Catastrophic Failure Evaluation *

John M. Macdonald[1]
Los Alamos National Laboratory
M.S. E516

Howard Nekimken[2]
Los Alamos National Laboratory
M.S. E516

Rick Picard[3]
Los Alamos National Laboratory
M.S. F600

Keith Olson[4]
Los Alamos National Laboratory
M.S. E516

Adam Bates[5]
Los Alamos National Laboratory
M.S. E516

Augustine Ortiz[6]
Los Alamos National Laboratory
M.S. E516

Keywords

System Criticality Value, Criticality Values, Process Control, Catastrophic Failures, Redundancy, Internet, SCADA, Industrial Control, Networking, Vulnerability, Integrity.

Abstract

The random events of catastrophic failures impacting process control systems and networks are the topic of this paper. In an unpredictable catastrophic event such as a lighting strike, power outage, or failures only affecting certain portions of the overall system, how is the integrity of a system determined? This investigation includes overall the system impact on random catastrophic failures. System scenarios are evaluated with a method for determining impacts on these systems. Criticality Values and a composite System Criticality Value are introduced. A system vulnerability value is derived and investigated. A suggestion for mapping this methodology onto a network is encouraged.

* A special note of appreciation goes to Joel Williams, Pat Burg, Steve Yarbro, Steve Schreiber, Don Mullins, Noah Pope, Max Evans and Alan Hoff for reviewing this paper.

Work performed under the auspices of the United States Department of Energy.

[1] jmac@lanl.gov
[2] hnek@lanl.gov
[3] picard@lanl.gov
[4] kolson@lanl.gov
[5] adamb@lanl.gov
[6] aortizjr@lanl.gov

1. Background

In the normal life of a system it is not uncommon to experience random catastrophic failures of a system. Statistically, random catastrophic events appear rarely. However, events such as a power outage can have a major impact on a system. It is very common to experience lighting strikes during summer months that can randomly effect a process control or network system.
For example, during a summer thunderstorm an electrical strike could occur disabling a Supervisor Collection and Data Acquisition (SCADA) computer. The overall system may contain a Programmable Logic Controller (PLC) which was unaffected by the lighting strike.
The PLC still has the capability to control the process; however, the Human Machine Interface (HMI) is disabled so human intervention of the process is very difficult. Is the system completely inoperative?

In the above example the process control subsystem is still able to function and the SCADA computer may later be replaced. Therefore, only half of the system is not operating correctly.
In everyday life, we are occasionally faced with catastrophic failures of systems.
Known phenomena such as experiencing car problems or even having Random Access Memory problems with a computer can occur during some point in life. In this paper, we present some ideas to evaluate the possible impacts of catastrophic failures on systems.

As a comparison, the longstanding system evaluation methodology, the Emergency Medical Service (EMS) system, uses the process of triage for sorting patients into categories of priority for care and transport based on the severity of injuries and medical emergencies. "The sorting of patients begins as soon as trained personnel reach the sick and injured persons. Through careful triage, the patient can be placed into one of three categories: highest priority, second priority, and lowest priority"[1]. The methodology covered in this paper attempts to mathematically assign values for system evaluations and does not address priority levels. In addition, mathematical reliability for system evaluations is not specifically addressed in this paper. During the process of triage, a patient assessment is performed to obtain measurements for the triage process. Measurements such as pulse, respiration, blood pressure, temperature, skin color, dilation of pupils, state of consciousness, paralysis or loss of sensation are usual information obtained during the triage process. A similar measurement approach is contained in this paper. The methodology suggested in this paper evaluates the effects of catastrophic failures impacting process control systems; however, this methodology may be applied to other areas of engineering and science disciplines.

2. Method

In an attempt to understand the effect of catastrophic events on a system, the overall system is evaluated by the sums of all the system components. The overall system usually can be divided into smaller subsystems.

A System Criticality Value (SCV) may be derived by adding the sum of its subsystems. The ssx notation indicates a subsystem. Subsystem elements are defined by Criticality Values (CV) and arbitrarily defined based on the failure time, recovery costs, resources available, impact on the system controlling properties, and concentration point of system activities. CV values ordinarily range from 0 to 1. Lesser CVs can be assigned to elements of subsystems that have an impact but would not be overwhelming or time critical for the system. These lesser CVs can be expressed as a fraction, for example 0.80 (i.e., thought of as a percentage). Less important elements in the subsystem can assume smaller CVs. Since an overall system has the capability of existing in a state not fully functional and still retain some functionality, it can exist between whole numbers of 0 and 1. It is also important to notice the higher the CV value, the more critical the element is to the system and as the CV approaches 0 the less critical. This approach allows for possible binary mapping, which is, explained further in the Future section of this paper.

