|  |
| --- |
| IALA Guideline |

1???

Resilient PNT

Edition 1.0

Document date

Revisions to this IALA Document are to be noted in the table prior to the issue of a revised document.

|  |  |  |
| --- | --- | --- |
| Date | Page / Section Revised | Requirement for Revision |
| month/year approved by Council | aaaaa | aaaaaa |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1 INTRODUCTION 7

1.1 Why is Resilient PNT needed 7

1.2 E-Navigation statement on resilience 7

2 Sources of vulnerabitilies 7

2.1 real-life examples of jamming 8

2.2 real-life examples of spoofing 8

2.3 Constellation failures 8

2.4 Space weather effects 8

2.5 cyber security 8

3 Potential impact of the vulnerabilities on AtoN operations and a vessel's ability to navigate safely 8

3.1 Effect on maritime AtoN 8

3.2 Effect on shipborne equipment 8

3.3 Effect on future systems 8

4 Potential Detection Options 8

4.1 GNSS monitoring and integrity systems 8

4.2 Risk assessment 9

4.3 example risk assessment process 9

4.3.1 Identification of primary assets 9

4.3.2 Dependent systems 9

4.3.3 Classification of risk 9

4.3.4 Area affected 9

4.3.5 Duration of event 9

4.3.6 Probability of event 10

4.3.7 Impact of event 10

4.3.8 Severity of event (based on probability and impact) 10

4.4 Alerting 10

4.5 Potential Alerting options 10

5 Mitigation 10

5.1 fail safe design 11

5.2 use of multiple PNT options 11

5.3 updates to receivers and antennas 11

6 Potential Mitigation options 11

6.1 Platform based sensors 11

6.2 GNSS 11

6.3 Augmentation 11

6.4 Terrestrial systems 11

6.5 vISUAL aTOnS 11

6.6 External support 11

6.7 cyber security 11

6.8 Integrity 12

7 Implementation 12

7.1 User receiver 12

7.2 MSR &PNT Data Processor 12

7.3 Plausibility checks 12

7.4 timing 12

7.5 Integrity monitoring 12

7.6 Training and monitoring 12

7.7 Scenarios 12

7.8 Scenario 1, vessel A, jamming threat 12

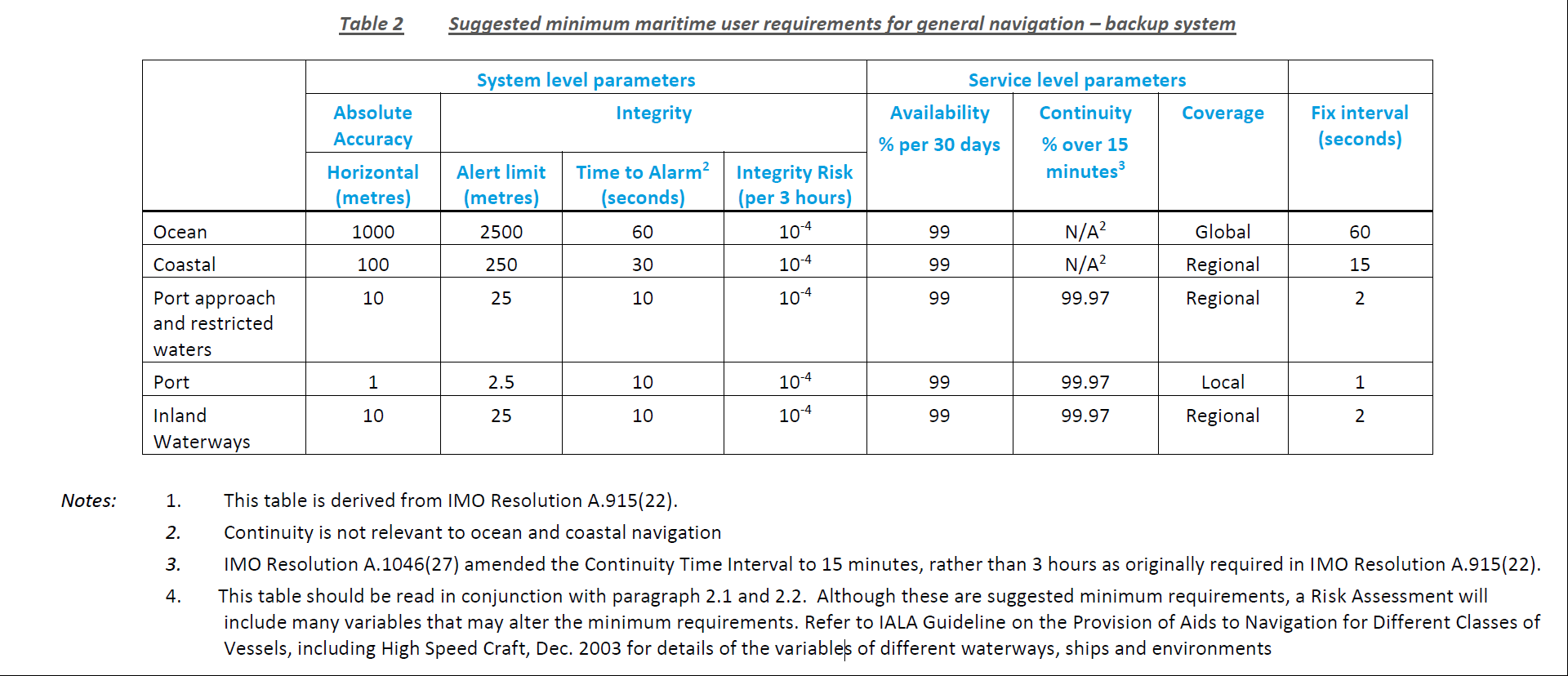
7.9 Scenario x, vessel x, threat x 12

8 DEFINITIONS 12

9 ACRONYMS 13

10 REFERENCES 13

ANNEX A SUGGESTED MINIMUM MARITIME USER REQUIREMENTS FOR GENERAL NAVIGATION – BACKUP SYSTEM 14

 14

