Information Paper and Guidance on Compliance and Oversight of the Mode S Interrogator IR (MSI IR)

Issue 1.1 May 2014

(COMMISSION REGULATION (EC) No 262/2009 laying down requirements for the coordinated allocation and use of Mode S interrogator codes for the Single European Sky)

INTENTIONALLY LEFT BLANK

Overview of Commission Regulation (EC) No 262/2009 (MSI IR)

Introduction

The Mode S IR (COMMISSION REGULATION (EU) No 262/2009 laying down requirements for the coordinated allocation and use of Mode S interrogator codes for the single European sky) is one of the three Interoperability Regulations that have been introduced to date that are applicable to Surveillance Systems, under the Single European Sky Interoperability Regulations. As such the UK CAA, as the national regulator provides oversight of compliance with this IR by the ANSPs since the date the IR came into force.

This paper is prepared to bring the key provisions of this IR to the attention of the Air Navigation Service Providers who will be required to demonstrate compliance with the provisions of the IR, to raise awareness of the potential impact of IC code conflicts, the symptoms, detection and mitigation mechanisms, future developments, and the methods by which the CAA would expect the ANSPs to demonstrate compliance with the provisions of this IR.

The IR is attached to this paper for information.

MODE S IC IR.pdf

Applicability

Key points of note regarding the IR are;

The IR came into force in March 2009.

Article 3; “Interoperability and Performance requirements” applies from 1st Jan 2011.

The IR lays down no requirements or responsibility on military organisations.

It applies to all Mode S Interrogators and related surveillance systems, for which at least one of the following conditions is satisfied:

- the interrogator relies, at least partly, on Mode S "all call" interrogations and replies for Mode S targets acquisition
- the interrogator locks out acquired Mode S targets in reply to Mode S all-call interrogations, permanently or intermittently, in part or in the totality of its coverage; or
- the interrogator uses multisite communications protocols for data link applications

Impact by Military Platforms

Under the UK's joint and integrated approach to Air Traffic Management, allocation of Military Interrogator Codes is co-ordinated, controlled and licensed by the National IFF/SSR Committee (NISC) There are a number of challenges that NISC face in planning the operation of Mode S in the presence of military platforms, the first is the number of fixed MoD interrogators in the UK and the second is the issue of Mobile Platforms.

MOD's procurement has lagged behind UK Civil legislation, which required Mode A/C interrogators to be switched off by 31 Dec 2011. Military Terminal ATM Interrogators are unlikely to be Mode S compliant until after 2016, as the procurement is subject to a MOD project called Marshall. Once the Military Terminal ATM interrogators are retro-fitted for Mode S, post 2016, the National IFF and SSR Committee (NISC) will have the challenge of incorporating another 16-17 sites into the UK plan, thereby depleting the IC availability and increasing the likelihood of IC conflict.

Mobile interrogators add extra complexity to the allocation of Interrogator Codes. By their very nature, mobile interrogators have no fixed position, and it is not possible to issue a lockout map for them to adhere to. This has long been recognised as an issue in the Mode S community, which led to the ICAO standard defining IC=0 as being the Interrogator Code issued to mobile platforms. The ICAO standard requires that interrogators operating IC=0 do not lockout on this code. This ensures that if two mobile interrogators have overlapping coverage, both will be able to acquire targets within the coverage of

the other interrogator. In areas where mobile interrogators are not limited to interrogator code 0 then there should be a means of monitoring the interrogator operation to ensure that non-approved codes are not used. Although this mode does not require IC coordination, it is subject to strict interrogation rate limits. Further, the usage of this mode must be kept to a minimum due to increased FRUIT.

The IR states that “A limited number of interrogator codes are reserved for exclusive use and management by military entities, including intergovernmental organisations, in particular the NATO. Mode S interrogators using these codes therefore do not need to be subject to the coordinated allocation process. Member States should however be required to take the necessary measures to ensure that the use of these interrogator codes has no detrimental impact on the safety of general air traffic.”, although it does not contain any mandatory requirements for the military sector to comply with.

It is expected that any requirements for allocating codes for the military platforms mentioned earlier will be planned and any requirement to change civil interrogator codes resulting from future military Mode S platforms will be managed robustly via the NISC process.

What are the Criteria that an Interrogator has to meet in order that this IR becomes applicable to its operation?

- Mode S Interrogator
- Not a Mode S interrogator that uses special codes listed in section 3 above and should therefore be part of the coordinated IC code allocation process.
- Must have overlapping coverage with another Mode S Interrogator (civil or military)

And

- use all-call interrogations for Mode S target acquisition in part or the totality of its coverage

or

- use lock-out protocols

or

- use multisite communication protocols (See Article 2 in the IR for definition) for data link applications

Applicability to Multilateration(MLAT) Systems

ICAO Annex 10 Volume 4 Chapter 6, contains a requirement that MLAT systems shall not use Mode S all-call interrogations. Whilst this remains the SARPS requirement, this section discusses the potential for MLAT systems to be subjected to an interrogator code conflict.

This IR is applicable to MLAT systems meeting the following criteria:

- Must be an active multilateration system
- The Interrogator/s must be Mode S capable
- The interrogator (active sensor) shall have overlap coverage area with a Mode S radar interrogator or another Mode S capable active Mode S interrogator

And

- use all-call interrogations for Mode S target acquisition in part or totality of its coverage

or

- use lock-out protocols

or

- use multisite communication protocols (See article 2 in the IR for definition) for data link applications

It is possible that MLAT systems be affected by IC conflicts provided that the above conditions are satisfied.

MLAT systems could be active, passive or a combination of the two. The passive MLAT systems are not affected by IC conflicts since no SI/II code is

required due to the passive elicitation of targets. Hence there will be no IC conflicts.

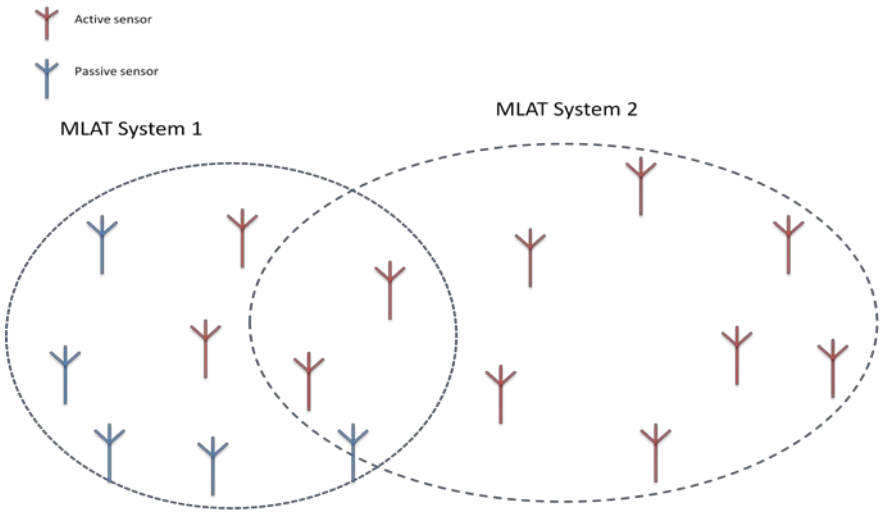
However active MLAT systems contain active interrogators within it sensor network that can interrogate transponders.

