VIRTUAL DESIGN MASTER 3

REDFOG DESIGN DOCUMENT V1.5

Challenge 2

Steven Viljoen
7-9-2015

Contents

Revision History

Date	Revision number	Author	Comments
9 July 2015	V1.0	S.Viljoen	Initial document draft
10 July 2015	V1.1	S.Viljoen	Added Level 3 storage capacity and wishing I had paid more attention in maths class.
11 July 2015	v1.2	S.Viljoen	Hmm, is this really what was required?
12 July 2015	v1.3	S.Viljoen	Think that I have misunderstood the challenge requirements completely.
12 July 2015	v1.4	S.Viljoen	All kinds of lost.
13 July 2015	v1.5	S.Viljoen	Redfog descending

Executive summary

The first part of this document defines the infrastructure agnostic layout and interaction for 2 applications:

1) Time tracking application
   This is a non-critical application that will be used by the greenhouse botanists to track their working hours. It has been defined as a single layer system.
2) Critical Life Support System application.
   This is a critical system that is used to monitor and maintain the environment in all habitable environments on Mars. This system is highly available on all levels to ensure that the 20 minute MTD is not breached.

The second part identifies an existing Earth based public cloud infrastructure provider that will be recreated on Mars.

The 2 applications defined in the first section are then mapped to the public cloud provider products to illustrate the final layout and requirements of the entire environment.

Executive objectives

This project has 2 main objectives

Objective A

1. Design an environment that includes
   a. A web based time tracking application for the botanists in the greenhouses.
   b. A critical enterprise life support system application.
2. Define all application requirements.

Objective B

1. Select an existing public cloud infrastructure that will be recreated on mars and justify why it was chosen.
2. Publish the environment to the selected public cloud infrastructure.

General Application Requirements

Reference	Description
APR01	Must run autonomously
APR02	Must ensure a 20min MTD.
APR03	Must include a failsafe located outside the cloud environment.
APR04	Must store logs for at least 2 years.
APR05	Must be highly available.
APR06	Must facilitate base expansion.
APR07	Must store environment data for 5 years for environment analysis
APR08	Initial Application design should be infrastructure agnostic so that it can be mapped to any chosen public cloud infrastructure.

Constraints

Reference	Description
CS001	Infrastructure must be based on an existing public cloud infrastructure
CS002	Design needs to be completed in 5 days.
CS003	

Risks

Reference	Description
RI001	Moving the Life Support Systems away from the local environment introduces risk of NW failures leading to fatalities.
RI002	Critical life support systems are outside the direct control of the local admins.

Assumptions

Reference	Description
AS001	The benefits of moving the LSS systems to a cloud environment outweigh the risks.
AS002	The alarm module (not in scope for this document) is configured to be highly available.
AS003	Someone with more than 2 days of AWS ‘knowledge’ will implement the final solution.

OBJECTIVE A

1. Design an environment that includes
    a. A web based time tracking application for the botanists in the greenhouses.
    b. A critical enterprise life support system application.
2. Define all application requirements.

Common Infrastructure services

The following systems will be centrally installed to provide infrastructure services to, amongst others, both the LSS application and the Time tracking application.

PTP Time synchronization

Accurate time synchronization is essential in any environment and especially in a control environment like the LSS to ensure that data\time stamp records from all the sensor driven components are accurate. This allows specific condition sets to be identified and acted upon. (I.e. increased light, pressure and thermal reading at the same time probably means that someone just lit a cigarette in the oxygen chamber and will be requiring medical assistance).

In addition to this the time synchronization sub system will most likely also be used for scientific systems (which are not in scope for this document) but would need highly precise time synchronization.

This environment will use the IEEE 1588 PTP (Precision Time Protocol) as it is:

- More accurate than NTP and
- Less expensive than GPS (especially if you need to start launching satellites.)

Requirements:

- Boundary clocks located in both the cloud environment + onsite environment.
- Grandmaster and clients must reside in the same PTP domain.
- PTP will be run in Unicast mode (Redfog (AWS) does not support multicast) which will require that the master is added to the Acceptable Master Table in each slave.

LDAP and DNS

LDAP and DNS services will be provided throughout the environment by the 3 Domain controllers for ‘base.mars’ domain.

- APDC1.base.mars
- WPDC1.base.mars
- FPDC1.base.mars

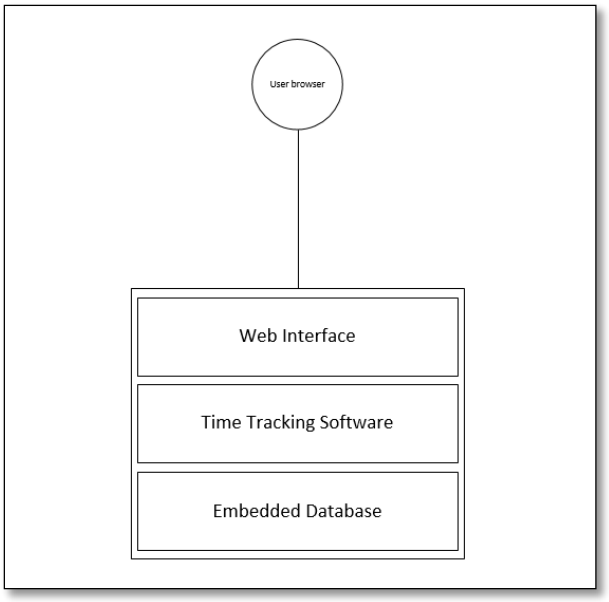
Each domain controller will be deployed to a separate availability zone and each will be configured as Global Catalog Servers.