1 Annex 2: Equipment comparisons (review of equipment and it's strengths and weaknesses) 15

ANNEX B PERMITTED COLOUR PALETTE 16

List of Tables

Table 1 Example of a table with the significant information in the first column 3

Table 2 Example of a table with the significant information in the first row 3

Table 3 Example of a table with coloured rows 3

Table 4 Example table 3

List of Figures

Figure 1 Example figure caption 3

Figure 2 Another example figure caption 3

List of Equations

Equation 1 Geographical range 3

Equation 2 Theory of Special Relativity 3

# INTRODUCTION

## Why is Resilient PNT needed

consider P, N and T.

## E-Navigation statement on resilience

The IMO Strategy for e-Navigation contains a high-level user need for data and system integrity that states:

*“e-Navigation systems should be resilient and take into account issues of data validity, plausibility and integrity for the system to be robust, reliable and dependable. Requirements for redundancy, particularly in relation to position fixing systems, should be considered.”*

In addressing the issue of Position Fixing, it can be defined as accurate and reliable electronic position, navigation and timing signals, with ‘fail-safe’ performance (probably provided through multiple redundancy, e.g. GNSS, differential transmitters, eLoran and defaulting receivers or onboard inertial navigation devices).

The increasing reliance on GNSS in all types of position finding and navigation, including position and time inputs to Automatic Identification Systems (AIS), underlines the importance of an objective consideration of possible areas of vulnerability and a consideration of measures to reduce or mitigate such effects. The need for measures to counteract vulnerability has become particularly important with the phasing out of other systems and should be taken into account in the formulation of radio-navigation plans. In the aviation context, [6] indicates that the problem of GNSS vulnerability is manageable by the retention of existing terrestrial systems (VOR/DME, NDBs) as backups. Similar consideration is given here to the maritime environment.