The basic formula is:

$$SCV = \{(ss1cv) + (ss2cv) + (ss3cv)\ldots\}$$

or

$$SCV = \sum_{i=1}^{Nssi} ssi$$

Where ssi is the sum of the Criticality Values of a subsystem.

3. Network Example Application

This method can be applied to a network scenario with the following diagram:

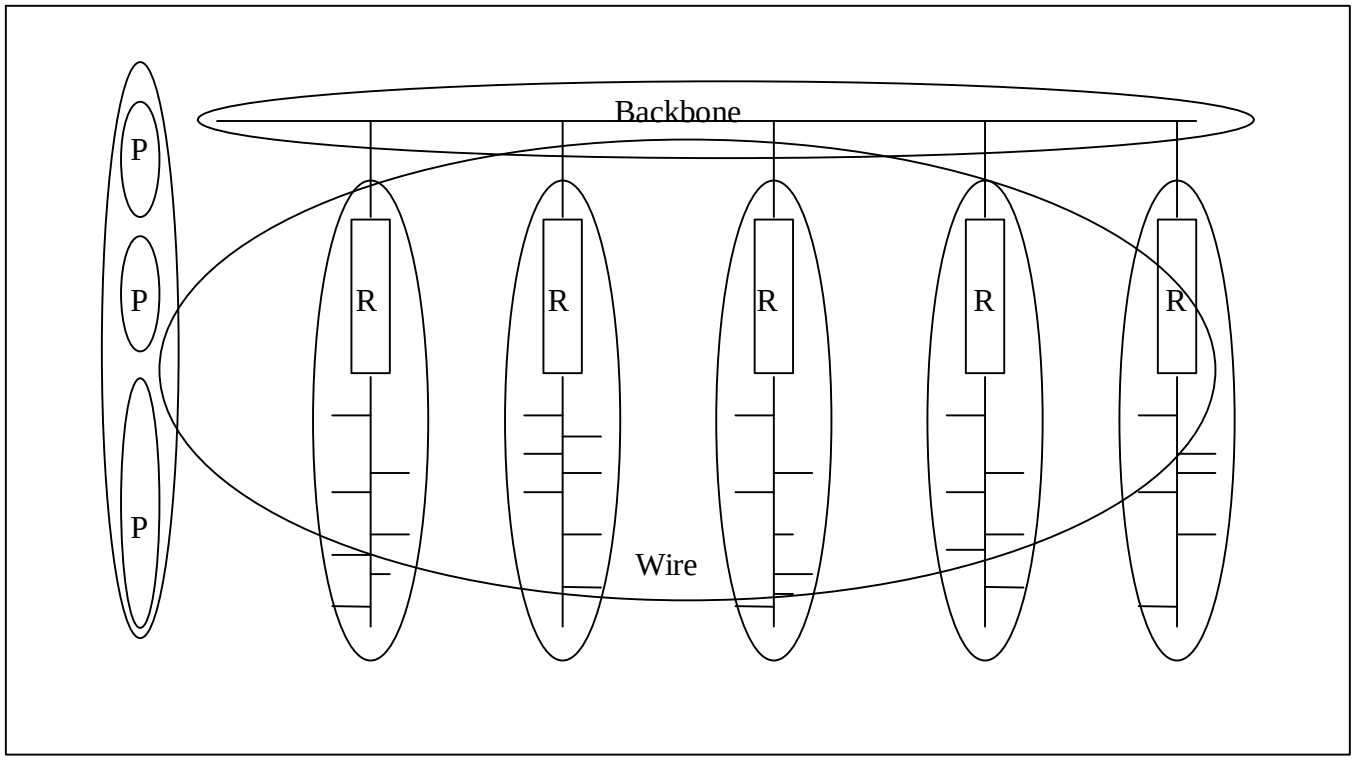

Diagram 1. Network Example.

The ellipses indicate subsystems and the rectangles indicate routers. The network is a TCP/IP network.

For the above diagram the following key subsystems notations apply:

Backbone = Network Backbone
R = Router which includes user nodes
P = Power subsystems
Wire = Network Wiring

The following subsystems are not shown on the diagram:

BAND = Network Bandwidth	Soft = Software contained in system
EnvOp = Environmental Operating parameters	CI = Criticality of Information
Mhs = Maintenance Hardware and/or Software	Age = Aging of system

An SCV is comprised of subsystem CV definitions contained within the total system of interest. Subsystems can have values ranging between 0 and 1 indicating an intermediate operational status, a percentage of fully operational.