Time tracking application

Functional Requirements:

Reference	Description
TTR01	Should provide web based access to botanists.
TTR02	Should store time data the last 15 months.
TTR03	Last 30 days of data must be backed up.

Level Overview



High Availability

The time tracking system is not considered to be critical and as such does not require any level of redundancy.

Backups will be taken every day to ensure that data can be restored if needed.

Retention period is set to 30 days as the botanists are known to query each pay slip and it is needed to have at least the last month's data available if challenged.

Components

The time tracking environment will consist of a single server with the following 3 applications running.

1. Web interface: **nginx**
2. Application layer: **PHP running Symfony 2**
3. Database layer: **MySQL**

Requirements

Scope	Requirement
CPU	1
Memory	2 GB
Storage – OS + Application	30 GB
Storage - Data	70 GB
Network - Connections	1x Ethernet
Network – Bandwidth	Low Botanists are not known to track their time regularly.

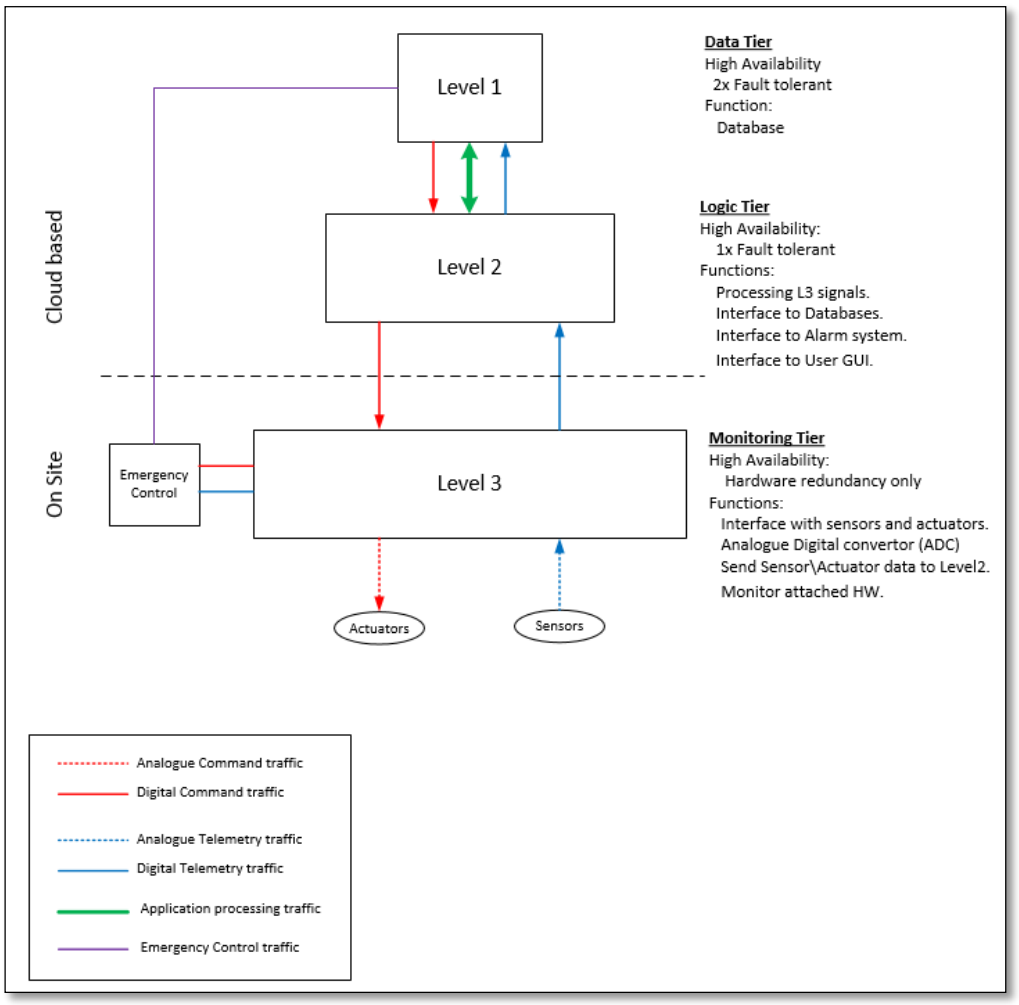
LSS Conceptual Design

Application layout

The LSS will use a 3 level structure as shown in the diagram below. It will also be split between local onsite components that require hardwire analogue connections to the various sensors and actuators and the cloud based components that will communicate via Ethernet.

The benefits of using this approach are:

1. **Modularity**: Allows new components (upgrades, repairs, etc.) to be inserted without requiring a complete redesign of all levels.
2. **Scalability**: As the base grows, new habitable areas requiring LSS can easily be added by installing local level 3 components and connecting them to the existing level 2 systems. [APR06]
3. **Granularity**: Provides multiple differing layers of redundancy that can be defined on a level by level basis to reduce costs and increase HA.