# Sources of vulnerabitilies

Some failure modes are common to all types of electronic navigation system. The system itself can fail, for example because of deliberate or accidental damage to the ground infrastructure. Given the military nature of present GNSS – GPS & GLONASS, it may be assumed that security levels are high and that standby equipment is provided. Experience with GPS bears this out and system failure can be assumed to be a very rare event. Security measures for Galileo are comparable to those for GPS, with the exception that the satellites are not hardened to resist electro-magnetic pulses from nuclear explosions. Failure of individual GPS satellites is not unusual, although the Mean-Time-To-Repair is less than 48 hours.

GNSS is particularly susceptible to accidental or malicious interference due to the extremely low level of the signal at the user receiver. Unintentional sources of interference or interruption in service include ionospheric variability, the effects of solar activity, and also strong signals, harmonics or intermodulation products from powerful transmitters operating in other bands or from sources close to the GNSS receiver. Intentional causes of interference include the radiating of deliberate narrow-band or broad-band jamming signals. The Volpe Report also identifies as a hazard “spoofing” in which a false GNSS signal is radiated with the intention of deceiving the user.

Failure of electronic equipment on board a vessel is also not uncommon, due to power supply failure or to a fault, temporary or permanent, in the receiver or antenna. The measures to counteract these problems are the same as for other onboard systems - the use of standby power supplies (required for SOLAS vessels), and following installation and fault-finding guidelines. Although the IMO carriage requirement is for a single Electronic Position Fixing System, it is quite common for more than one receiver for that system to be fitted to provide redundancy in the event of equipment failure.

A less commonly observed failure mode is the permanent or temporary disablement of GNSS receiver antennae subjected to high power radar transmissions, owing to microwave damage to, or saturation of, internal components [7].

The widespread adoption of GNSS has resulted in a tendency to rely heavily on electronic systems – ‘heads down’ navigation – with a perceived reluctance to use alternative means

## real-life examples of jamming

## real-life examples of spoofing

## Constellation failures

## Space weather effects

## cyber security

(GRAD report on cyber security in AtoNs & also cyber security workshop)

# Potential impact of the vulnerabilities on AtoN operations and a vessel's ability to navigate safely

## Effect on maritime AtoN

* Timing of AtoN management
* AIS timing
* DGPS operations
* AtoN guard ring monitoring
* AIS AtoN position reporting
* Synchronised lights

## Effect on shipborne equipment

(D)GNSS receivers

ECDIS

Radar

Gyro

GMDSS

etc.

## Effect on future systems

MASS

# Potential Detection Options

## GNSS monitoring and integrity systems

<include monitoring and integrity solutions, use of existing receivers to detect amonalies etc).

Services providers should consider the use of integrity information when conducting their risk assessment. Integrity information can be provided through different means.

A GNSS failure may be of such a nature that it is instantly perceived by the navigator. However, onboard systems like an Integrated Navigation System or using RAIM, GBAS, or SBAS can provide integrity warnings.

Service providers who operate IALA-DGPS infrastructure already provide integrity to the mariner. IALA and other relevant organizations have maintained appropriate recommendations for the system [14].

## Risk assessment

Understanding each system and looking deep into where time comes from.

## example risk assessment process

Need to check whether there is an IMO or BIMCO assessments available already?

### Identification of primary assets

* Capability to compute the vessel's position
* Capability to communicate vessel's position
* capability to know other vessels' positions
* capability to navigate with good weather conditions (good vis)
* capability to navigate with bad weather conditions (poor vis)
* capability to avoid collision with good weather conditions
* capability to avoid collision with poor weather conditions
* capability to arrive at destination on time (good weather)
* capability to arrive at destination on time (poor weather)

### Dependent systems

Where the risk assessment concludes that a backup system (i.e. a system ensuring continued operation, but not necessarily with the full functionality of the primary system) is necessary, suggested minimum maritime user requirements (derived from IMO Resolution A.915(22)) for such a system are listed at Appendix 1. It may however be impractical to expect backup systems to achieve some of these standards, such as global coverage in the ocean phase of navigation or metre level accuracy in the port phase. In these cases it might be necessary to navigate the ocean phase by dead-reckoning, or delay port manoeuvres until the primary navigation system is restored. The argument for a backup system may be dependent on the perceived threat to the primary system and the likely duration of primary system outages.

