

# Misguided sense of security on Data Centre availability when FIRE PROTECTION is not addressed

\*LD Durand and HC v Z Pienaar

**The persistent increase for superior availability of data centres is constantly adding pressure on the selection and application methodologies for technology, applicable to both IT related and support systems. Given the proposed configuration of electrical systems to produce higher availability, as promoted through the Uptime Institute's 'tier-level' principles, research has shown that 25 percent [8] of reported down-time is still credited to failure on the part of these electrical systems.**

**The perception that the application of 'dual' electrical systems in itself will increase availability of a data centre's electrical reticulation is misleading and largely untrue. Upon close examination and fire incident scenario identification, it is evident that these dual electrical system architectures (tier-levels III and IV) are still inundated with hidden single points of failures.**

**This paper describes fire protection measures to address these hidden single-points of failure. It is therefore stated that, where sufficient fire protection is not provided, the perception of limited or no single-points of failure on the part of the electrical power supply will result in extended down-time of the entire data centre.**

**Index Terms — Availability, Data Centre, Fire protection, Mission-critical facility (MCF)**

## I. INTRODUCTION

**B**ecause end-user availability expectations are continuously increasing, the need to improve modern data centre operations are increasing at a similar rate. This results into exceptional high business continuity requirements with business interruptions becoming even less tolerable. In terms of many 'Service Level Agreements', it is generally inexcusable, and in most instances severely penalized from a financial perspective.

\*Authors: L.D. Durand is with Total Facilities Management Company (TFMC), Design Solutions, Mechanical Division.

Contact details: Telephone: +2712-641-8012; Facsimile: +2712-641-8612; e-mail: [DurandL2@tfmc.co.za](mailto:DurandL2@tfmc.co.za)

Co-author: Prof. H.C. vZ Pienaar is the Director: Institute of Applied Electronics, Faculty of Engineering and Technology, Vaal University of Technology.

Contact details: Telephone: +2716-950-9381; Facsimile: +2786-612-8675; e-mail: [christop@vut.ac.za](mailto:christop@vut.ac.za)

If AFCOM's<sup>1</sup> 1<sup>st</sup> and 5<sup>th</sup> predictions [1] are seriously considered being a possibility, the mere thought thereof should be a valid concern for data centre operators and facility managers. In addition to AFCOM's predictions, similar research by Site Infrastructure [6] has determined that over 50% of these failures occur within the site infrastructure domain, and more than 60% of all failures are attributed to human activity [4]. These results (published in 2006) indicated that 25% of all data centres will experience a failure that will affect such company's ability to perform business as usual [1]. AFCOM has further predicted that up to 90% of all companies may stop its data centre operations as a direct result of power failures, power restrictions or shortages.

Two important facts are derived from the above statements and predictions: (i) that companies have to source additional and alternative means of power; and (ii) these power sources are likely to contribute to higher individual fire loads and ignition sources. The question therefore is: How many of these failures can be attributed to the lack of fire protection systems provided and, how many failures are as a result of it being provided, such as the automatic shut-down of CRAC units?

## II. VALUE STATEMENT FOR DATA CENTRES

In the modern business environment, Data Centres are probably the most common example of a mission-critical facility (MCF) [2]. Because fire protection for mission-critical facilities is generally perceived to be a complex and challenging topic, it is critical to appreciate the value of the facility in order to attain an elevated sense of awareness towards fire protection requirements. For this purpose, the primary value of a typical data centre is defined in two ways: (i) asset value; and (ii) business continuity value (also known as 'Operational value').

## III. DATA CENTRES AND DESIGN CODES

Life safety is and will always be a mandatory requirement, but since regulatory code compliance does not sufficiently address the abovementioned value statement for data centres in terms of fire protection, provision for life

<sup>1</sup> AFCOM is a non-profit organization consisting of data centre managers, solution providers and industry leaders from several independent data centre providers across the globe, whose charter it is to identify and examine issues affecting operations of data centres.

safety should be considered as a separate issue. The impression that fire protection to modern data centres can be achieved only through strict enforcement of prescriptive codes-based standards and guidance from local authorities may be a costly mistake. These methods do indeed have its place in simple environments and common workplaces, but, for modern data centres, the complexities in such facilities' operations necessitate that traditional fire protection measures be applied in a more innovative manner to produce the required levels of fire protection.