Emergency Control (EC)

The emergency control module is located in the local site. As it is a separated fail safe mechanism for the core Life Support System no independent redundancy is required.

The EC monitors upper level availability and in case of catastrophic failure of Level 1 or 2 will take over control of Level 3 and maintain a basic life supporting environment until the issues are repaired.[APR03]

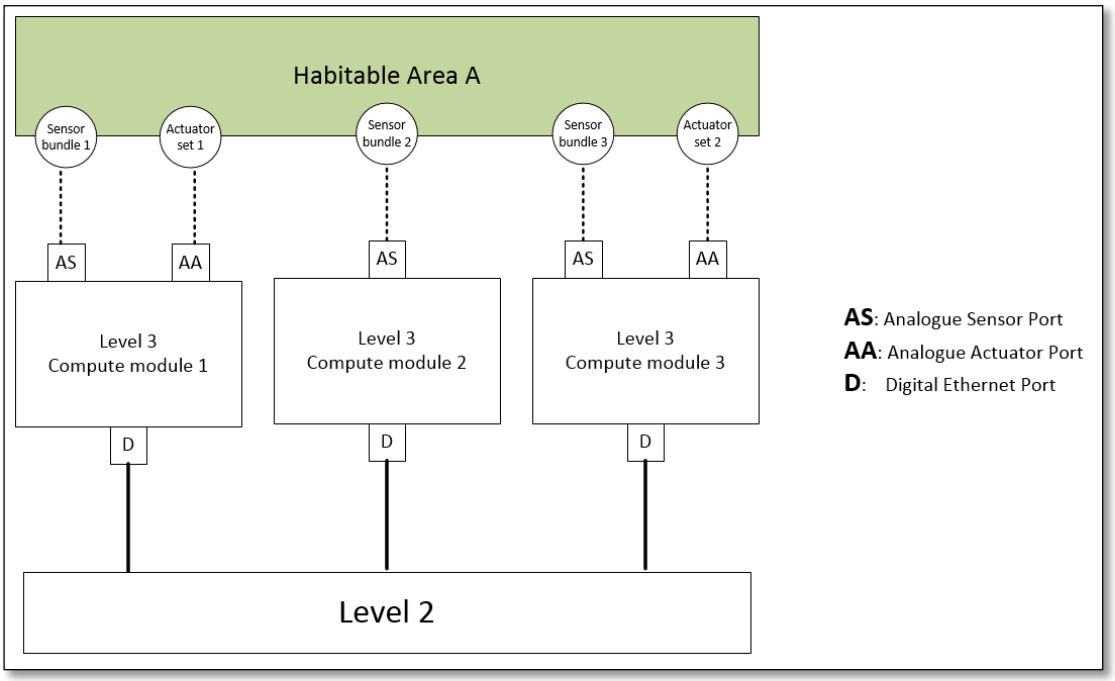
The module will be completely segregated (different Hardware, OS and software) from the core LSS as shown below to prevent issues bringing down the core systems and also affecting the Emergency control:

Level 3 Architectural design

Functional Requirements:

Reference	Description
L3R01	Receive and send analogue data
L3R02	Convert analogue signals to digital and vice versa
L3R03	Receive and send digital data via Ethernet to and from Level 2

Level Overview



High Availability

No application level high availability is needed as redundancy is ensured on the hardware level as shown above.

Each Sensor bundle and Actuator set is connected to its own separated Level 3 compute module. Each habitable area will have at least 3 sensor bundles and 2 actuator sets per room as illustrated.

This forms a hardware redundancy group for that habitable area.

Components

Sensors

The sensors are responsible for providing environmental data to the L3 compute modules.

Each sensor bundle will consist of a number of different sensors types, each of which will send telemetry data messages at fixed intervals based on criticality of that metric.