### Classification of risk

* GNSS outages (planned or unplanned)
* DGNSS outages (planned or unplanned)
* Interferences (unintentional)
* Attacks (spoofing, jamming)
* others

### Area affected

Phase of navigation: Ocean, Coastal, Port (or other restricted waters)

Local (<50nm), Regional (>50nm), Global

### Duration of event

Order of magnitude: Minutes, Hours, Days, Months

### Probability of event

* Very low (e.g. none in 20 years)
* Low
* Moderate
* High
* Very High (e.g. everyday)

### Impact of event

* Very low: minor delay
* Low: Delay without economic impact
* Moderate: Important delay with economic impact
* High: Accident without deaths
* Very high: Accident with deaths

### Severity of event (based on probability and impact)

## Alerting

* Raising awareness of the issues in general
* active monitoring and alarms
* Recognising interference/jamming/spoofing and reporting of incidents
* e-Navigation communications
* NtoM and Notices to shipping

## Potential Alerting options

* Training
* GNSS interference monitoring systems
* Reporting lines
* Other PNT systems

# Mitigation

This subjective risk analysis helps to identify the threats that should be addressed by the user, particularly those with high probability, high consequences and low mitigation cost. The use of GNSS receiver equipment compliant with the latest performance standards will significantly reduce susceptibility to interference.

Awareness of the problem and changes in the design of future systems such as greater radiated power, increased receiver sophistication and added operating frequencies can serve to mitigate the impact of some of the threats to some degree. However, system vulnerability, particularly to deliberate attack, cannot be fully eliminated. This message was clear and repeated several times in the Volpe Report. Modification of the present systems can reduce the effect of natural and inadvertent sources of noise and interference. Calculated attempts to jam or otherwise deny the user community the positioning and timing services of GNSS will be far more difficult to anticipate and combat. Therefore maintenance and development of adequate alternative systems is essential.

Through using an integrated PNT approach as part of the INS, it may be possible to indicate to the mariner the level of performance available (i.e. accuracy, integrity, continuity etc). Should the primary and redundant means of PNT become unavailable, the system could then indicate whether the primary or back-up requirements can be achieved, or not.

## fail safe design

## use of multiple PNT options

## updates to receivers and antennas

* hardening options
* plausibility checks

# Potential Mitigation options

## Platform based sensors

* Inertial
* Depth sounder
* gyro compass
* ePelorus

## GNSS

* Multiple constellations
* Multiple frequencies
* Integrity options

## Augmentation

* radiobeacon DGNSS
* SBAS

## Terrestrial systems

* eLoran
* R-Mode
* Locata
* STL
* radar absolute positioning

## vISUAL aTOnS

## External support

* VTS
* Sea Traffic Management (?)

## cyber security

Authentication

## Integrity

* Consistency checks (multi-constellation, multiple systems, etc)
* External support information (VTS, Aton Information, etc)
* Autonomous PNT systems (Inertial, Compass, etc)
* Integrity Algorithms
* RAIM
* Single constellation RAIM
* M-RAIM
* etc.

(This is probably all now covered above somewhere)

# Implementation

## User receiver

It is noted that appropriate backup system user equipment would probably exist in a multi-modal form with a common output terminal (an integrated receiver). Such equipment has advantages with respect to monitoring the primary navigation system for interference, and using the last reliable primary data received as an initial position source for the backup receiver.

As with existing primary navigation systems, it is considered essential that the user is notified of the status of both primary and backup navigation systems by means of obvious visual and audio alarms and messages.

The output of a backup navigation system should be in a recognised electronic format (i.e. IEC 61162) for input into electronic chart displays and GMDSS.