Given the 1<sup>st</sup> data centre value statement being 'asset value', and that many regulatory building codes do not allow for asset protection [5] as a compliance objective, other "industry accepted" but non-prescriptive standards need to be consulted. In such instances where asset protection is omitted from regulatory codes, measures to provide for asset protection are left to the facility owner and its insurers to address.

Certain regulatory codes, such as the BS6266 and NFPA75 [3] (through adoption of the TIA-942) [7], to a limited extent, do make provision for asset protection. Ultimately, it is each designer's responsibility to familiarize him or herself with the building codes applicable to that country.

With regards to the 2<sup>nd</sup> data centre value statement, research has shown that there is no regulatory code that addresses business continuity as a compliance objective. Therefore, and despite any fire protection measure that might be provided towards life safety requirements, it is left to the fire protection engineer to motivate and specify additional (if required) fire protection systems to satisfy both asset protection and business continuity objectives.

The cross-functional integration and emergency operational procedures is yet another concern which might pose significant challenges towards meeting the quoted availability expectation.

#### IV. FIRE PROTECTION TRENDS

With the author having performed research on several international data centres, specifically evaluating the level of fire protection incorporated therein, significant trends were established. These trends suggest that no uniform approach was followed since the level and type of fire protection provided on a facility specific basis varied significantly.

It further become evident that the choice of fire protection technology applied appeared to be based on regional (continent and/or country) preferences. The preferred choice for extinguishing medium in gaseous fire suppression systems in Europe, for example, preferred "Inert gasses" (IG-55 and IG-541) over chemical-based mediums. In the United State, however, chemical-based extinguishing mediums such as FM-200<sup>TM</sup> and NOVEC1230<sup>TM</sup> appear to be the preferred choice.

There also appears to be no scientific-based reason towards the preference between traditional point-type detection over VEWSD (aspirating type) systems, where both system types are installed on a typical dual system (2N) principle. The Australian-based data centres where the only facilities utilizing only VEWSD technology.

Evidently, the most significant trend observed was the

absence of fire protection measures towards the mission-critical electrical reticulation and distribution systems, inclusive of the protection to the emergency standby power generators. With the exception of only a few of the data centres researched, all claims to maintain availability of 99.982% (therefore equal to the Uptime Institute's tier-level III), not one data centre specification mentioned provision of dedicated means of fire-rated compartmentation, with the apparent omission thereof clearly in direct conflict with requirements listed in the TIA-942, NFPA75 and BS6266.

The question can be raised whether the omission of such fire protection measures from the published specifications was deliberate or not?

Regardless, this research has yet again highlighted the need to implement a uniform design approach that will address fire protection measures based on a common but singular philosophy directly aimed at the required performance parameters for a specific risk.

#### V. DATA CENTRE DESIGN PHILOSOPHY

For the purpose of meeting the stated data centre value objectives, the following design philosophies were developed as a direct outcome of the author's research. These philosophies are:

- 1) *limit the possibility of the 'out-break' of a fire,*
- 2) *limit the content of combustible material,*
- 3) *provide 'early-warning' notification of fire,*
- 4) *provide 1<sup>st</sup>-defense fire equipment,*
- 5) *provide fixed fire suppression systems, and*
- 6) *provide fire-rated compartmentation.*

In practice, the logic in applying these fire protection philosophies is as follows:

##### 1) *Limit the possibility of the 'out-break' of a fire*

Efforts to limit the outbreak of fires can be achieved by influencing operational processes on site. This is possible through a combination of safety instructions, staff competencies and specified responsibilities, informative and prohibiting signage intended to raise awareness and general preparedness (or incident prevention) initiatives and is solely the responsibility of the data centre operator.

##### 2) *Limit the content of combustible material*

In an acknowledgement that fires *WILL* occur, a fire's intensity can be reduced by limiting the quantity of combustible material. This effectively involves the removal of non-essential services from mission-critical areas. Where the installation of combustible material is unavoidable and likely, as would be applicable to data centres, it should be specified to have the lowest possible ignition probability and surface fire index values, and drastically reduced flame propagation characteristics.

