an independent fault monitoring network.

The GUI manages the control data and always sends a number of test packets even if no commands are initiated. These, as are the control commands, are only confirmed onto the GUI control screen when it has navigated the network.

We now have a seventh guideline in designing critical systems: -

Design point 7. 'Only indicate an operation when it has been confirmed and not only initiated.'

Returning to the schematic, you can see that we have both primary and secondary networks for resilience. It's unfortunately all to common when dual networks are used

to rely on one all the time and only change when a fault occurs, not a good idea. You only need to look at the recent problems experienced by Blackberry when the primary network switch failed and whilst there is a backup, this also had problems.

In our example system, testing of both networks is carried out automatically and continuously so the operational state is known at all times.

We now have an eighth guideline in designing critical systems: -

Design point 8. 'Regularly test all backup systems to ensure that they will work when required and as expected.'

So now we move onto our final scenario.

7. Command and Control Room

For our final example we are looking at a typical Command and Control room and whilst based upon a number of operational systems, this one is a fabrication created for the purpose of this seminar.

Before we can look at design and implementation we need to know what elements we are dealing with.

Lets start with a few displays – say 5.

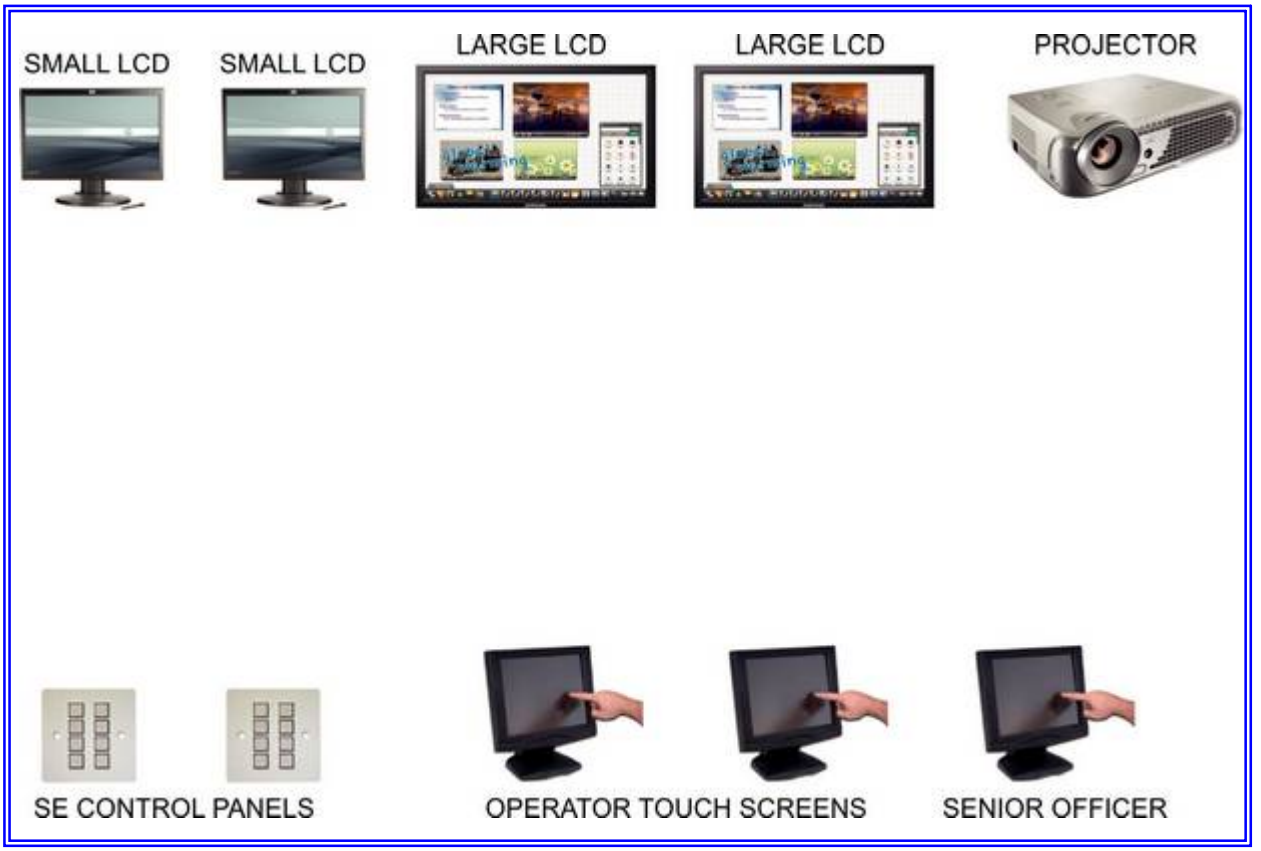
Display 1 is a large screen projector.
Displays 2 and 3 are large LCD screens.
Displays 4 and 5 are smaller screens located for use with two sets of subject experts (SE).

Next lets add the all important control panels and touch screens.

The two main operator desks need control over the projector & two LCD screens.

A senior office also requires a similar degree of control.

Finally the SE's need control over their local screens.



The next step is to include the possible input sources. Whilst these are more or less irrelevant for the principle of reliable control, lets allow for:-

10 x PC workstations and similar analogue XVGA sources.