In the network example the formula for calculating the SCV is as follows:

SCV = {(Backbonex +Backbonex…) + (Rx + Rx…) + (Px+Px…) + (BANDx + BANDx…) + (Wirex +Wirex…) + (Softx + Softx…) + (EnvOPx + EnvOPx…) + (CIx + CIx…) + (Mhsx + Mhsx…) +(Agex + Agex…)}

The backbone is comparable to a carotid artery providing high-speed data flow through the system. Since the backbone is critical to overall system performance, if it goes down the system will not function. Therefore a CV of 1.0 is assigned.

The router subsystem, R, which contains the nodes, is an interesting subsystem in which the routers are assigned a CV of 0.80 and the user node a CV of 0.20. An exception is higher CVs for user nodes such as when your supervisor's machine is inoperable. Dynamically one can assign the CVs as applicable.

The power system, P, can span across various electrical circuits, by allowing one circuit to be operational while another circuit is down. A CV of 1.0 is applied for each system and associated electrical circuits.

Network bandwidth, BAND, can be measured with network analyzers and usually runs no more than 9% capacity, so a CV of 0.09 is assigned.

The wiring subsystem, Wire, is an interesting subsystem to assign a CV. If the backbone is down then no other communication is allowed between the other routers. However, the router segment can act independently, thus allowing the segment to operate independently of the backbone. Dependent on the organization's use and the backbone's physical location of the wire, the CV may be derived differently. For this example, 0.70 is assigned for backbone requirements and 0.30 for the segments.

The Soft subsystem is the software used to run the system. Based on down time experienced with software upgrades, revision levels, applying patches, and Y2K problems. In this example a CV of 0.02 is assigned.

Environmental operation parameters, EvnOp, are composites of the total system that are determined by operational environmental standards (i.e. temperature, pressure) recommended by the manufacturer. The CV of 0.01 is assigned for the EvnOp subsystem for this evaluation.

CI or the Criticality Information subsystem is defined by how important the information is to normal operations of the organization. CI needs to be determined by your organization and is based on whether the system can function in a limited capacity without the information or is it completely inoperative if this information is not available to the organization. A CV of 0.80 is applied for this subsystem because of its importance and the organization's strong dependency on this subsystem.

The maintenance on hardware and/or software, Mhs, subsystem can effect the overall stability of the system and is a composed of estimated downtime for a year. In this case the number is estimated at 0.08 downtime.

Age or Aging subsystem is defined as the current age of the system. For example, if the system lifespan is 10 years and the system has been running for 2 years then the Age CV is 0.20.

The following weighted process diagram outlines the example for a network system:

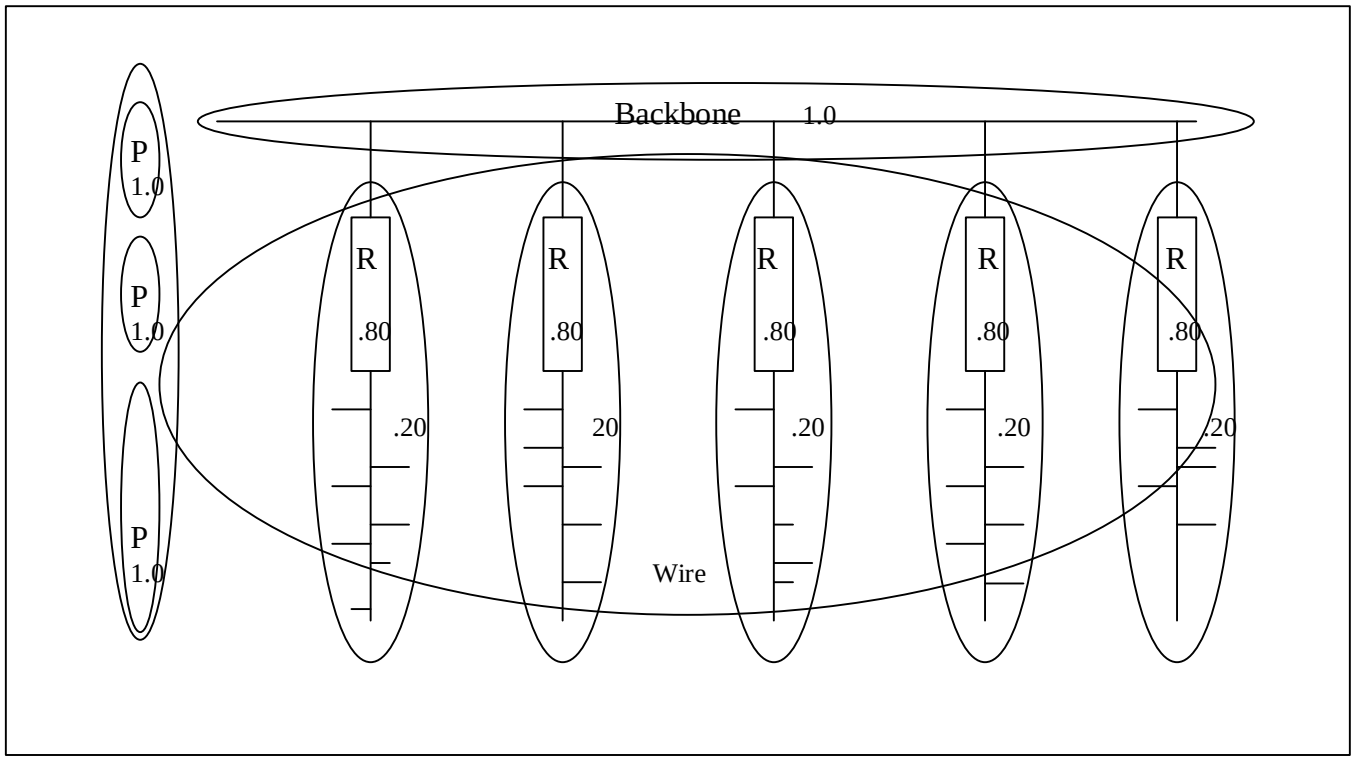

Diagram 2. Modeled Network Example.

The evaluation of the network example is:

SCV = {(Backbonex +Backbonex…) + (Rx + Rx…) + (Px+Px…) + (BANDx + BANDx…) + (Wirex +Wirex…) + (Softx + Softx…) + (EnvOPx + EnvOPx…) + (CIx + CIx…)+ (Mhsx + Mhsx…) + (Agex + Agex…)}

11.20 = {(1.0) + (.80 +.20 +.80 + .20 + .80 + .20 +. 80 + .20 +.80 +.20) + (1.0 + 1.0 + 1.0) + (.09) + (.70 +.30) + (.02) + (.01) + (.80) + (.08)+ (.20)}

One can gain insight to overall system integrity by evaluations of the subsystem elements. As the element values approach one, this may suggest the need for redundancy. Also of interest is the BANDx CV, which is 0.09. This is the bandwidth at a given instance. If BANDx would equal 1.0, then the network would be in a state of saturation and would be inoperable. The same approach is applied with Softx and EnvOPx, while CI is an arbitrary independent value. It is of interest, this method can employ CV values that can be dynamically allocated based on the present time. The overall dependability of the system can be improved by taking the 1.0 CV single elements and dividing them into multiple elements. For example, a secondary backbone line can be added, or routers which include switching units that switch over when a router is inoperable during peak bandwidth times. However, there is a point of diminished return on investments concerning the implementation of redundancy for a system [2].

4. Process Control Example

The following process diagram outlines an example for a process control system:

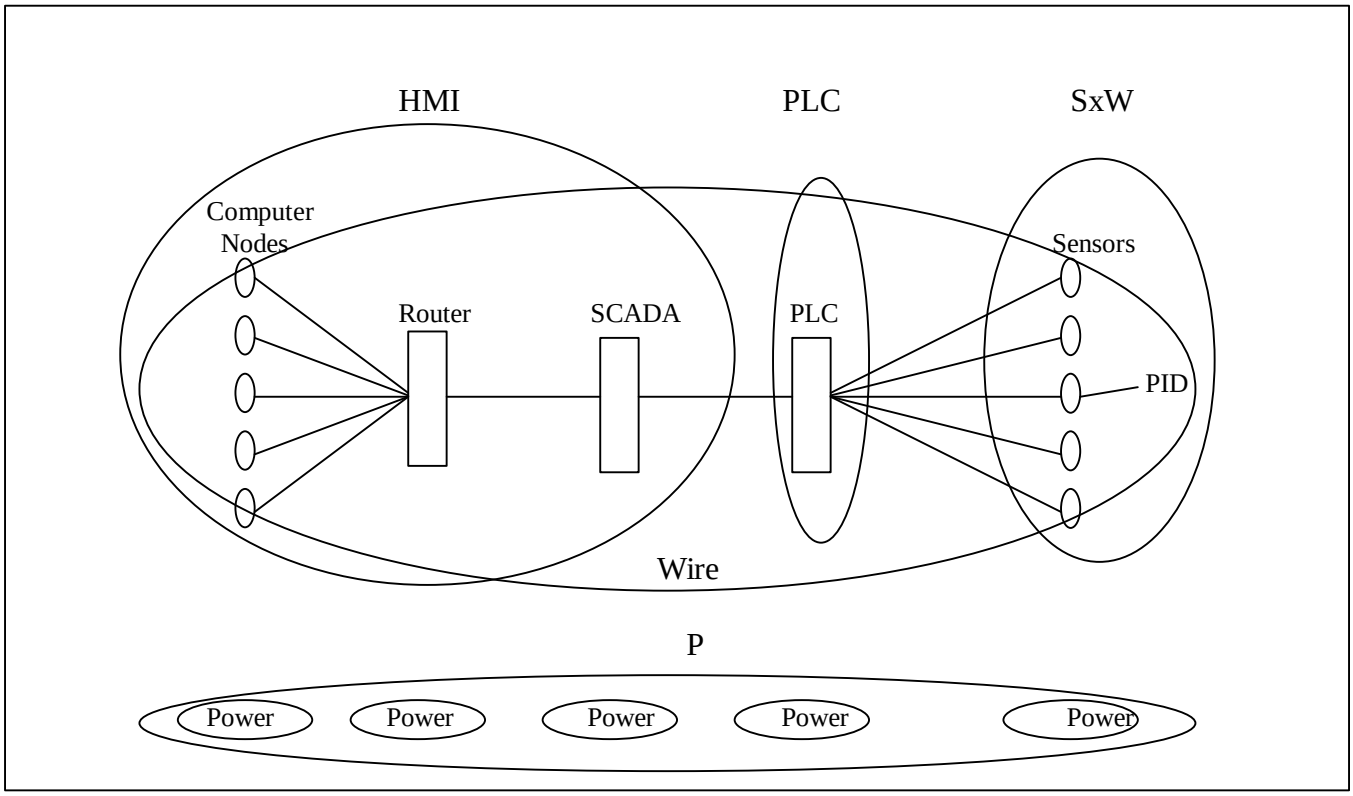

Diagram 3. Process Control Example.

For the above diagram the following key subsystems are applied:

HMI = Human Machine Interface systems
PLC = Programmable Logic Controllers
SxW = Sensors with Weighted values
P = Power subsystems
Wire = Wiring subsystem

The following subsystems are not show on the diagram:

BAND = Network Bandwidth	Soft = Software contained in system
EnvOp = Environmental Operating parameters	CI = Criticality of Information
Mhs = Maintenance Hardware and/or Software	Age = Aging of system

The SCV formula is as follows:

SCV = {(HMIx +HMIx…) + (PLCx + PLCx…) + (SxW+SxW…) + (Px + Px…) + (Wirex +Wirex…) + (BANDx + BANDx…) + (SOFTx + SOFTx…) + (EnvOpx +EnvOpx…) + (CIx + CIx…) + (Mhsx + Mhsx…) + (Agex + Agex…)}

The HMI subsystem defined is of interest because the SCADA, router and computer nodes are contained in this subsystem. This system could be broken down into further subsystems for evaluation. Since a historical database of the process exists on the SCADA machine, a user has the capability to view historical data. If the historical data is all the user is concerned about, it would be of little concern to the user if the process is inoperable. If a computer node is down or a user is unable to access process control data then the CV of computer node will go up appreciably.

If a subsystem with one element has a CV equal to one, that subsystem would be a great candidate for redundancy. In the above example, the PLC is a prime candidate for considering redundancy. One way redundancy can be incorporated into this subsystem is by tying the Proportional Integral Derivative (PID) loop control to sensors.

The SxW sensor subsystem has a weighted value incorporated into the evaluation for one sensor which contains the PID Loop. The sensor is a control point for the process, and therefore it has a higher value in the subsystem than other sensors that are important but do not control the process. An actual example of this system is a column with a control thermocouple at the bottom of the column. This sensor controls the process. The other sensors can be lost without greatly impacting the overall control of the system. For example, the PID sensor could be weighted at 0.80 whereas the other four sensors would have a rating of 0.05 apiece.

The P subsystem is composed of the electrical power circuits that supply other subsystems. Since a system can cover large areas, usually the power is on different circuits. Isolated, regulated electrical power with battery backup can be critical to the higher weighted or essential elements.

The Wire subsystem's importance can readily be seen by losing the system when wires associated with a working system are cut or removed. Wiring to critical components of the system is given higher weights than wiring to the lower weighted components.

Network bandwidth indicated by the BAND subsystem covers the whole networked system and can vary in instances of time based on what users are utilizing the system.

The Soft subsystem indicates the software used throughout the system and can inherit problems associated with software incompatibilities, revision level, upgrades, viruses and even Y2K problems.

Environmental operating parameters, EnvOp, can have a large impact on a system.
For example, the computer display on a SCADA node contained in a rack can experience heat related failures. Therefore, the entire system can be impacted by the loss of a computer display, a dependency on environmental conditions.

The CI or Criticality Information variable is dependent on who evaluated it. For example, the person responsible for the process would probably apply a higher CV than a network administrator who maintains the networks. Different people could reasonably assign different CV values to different hypothetical circumstances: by their very nature, some catastrophic events have never occurred to the system of interest and assessing potential damages involve educated guesswork.