##### 3) *Provide 'Early-warning' notification of fire*

While acknowledging that a fire will occur, despite the size and intensity of a fire being reduced, it is critical to accept that there will always be combustible material to fuel fires. This realization is subsequently the ultimate motivation to be aware that a fire is immanent and, even more important that emergency response personnel are made aware that a fire is in its inception phase.

Given the nature of human behaviour, building occupants and emergency response personal must be made aware of such fire occurrences by means of notification that is principally independent from human intervention. Hence, the provision of automatic smoke detection is critical. In addition and taking the chemical decomposition process taking place as early as the incipient stages of a fire, and to limit damage as much as possible, very early warning is essential.

This, in some instances, is achieved in the form of point-type and/or VEWS systems, and despite the variance in its sensitivity it usually operates on a similar 2N redundancy principle than the electrical systems.

#### 4) Provide 1<sup>st</sup>-defense Fire Equipment

Assuming that notification of a potential fire has alerted the building occupants and emergency response personal, immediate but appropriate action must be initiated to extinguish, or at least control the fire. This would, as a 1<sup>st</sup> line of defense, be by means of the 1<sup>st</sup>-defense portable fire equipment provided throughout the facility in accordance with relevant minimum statutory requirements. This will create an opportunity to limit the effects (severity) of the fire and should contribute to reducing the generation of combustion by-products such as smoke, hot (combustible) gasses, acidic (HF) and corrosive (HCl) fumes and vapor.

#### 5) Provide Fixed Fire suppression systems

In the event where the above efforts of 'human intervention' were unsuccessful, therefore growing in size and intensity, or upon conditions where there were no response to the initial smoke/fire alarm, automatic means of fire suppression must be provided. This is normally achieved in the form of fixed (automatic) fire suppression and extinguishing systems. In some instances, as with the detection systems, these systems may also follow a 2N redundancy principle.

The 1<sup>st</sup> system (gaseous systems) will have the potential to suppress ignition while still in its incipient phase, thus preventing an actual (flaming) fire. With the 2<sup>nd</sup> system being a derivatives of an automatic fire sprinkler system, and intended to extinguish an actual flaming fire, it's primarily focus is to limit fire spread and to protect the building from major structural damage and subsequent possibility of collapse.

#### 6) Provide fire-rated compartmentation

Regardless of any reliability perceptions over fire systems, the consequential damage of the fire can further be reduced by means of dedicated smoke and fire-rated compartments to: (i) isolate the fire affected area preventing the spread of fire; or (ii) to protect adjacent mission-critical areas from the effects of the fire; or (iii) to protect the redundant (2N) system configuration of essential support services such as the emergency standby generators and dual electrical supply paths.

Owing to the physical operating environment of some mission critical ICT equipment, certain equipment's efficiencies are dependent upon high airflow conditions. For gaseous fire suppression systems to be effective, a fairly airtight environment is a requirement. In these circumstances, actuation of fire compartmentation

equipment (to close) must be initiated prior to the actuation of any gaseous fire suppression system.

## VI. SOURCES OF ELECTRICAL FIRES

With various publications pointing towards electrical systems and components as the most likely source of fire in data centres, it would only be fitting to briefly address this potential source. Based on the above, it is understandable that the highest number of fires are caused as a result of an electrical system or component failure that originates due to: (i) short-circuit conditions; (ii) over-current conditions; (iii) incorrect discrimination and cascading; (iv) harmonics that are not corrected; and (v) transformer failure.

In terms of short-circuit and over-current conditions, Zalosh [9] established that multiple failure conditions must exist to cause a failure on dual electrical systems, e.g. the simultaneous failure of a circuit-breaker combined with conditions of over-current, or an over-loaded cable combined with short-circuit conditions. When a protection device (circuit breaker) fails to isolate power supply to the affected reticulation medium, it will cause instant fire ignition of the isolation material, or worse, vaporization. This leaves the affected reticulation medium (Copper/Aluminium) bare and normally causes further short-circuit conditions to the unaffected reticulation network.