Actuators

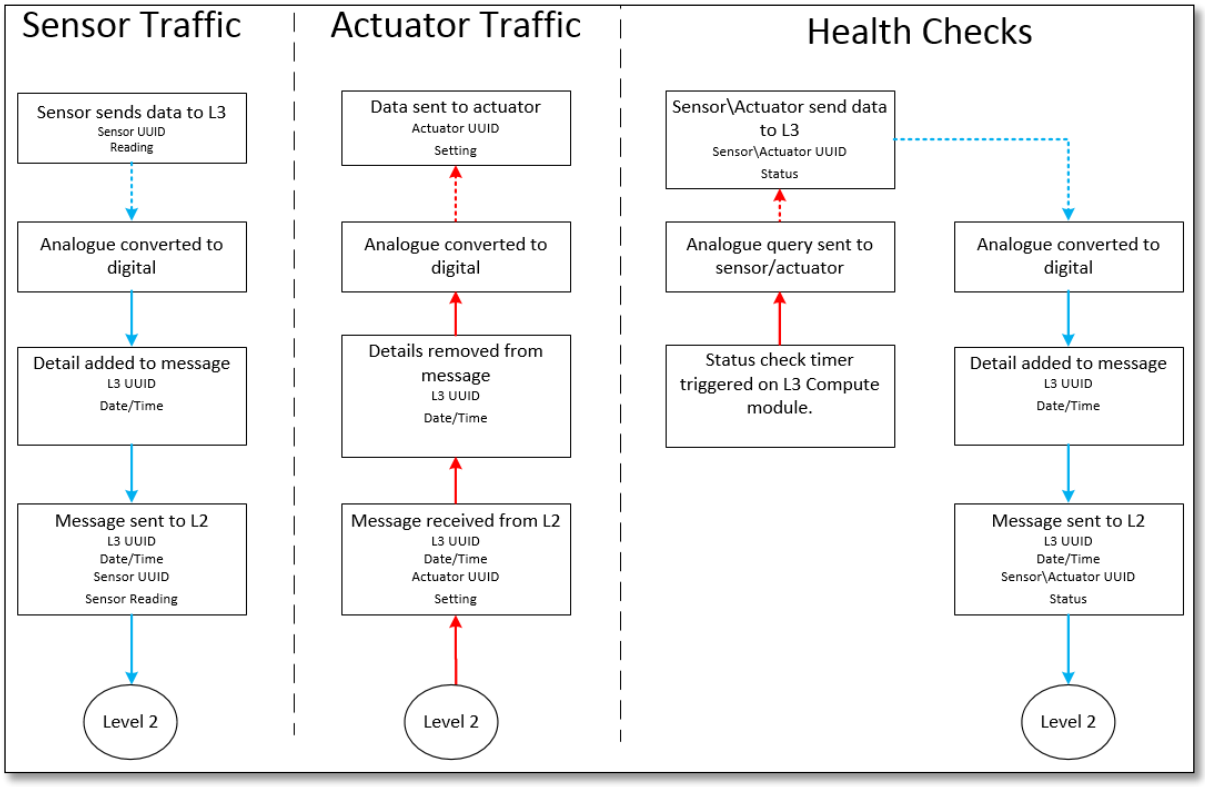
The actuators are responsible for carrying out the command messages sent from L3 Compute modules to influence various aspects of the environment.

Compute modules

Level 3 compute modules will not need to be very powerful as their main role will be to function as Analogue Digital convertors. Any microcomputer (i.e. Raspberry Pi) with an ADC module will suffice.

Data flows

The following diagram details the basic data flows derived from the Level 3 functions.



Capacity requirements

Level 3 does not store any data locally but does generate data that needs to be accounted for in the higher levels. The table below summarizes the minimum storage capacity requirement as generated by Level 3 components.

Capacity calculations are shown in Appendix A.

Daily Total sensor data (GB)	Daily Total actuator data (GB)	Daily Total combined data (GB)	Yearly Total combined data
0.484	0.155	0.623	**233 GB**

Network requirements

Connections

1. Analogue connections : Level 3 - Sensors\Arrays
2. Ethernet: Level 3 - Level 2

Bandwidth

The minimum required Bandwidth between Level 3 and Level 2 is, based on similar systems and data size calculations (Appendix A), to be at least 16kbps.

Compute requirements

As each sensor bundle is connected to its own level 3 compute module and tasks performed by each compute module are not CPU nor Memory intensive, it is possible to benchmark against industry standard microcomputers.

(Raspberry Pi for instance is able to convert analogue to digital and transmit data via Ethernet at the required messaging frequencies)

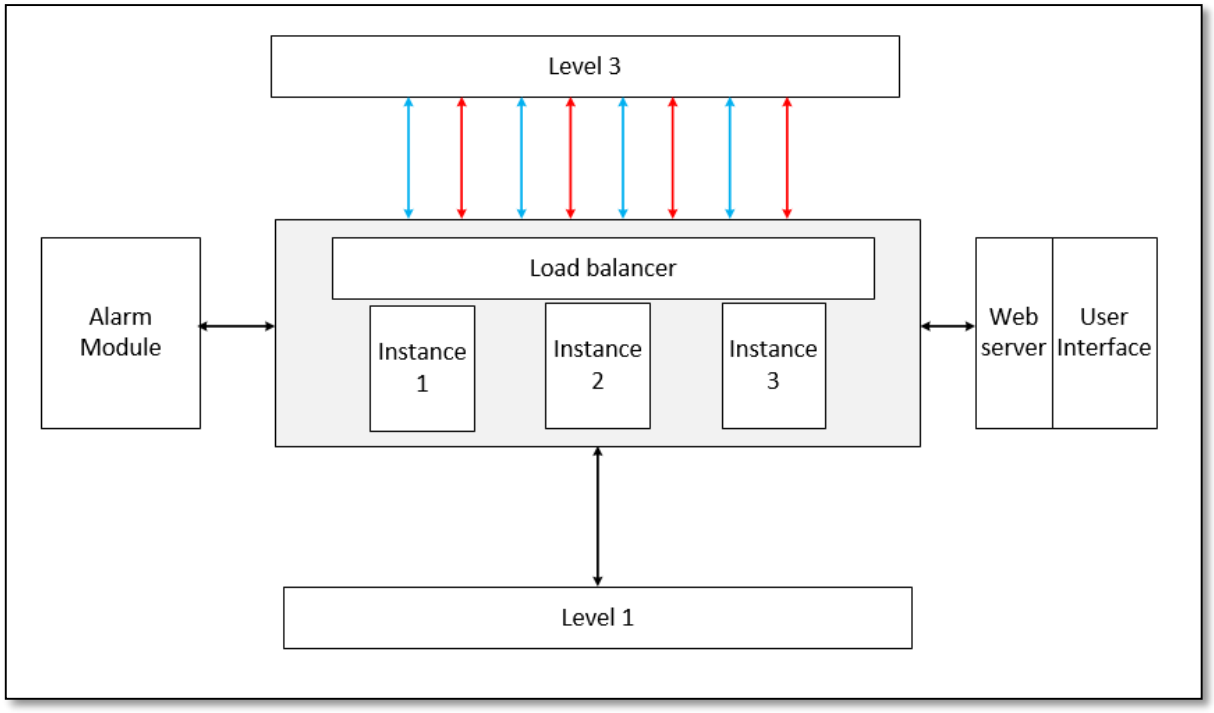
CPU: Single core (700MHz) Memory: 512 MB