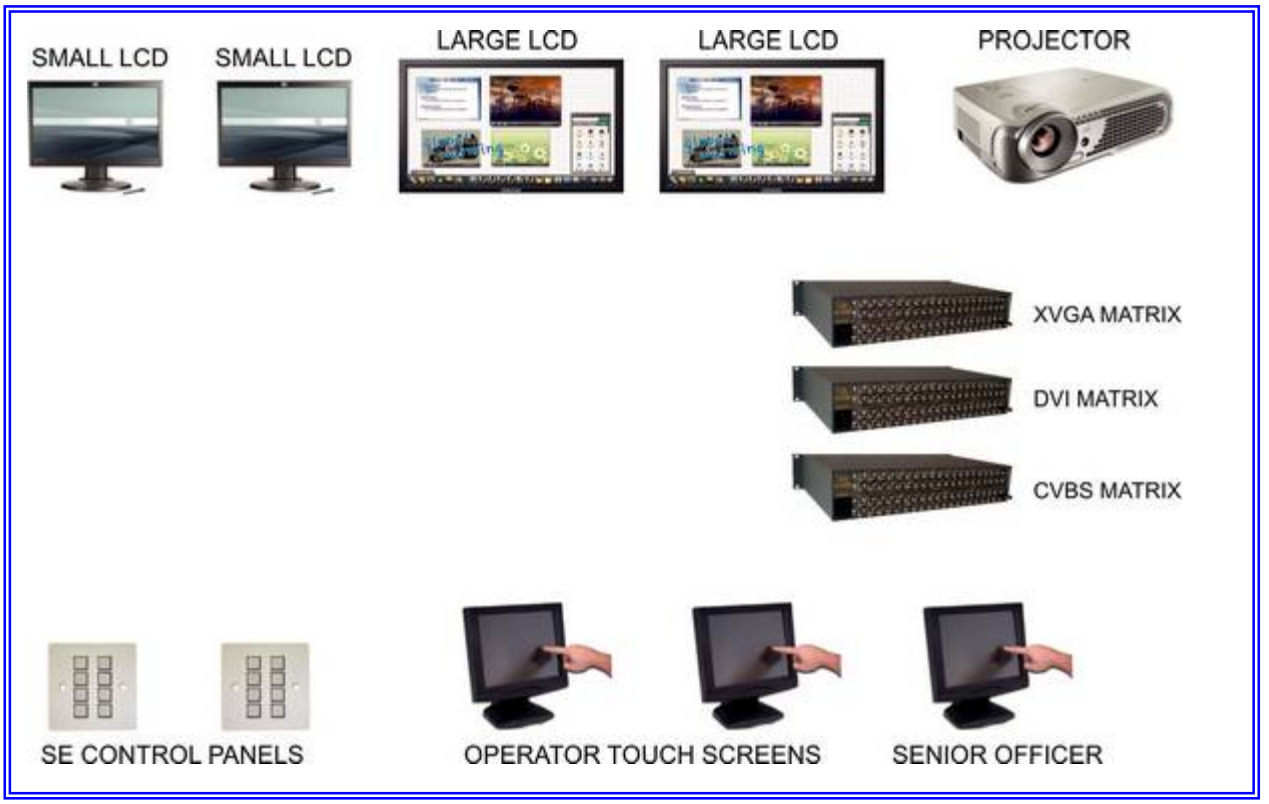
10 x Computers with DVI, HDMI and Displayport.

20 x Cameras with composite video.

[I have deliberately ignored IP cameras and similar sources as these require a greater level of complexity to handle and we just haven the time to cover these here. Perhaps next time?]

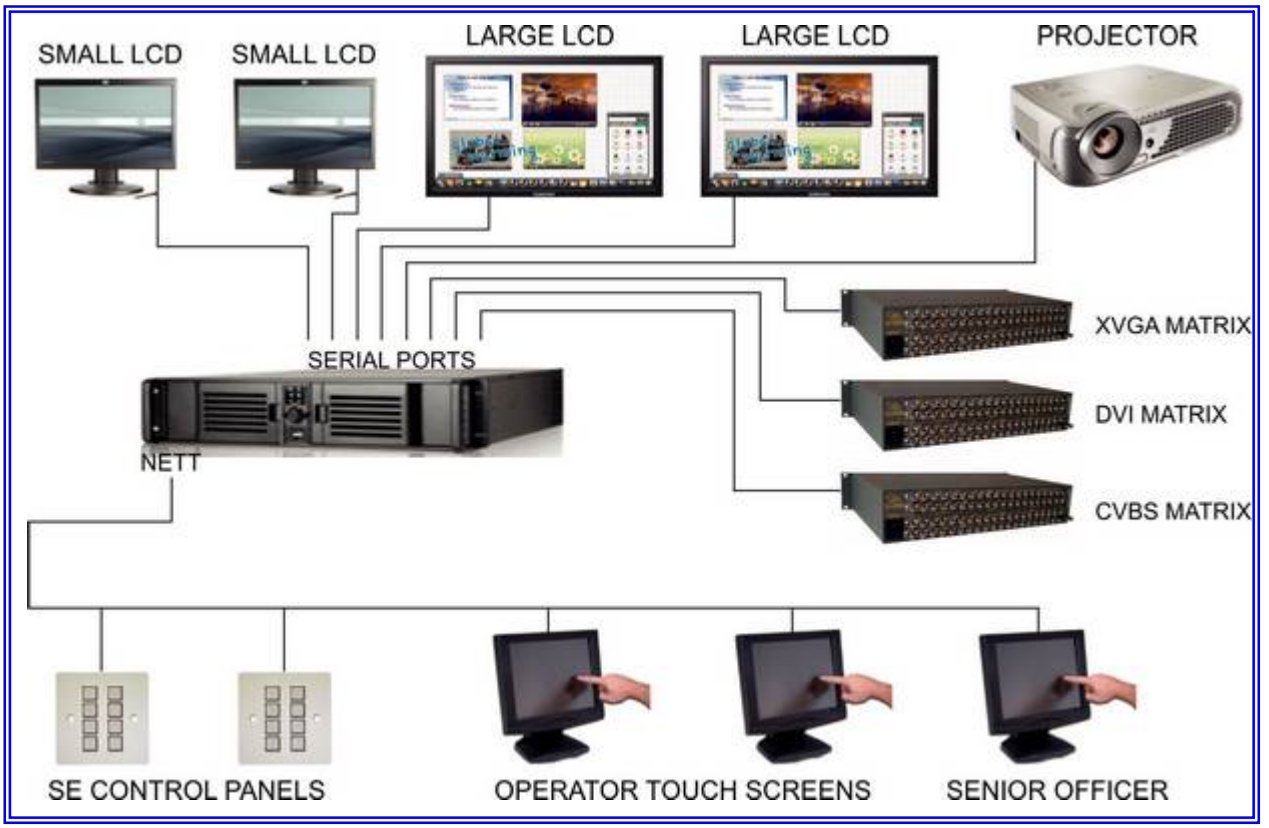
Finally lets add a couple of Freeview tuners, a DVD player and a Videoconference interface.