In extreme (simulated) cases of overload conditions, the cable insulation has been reported to vaporize. The same research [9] has also shown that, if an ignition source is present when vaporization of cable insulation occurs, it happens across the entire length of the cable and produces an extended flammable vapor-air mixture around such cable. In these circumstances, flame propagation through the vapor-air mixture occurs at rates two orders-of-magnitude greater than those for diffusion flame propagation – this is basically instantaneous ignition over the length of the cable and all combustible material in the immediate surroundings of such cable.

Based on independent tests conducted on cable fires, the normal diffusion flame propagation patterns for horizontal cable trays recorded a maximum flame spread of 3m/min, with the average flame spread ranging from 4 to 43cm/min, depending on site condition, cable type, the number and position of cable trays and individual tray loading. For vertical cable trays, the measured flame propagation of 1m/sec is significantly higher. It is further important to note that maximum vertical flame propagation was determined to spread the fastest under forced ventilation conditions.

Fires in cabinets/servers develop slower, but does reach a peak heat release rate (HRR) of 800-1300 kW (according to tests) with about 50% of the cabinet's internal content involved [9]. The measured HRR normally occur from 10 to 27 minutes after ignition. In these conditions, total obscuration of visibility (% visibility/m) is reached as early as 6 minutes from the time of ignition in an (research/test) environment where the ceiling height measured 5.5 m. The maximum temperatures of the combustible products inside the cabinet were measured at 660°C.

A further concern identified was that cabinet wall temperatures can become sufficiently high to ignite cables against the wall of an adjacent cabinet. It is therefore

concluded that the fire may spread horizontally from cabinet to cabinet from as early as 11 minutes after ignition. A further concern was identified where fires involving PVC jacketed cable insulations causes formulation of a chloride layer (after Zinc Chloride formed from the reaction of HCl with transistor chip coatings) on the circuit boards, causing further short-circuit conditions inside the cabinet.

## VII. DESIGN PARAMETERS

In order to facilitate an objective driven design solution, a properly drafted design brief (facility performance expectations) is of the utmost importance. Minimum expected down-time (in %) must be clearly specified as that will directly impact on the site infrastructure support systems, specifically that of the electrical and HVAC systems. Specific legal and industry “Best operating practices” and standards should be included in this brief as compliance thereto also has a direct and significant cost implication both from a capital and operational expenditure perspective. A further important criterion that must be included in this design brief is the expectations towards compliance to and with environmental protocols in terms of ‘greenhouse gasses’ and other contributing factors towards global warming.

Obviously, the data centre’s criticality rating or risk category must be determined and agreed upon prior to the issuing of the said design brief to enable a uniform design approach for fire protection. An approach similar to the method described in the BS6266 should be developed and implemented by the data centre owners to determine the facility’s risk category since the rating determined through a formal process normally influences availability requirements and must be aimed at a facility’s specific risk profile and operational requirement.

The design solution, in following the objectives of the proposed design ‘philosophy’, (from paragraph V) can be addressed by applying the criteria as discussed below in more detail:

### 1) *Limit the possibility of the ‘out-break’ of a fire*

The responsibility to ensure an acceptable level of fire “prevention” resides solely with the data centre owner and its employees, or duly appointed agent. The following items serves to elaborate more on these issues to which the owner must take cognizance of and implement as far as reasonably and practically possible. From an engineering perspective, it is not advisable to assume that the owner will apply reasonable practice in terms of site management as it may lead to the installation of sub-standard infrastructure support systems, with insufficient configuration and redundancy.

As part of this practice, the following plans and procedures can be considered to be implemented towards guidance in preventing fire ignition these are:

- (i) a fire/emergency incident action plan;
- (ii) procedure for safe working conditions;
- (iii) a workplace waste management policy;
- and
- (iv) a general house-keeping policy.

### 2) *Limit the content of combustible material*

In actively designing-out and managing the combustible content and flammability of any building element or equipment installed, both the intensity and size of the fire is reduced since no additional, or significantly less, ignition sources and fuel are added to the fire other than the original material involved during ignition.