Level 2 Architectural design

Functional requirements

Reference	Description
L2R01	Must be at least 1 failure
L2R02	Connectivity to Level 1 and Level 3
L2R03	Connectivity to User interface module
L2R04	Connectivity to Alarm module
L2R05	Support CPU and Memory intensive processing

Level Overview



High Availability

High availability will be provided by having 3 application instances running behind a central load balancer. As these are processing units and do not have large amounts of data stored locally deployment could be scripted to quickly deploy a new instance if 1 fails.

Components

Processing module

- Critical component
- 3 Application instances
- 1 load balancer to distribute load amongst them.
- This setup provides HA [APR05] and also allows for the environment to be expanded [APR06] by simply adding additional application instances behind the load balancer.

User interface module

- Non critical [APR01]
- 1 web server

Alarm module

- Not in scope for the LSS design document but will be set up for high availability. [AS003]

Capacity requirements

Level 2 compute modules do not store data locally but do generate data that needs to be accounted for in the higher level (level 1). The majority of the data generated from level 2 will be related to logging.

Based on similar systems and anticipated data flows it is possible to define the minimum expected storage capacity requirement generated by level 2. This is shown in the table below.

Monthly log size: User interface (MB)	Monthly log size: Alarm module (MB)	Monthly log size: Level 3 (MB)	Monthly log size: Level 1 (MB)
200	100	750	300

Total capacity requirements

Monthly Combined log size (MB)	Yearly Combined log size (MB)
1350	16200

Network requirements

Connections

1. Ethernet: Load balancer – Level 3
2. Ethernet: Load balancer - Level 2
3. Ethernet: Level 2 – Level 1
4. Ethernet: level 2 – Level 2 (Inter instance communication)
5. Ethernet: Level 2 – Web server (user interface module)
6. Ethernet: Level 2 – Alarm module

Bandwidth

Peak Level 3 bandwidth (16kbps) is already incorporated above in Level 3 network requirements so will not be duplicated here.

Logging traffic is expected to be 4 times more than data traffic given the anticipated checkpoints at which log data would be written to the database for each data message received from Level 3.

The additional traffic generated by the User interface and Alarm module is expected, based on similar systems, to add an additional 20kbps.

The minimum required bandwidth for level 2 would then be:

16kbps + 64kbps + 20kbps = 100kbps

Note: As these will be the central instances for any base expansion plans that require LSS the minimum bandwidth will be defined as 10 Mbps.

Compute requirements

As the layer 2 processing modules are relatively memory intensive as compared to other resource usage the following specifications have been calculated as being the minimum requirements per instance.

CPU: 2 x 2.2MHz Memory: 15 GB

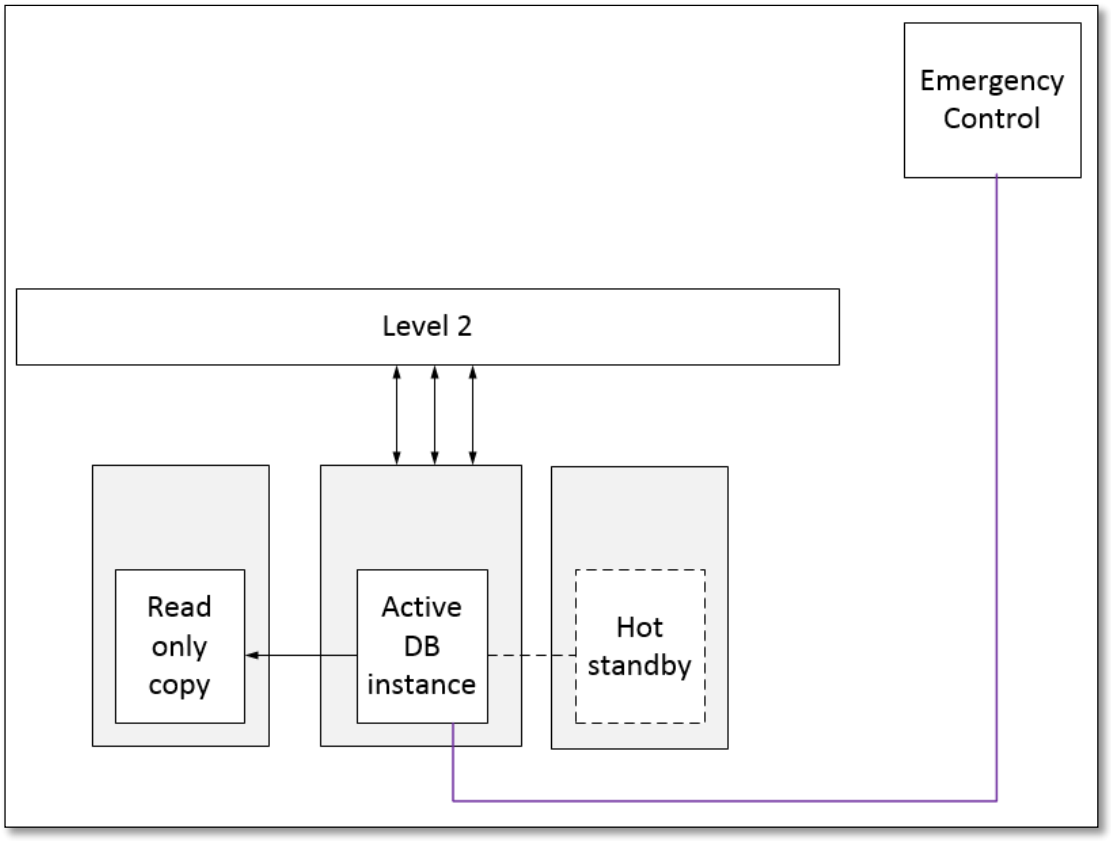
Instances will be monitored throughout the initial first month and if required then additional resources can be added.