Typically active MLAT systems are normally set to transmit with IC code “0” only. Hence all of the active sensors must use code “0”. It is thought that within the same MLAT system the use of IC code “0” by all of its active sensors do not cause any code conflict as long as the system does not rely on all-call interrogations for Mode S target acquisition. However garbling or missing replies could be a potential effect.

It is believed that the use of code “0” by two independent MLAT systems that have overlapping coverage have the potential to cause code conflicts if either one of the systems use all-call interrogations for Mode S target acquisition. This is to be further investigated.

Countries such as Namibia have countrywide MLAT systems, and in the UK it is possible that such large wide area multilateration systems will be deployed in the future which requires coordinated discrete codes to be allocated in order to prevent two MLAT systems with overlapping coverage from causing code conflicts.

The example below considers two wide area MLAT systems that have overlapping coverage. if MLAT system 2 is using all-call interrogations for Mode S target acquisition and both systems were using the same IC code, it is possible for MLAT system 2 to cause lockout of Mode S targets in MLAT system 1 causing active interrogators in the MLAT system 1 in the overlapping coverage area unable to detect Mode S targets during Mode S all-call interrogations. As a consequence, the some passive sensors in MLAT system 1 may also not receive Mode S target responses, as they rely on active interrogators to elicit Mode S replies from targets.



However it has to be noted that such scenario could only occur if MLAT systems use all-call interrogations for Mode S target acquisition. Any overlapping areas with Mode S Secondary radars should also be taken into consideration.

One technique that is adopted by NISC, when issuing interrogator licences for MLAT systems in order to prevent potential impact from the active MLAT systems on other systems is to limit the interrogation rates to 1Hz per target per uplink format. This ensures that active mode operation would not take up transponder occupancy and enables an aircraft to reply to other interrogations within coverage (for example an MSSR).

Overview of the Mode S Operation and IC Conflicts

Surveillance Using Interrogators Allocated with Interrogator Codes

The purpose of a Mode S system is to be able to selectively address and interrogate Mode S capable transponders. This helps minimise the RF activity and overcome inherent issues such as FRUIT and Garbling that can often happen in a Mode A/C environment.

Interrogator Codes (IC) are necessary for the purpose of the selective operation mentioned above. Each Mode S interrogator is allocated a discrete IC which it can use to uniquely identify itself. The IC is also included in the reply from a Mode S transponder to indicate the interrogator being replied to. Each interrogator sensor should be using an allocated IC. In Europe, MICA the centralised IC allocation office, co-ordinated by EUROCONTROL, is in place to deal with requests to derive valid allocations.

Also, a Mode S transponder may be locked out to many different ICs simultaneously (up to 79 ICs if it is SI Code capable!). This requires that 79 independent timers to be available in a SI capable transponder to manage this multi-site lockout in the transponder.

As per ICAO Annex 10, there are a defined number of available ICs;

16 II-Codes (Interrogator Identifier Codes) are available, 15 of these allow ‘multisite operation’ and;

63 SI-Codes (Surveillance Identifier Codes) which function in the same way as II-Codes (multi-site operation) but are limited in their use until a high percentage (or full population) of the airborne traffic is equipped with transponder functionality that recognises SI-Code ground interrogators.

Initially the Mode S system was designed to operate with only 15 allocatable II codes. As Mode S implementation continues, in areas where there are many

radars with overlapping coverage, 15 allocatable II-Codes is not enough to support allocation of a discrete code to every sensor and it is impossible to avoid having overlapping coverage areas with another sensor using the same II-Code. This is an original design flaw of Mode S SSR.

The concept of all-call lockout is used to suppress acquisition replies from Mode S targets that have already been acquired. This controls the RF environment in the all-call period and relies on each sensor having a discrete IC in the areas for which it has lockout responsibility.

This lock-out responsibility is allocated in the form of a lock-out map which is issued by MICA along with the IC code allocation as an interrogator configuration file.

II code 14 has been reserved for shared use by test systems.

All mobile interrogators and interrogators that have not yet been assigned a discrete multi-site IC should normally use II-Code=0.

IC Allocation Process, CAA's Role and Action by ANSPs

The process of SI/II code allocation throughout the European region is managed by Eurocontrol through the MICA code allocation process which is implemented as a bi-annual cycle. CAA co-ordinates the allocation process and acts as a focal point on behalf of the NISC to co-ordinate the allocation process between Eurocontrol MICA cell and ANSPs.

The focal point for the UK currently is Alistair Abington with the back up as Colin Chesterton at the ATM Infrastructure section at the CAA SARG. ANSPs typically make an application to obtain an II/SI code and coverage map via CAA. Any application made by an ANSP has to be endorsed by the state focal point. Generally, submission for a Mode S code and coverage map is activated following the completion of the NISC approval (DAP1910) application and contact with the ANSP by the UK focal point who acts as the technical officer for the NISC.

In summary the IC code and coverage map is issued by MICA but has to be sanctioned by CAA as the UK focal point. ANSPs are not able to apply for an IC

code without approval from the NISC.

MICA web site

A web facility is available by Eurocontrol MICA cell to allow registered ANSPs to get direct access to their radar coverage map files and formal IC allocation documents including the ICD coverage file that are necessary for configuring their radars with their allocate IC codes. The MICA web facility allows the ANSP to make an application for an SI/II Mode S code. Presently, not all ANSPs are registered, therefore the exchange of the necessary files is currently done via the state focal point (CAA). This is an unnecessary step between the ANSP and the UK focal point, hence the NISC has been encouraging ANSP's operating Mode S radars to register with MICA as this allows them access to the coverage map, lock out map and code assignment which can be directly loaded into the radar by the ANSP or the radar manufacturer to ensure correct lockout/coverage operation. An ANSP can only access the files relevant to their individual operation and have limited visibility of adjacent Mode S operators' information. The MICA facility is also a web tool that provides a conflict report mechanism to help Mode S operators to investigate potential Mode S conflicts.

All state focal points have access to Interrogator Code allocation files and the relevant formal documentation of the interrogators operating within their state.

Detailed requirements that must be complied with by the ANSP and by the focal point in the IC code application and co-ordination process can be found in the "EUROCONTROL Specification for the Mode S IC Allocation Coordination and IC Conflict Management" attached below (Note: this document is under review).

http://www.eurocontrol.int/sites/default/files/content/documents/single-sky/specifications/20130116-mica-draft-spec-v0.14.pdf

enprm-13-001-ECTL-SPEC-153-MICA v0 1

With regards to a Mode S interrogator the IC code is issued by MICA in the form of a MICA IC Code Certificate. NISC also issues a NISC approval certificate to the ANSP, approving the interrogator for its operation. The MICA IC Code Certificate can be accessed by the ANSP (if registered) and the state focal point via the MICA web tool in the form of a PDF document and the coverage map

and other relevant documentation is also embedded in a downloadable zip file. If the ANSP does not have access to MICA web tool, all files issued by MICA are sent to the ANSP by the focal point.

NISC Approval Certificate and Changes to the allocated IC codes

The NISC approval certificate typically contains;

- Details of equipment subject to the approval
- Interrogation rates
- Approved Interrogation modes
- Maximum Radiated Output Power
- Operating restrictions
- Additional conditions and instructions where necessary

An example NISC approval certificate is attached below.

Interrogator
pproval Anytown .