The actual quantity of material having a fairly high combustible content, e.g. IT and communication equipment, network and power cables need to be managed effectively to address concerns regarding its anticipated/proposed use (wrt its mission-critical purpose), positioning, routing and distribution, separation and protection strategies.

Efforts to limit the (exposed) combustible content of a data centre must be addressed through a material selection process to ensure the least possible combustible material is present at any given time, provided the facility is operated and managed in accordance with the following criteria:

- (i) removal of redundant electronic and other communication equipment;
- (ii) prohibit/limit the use of combustible furniture;
- (iii) provision of steel lockers and cabinets for essential product manual;
- and
- (iv) prohibit non-essential administrative functions within mission-critical areas.

### 3) *Provide ‘Early-warning’ notification of fire*

Conventional building and systems specifications primarily address detection of fire from a life safety perspective. From an asset protection and business continuity point of view, this practice may be interpreted as a common oversight given the probable damage that can be caused to critical assets supporting the physical operations of a data centre. From a (design) philosophy point of view, the provision of appropriate detection is to enable the data centre manager to be timeously informed to proactively prevent, act upon, and minimize the effect the fire could have on the facility’s availability.

Point-type smoke detectors are ‘passive’ in nature in that they rely heavily on the thermal-lift characteristics of hot smoke (gasses) to rise to the ceiling, thereby relying on a dense enough smoke plume to permit detection. In high airflow conditions, such as in data centres, these smoke detectors are less effective and reliable. Furthermore, the temperature of the smoke generated during the incipient phase of a fire is quite low, failing to achieve to required thermal lift necessary for detection, while not even considering the influence of dilution with cooled-air.

Traditional methodology and thought processes applied resulted in the CRAC units being shut-down. Modern servers however require continuous cooling for the data centre to remain operational. The Uptime Institute stated that a server with the dimensions of 0.61 m by 0.76 m can produce up to 10 kW of heat. When considering a projected heat load of 5.0 kW per server rack, critical shut-down of the server is expected to occur after about five seconds from the time positive cooling is discontinued. Since heat production can be as high as 10 kW or more per server rack, according to the Uptime Institute [7], critical thermal

shut-down can occur in less than three seconds. To enhance data centre availability, it should become common practice not to wire CRAC units for auto-shutdown during general fire alarm conditions but only under special and pre-engineered alarm conditions that occur within a specific operational environment.

Aspirating type VEWS systems are 'active' in that they constantly sample air from multiple points throughout the environment. They are not dependant on thermal energy for smoke transportation. Furthermore, these systems lend themselves to much more efficient siting since capillary sampling tubes that can be installed directly in the path of the air-flow pattern and in some instances, in the server itself. Apart from the obvious advantages from a cooling perspective, air-flow patterns common to the 'Hot & Cold Aisle' principles must be applied as a fundamental approach as it increases the VEWS system's efficiency. In addition, air-flow patterns are important where attention to the actual server configurations relevant to the cooling principles should be applied.

The point-type detection system can however be viewed as a backup to enhance the availability of the smoke detection function, but is not essential. It is therefore recommended that both system types be considered, but that preference is given to the aspirating type. The design of these systems must, when selected to be installed in isolation or in combination, be designed in accordance with minimum design parameters and detector spacing, such as the NFPA72 and BS6266.

#### 4) Provide 1<sup>st</sup>-defense Fire Extinguishing Equipment

Hand-held fire extinguishers of the correct type and size appropriate to the risk must be provided as specified in relevant building codes. Fire extinguishers of the dry chemical powder (DCP-stored-type pressure) and carbon dioxide (CO<sub>2</sub>) types are the norm in most instances. DCP type units must be appropriate for the specific risk, with the extinguishing medium to be a multi-purpose powder suitable for classes A, B and C fires. This type of unit should not be installed in the IT Server/Data Room or Control room, instead, CO<sub>2</sub> type units must be installed.

Final positioning will normally be determined once site layout drawings are finalized and shall incorporate all relevant signage.