Level 1 Architectural design

Functional requirements

Reference	Description
L1R01	Must support at least 1 failure
L1R02	Connectivity to Level 2
L1R03	Support high IOPS
L1R04	Must have enough capacity to store 2 years logs
L1R05	Must have enough capacity to store 5 years of environmental data

Level Overview



High Availability

High availability will be ensured by running an additional hot standby instance that will be able to take over in case of any issues with the active instance. In addition to this a read only copy will be created to provide additional redundancy and also allow for future expansion. [APR06]

Components

1. 1 Active database instance
2. 1 hot standby database instance
3. 1 read only copy

Capacity requirements

The total database capacity requirement (taking into account required retention periods for environmental data [APR04] and log data [APR04] and including log data generated by level 1 components) is shown below.

[APR07] 5 Year environmental data - Level 3 (GB)	[APR04] 2 Year log size - Level 2 (GB)	[APR04] 2 Year log size - Level 1 (GB)	Total Combined database size (GB)
1165	32.4	20	**1217.4**

IOPS requirements

Calculated IOPS requirement is <3500

Network requirements

Connections

1. Ethernet: Level 2 – level 1
2. Ethernet: Level 1 – Emergency Control module

The Hot standby and read only copy will be created on the hypervisor layer.

Bandwidth

Minimum bandwidth requirements are the same as calculated above for level 2.

Minimum bandwidth: 100kbps

Note: As these will be the central instances for any base expansion plans that require LSS the minimum bandwidth will be defined as 10 Mbps.

Compute requirements

Database compute specifications will be based on similar systems.

CPU: 2 x 2.5MHz Memory: 15 GB

Instances will be monitored throughout the initial first month and if required then additional resources can be added.

OBJECTIVE B

1. Select an existing public cloud infrastructure that will be recreated on mars and justify why it was chosen.
2. Publish the environment to the selected public cloud infrastructure.

Redfog cloud infrastructure

While most of the major Earth based public cloud providers offer similar services and functionality Amazon web services (AWS) has been selected as the model on which to base Mars' first public cloud infrastructure.

Maturity

AWS was launched in 2006 (4 years before Azure and 7 years before vCloud Air) and as such has the most experience in the field.

They are (were?) also trusted by major companies with customers including NASA and the CIA proving that they are able to handle space related data and keep it safe.

Functionality

AWS provides a number of supported functionalities that while not used for this project could be required at a later date.

1. Native Windows Failover Clusters (even Azure has issues with this).
2. Support for Hyper-V on-premises connectivity (AWS storage gateway)
3. Multiple OS version support (RHEL for instance is not supported in Azure)
4. AWS marketplace which has the largest number of solutions available.

Availability

AWS provides a number of crucial availability products.