The Mhs maintenance of hardware and/or software, is typical maintenance of the system including new hardware/software upgrades, patches, calibration, diagnostics, repair and other related activities.

Again the BAND, SOFT, EvnOP, CI and Mhs subsystems are not defined on the diagram and are assigned 0.09, 0.02, 0.05, 0.60, 0.08 respectively for this example.

Age subsystem is the current age of the system divided by the projected lifespan of the system. For this example we will again use an age of 2 years and a projected 10-year system lifespan or 0.20.

An introduction of a random failure such as a lighting strike can effect one or more subsystems. Analysis of the critical components may be evaluated, and redundancy can be built into a system increasing the overall stability. However, by increasing the number of subsystems, the complexity of the analysis increases as well as the probability of error in the analysis of the system.

An evaluation of the system is diagrammed as follows:

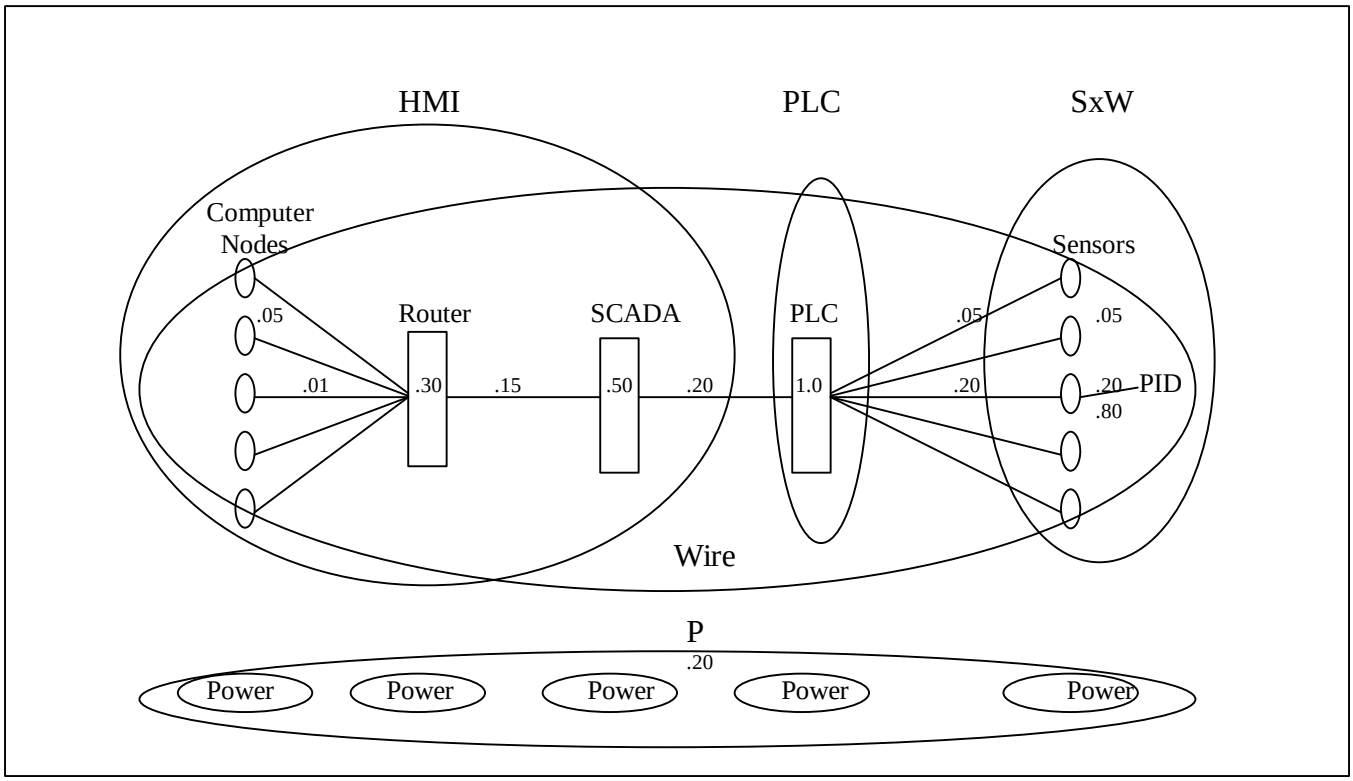

Diagram 4. Modeled Process Control Example.