## MSR &PNT Data Processor

Point to the MSR and Data processor reports from previous IALA input/reports & IMO Docs.

## Plausibility checks

Receivers could be designed to take into account the general dynamics of the vessel they are fitted to as a user configured entry.

## timing

* Holdover clocks
* Synchronised timing across PNT sources

## Integrity monitoring

## Training and monitoring

## Scenarios

## Scenario 1, vessel A, jamming threat

## Scenario x, vessel x, threat x

# DEFINITIONS

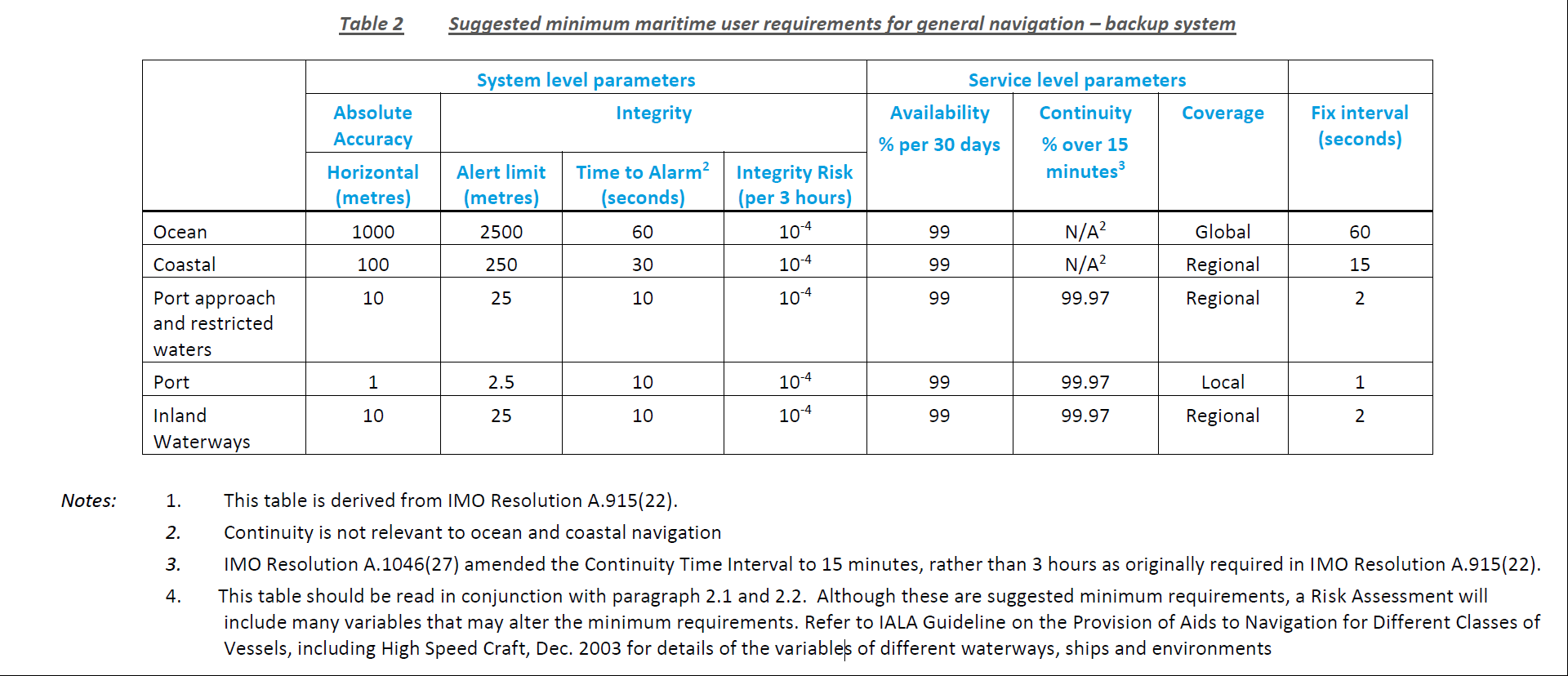
*Suggested text:* The definitions of terms used in this IALA Guideline can be found in the International Dictionary of Marine Aids to Navigation (IALA Dictionary) at <http://www.iala-aism.org/wiki/dictionary> and were checked as correct at the time of going to print. Where conflict arises, the IALA Dictionary should be considered as the authoritative source of definitions used in IALA documents.