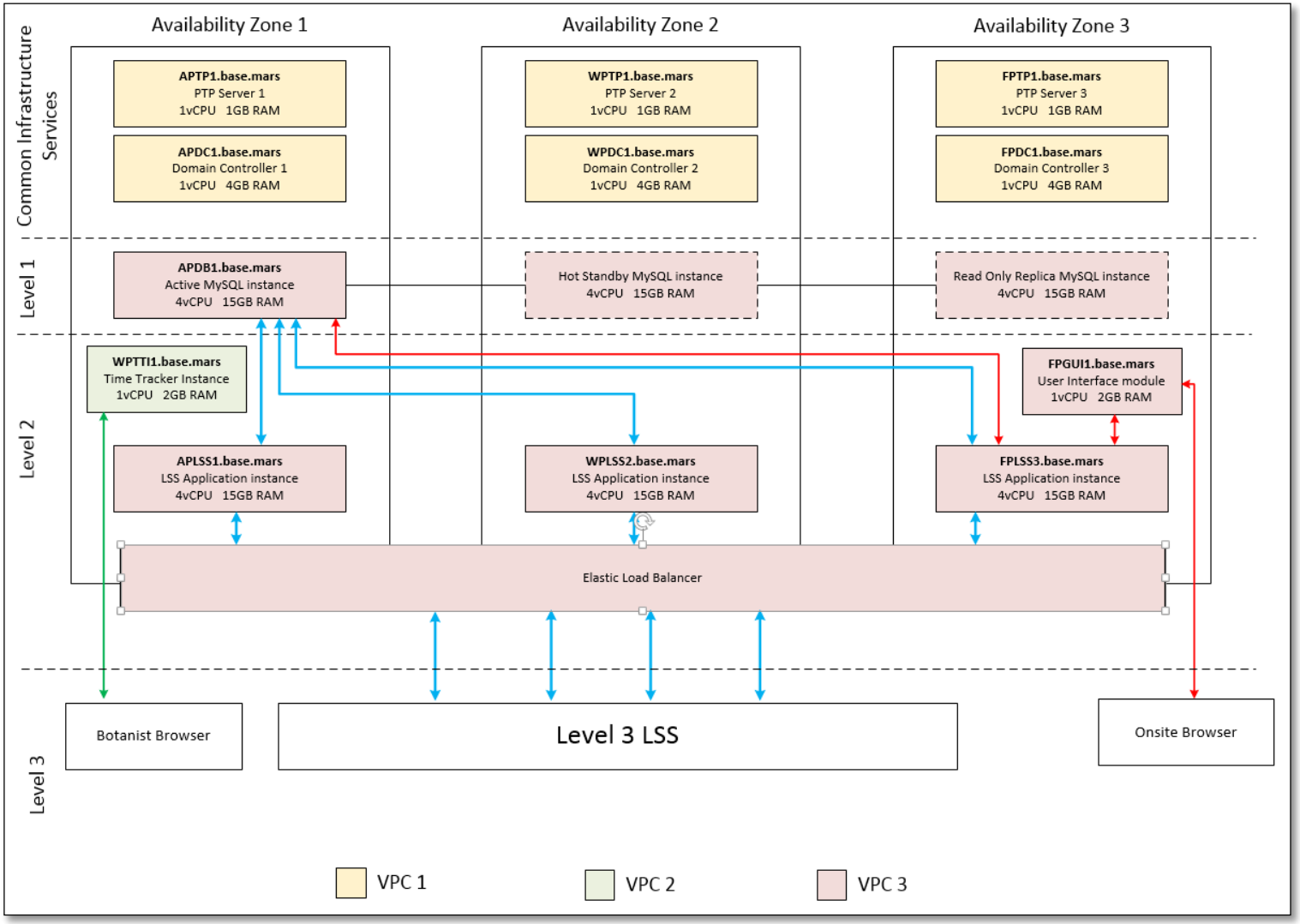
1. Availability zones and the possibility of deploying environments across multiple availability zones.
2. Auto scaling which allows new instances to be deployed automatically based on certain user defined thresholds.
3. Database hot standby and Read replicas provide simple to implement high availability protection.

Compatibility

Assuming that the designs from challenge 1 will be put in place then Zerto (the replication product chosen) already provides a way to easily a) migrate or b) failover to cloud the entire local environment using Zerto Virtual Replication for Amazon AWS.

REDFOG environment

The following section provides an overview of the application environment layout once deployed to Redfog and follows up with the mapping of the individual infrastructure agnostic components defined in Objective A onto the individual Redfog products.



Common infrastructure services

PTP server

3 Servers will be deployed (1 Grandmaster + 2 Boundary clocks) in VPC 1.

Instance	Instance Type	OS	CPU	Mem	Network	Availability Zone	Storage	AWS Backups	Notes
APTP1	t2.micro	RHEL 7.1	1 (2.5GHz)	1GB	VPC1 – Low\Moderate	Zone 1	20GB Magnetic	No	
WPTP2	t2.micro	RHEL 7.1	1 (2.5GHz)	1GB	VPC1 – Low\Moderate	Zone 1	20GB Magnetic	No	
FPTP3	t2.micro	RHEL 7.1	1 (2.5GHz)	1GB	VPC1 – Low\Moderate	Zone2	20GB Magnetic	No	

Domain controllers

3 deployed (VPC1) Domain controllers will be used instead of the AWS Directory service as this does not provide future capabilities like multi-factor authentication or domain trusts except when deploying an AD Connector however that would require an existing onsite MS Active Directory which is not available.

Instance	Instance Type	OS	CPU	Mem	Network	Availability Zone	Storage	AWS Backups	Notes
APDC1	t2.medium	WS2012 Std.	2(2.5GHz)	4GB	VPC1 – Low\Moderate	Zone 1	50GB Magnetic	No	
WPDC1	t2.medium	WS2012 Std.	2(2.5GHz)	4GB	VPC1 – Low\Moderate	Zone 2	50GB Magnetic	No	
FPDC1	t2.medium	WS2012 Std.	2(2.5GHz)	4GB	VPC1 – Low\Moderate	Zone 3	50GB Magnetic	No	

Time tracker

Based on requirements the following product will be deployed in a separate subnet (VPC2) as follows:

Instance	Instance Type	CPU	Mem	Network	Multi-AZ	Storage	AWS Backups	Notes
WPTT1	db.t2.small	1	2GB	VPC2 -Low	No	100 GB Magnetic	35 day retention	Publicly accessible: Yes

The following components will be used

- Web: nginx
- App: PHP running Symfony 2
- DB: MySQL

Life Support system

Level 2

Application layer

The LSS Application modules will be set up as part of an Auto scaling group to ensure that there are always 3 instances available.