The mathematical evaluation appears as follows:

SCV = {(HMIx +HMIx…) + (PLCx + PLCx…) + (SxW+SxW…) + (Px + Px…) + (Wirex +Wirex…) + (BANDx + BANDx…) + (SOFTx + SOFTx…) + (EnvOpx +EnvOpx…) + (CIx + CIx…) + (Mhsx + Mhsx…) + (Agex + Agex…)}

6.04 = {(.50 + .30 + .05 +.05 +.05 +.025 + .025) + (1.0) + (.80 +.05 +.05 + .05 + .05) + (.20 + .20 + .20 + .20 + .20) + (.01+.01+.01+.01+.01+.15 + .20 +.05 + .05 +.20 + .05 +.05 +.20) + (.09) + (.02) + (.05) + (.60) + (.08)+(.20)}

A more accurate summary of the overall process control system can be derived if the total network and process control system evaluations are combined. In this case the diagram would be as follows:

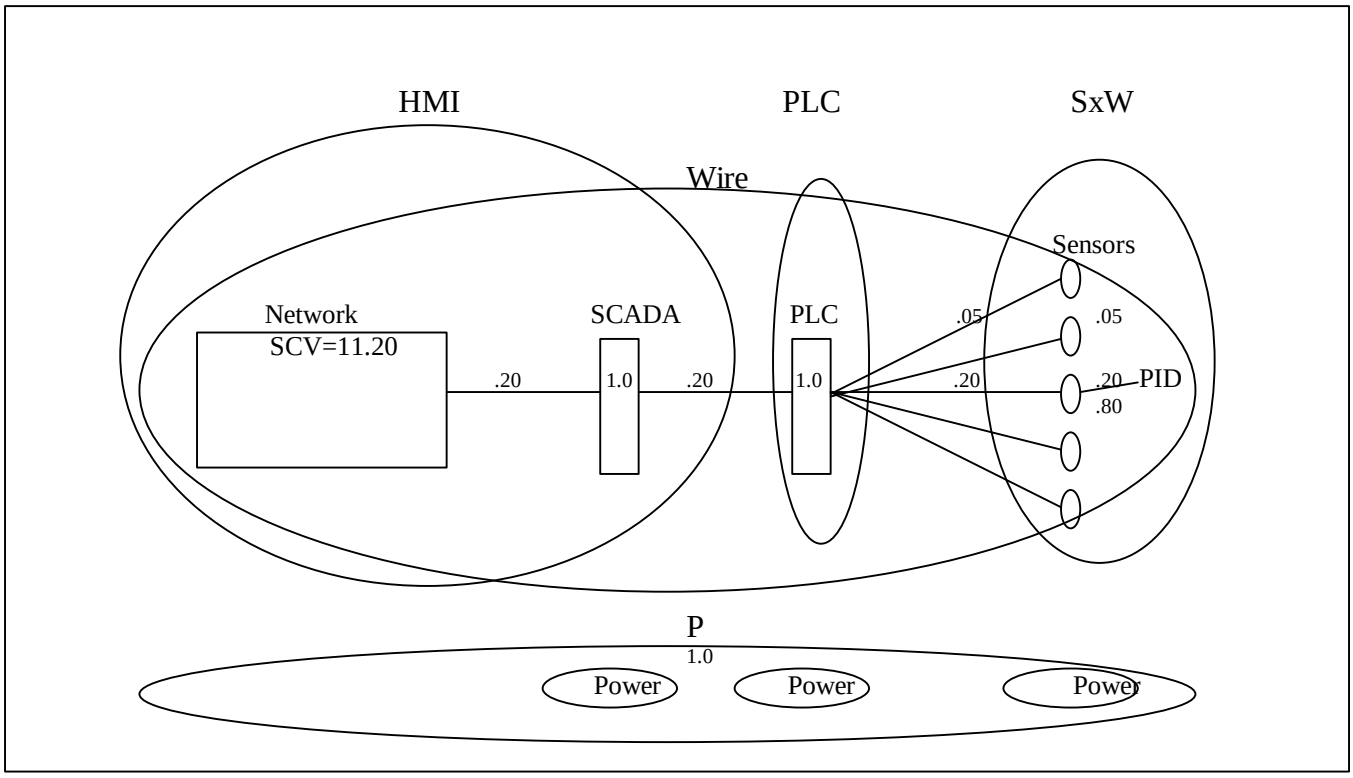

Diagram 5. Combined Modeled Network/Process Control Example.

Adding both earlier evaluations and allowing only one instance for every subsystem produces a combined network and process control SCV.