Now to handle these sources lets add three matrix switchers.

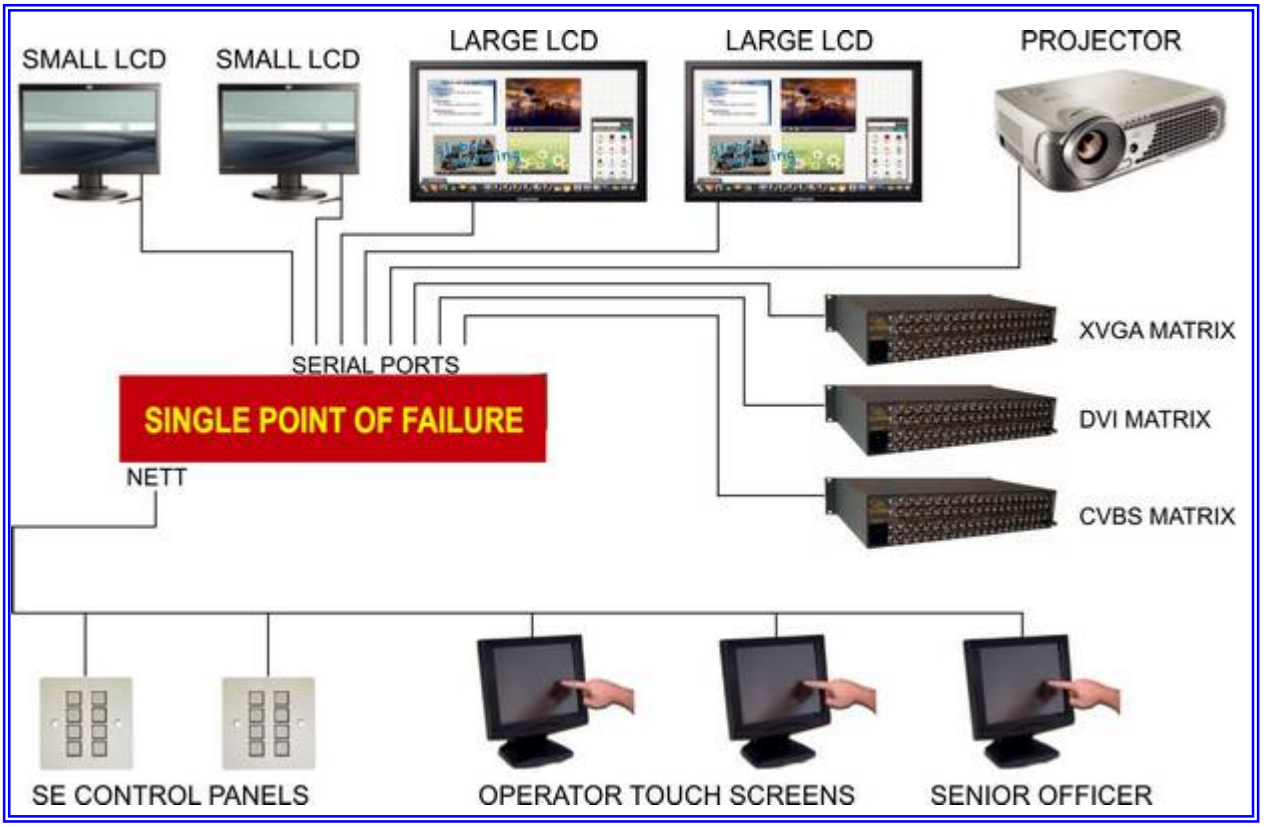


We now have a line up of equipment and all this needs to be controlled.

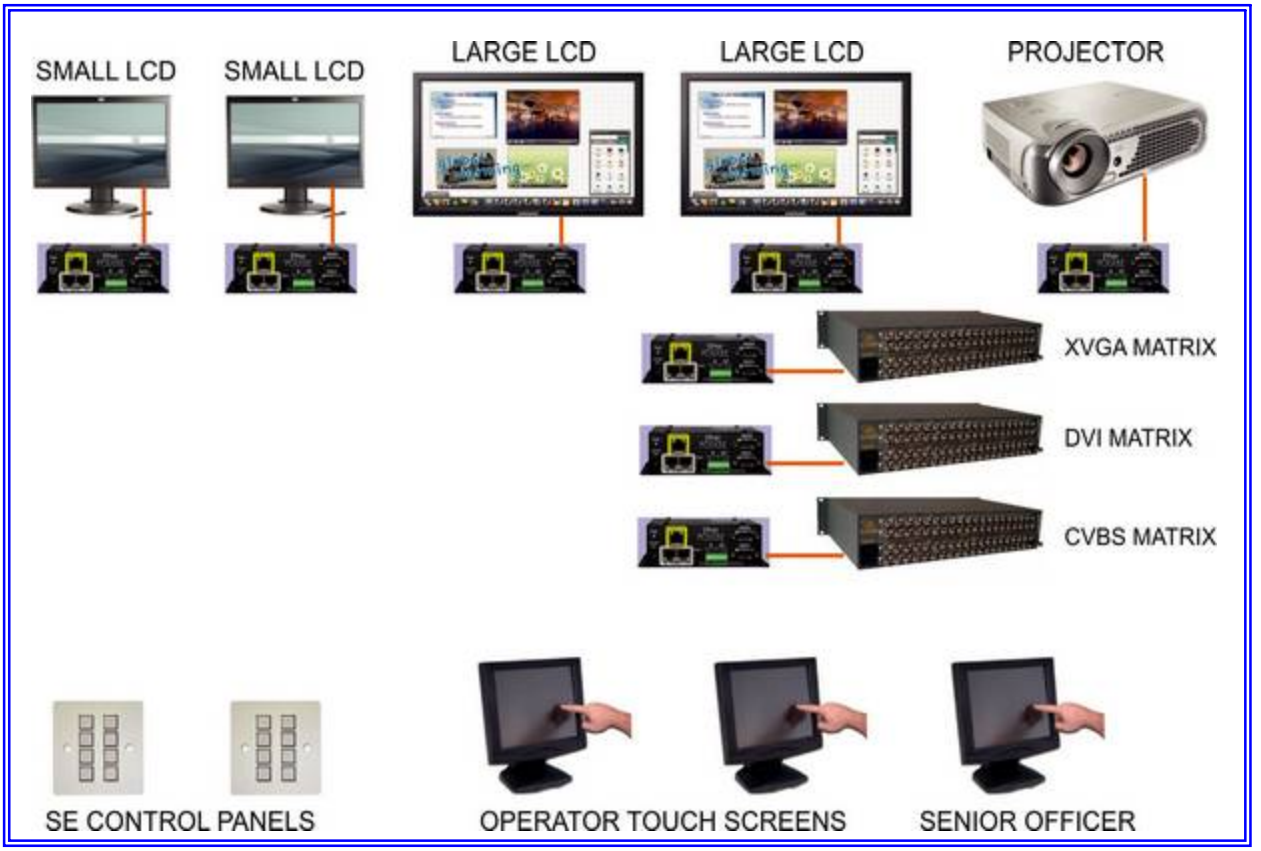
If this was a very large boardroom then perhaps we can use a central control processor and use its own network for the control panels and touch screens along with a set of serial ports to control the displays and matrix switches;-