The specific allocated IC code on the NISC approval certificate is no longer included. There are occasions where the initially allocated II/SI code or the coverage map may subject to change as a consequence of a new requirement, hence it may be necessary for an ANSP to modify the coverage map (apply some sector coverage reduction) or change SI/II code. Eurocontrol MICA cell plan these changes to accommodate new requirements, and to avoid possible conflicts as a result. The updated MICA IC Code Certificate will be available on the MICA web tool for the ANSP or the focal point to access and the Article 205 ANO approval issued by SARG for the equipment however includes the code allocation, hence the relevant ATS Inspector will be required to update the ANO approval should the code allocations change from the originally assigned code.

Such requirements to change the already issued II/SI codes or the coverage maps are informed by the MICA to the State focal point and this process is co-ordinated with the ANSP. Once the UK focal point is informed of the changes

necessary, the ANSPs are contacted and informed by the UK focal point. In certain circumstances, the ANSP will be involved through this change process. Once the changes are finalised by MICA, the UK focal point is informed and ANSPs are then contacted and informed by focal point. If the ANSP is not a registered user of the MICA web facility, the relevant documentation, new MICA Code Certificate, and relevant map files are sent to the ANSP by the UK focal point. However a change to the IC Code will not require NISC to issue a new interrogator approval certificate. A change to the NISC approval is only necessary in circumstances where the technical specification of the interrogator or its operation has changed from the original NISC approval.

The ANSP is required to implement the changes as per the MICA issued IC Code Certificate and Coverage Map, and to inform the UK focal point of the successful implementation of the change. This will then be communicated by the focal point back to MICA Cell.

However once ANSPs have registered on the MICA web site, whilst the focal point still acts as a co-ordinator between the ANSPs and the MICA cell, the ANSP can access the new IC Code Certificate and the relevant files from the MICA web site without the need to exchange this information via the focal point. Instead a new code allocation certificate will be made available on the MICA web for the ANSP to access along with any coverage map changes. MICA makes them available on the web, upon notification by the UK focal point that it has been confirmed with the relevant ANSP that it is able to make the required code change.

SARPS and Relevant European Specifications for the II/SI Code Operation

Transponders

Mode S transponders are required to have the ability to process Surveillance Identifier (SI) codes in addition to Interrogator Identifier (II) codes as prescribed in ICAO Annex10, Vol. IV, 2.1.5.1.7.1.

Ground based Mode S systems

The II/SII code operation can be found in ICAO Doc 9684 Manual on SSR Systems chapter 6 and SARPS Annex 10 Volume 4 Chapter 3 section 3.1.2.

The European II/SI code operation shall be in accordance with EUROCONTROL European Mode S Station Functional Specification SUR/MODES/EMS/SPE-01 which can be accessed via the following web link

https://www.eurocontrol.int/msa/gallery/content/public/documents/EMS-SPE-01-3.11.pdf

What Can Cause an Interrogator Code Conflict?

The ANSP or the manufacturer when implementing a Mode S system must configure the Mode S Interrogator with the correct IC and the lock-out map issued by the MICA Cell.

- Erroneous setting of the IC or the coverage map when configuring an Interrogator during initial installation or during maintenance activities (human error)
- The IC code was issued without careful planning
- The Coverage map was issued with discrepancies
- Once set in the Interrogator, corruption of IC or the coverage map configuration file in the system
- Using an IC not co-ordinated and allocated for use with a particular interrogator.

Operational Impact and Phenomena on ATC Display

In an event of a code conflict there are several factors that decide the nature of the operational impact and the severity of the impact. The phenomena on the controllers display can also vary significantly from one unit to another depending on their contextual factors. For some units the result will be a serious safety concern whereas for some units it may have no operational impact at all.

The possible consequences are;

- Loss of all Mode S targets on full or part of the display

- In a full Mode S airspace loss of all targets on display
- Potential loss of combined plots (with PSR) depending on RDP configuration and plot combination algorithm
- Loss of updated position reports from affected Mode S targets resulting in intermittent tracks or track discontinuation or lost updates whilst the history trails of Mode S targets are still being displayed on screen

It is possible that depending on the combination of the sensor types and configuration used at a particular ANSP unit, the phenomena on the ATC display to vary significantly. The resulting phenomena could present a significant risk when Mode S target positions are not updated for a considerable period of time where the position uncertainty of targets increases the risk of potential collision.

Overview of the Mode S Interoperability Regulation

Safety Assessment of Mode S Systems

Article 9 of the regulation (EC) No 262/2009 requires Mode S operators to ensure that potential interrogator code conflict hazards affecting their Mode S interrogators are properly assessed and mitigated. The following section highlights the issues that should be taken into consideration when assessing the possible impact.

Factors regarding the context in which the air traffic service is being provided.

These include, the type of airspace, traffic densities, transponder mandatory zones, type of air traffic service provided, use of safety nets, the type of Mode S data items deemed essential for the provision of air traffic services.

For example it may be that in some airspace, ANSPs require Mode S Enhanced Surveillance Data items in order to provide specific types of services. Hence potential loss of Mode S data items due to a code conflict situation would mean that the same service can no longer be provided. Also some elements like safety nets that rely on such data items to raise alerts may also be affected.

Is the coverage overlapped by only one other Mode S interrogator or are there several overlap areas?

Some ANSPs may have several overlapping areas with other Mode S interrogators within the ANSPs coverage area displayed on the screen. Others may only have one overlap area with another interrogator. Such overlap areas also differ in size. The ANSP may not always be aware of all the interrogators that have a potential overlap with the coverage area of their mode S interrogator. Depending on the number of potential overlap areas and their sizes, the phenomena on the ATC display may be such that the loss of Mode S

targets or corrupted Mode S targets is immediately recognisable, or it may not be recognisable at all to the controller.

Is there dual Mode S radar coverage over any of the areas affected?

Where there are dual layers of Mode S coverage over a particular area, each interrogator will still be using discrete interrogator codes (since they are not clustered in the UK). For this reason one interrogator may not be affected whilst the other may be affected by a code conflict. This provides mitigation at least for the area on the display where coverage is provided by the Mode S interrogator that is unaffected.

Are there any primary surveillance radars over the coverage areas of the interrogators involved in a code conflict?

Primary radar is typically the minimum surveillance capability that is necessary for providing a radar based surveillance service in the UK, although other European states seem to treat PSR as non-essential in providing services in most airspace.

PSR may provide the primary mitigation to such code conflict events. However in order to continue the service with PSR only, the PSR performance has to be such that it meets the full operational criteria and it can be relied upon.

Some units seem to have a greater reliance on SSR than PSR due to issues such as PSR performance not being satisfactory on its own. For such units the loss of SSR or any integrity issues associated with the SSR may be critical to a safe operation.

It may be worth noting that with the increased number of In-fill radars being implemented to overcome the wind farm effects on ATC radars, these In-fill radars may also contribute valuably for maintaining reliable PSR coverage at certain airfields.

Are there any Mode A/C radars over the coverage areas of the interrogators involved?

If there are any mode A/C radars they will provide an obvious mitigation against the loss of Mode S targets resulting from a code conflict. In the Ireland, the main

mitigation mechanism for code conflicts is maintaining a full Mode A/C layer in addition to Mode S coverage. However this is not a feasible mitigation mechanism to the UK, as the Mode A/C interrogators are no longer approved.

Are there any other surveillance systems (e.g. ADS-B or passive MLAT) that are in the coverage area of the Mode S interrogator and what are the capability levels of the transponders in that airspace?

Availability of other co-operative surveillance means such as ADS-B and active MLAT systems could also act as a mitigation mechanism for the code conflicts that could be induced by Mode S interrogators.