#### 5) Provide Fixed Fire suppression systems

Where redundant duplicate system technology is applied, the primary system is intended to extinguish a fire in its incipient phase whereas the secondary system is intended to perform a dual role of suppressing and extinguishing the fire and to protect the facility from structural failure. With relation to the protection requirements in accordance with the philosophy, these fire suppression and extinguishing systems are regarded as essential to the **operational continuity** of the IT server/data room, the essential support services, as well as the rest of the facility if so specified.

In order to reduce maintenance and operating costs and to reduce carbon dioxide emissions in pursuit of a more environmentally friendly data centre (so-called 'green' data centres), 'economy-' or 'free-cooling' has become a common phenomenon. This has unfortunately a direct impact on the selection and application of fire suppression

systems.

The requirements and provisions of the Environmental Protection Agency (EPA), the Significant New Alternative Policy (SNAP), the Montreal and Kyoto protocols and the resolution from the 2007 Bali conference, should be adhered to on a non-negotiable basis through policy making.

Due to the possibility of arcing of over-loaded cables causing re-ignition after the extinguishing gas has dissipated, serious consideration must be given to manually de-energize the electrical systems specific and dedicated to the affected equipment. As a result, provision for localized "Emergency Power Off" (EPO) switches must be made, and where so provided, must comply with the NFPA70: National Electrical Code and the TIA-942, section G.5.1.4.

As alternative to 'total flooding' systems, localized application system technology is also available. These systems normally do not require additional electrical or plumbing connections to operate, which makes them perfect for new construction, retro-fitting and electrical distribution boards and controllers, but less suitable for tele-communication and server cabinets due to the 'economy-' or 'free-cooling' principles mentioned earlier.

Despite many reports suggesting that water as an extinguishing medium in data centres is to be avoided, resulting in equipment damage, downtime and loss of revenue as well as the possible electrocution of tenants/staff, automatic fire sprinkler systems in addition to the gas suppression systems must still be seriously considered.

With water having a direct influence on the availability rating of the electrical systems and power supply capacity, and therefore, the data centre in total, several safety measures are to be incorporated through the design process. This shall include, but not limited to, the provisioning of pre-action actuation principles based on a normally dry-pipe system configuration with methods to manually operate and mechanically 'power-down' all IT and data equipment in the hazard area. The method of 'power-down' must comply with NFPA 70: National Electrical Code and the TIA-942: section G.5.1.4.

#### 6) Provide fire-rated compartmentation

Since no system on its own is totally reliable, with the potential to fail an ever-present possibility, consideration should be given to the resultant risk created in the event where such system failure does occur. As a last alternative to minimize the potential of the data centre to be affected severely enough to cause failure, mission-critical areas and services are to be compartmentalized into specified fire-rated zones to isolate them from the effects of fire in any other area or, to protect the duplicate configuration of the support services, such as generators, dual electrical supply paths and cooling equipment in order to maintain operational continuity for as long as possible.

In providing fire separation between the critical support systems as mentioned above, it directly contributes to an earlier proposal to manage the fire impact. In order to limit the effects of a fire, or by limiting the area so exposed, the impact of the fire is reduced, thereby minimizing or potentially eliminating the possibility of down-time. This approach effectively introduces the concept of 'fail small'.

Apart from concerns regarding possible electro-magnetic interference, but based on 'cable-vaporization' possibilities, IT and communication cables must be physically separated from the electrical reticulation and distribution systems.

All communication equipment and IT areas should further be supplied with air-conditioning systems which are totally separate from those systems supplying any other occupancy within the data centre. With relation to the data floor, it is recommended that the air-conditioning system be dedicated to that area, with all air handling equipment (CRAC's) preferably housed inside the cooled data floor, thus eliminating the extensive use of ducts that normally penetrates fire-rated separating elements. Fresh air intake supplied in pursuit of 'free-cooling' objectives, must then be supplied with a means of an automatic closing device/dampers upon activation of the gas suppression system.

Essential services must be fire separated from each other and the data floor in accordance with a risk determining process to ensure that if one of the duplicate services is lost due to fire, the other will continue to operate unaffected.