But Oh Dear, we have a single point of failure.

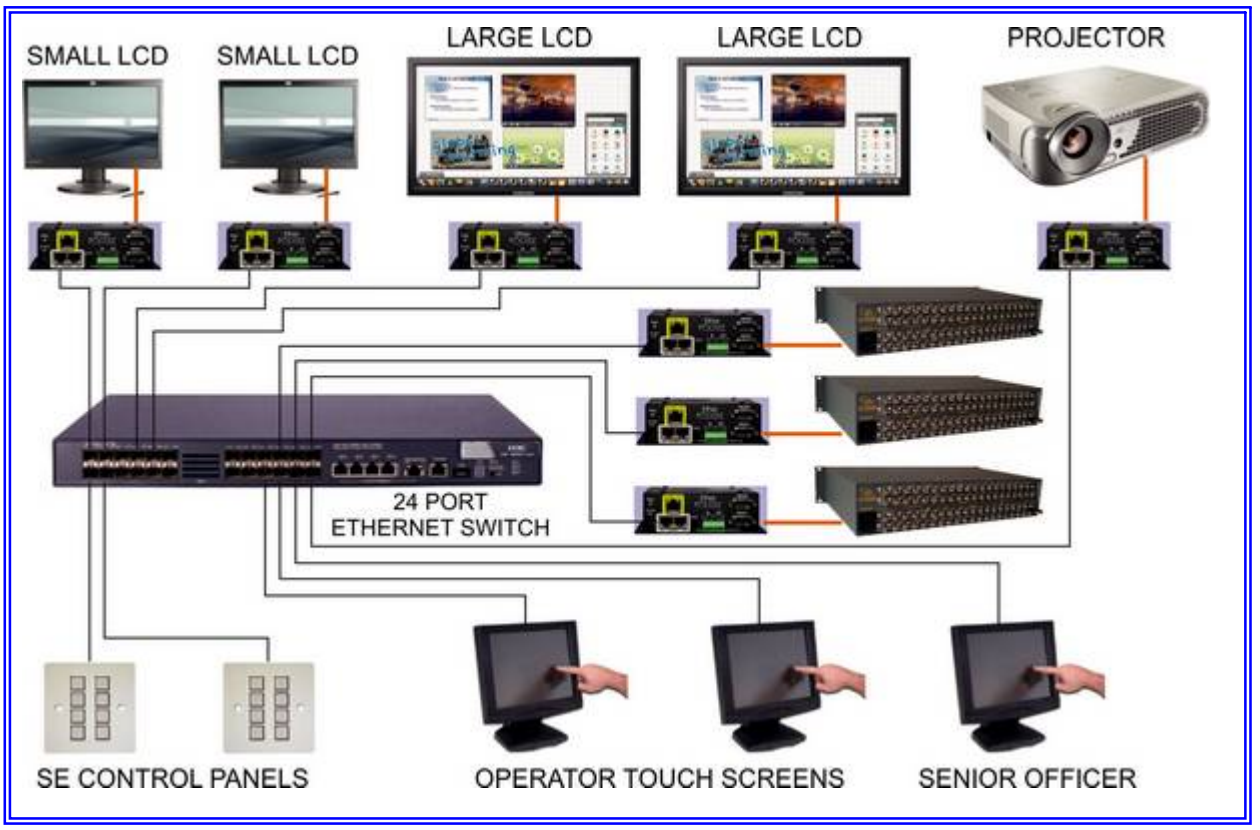


A far better solution, and one I have used with great effectiveness and robustness is to do as we did with the prison lighting, and deploy distributed processing.