For ADS-B based systems, since no interrogation occurs, a code conflict is an irrelevant issue. However for MLAT systems the situation can be more complicated as discussed earlier.

Is there an automated IC code conflict alerter implemented?

It has come to light, that certain aviation solution providers are developing automatic detection systems in order to detect and alert to potential IC code conflicts. ANSPs both in the UK and in Europe are considering implementing such solutions. Some European states have already implemented code conflict alerter systems. An effective and reliable detection and mitigation mechanism may help reduce the potential safety risks resulting from IC code conflicts.

However some of these alerting mechanisms may not be very effective or only work in a given context whilst others may provide reliable and effective detection and alerting method. If such solutions have been implemented by ANSPs the inspectors need to assess how effective they are to the circumstances of a particular ANSP's context. (e.g. timeliness of the alerts, how effective the alerts are in capturing human attention etc)

For those units that intend to implement such automated mechanisms the conflict procedures and processes have to be designed accordingly. Where there are reliable means of code conflict detection, the need to maintain an additional layer of surveillance such as PSR or another source of co-operative surveillance data for the purposes of maintaining target detection capability may be reconsidered.

Does the site have engineers who can fix such a conflict in a relatively short period?

As for any system, the level of available on site support can make a considerable difference to the maintenance procedures and the level of mitigation necessary. Some ANSPs may not have on site engineers who can fix a code configuration issue. Also the sites that are normally manned with on-site engineers may not have support 24 hours a day. A code conflict may happen any time during the day, whilst the site is operational.

Where the code conflict was caused by another ANSP operating an interrogator that overlaps with the ANSPs interrogators' coverage, resolving the cause for the code conflict may take time since the cause is beyond the control of the ANSP whose interrogator was impacted by IC conflict.

Do the Mode-S surveillance system processors have in-built code conflict monitoring capability? If so is that capability enabled in the system?

It is unknown as to whether the manufactures are looking into incorporating Mode S code conflict detection and alerting mechanism in future Mode S capable systems. It is expected that manufacturers are fully aware of the need for the European surveillance systems to comply with the Mode S IR, realise the importance of the correct use of codes and the consequences that could occur as a result of a code conflict.

Some systems are able to perform simple test such as testing the correct use of an interrogator code with a site monitor. Some detection mechanisms that are currently being considered by various ANSPs do not seem to have the full detection and alerting capability should their systems in the case of a code conflict. If a manufacturer offers to implement a solution, ANSP and inspectors overseeing the systems, should give careful attention as to whether the solution is truly capable of detecting a code conflict in the context of the ANSPs airspace in which the system operates.

Is the affected area operationally significant to the units that have overlapping mode S coverage?

During a code conflict that happened historically it was found that no significant operational impact was caused as a result of the interrogator being affected by a code conflict due to the fact that the affected area was not operationally

significant. ANSPs must consider various overlap areas with other interrogators (if known) for their operational significance when considering the solutions for detection and monitoring mechanisms and mitigations.

Do the units use multi radar tracking to form a track for a single target from multiple radar feeds?

Some ANSPS use multi radar tracking for generating tracks displayed to the controller. A multi radar tracker associates consecutive radar observations of the same target from multiple radars to form tracks from the combination of detections for the target. Where multi radar tracker is used, the code conflict affected to one interrogator may not have a significant impact on the track output as multiple interrogators contribute to detection of the same target.

What is the RDP and display configuration at the site?

Modern surveillance systems employ different tracking algorithms and plot association/combination mechanisms. Some ANSPs may use SSR for labelling purposes only; therefore overlay the SSR information on to the PSR target reports. Some other ANSPs may actually combine PSR together with SSR and apply various algorithms in choosing the best target position. Some ANSPs may have more than one source of co-operative surveillance data which are used for forming a track whilst others may have such feeds as alternate or redundant feeds.

It is therefore important to understand these subtle differences in the processing systems used by an ANSP. For example for a system that only display tracks using 1 PSR and 1 SSR feed, how does the tracking algorithm work? Does the unit have a combined PSR and SSR system? Does it need plots from both PSR and SSR to display a track? What happens if the SSR plots were lost? Will it loose the track completely or will it still show the PSR information reliably? (e.g. it has been observed that some combined systems, in the presence of both PSR and SSR plots for the same target, ignores the PSR and displays the SSR reply as the combined)

It also came to light recently that at some airfields the engineers have optimised the system (in the case of combined PSR and SSR) to the combined situation only. Hence in the loss of PSR or the SSR signal, the system is not optimised for individual operation. This can also be a potential issue where the loss of

Mode S targets would mean that further issues are experienced.

What are essential data items to be displayed to controllers in order to provide the intended service?

Although the UK has transferred to a full Mode S environment, ANSPs do not necessarily use or require Mode S specific data items in order to provide services . This of course depends on the type of application for which the Mode S system is used (e.g. Separation services, surface surveillance, safety nets etc).

It has been found that most Mode S operators do not make use of any Mode S specific data items (other than vertical level and Identification), therefore such data items are not essential for their operation. In assessing the criticality of the risk of losing Mode S targets as a result of an IC conflict, it has to be considered whether there are other surveillance systems that can still provide the minimum data set (e.g. primary or Legacy Mode A/C radar) required in order to retain the service.

Is the system operating in MIX MIP or in full Mode S configuration?

The occurrences of IC conflicts depend on whether the Mode S system is operating in a mixed MIP configuration or in a full Mode S configuration.

ANSPs operating in mixed MIP configuration will not be impacted by a Mode S IC conflict. The reasons are that in the mixed MIP configuration Mode S targets will not be acquired by Mode S only all call interrogations, hence there will be no requirement to lock out mode S targets to subsequent Mode S all call interrogations. In the mixed MIP operation mode S targets are acquired by legacy Mode A/C all call interrogations, whereby all Mode A, C and S targets respond. This is however not a normally approved interrogator configuration in the UK.

Also, in the event of an IC conflict, where the ANSP has already identified the loss of Mode S targets on a display, mixed MIP configuration may be temporarily used for the purpose of acquiring Mode S targets for safety reasons, until the code conflict situation is resolved. However this type of mitigation is not encouraged and it is likely that the NISC certificate for the interrogator to mention any modes allowed temporarily under interrogators operating conditions. The ANSPs are typically required to inform NISC (the UK focal

point) about any such temporary measures taken and upon ceasing such operation.

Is the system using stochastic lockout override to enable override?

The lock-out override mode allows an ANSP that has an overlapping coverage area with another ANSPs responsible area of airspace to, be allowed to override the lock out status imposed by the other ANSP, thereby to have the capability to acquire any targets that have been locked out by the ANSP that locked out those targets.

It is unlikely however that any such lock-out configurations will be issued with the IC code certificates. The ANSP, if issued with such lock-out override capabilities to be enabled in certain sectors of airspace, should configure the system as per the issued data.

Lockout override status can also be used an interim measure to acquire Mode S targets in the event of a code conflict situation, where the loss of Mode S targets has already been evident. This is not to be used as a permanent measure unless issued with the NISC approval certificate or MICA Code Certificate for the mitigation of such conflicts. The NISC certificate is likely mention whether lockout override is allowed in the event of a code conflict under interrogators' operating conditions. The ANSP is required to inform NISC of such temporary use of lockout override mode and upon ceasing such operation.

What are the Detection and Monitoring Mechanisms?

The regulation ((EC) No 262/2009- Article 7) requires ANSPs to implement monitoring means for the detection of IC conflicts. Code conflicts can be detected in two ways.