The Auto Scaling Group will stretch across 3 Availability Zones.

Application deployment will be handled using AWS CodeDeploy.

Instance	Instance Type		CPU	Mem	Network	Availability Zone	Storage	Backups	Notes
APLSS1	m4.large	WS2012 Standard	2 (2.4GHz)	15GB	VPC – High	Multi AZ	100GB - SSD	35 day retention	300 IOPS
APLSS2	m4.large	WS2012 Standard	2 (2.4GHz)	15GB	VPC – High	Multi AZ	100GB - SSD	35 day retention	300 IOPS
APLSS3	m4.large	WS2012 Standard	2 (2.4GHz)	15GB	VPC – High	Multi AZ	100GB - SSD	35 day retention	300 IOPS

Load balancer

An Elastic Load Balancer will be created within the main VPC to balance the load across the Application instances.

The ELB will stretch **across all AZ subnets**.

Health Check Protocol: **TCP** Ping Port: **4700**

Response timeout: **5 seconds** Health Check Interval: **10 seconds** Unhealthy Threshold: **3** Healthy Threshold: **5**

ELB will be **bound to all 3 Application instances** and **Cross zone load balancing will be enabled**

User Interface

The web server for the user interface will use the following to run nginx web server.

Instance	Instance Type		CPU	Mem	Network	Availability Zone	Storage	Notes
FPGUI1	t2.small	RHEL 7.1	1 (2.4GHz)	2GB	VPC –Low to Moderate	default to Zone 3	30GB - Magnetic	300 IOPS – auto config

Level 1

MySQL 5.6 has been chosen for this environment as it allows the following:

- Allows the creation of read replicas
- Allows the read replica to be created in a separate Availability Zone (MySQL 5.6 only)

The level 1 database layer will be deployed as follows:

Instance	Instance Type	CPU	Mem	Network	Availability Zone	Storage	Backups	Notes
APDB1	db.m3.xlarge	4 (2.5GHz)	15GB	VPC – High	Multi AZ	2TB - SSD	35 day retention	MySQL 5.6.23 6000 IOPS – minimum configurable Not publicly accessible Includes Hot standby Includes read replica

Appendix A – Level 3 Data sizing Telemetry and Command traffic.

Sensors

Telemetry and status message size (including sensor ID, date\time stamp, and meter reading) is estimated at 50 Bytes per message.

Sensor type	Messaging frequency	Telemetry message size (Bytes)	Status check frequency	Status message size – return trip
Oxygen	3s	50	2s	50
Nitrogen	3s	50	2s	50
CO^2	3s	50	2s	50
Hydrogen	3s	50	2s	50
Contaminates	3s	50	2s	50
Pressure	3s	50	2s	50
Radiation	3s	50	2s	50
Heat	10s	50	2s	50
Light	60s	50	2s	50
Humidity	60s	50	2s	50

Number of sensors required

- 1 Sensor bundle per 200M^3 or per room if smaller separated rooms are used.
- Assuming that the maximum measured area would be a single 1000M^3 room.

Measured area (M^3)	Sensor bundles needed per 200M^3	Number of sensor bundles (N)	Total number of redundant sensor bundles (3N)	Daily data size per bundle (MB)	Total daily data size (MB)
1000	1	5	15	32	484

Actuators

The actuators are responsible for carrying out the command messages sent from L3 Compute modules to influence various aspects of the environment. Command and status message size (including sensor ID, date\time stamp, and meter reading) is estimated at 50 Bytes per message.

Actuator type	Messaging frequency - **estimated average**	Command message size (Bytes)	Status check frequency	Status message size – return trip (Bytes)
Light control	120s	50	2s	50
Atmosphere control	120s	50	2s	50
Vent control	120s	50	2s	50
Pressure control	60s	50	2s	50
Thermal control	30s	50	2s	50
Fire suppressing control	240s	50	2s	50
Alarm control	240s	50	2s	50

Number of actuator sets required

- Estimated at 1 actuator set per 100M^3 or per room if smaller separated rooms are used.
- Assuming that the maximum measured area would be a single 1000M^3 room.

Measured area (M^3)	Actuator sets needed per 100M^3	Number of actuator sets (N)	Total number of redundant actuator sets (2N)	Daily data size per set (MB)	Total daily data size (MB)
1000	1	5	10	15	155

References

Arnold, Douglas. "Unicast PTP." 2014. <http://blog.meinbergglobal.com/2014/04/16/unicast-ptp/>.

Texas Instruments. "AN-1728 IEEE 1588 Precision Time Protocol Time." 2013. <http://www.ti.com/lit/an/snla098a/snla098a.pdf>.