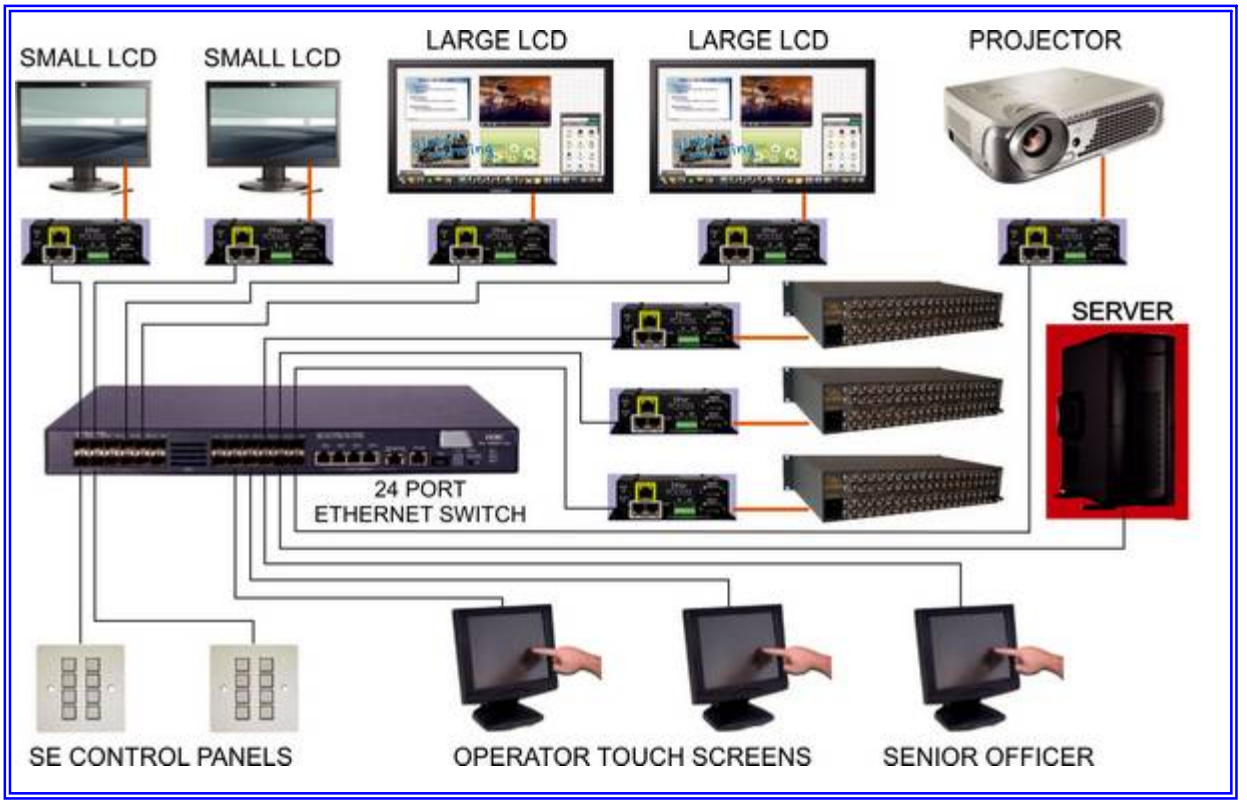


What we have here is for each matrix and each display we have a dedicated control interface. These each communicate with the matrix or display via RS232 and are configured to carry out the handshaking of commands we discussed right back at the beginning with the projector control example. Having assigned this level of 'housekeeping' to each controller we can minimise network traffic required for this important function.

Now this could be Ethernet but as we saw earlier, this has its potential drawbacks, but to be fair this would almost certainly be one of the situations where you supply and control the network switch.



A more major problem though is that you need to communicate from each control point to multiple controllers. You could use controllers with a web browser interface that supports multiple simultaneous users, but that's a very ineffective method of control and certainly has reliability concerns. Alternatively you could use a single PC or similar as a server and communicate with this.

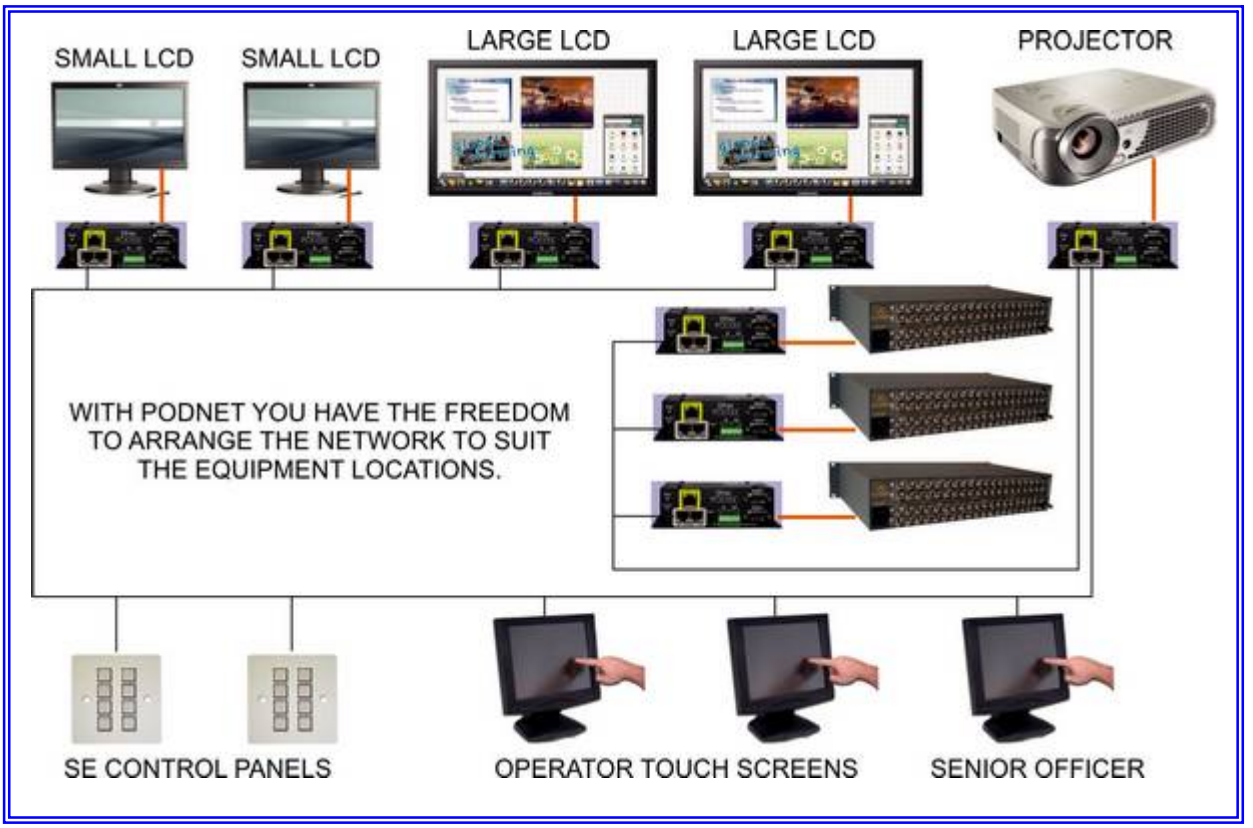


But here again we have the same single point of failure.