- Manual Detection
- Automated detection and alerting systems

However the IR does not specify a particular type of monitoring mechanism i.e. automatic or manual as the accepted method.

Manual Detection

The key mechanism that is currently used by majority of the ANSPs in the UK to detect IC code conflicts is via controllers observations of the displayed targets, hence by manual detection.

However it is debatable as to whether, manual detection is acceptable as a mitigation mechanism. It is unlikely to work for all ANSP units as the code conflict situation may not be so obvious by manual observation on the surveillance display.

Automatic Detection

Mode S radar systems in use today do not have automated code conflict detection capability built into their automatic testing processes.

However it is possible that surveillance data analysis techniques in tools such as SASS, can be utilised to determine existence of a code conflict situation. It is believed that a SASS tool based mechanism is currently installed in Shannon centre in Ireland.

It was also found that Germany's DFS has developed a solution called MICCA – Mode S Interrogator Code Conflict Alerter where the application detects incorrect, delayed and missing Mode S target acquisitions where it will generate both optical and acoustic alert signals. Further information can be found in the attachment and the link below.

http://www.dfs.de/dfs_homepage/de/Consulting/%C3%9Cber%20uns/News%20&%20Brosch%C3%BCren/Brosch%C3%BCren/2012_micca_folder.pdf

DFS IC Code Conflict Aleerter.pdf

It appears that since the publication of this IR several state level organisations as well as independent manufacturers have focused their attention to developing solutions to monitor and alert IC conflicts. The challenge faced by many developers is that although symptoms of a code conflict can be detected real time it cannot be concluded that the symptoms were caused by an IC code conflict without further analysis.

It may be that such a solution needs to be developed in the UK, if the solutions already developed elsewhere in Europe do not provide cost-effectiveness and technical feasibility necessary for such solution to be implemented at UK airfields.

What are the Possible Mitigations?

Article 7 of the regulation requires ANSPs to implement appropriate fall-back mode of operations and mitigation mechanisms in the event of an IC conflict. Below is a list of possible mitigations that has to be considered.

- PSR only operation
- Having a Mode A/C radar layer(not in UK) or a redundant Mode S radar
- Having a different co-operative surveillance method such as MLAT or ADS-B
- Procedural control
- Effective and timely detection, alerting and correction mechanism whereby the conflict may be resolved within a relatively short period of time, without affecting the operations if caused by the ANSP themselves.

Since the use of Mode A/C interrogators are no longer approved in the UK, the applicability of other mitigation mechanisms has to be considered by ANSPs and by the CAA when considering the suitability of mitigations to each ANSP's individual circumstances. It is assumed due to the high usage of PSR in the UKs' current surveillance environment, most ANSPs would suggest PSR as being the key mitigation.

Although the use of PSR may be considered acceptable as a fall back mode of operation to mitigate code conflict hazards, this will not suffice to meet the detection and monitoring mechanisms that shall be complied with, as required by article 7 of the Mode S IR.

Furthermore where an ANSP requires Mode S data to provide a certain service PSR will not be sufficient as it only provides horizontal position information.

Have there been any Interrogator Code Conflicts in the UK?

There have been two occurrences of Mode S IC conflict in the UK since 2011. One occurrence was caused due to an erroneous code being configured into a mode S system causing the targets to remain locked out to the adjutant interrogator. However the affected ANSP maintained additional layers of surveillance which provided basic mode S data. In addition the affected area of the airspace was not an operationally significant area for the ANSP. These mitigations meant that the operational impact of the code conflict was kept to a minimum.

The second code conflict was caused by an unintentional wrong code setting by the radar engineer at the ANSP unit causing the adjutant interrogator to non-detection of Mode S targets. However use of multi radar tracking where several Mode S radars feed into a tracking system to cause a single track, meant that the SSR target data were maintained and remained visible throughout the track.

Further Reading

1. Principles of Mode S Operation and Interrogator Codes

http://www.eurocontrol.int/msa/gallery/content/public/documents/Principles%20of%20Mode%20S%20Operation%20and%20Interrogator%20Codes%202.pdf

2. Applicable SARPS on Mode S ground station operation can be found in ICAO SARPS Annex 10 Volume IV, Surveillance Radar and Collision Avoidance Systems Chapter 3 Section 3.1.2.

APPENDIX A

Regulatory Compliance Matrix

Introduction

The following table provides guidance to the ANSPs regarding how compliance with the IR can be claimed and demonstrated. The table only contains the provisions of the IR that are relevant to the Mode S operators/ ANSPs. Please note that the example responses stated in this table are for guidance only and should not be presumed as the only response possible to demonstrate compliance with the IR.

ARTICLE	ANSP RESPONSIBILITIES AND GUIDANCE MATERIAL	ANSP RESPONSE
3 Interoperability and performance requirements		
Mode S operators shall ensure that the radar head electronics constituent of their Mode S interrogators using an operational interrogator code: 3(1) support the use of SI codes and II codes in compliance with the International Civil Aviation Organisation provisions specified in Annex I point 1.	The relevant ICAO provisions are extracted In Annex 2 for ANSP reference. Depending on the type of interrogator code used by the ANSP interrogator (II or SI) the relevant requirements in ICAO Annex 10 Chapter 3 section 3.1.2.5.2.1.2 must be complied with.	ANSP Example response: The {airport} surveillance sensor (SSR) operates on a single II/SI code issued by the MICA cell. The II/SI code is used in accordance with requirements in ICAO Annex 10 Chapter 3 section 3.1.2.5.2.1.2.
3(2) support the use of II/SI code operation in compliance with the requirements specified in Annex III.	Where the Mode S interrogator uses an II code the relevant requirements in ANNEX 3 of the IR must be satisfied. Where the Mode S interrogator operates with an SI code the relevant requirements for an SI code in ANNEX 3 of the IR must be complied with.	ANSP Example response: The {airport} surveillance sensor (Mode S SSR) uses an SI code issued by MICA and support the functionality stated in Annex 3 for the Interrogators operating with an SI code. This has been assessed during Site Acceptance Test Report {reference}.
4 Associated procedures for Mode S operators		
4(1) Mode S operators shall only operate an eligible Mode S interrogator, using an eligible interrogator code allocation, for this purpose,	In order to operate a Mode S radar in the UK ANSPs must have applied for and obtained; An approval to operate a Mode S interrogator in	ANSP Example response: {airport} operates an eligible Mode S interrogator for

from the competent Member State.	the UK from the NISC (NISC Interrogator Certificate) Obtain an IC allocation and lock-out coverage map from the MICA Cell (MICA Interrogator Code Certificate) ANO Approval from the SARG Aeronautical Radio Licence issued under the Wireless Telegraphy Act 2006 The process for applying for a NISC Interrogator Certificate can be found in CAP 761. DAP Form 1910 must be used for application to operate a Mode S Interrogator in the UK. ANSPs must use the MICA Web portal for the application and obtaining of MICA Interrogator Code Certificate and relevant lockout coverage map files. The application for obtaining an IC is available on the MICA web site (Mode S IC Application Form). ANSPs should follow the EUROCONTROL Specification for the Mode S IC Allocation Coordination and IC Conflict Management. (Eurocontrol Spec -153) http://www.eurocontrol.int/sites/default/files/content/documents/single-sky/specifications/20130614-mica-spec-v1.0.pdf	which approval was granted by the NISC. See the NISC Interrogator Certificate attached. Mode S IC allocation issued by the MICA Cell has been correctly implemented in the interrogator. {airport} has implemented the assigned interrogator code and lockout map, and fully in accordance with the operating conditions attached to the NISC Interrogator Certificate and the MICA Interrogator Code Certificate No {xxxx}. The interrogator code and lockout map configuration is defined in the Software Configuration File ref {xxxx}.