# ACRONYMS

IMO International Maritime Organization (Acronym style)

# REFERENCES

1. Abcd
2. Efgh
4. SUGGESTED MINIMUM MARITIME USER REQUIREMENTS FOR GENERAL NAVIGATION – BACKUP SYSTEM



1. Annex 2: Equipment comparisons (review of equipment and it's strengths and weaknesses)

re GMV e-mail. A chance to list equipment and review how each system works, which threats they are able to detect and those they can't etc.

1. PERMITTED COLOUR PALETTE

The IALA colour palette is divided in 3 palettes of different level of hierarchy that has to be respected.

Corporate colours (Not shown)

IALA’s corporate colour palette is directly inspired from the colours in our logotype:

* dark blue
* white
* yellow
* gradient blue

Primary & secondary colours

The primary colours are to be applied in complement with the corporate colours.

This second level of colours gives rhythm and helps to segment our publications.

The secondary colours are used to highlight information, titles in a minor proportion only.

These colours can’t be replaced by other tints.

**PANTONE PROCESS CYAN C CMYK :** C 100

**RGB :** R 0 - G 159 - B 223

**CMYK : 50 % OF THE TONE RGB :** R 131 - G 208 - B 245

**CMYK : 50 % OF THE TONE RGB :** R 148 - G 217 - B 213

**CMYK : 50 % OF THE TONE RGB :** R171 - G 219 - B 233

**CMYK : 50 % OF THE TONE RGB :** R 178 - G 193 - B 237

**PANTONE 326C CMYK :** C 81 - Y 39

**RGB :** R 0 - G 175 - B 170

**PANTONE 7703 C**

**CMYK :** C 79 - M 2 - Y 10 - K 11

**RGB :** R 0 - G 181 - B 208

**PANTONE 660 C CMYK :** C 88 - M 50

**RGB :** R 64 - G 126 - B 201

**CMYK : 20 % OF THE TONE RGB :** R 212 - G 237 - B 252

**CMYK : 20 % OF THE TONE RGB :** R 213 - G 240 - B 237

**CMYK : 20 % OF THE TONE RGB :** R 216 - G238 - B 245

**CMYK : 20 % OF THE TONE RGB :** R 218 - G 223 - B 246

**PANTONE 258 C CMYK :** C 51 - M 79

**RGB :** R 153 - G 80 - B 159

**CMYK : 50 % OF THE TONE RGB :** R 201 - G 169 - B 208

**CMYK : 50 % OF THE TONE RGB :** R 183 - G214 - B 155

**CMYK : 50 % OF THE TONE RGB :** R 246 - G 174- B 135

**CMYK : 50 % OF THE TONE RGB :** R 157 - G 157 - B 156

**PANTONE 739 C**

**CMYK :** C 78- Y 95- K 5

**RGB :** R82 - G 174 - B 50

**PANTONE 2347 C**

**CMYK :**M 88 - Y 100

**RGB :** R 230 - G 56 - B 17

**PANTONE COOL GRAY 11 C CMYK :** K 100

**RGB :** R 87 - G 87 - B 86

**CMYK : 20 % OF THE TONE RGB :** R 232 - G 221 - B 288

**CMYK : 20 % OF THE TONE RGB :** R226 - G 238 - B 217

**CMYK : 20 % OF THE TONE RGB :** R 253 - G 224- B 208

**CMYK : 20 % OF THE TONE RGB :** R218 - G 218 - B 218

**CMYK : 10 % OF THE TONE RGB :** R 237 - G 237 - B 237

Guideline

Recommendation

Model Course

PRIMARY COLOURS

SECONDARY COLOURS