#### VIII. CONCLUSION

In closing, the opening statement is reiterated in that failure to address fire protection to a level commensurate to the facility criticality and specific risk, one effectively fails to address potential and extended (if not permanent) facility down-time. Therefore and based on the preceding discussions and other factors, with all information taken into consideration for developing the input specification for a comprehensive fire protection solution, a holistic fire protection philosophy must be applied.

#### ACKNOWLEDGMENT

The author thanks TFMC, Telkom SA and the Vaal University of Technology (VUT) for the opportunity to research fire protection to modern Data Centres. Special recognition is also owed to Professor H.C. vZ Pienaar (VUT), Professor H.J. de Jager (NMMU) and Mr. F.A.C. Smit (TFMC).

#### REFERENCES

- [1] CAPRIO, C., ECKHAUS, L., HEATH, R., ROBERTS, T., SAWYER, R., March 22, 2006. *AFCOM's Data Center Institute Issues Five Bold Predictions for the future of the Data Center Industry*. [Online]. Available at: [http://www.afcom.com/News\\_Releases/Afcom](http://www.afcom.com/News_Releases/Afcom)
- [2] Lance, H. 2008. Fenwal Protection Systems, Consulting-Specifying Engineer. *Fire Protection in mission-critical facilities*. [Online] Available at: <http://www.csemag.com/article/CA6537323.html>.
- [3] NFPA 75 (National Fire Protection Agency). 1999 Edition. Standard for the protection of Electronic Computer/Data processing equipment.
- [4] RICKETTS, KEVIN. Literature presented at the central 'Knowledge Exchange Meeting'. (Paper presented as part of a workshop held with TFMC representatives on 15 June 2006). London, UK (Unpublished).
- [5] SFPE (Fire Protection Engineering Journal). 2007. Issue 34. pp. 46-52. Article published on: *The Fire Engineering Brief: An essential tool for regulatory approval of performance-based design* (FEENY, M., SCHULTZ, J.). Printers: SFPE, Lanchester, England.
- [6] SITE INFRASTRUCTURE. 2002. White Paper. *Product certification for fault-tolerance is essential for verification of high availability*. [Online]. Available at: <http://www.uptimeinstitute.org/spec.html>.
- [7] TIA-942 (Telecommunications Industry Association). 2005. *Telecommunications Infrastructure Standard for Data Centres*. Printers: TIA Standards and Engineering Department, Arlington, VA 22201, U.S.A.
- [8] TURNER, W.P. SEADER, J.H. BRILL, K.E. BRILL, P.E. 2001-2005. White Paper. *Industry Standard Tier classifications define site infrastructure performance*. S.I. The Uptime Institute. [Online]. Available at: <http://www.uptimeinstitute.org/wp>.
- [9] ZALOSH, R.G., 2003. *Industrial Fire Protection Engineering*. ISBN 0-471-49677-4. Printers: John Wiley & Sons Ltd, West Sussex, England.

#### AUTHOR BIOGRAPHY

**L.D. Durand** was born on September 7<sup>th</sup>, 1968. In 1987, he joined the Pretoria Fire and Emergency Services Department as a recruit fire fighter. His 1<sup>st</sup> 6 years at the Pretoria Fire and Emergency Services Department were in an operational environment, with the last 4 years at the Fire Safety Division.

Since March 1997 he was involved with several fire protection designs to MCF's and other large developments as an independent consultant. He joined Infracom in August 2000 and in January 2001, he accepted employment at TFMC's Centurion-based (Pretoria, RSA) headquarters, assuming responsible for the Maintenance Engineering duties for Fire Protection on a national basis. He was recently transferred to TFMC's professional design team assuming national responsibility for the performance-based fire protection designs to, amongst others, MCF's and other Telecommunication facilities.

Formal qualifications obtained through-out his career are: (a) National Diploma, Fire Technology, Pretoria Technikon (Now TUT), 1993; (b) Baccalaureus Technologiae Degree, Fire Technology, Pretoria Technikon, 2003; and (c) MTech:Eng:Elec from the Vaal University of Technology, Vanderbijlpark, SA, 2008, of which the research subject is also the focus of this paper.