A Better way?

Whilst there are probably other methods of achieving the same resilience, in our case to eliminate this problem we use a buss that we call PodNet. This is a subset of the Control Area network (CAN) protocol, widely used in electrically noisy industrial environments and supporting a large number of ports and can be carried by multiple media. A major benefit for this application is that the data collision detection and network handling is embedded into the silicon and needs no additional programming from the system designer to implement.

In our version, each device on the network communicates instantly with others as soon as a command changes and all devices automatically resynchronise to each other every 30 second or so. This allows controllers, touch screens etc to be exchanged or added whilst the system is operating knowing that within 30 seconds they will have resynchronised with the complete system.



Here it is a simple matter of assigning network messages to each control panel and programming each control processor with the messages it needs to respond to. As each processor received messages directly, via the network, from any and all control panels assigned to it, any network delays are reduced and even in the event of a panel failing, the others will still operate the controllers. We now have our ninth guideline in designing critical systems: -

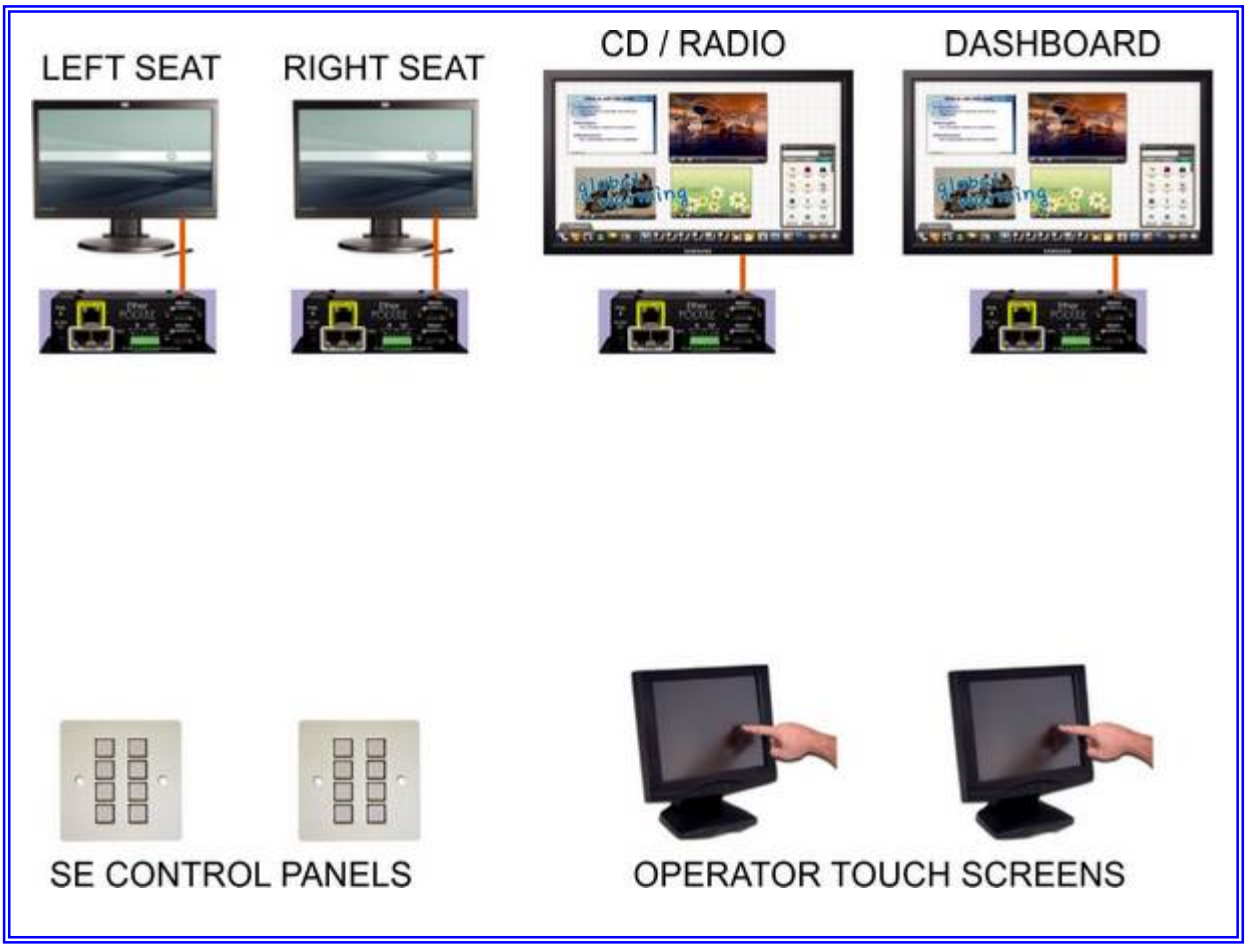
Design point 9. 'If a control panel fails it should not inhibit the correct operation of others – but must be reported to them.'

Buy AH! I hear you say, what if the processor controlling the matrix fails? Then it's the same as if the matrix fails but unlike the matrix, you can hot swap a spare knowing it will resynchronise within 30 seconds.