	The application for obtaining a WTA Act Licence should be made on the form SRG1417.	
4(2) Mode S operators intending to operate, or operating, an eligible Mode S interrogator for which no interrogator code allocation has been provided, shall submit an interrogator code application to the competent Member State in accordance with the requirements specified in Annex II, Part A	The co-ordination process between the ANSP, UK MICA State Focal Point and MICA Cell for IC allocation is described in Section 4 of the above guidance document. ANSPs must register themselves on the MICA Cell and use the Mode S IC Application on the MICA portal, fill the form correctly and completely. The application will then be sanctioned by the UK State Focal Point (CAA) and be passed on to MICA for issuing an interrogator code.	ANSP Example response: {airport} has obtained the NISC approval to operate the Mode S interrogator {NISC Interrogator Certificate No. xxx}. Application to obtain an IC was submitted via the MICA Cell portal. The requirements in Annex II Part A were complied with and all items as required in Annex II were submitted as part of the application.

4(3) Mode S operators shall comply with the key items of the interrogator code allocations they receive as listed in Annex II, Part B.	Evidence must be available that the radar has been configured in compliance with the conditions and settings specified on the MICA Interrogator Code Certificate. Evidence must be available for each item (from (a) to (i) listed in Annex II Part B.	ANSP Example response: All provisions listed in the MICA Code Allocation files were correctly implemented in the {airport} Mode S Interrogator. Surveillance and Lockout coverage restrictions applied as per the code certificate. The correct and current IC implemented as per the current interrogator code allocation. Implementation sequence followed as specified by MICA Cell. All operational restrictions in the interrogator code allocation have been correctly implemented in the system.
4(4) Mode S operators shall inform the competent Member State at least every six months of any change in the installation planning or in the operational status of the eligible Mode S interrogators regarding any of the interrogator code allocation key items listed in Annex II, Part B	Six-monthly reporting is not necessary providing that no change has been made to the operational status of Mode S interrogators. Changes regarding any elements specified in Annex II Part B, stated in the MICA Code Allocation must be informed to the MICA State Focal Point. Internal procedures must be in place to communicate the changes to the state focal point in an effective manner. Any changes with regard to elements stated in the	ANSP Example response: Any changes affecting the items of the IC allocation listed in Annex II Part B will be communicated to the MICA UK State Focal Point. Airport operational procedure {xxx} section {xxx} specifies the process. Any planned change in the operational status of the Mode S interrogator will be reported to the National IFF/SSR Committee in accordance with the national

	NISC certificate must be reported In accordance with CAP 761: If a change to the technical or operational details of an interrogator is required, applicants are to reapply to NISC in accordance with CAP 761. Should the requirement for an interrogator, for which an approval has already been granted, cease to exist then the NISC Secretariat and the MICA State Focal Point must be informed by the operator.	procedures laid down in CAP761 and the associated {airport} process {reference}
4(5) Mode S operators shall ensure that each of their Mode S interrogators uses exclusively its allocated interrogator code.	The Interrogator, at any given time, must only be operating with the allocated interrogator code as specified in the current MICA Code Certificate. Procedures must be in place to allocate the current interrogator code including when the code allocation is changed, effectively in accordance with the implementation sequence.	ANSP Example response: The {airport} procedure {xxx} for deploying interrogator codes details checks to be made and recorded on site to ensure that the interrogator codes and lockout map have been correctly implemented and are in line with the IC allocation.
6 Associated procedures for air traffic service providers		
Air traffic service providers shall not use data from Mode S interrogators operating under the responsibility of a third country if the interrogator code allocation has not been co-ordinated.	Where an ANSP intends to use surveillance data from a country other than from within their state, the ANSPs must only use Mode S data from interrogators where the Code Allocations have been co-ordinated as per the MICA Code Allocation process and state co-ordination	ANSP Example response: N/A – At the present time {airport} does not make use of any radar data from third countries which are Mode S capable.

	process. Where there is a requirement to use surveillance data from a 3rd country, the ANSPs should contact the MICA UK state focal point to ensure such sensors operate on MICA allocated IC codes.	
7 Contingency requirements	In addition to the guidance provided in this table, the requirements in CAP 670 SUR 05 must be complied with.	
7(1) Air Traffic Service Providers shall assess the possible impact on air traffic services of interrogator code conflicts, and the corresponding potential loss of Mode S target surveillance data from the impacted Mode S interrogators, taking into account their operational requirements and available redundancy.	The risk assessment should take into account the items identified in section 9 of the ANSP guidance material published in the CAA interoperability web site. ANSPs must assess this risk and where considered safety significant, provide mitigation(s) (for example changing the configuration to an alternative and approved configuration or making use of alternative surveillance systems).	ANSP Example response: A hazard identification and risk assessment has been conducted by the {airport} to assess the impact of potential interrogator code conflict situation at the airport. This is recorded in {airport} safety case (reference/section}.
7(2) Unless the potential loss of Mode S target surveillance data has been assessed to have no safety significance, Mode S operators shall: Implement monitoring means to detect interrogator code conflicts caused by other Mode S interrogators impacting eligible Mode	Information presentation on the display HMI may consider potential benefits of highlighting overlapping regions.	ANSP Example response: The {xxx} airport will monitor interrogator code conflicts by manual detection. The {airport} ATE department will be alerted to any potential interrogator code conflicts following a

S interrogators they operate on any operational interrogator code.		suspected or detected code conflict. Controllers have been made fully aware of manual detection of interrogator code conflict situations and possible impact on the display. The {airport} PSR has coverage over the Mode S overlap area, hence any persistent loss of Mode S replies will be seen as a primary target. This does not impact separation services at the {xxxxx} airport or other services since no Mode S specific data items are used at present for any surveillance applications. Interrogator Code Conflict procedure is documented in {reference procedure for monitoring, addressing and resolving interrogator code conflicts}
7(2) (b) ensure that the interrogator code conflict detection provided by the implemented monitoring means is achieved in a timely manner and within a coverage that satisfy their safety requirements;	Where a PSR or any additional surveillance layer (a second SSR feed, MLAT data or ADS-B data) is not available loss of Mode S targets may not be manually detectable. Having additional secondary surveillance layer that provides Mode S data items may also mask the interrogator code conflict between the interrogators in question. Unless surveillance data items specifically obtained by the interrogator	ANSP Example response: The hazard identification and risk assessment documented in Safety Case {xxxxx} section {reference}. The airport does not operate in SSR only mode, but in combined mode with PSR or in PSR only mode. Hence no automatic interrogator code conflict detection mechanism is implemented since PSR