SCV = {(HMIx +HMIx…) + (PLCx + PLCx…) + (SxW+SxW…) + (Px + Px…) + (Wirex +Wirex…) +
(BANDx + BANDx…) + (SOFTx + SOFTx…) + (EnvOpx +EnvOpx…) + (CIx + CIx…) +
(Mhsx + Mhsx…) + (Agex + Agex…) + SCV network}

19.24 = {(1.0) + (1.0) + (.80 +.05 +.05 + .05 + .05) + (1.0 + 1.0 + 1.0) +
(.20 + .20 +.05 + .05 +.20 + .05 +.05 + .20)+ (.09) + (.02) + (.05) + (.60) + (.08) + (.20) + (11.20) }

Of interest is the example of a SCV containing 3 subsystems, each containing 1 element per subsystem (expressed by the following):

$$SCV = (1) + (1) + (1)$$

If the SCV of 3 is divided by the total subsystem's total elements, 3, we obtain 1, an indication of a System Vulnerability (SV) or SV = SCV/Total elements. The SV value of the above example would be 1. This indicates a worst case scenario of no redundancy, an unreliable system in the event of subsystem failures. By applying redundancy we obtain SCV = (.5 +.5) +(.5 + .5) + (.5 + .5). The SCV still is equal to 3, however now we have 6 elements so SV= 3 /6 or 0.5. This SV indicates a more dependable overall system. Further redundancy could be included into the system thus indicating as the SV approaches 0 the more dependable the system is.

Other evaluation methodologies exist for the evaluation of systems. Conventional reliability such as MTB[3], is perhaps the most widely known, although its use requires more extensive knowledge than for SCVs. That is, the detailed failure time distributions, their defining parameter values, and fault-tree-like dependence structures are needed, in contrast to the more easily derived CV values. There is a payoff, of course, in that the output from a full blown reliability analysis is arguably more valuable than that from the SCVs, but the necessary information base for reliability comes at a far greater cost and requires much greater technical expertise to implement. Similar comments apply to SCVs and detailed Monte Carlo simulation. For simulation, considerable effort is required to gather historical performance data, to model the system, to write and debug code, and so on. The type of analysis presented here allows for identifying major effects on the system from assorted failures, but without the considerable overhead needed for more detailed alternatives.

Functional Flows[4], evaluation uses a subsystem function and is somewhat similar to this methodology without deriving CVs or a SCV. Morkol models can also be employed for evaluation, however once again overhead on large systems can be intensive.

5. Future

As sensors in process control are moved onto the network, which is becoming more prevalent today, it will be possible to apply this methodology to obtain system integrity information[5]. For example, network applications can be applied similar to Simple Network Management Protocol (SNMP) which could give a composite SCV value of a system over a time domain[6]. If a fault of a subsystem element occurs then a 1 could be used in a binary method indicating malfunction of the element[3]. Subsystem elements could be indexed to CV values therefore deriving a SCV. Based on 16 bit or 32 bit computer word lengths, a number of system elements could be monitored via the network. System subsystems could be easily monitoring using bit memory space. Analog values such as bandwidth or aging of a system could be incorporated into the evaluating system. Mapping of the CVs is relatively straightforward because the upper CV limit is 1 and the lower CV limit is 0. It is suggested that an ongoing System Integrity (SI) value could be derived by evaluating the SCV over a time interval. Therefore, a system could be evaluated over a time domain with respect to vulnerability or integrity employing this methodology in a network environment.

System indices, such as CV, usually take some experience and practical application to fully understand. As with any new measure, such experience does not exist, almost by definition.

6. Summary

A summary of the presented methodology is as follows:

I. Diagram the system by dividing it into subsystems and illustrating the dependencies among subsystems.

II. Define Criticality Values for subsystem elements.

III. Apply the summation to determine the System's total Criticality Value.

IV. Evaluate means to reduce the System Criticality Value.
Determine the System Vulnerability.

V. Utilize a network to map the System's Criticality value to obtain system itegrity information and for isolation of faults or failures.

By accomplishing items I, II, III, and IV there is an undeniable benefit to diagramming systems, studying interdependencies of system components and thinking about performance at a component level.

Catastrophic failures of systems will continue to occur. However, by applying the suggested methodology we hope to minimize the effects of catastrophic failures in a system.

References

[1] Grant Harvey, Murray Robert, Bergeron David, 1982, *Emergency Care third edition*, Robert J. Brady Co., A Prentice-Hall Publishing and Communications Company, pp 340-344.

[2] Goldberg Harold, 1981, *Extending the Limits of Reliability Theory,* A Wiley-Interscience Publication, pp 110-121.

[3] Henley Ernest, Kumamoto Hiromitsu, 1981, *Reliability Engineering and Risk Assessment*, Prentice Hall, pp 44-109, 467-513, 185, 169-172.

[4] Addy Edward, 1996, *http://research.ivv.nasa.gov/~eadd/funcflow/*

[5] Institute of Electrical and Electronics Engineers (IEEE), IEEE-1451.2-1997, *Standards for a smart transducer interface for sensor and actuators - transducer to microprocessor*.

[6] Comer Douglas, Stevens David, 1991, *Internetworking With TCP/IP Vol II: Design, Implementation and Internals*, Prentice Hall, pp 367-401.