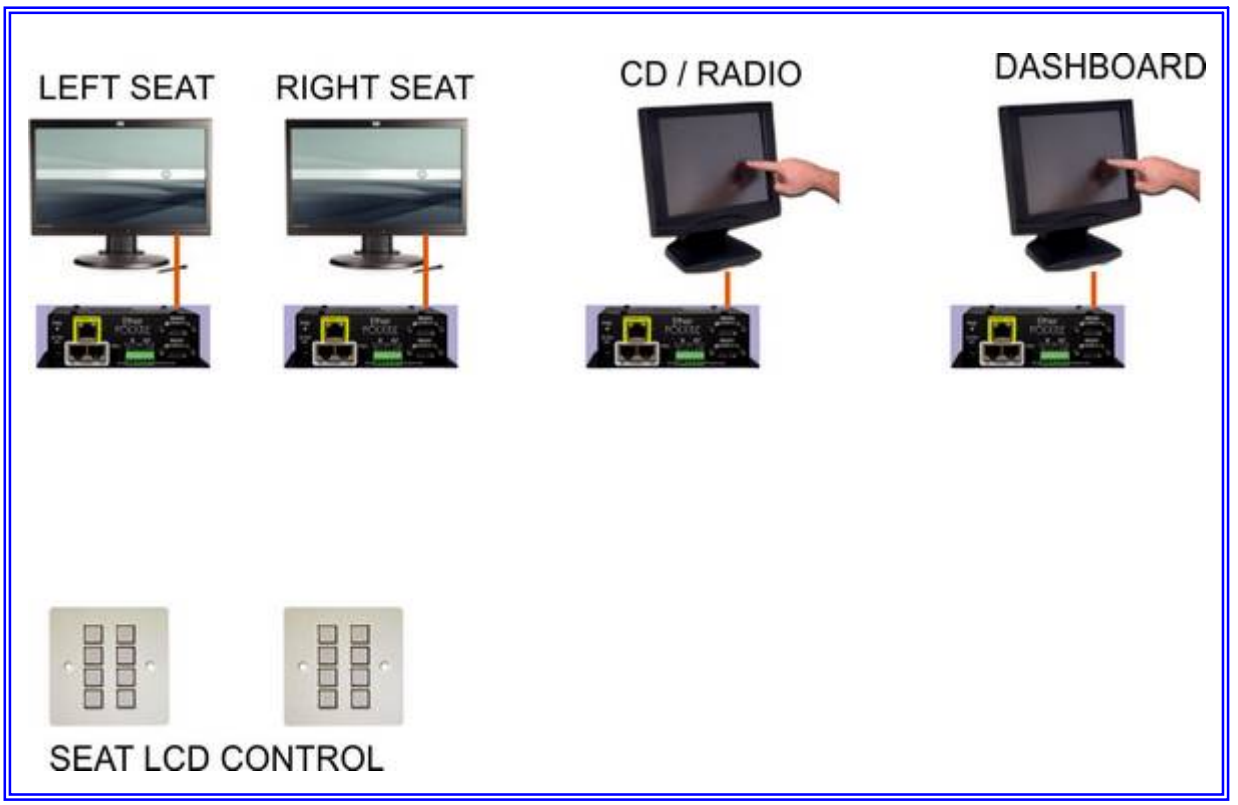
8. Everyday Application?

I can appreciate that to those unfamiliar with it, the CAN buss is probably an unknown factor, buts lets look at the application in a different way.

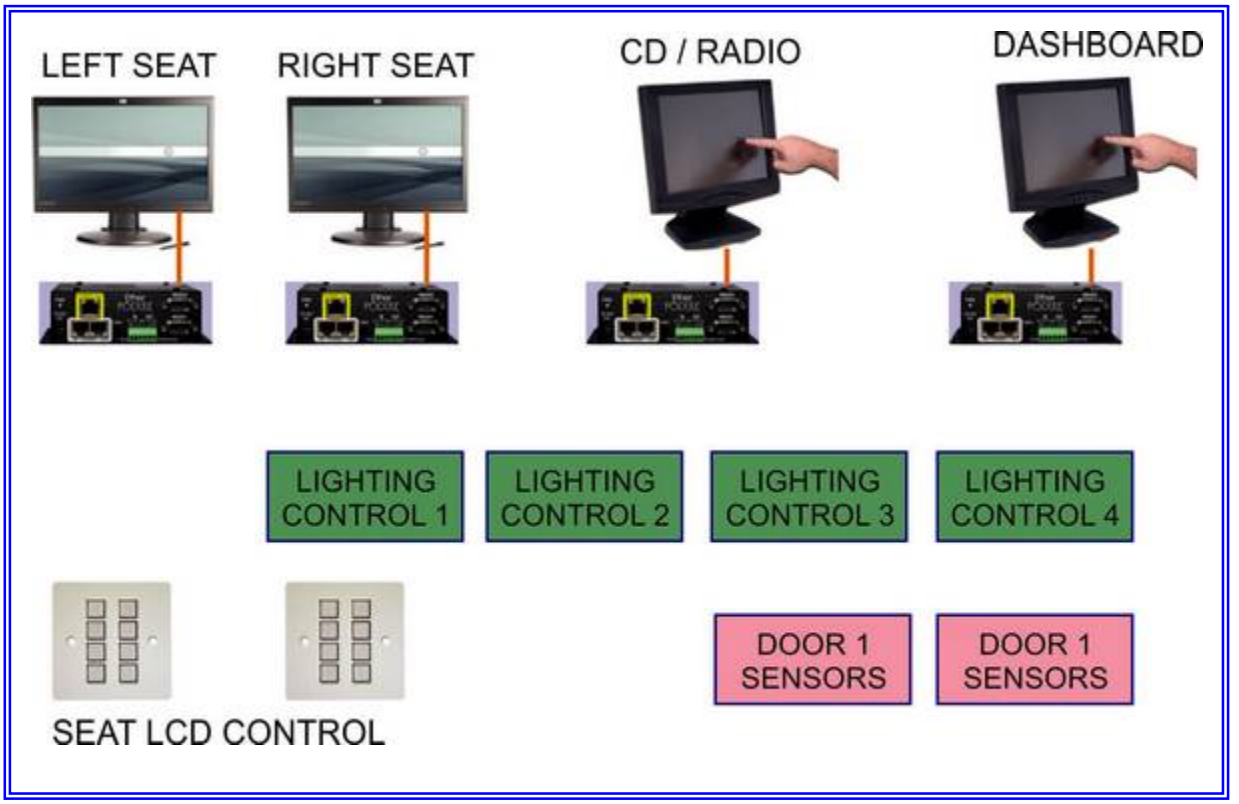
Lets first remove the projector and rename the displays, and while we are at it remove the matrix routers and one of the touch screens.