	were missing from the ATC display the loss of Mode S data hence interrogator code conflict may be hidden, However this ensure Mode S targets are detected(position information is known) and hence may provide adequate mitigation.	provides sufficient level of mitigation for potential loss of Mode S targets arising from an interrogator code conflict whenever service is provided.
7(2) (c) identify and implement as appropriate, a fallback mode of operation to mitigate the possible interrogator code conflict hazards on any operational code, identified in the assessment referred to in paragraph 1;	Where the risk of potential interrogator code conflicts are mitigated by having an additional surveillance layer (such as PSR/WAM), the ANSP may consider the operation with other surveillance systems as the fall back mode of operation.	ANSP Example response: In the event of possible interrogator code conflict {airport} ATC will use procedures described in: {MATS Part 2 reference}
7(2) (d) ensure that the implemented fallback mode of operation does not create any interrogator code conflict with other Mode S interrogators referred to by the interrogator code allocation plan.	Typical fallback modes of operation are unlikely to use different interrogator codes (unless an alternate Mode S interrogator is used as fall back mode) and therefore interrogator code conflicts in fallback modes would not be expected.	ANSP Example response: Approved fallback modes of operation do not rely on IC allocations and therefore interrogator code conflicts are not expected.
7(3) Mode S operators shall report any identified interrogator conflict involving an eligible Mode S interrogator they operate on any operational interrogator code to the competent Member State and shall make available, through the IC allocation system, the related information to the other Mode S operators.	ANSPs must report any conflicts to the National IFF/SSR Committee and to the UK MICA state focal point. The conflict reporting procedure is included in the EUROCONTROL Specification for the Mode S IC Allocation Coordination and IC Conflict Management.	ANSP Example response: In accordance with CAP761, interrogator conflict situations will be reported to the National IFF/SSR Committee using a DAP 1913 form and will also be reported via the MICA Online Tool.

	Any interrogator code conflicts must be reported to the NISC using DAP form 1913. In addition the ANSPs must also report the code conflict situation on the reporting mechanism available on the MICA web tool. The ANSP should also endeavour to inform the CAA Regional Inspectorate of the situation. ANSP must ensure that ANSP contact details are provided and kept up to date on the MICA web site and with the UK state focal point for the purposes of reporting and coordinating code conflicts.	
9 Safety requirements		
9(1) Mode S operators shall ensure that potential interrogator code conflict hazards affecting their Mode S interrogators are properly assessed and mitigated.	ANSPs are to ensure proper assessment of potential interrogator code conflicts and take appropriate mitigations. ANSPs must assess and mitigate the risk of code conflicts.	ANSP Example response: Refer to 7(1)
9(2) 2. Member States shall take the necessary measures to ensure that any changes to the existing systems and	ANSPs are to ensure a safety assessment, including hazard identification, risk assessment and mitigation is performed preceding any	ANSP Example response: {airport} has carried out a safety, risk and hazard

associated procedures referred to in Article 1(2) or the introduction of such new systems and procedures are preceded by a safety assessment, including hazard identification, risk assessment and mitigation, conducted by the parties concerned.	changes to existing systems or procedures ANSPs must conduct a safety assessment including hazard identification, risk assessment and mitigation before implementing any changes to systems and procedures. Such changes may include implementing a fall back mode of operation, additional procedures, or system changes such as implementation of a code conflict detector.	assessment addressing the change to the {airport} SSR/related procedures. This is reported in {airport} safety case {section/reference}
10 Conformity assessment		
10 Before issuing an EC declaration of conformity or suitability for use as referred to in Article 5 of Regulation (EC) No 552/2004, manufacturers of constituents of the systems or their authorised representatives established in the Community, of the systems referred to in Article 1(2) of this Regulation shall assess the conformity or suitability for use of those constituents in compliance with the requirements set out in Annex IV, Part A to this Regulation.	ANSPs must ensure that manufacturers provide an EC Declaration of Conformity or Suitability for Use in accordance with Article 5 of the Interoperability Regulation, and that the Declaration includes a statement of conformance with the Annex IV Part A of regulation 262/2009.	ANSP Example response: {airport} has ensured that its SSR constituent manufacturer has provided an EC declaration of conformity or suitability for use in accordance with Article 5 of the Interoperability regulation for incorporation with the related ANSP Interoperability Technical File.
11 Verification of systems		
11(1) Air Navigation Service Providers which can demonstrate or have demonstrated that	ANSPs must ensure that test activities including Factory Acceptance Testing, Site Acceptance	ANSP Example response:

they fulfil the conditions set out in Annex V shall conduct a verification of the systems referred to in Article 1(2) in compliance with the requirements set out in Annex VI Part A	Testing and Flight Checks demonstrate compliance with Annex VI Part A and that these tests have been witnessed and signed off by an ANSP representative who is independent and impartial. Where no notified body is used for this purpose, the ANSP must provide evidence that they meet requirements set in Annex V of this regulation.	The {airport} procedures for system verification ensure that the assessments performed by {airport} are independent and impartial in accordance with Annex V. {airport} has the following procedures in place which demonstrate the conformity of these systems with the interoperability, performance, contingency and safety requirements of this Regulation in an assessment environment that reflects the operational context of these systems {detail procedures and tests carried out}.
11(2) Air Navigation Service Providers which cannot demonstrate that they fulfil the conditions set out in Annex V shall subcontract to a notified body a verification of the systems referred to in Article 1(2). This verification shall be conducted in compliance with the requirements set out Annex VI, Part B	ANSPs must use a Notified Body if the ANSP cannot fulfil the verification requirements themselves, primarily in respect of competence, independence and impartiality.	ANSP Example response: Not applicable as the {airport} procedures for system verification ensure that the assessments performed by {airport} are independent and impartial in accordance with Annex V.
12 Additional requirements		
12(1) Mode S operators shall ensure that their personnel in charge of the implementation of interrogator code allocations are made duly	ANSPs are to ensure their personnel involved in interrogator code implementation are adequately trained and duly aware of the regulation.	ANSP Example response: Personnel involved with the implementation of IC

aware of the relevant provisions in this Regulation and that they are adequately trained for their job functions.	ANSP must ensure that the personnel that implement code allocations are competent for the task and necessary training provided. Where the ANSP relies on manufacturers or a third party to implement code changes or adjust system configurations as necessary, evidence shall demonstrate that this does not result in an increased risk in a code conflict situation.	allocations have been made aware of the Regulation and have received training through a variety of technical courses. Additionally those responsible for onsite implementation are assessed by the {airport} engineering manager for competency.
12(2) Mode S operators shall: a) develop and maintain Mode S operations manuals, including the necessary instructions and information to enable their personnel in charge of the implementation of interrogator code allocations to apply the provisions of this Regulation;	ANSP must develop and maintain operations manuals (including manufacturers' technical manuals) and procedures with regard to implementation of interrogator codes, to ensure that Interrogators can be configured in accordance with the conditions specified on the MICA Code Certificate and NISC approval.	ANSP Example response: {airport} maintains Mode S operation and maintenance manuals and information to enable the personnel in charge of the implementation of interrogator code allocations to apply the provisions of this Regulation.
(b) ensure that the manuals referred to in point (a) are accessible and kept up-to-date and that their update and distribution are subject to appropriate quality and documentation configuration management;	ANSPs must ensure that the manuals and procedures are accessible and up to date and subject to appropriate quality and document control. Established methods should already be in place as required in Annex 1 3.2 and 3.3 of the Common Requirements Regulation ANSPs must ensure that the operations and maintenance manuals are adequately controlled and distributed.	ANSP Example response: {airport} Mode S operation and maintenance manuals are controlled under the {airport} quality system and available to the authorised {airport} operators and maintenance personnel. The maintenance procedure is subject to configuration control and is readily accessible when required.