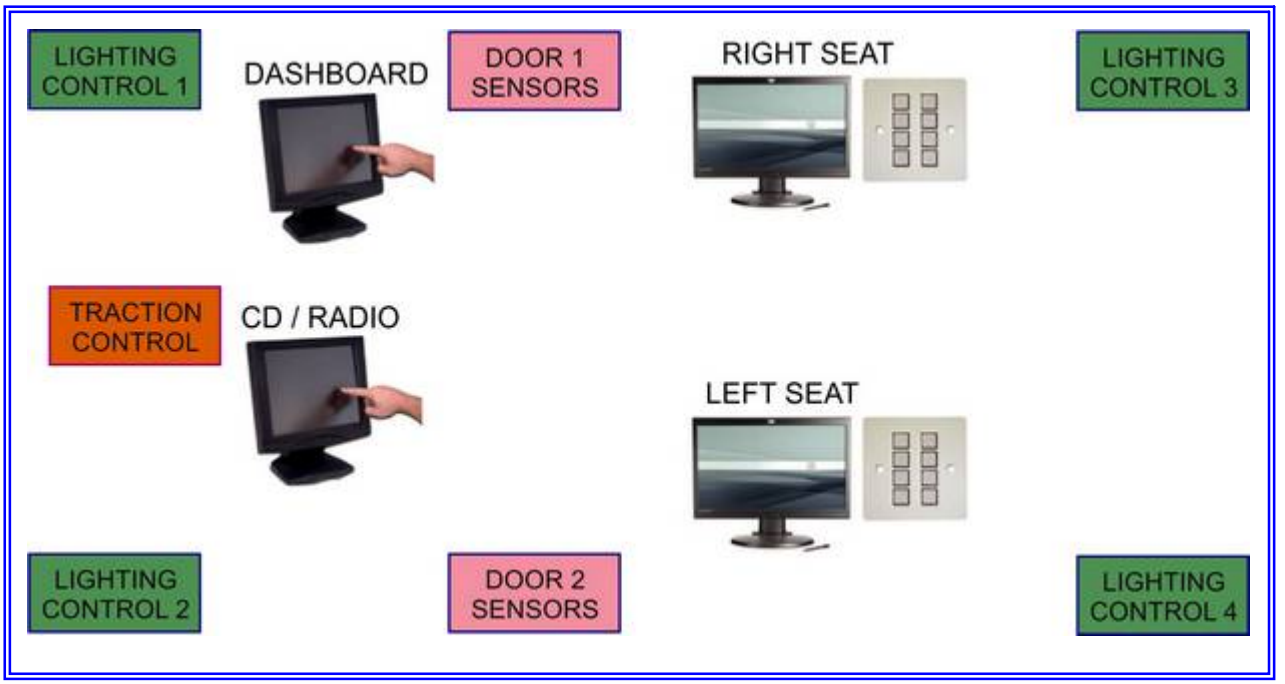
As the two main displays now have a more defined function, lets integrate them with the touch screens.



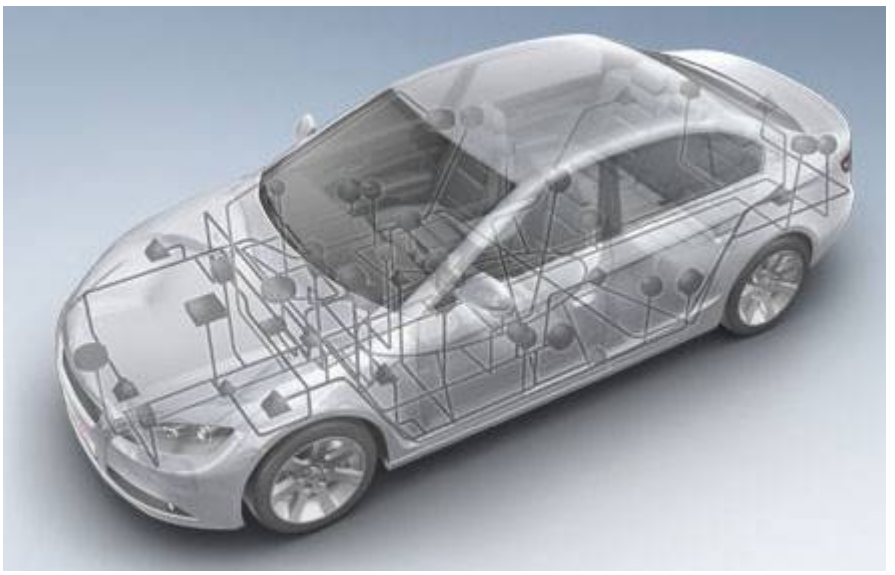
Now lets add four zones of lighting control, and sensors for if the doors are open.



Finally lets add traction control and re-arrange the diagram



Still confused? Perhaps if we look at it in a completely different way.



Now if a car doesn't rely on critical systems what does?

Now this brings us to the end and a summery of the design points.

9. Design Point Summery

Design point 1. **'Keep the user informed of the system status at all time.'**

Design point 2. **'Include a mechanism for error handling.'**

Design point 3. **'Carry out a risk assessment to define which parts of the systems are critical and which are not.'**

Design point 4. **'You must monitor not only that the system has operated but that it will operate when so instructed.'**

Design point 5. **'Unless you control the network, you can't rely on it for critical applications.'**

Design point 6. **'Keep any GUI clear, uncluttered and intuitive to operate, at least for the critical tasks.'**

Design point 7. **'Only indicate an operation when it has been confirmed and not only initiated.'**

Design point 8. **'Regularly test all backup systems to ensure that they will work when required and as expected.'**

Design point 9. **'If a control panel fails it should not inhibit the correct operation of others – but must be reported to them.'**