(c) ensure that the working methods and operating procedures required for the implementation of interrogator code allocations comply with the relevant provisions specified in this Regulation.	ANSPs must ensure that working methods and procedures comply with the regulation.	ANSP Example response: The {airport} working methods and operating procedures required for the implementation of interrogator code allocations are controlled under the {airport} quality system and comply with the relevant provisions specified in this Regulation
13 Entry into force and application	This regulation entered into force and became applicable for all Mode S interrogators on 19 April 2009. Article 3 applies from 1 January 2011. ANSPs must comply with this Regulation from 19 April 2009 except Article 3 which applies from 1 January 2011.	None

APPENDIX B

ICAO Requirements Mentioned in the IR

ICAO Provisions stated in Annex 1 paragraph 1

3.1.2.5.2.1.2 IC: Interrogator code. This 4-bit (10-13) uplink field shall contain either the 4-bit interrogator identifier code (3.1.2.5.2.1.2.3) or the lower 4 bits of the 6-bit surveillance identifier code (3.1.2.5.2.1.2.4) depending on the value of the CL field (3.1.2.5.2.1.3).

3.1.2.5.2.1.2.1 Recommendation — It is recommended that whenever possible an interrogator should operate using a single interrogator code.

3.1.2.5.2.1.2.2 The use of multiple interrogator codes by one interrogator. An interrogator shall not interleave Mode S-only all-call interrogations using different interrogator codes.

Note — An explanation of RF interference issues, sector size and impact on data link transactions is presented in the Aeronautical Surveillance Manual (Doc 9924).

3.1.2.5.2.1.2.3 II: Interrogator identifier. This 4-bit value shall define an interrogator identifier (II) code. These II codes shall be assigned to interrogators in the range from 0 to 15. The II code value of 0 shall only be used for supplementary acquisition in conjunction with acquisition based on lockout override (3.1.2.5.2.1.4 and 3.1.2.5.2.1.5). When two II codes are assigned to one interrogator only, one II code shall be used for full data link purposes.

Note— Limited data link activity including single segment Comm-A, uplink and downlink broadcast protocols and GICB extraction may be performed by both II codes.

3.1.2.5.2.1.2.4 SI: Surveillance identifier. This 6-bit value shall define a surveillance identifier (SI) code. These SI codes shall be assigned to interrogators in the range from 1 to 63. The SI code value of 0 shall not be used. The SI codes shall be used with the multisite lockout protocols (3.1.2.6.9.1). The SI codes shall not be used with the multisite communications protocols (3.1.2.6.11.3.2, 3.1.2.7.4 or 3.1.2.7.7).

ICAO Provisions stated in Annex 1 paragraph 2

3.1.2.6.10.2 Capability reporting protocol. The data structure and content of the data link capability report registers shall be implemented in such a way that interoperability is ensured.

Note 1— Aircraft capability is reported in special fields as defined in the following paragraphs.

Note 2— The data format of the registers for reporting capability is specified in the Technical Provisions for Mode S Services and Extended Squitter (Doc 9871).

3.1.2.6.10.2.1 Capability report. The 3-bit CA field, contained in the all-call reply, DF equals 11, shall report the basic capability of the Mode S transponder as described in 3.1.2.5.2.2.1. 3.1.2.6.10.2.2 Data link capability report. The data link capability report shall provide the interrogator with a description of the data link capability of the Mode S installation.

Note —The data link capability report is contained in register 1016 with a possible extension in registers 1116 to 1616 when any continuation will be required.

3.1.2.6.10.2.2.1 Extraction and subfields in MB for data link capability report

3.1.2.6.10.2.2.1.1 Extraction of the data link capability report contained in register 1016 .The report shall be obtained by a ground-initiated Comm-B reply in response to an interrogation containing RR equals 17 and DI is not equal to 7 or DI equals 7 and RRS equals 0 (3.1.2.6.11.2).

3.1.2.6.10.2.2.1.2 Sources of data link capability. Data link capability reports shall contain the capabilities provided by the transponder, the ADLP and the ACAS unit. If external inputs are lost, the transponder shall zero the corresponding bits in the data link report.

3.1.2.6.10.2.2.1.3 The data link capability report shall contain information on the following capabilities as specified in Table 3-6.

3.1.2.6.10.2.2.1.4 The Mode S sub network version number shall contain information to ensure interoperability with older airborne equipment.

3.1.2.6.10.2.2.1.4.1 The Mode S sub network version number shall indicate that all implemented sub network functions are in compliance with the requirements of the indicated version number. The Mode S sub network version number shall be set to a non-zero value if at least one DTE or Mode S specific service is installed.

Note — The version number does not indicate that all possible functions of that version are implemented.

3.1.2.6.10.2.2.2 Updating of the data link capability report. The transponder shall, at intervals not exceeding four seconds, compare the current data link capability status (bits 41-88 in the data link capability report) with that last reported and shall, if a difference is noted, initiate a revised data link capability report by Comm-B broadcast (3.1.2.6.11.4) for BDS1 = 1 (33-36) and BDS 2 = 0 (37-40). The transponder shall initiate, generate and announce the revised capability report even if the aircraft data link capability is degraded or lost. The transponder shall ensure that the BDS code is set for the data link capability report in all cases, including a loss of the interface.

Note —The setting of the BDS code by the transponder ensures that a broadcast change of capability report will contain the BDS code for all cases of data link failure (e.g. the loss of the transponder data link interface).

3.1.2.6.10.2.2.3 Zeroing of bits in the data link capability report

If capability information to the transponder fails to provide an update at a rate of at least once every 4 seconds, the transponder shall insert ZERO in bits 41 to 56 of the data link capability report (transponder register 1016).

Note — Bits 1 to 8 contain the BDS1 and BDS2 codes. Bits 16 and 37 to 40 contain ACAS capability information. Bit 33indicates the availability of aircraft identification data and is set by the transponder when the data comes from a separate interface and not from the ADLP. Bit 35 is the SI code indication. All of these bits are inserted by the transponder.

3.1.2.6.10.2.3 Common usage GICB capability report. Common usage GICB services which are being actively updated shall be indicated in transponder register 1716.

3.1.2.6.10.2.4 Mode S specific services GICB capability reports. GICB services that are installed shall be reported in registers 1816 to 1C16.

3.1.2.6.10.2.5 Mode S specific services MSP capability reports. MSP services that are installed shall be reported in registers 1D16 to 1F16.

APPENDIX C

Obtaining ANSP/Operator Access to MICA Web Tool

The ANSPs are required to register to the MICA Cell web tool. As part of this process, it is also expected that all relevant CAA SRG Engineering Inspectors will also gain access to MICA web tool. This will enable the ANSPs to access any files related to their Mode S allocations including the MICA Code Certificate and the Coverage Maps.

Please follow the following process to obtain access;

Access the Eurocontrol Onesky Web page (see the link below) and register to the OneSky Online

https://extranet.eurocontrol.int/http://onesky1.eurocontrol.int/amserver/UI/Login?gw=extranet.eurocontrol.int&org=eurocontrol&goto=http%3A%2F%2Fprisme-oas.hq.corp.eurocontrol.int%2Fmica%2FIndex.action

If you are not already a OneSky Online member, register online via the link provided on the website

Once registered to OneSky Online and access details received via e-mail to log on to OneSky Online, e-mail MICA State focal point requesting access to the MICA Cell Online portal.

The focal point to e-mail the relevant Eurocontrol MICA Cell authority requesting to grant access to the relevant Engineering Inspector.

Access details then passed to the operator directly by the Eurocontrol contact or via focal point.

Then the MICA Portal can be accessed via the following link;

https://extranet.eurocontrol.int/http://prisme-oas.hq.corp.eurocontrol.int/mica/Index.action

or

by clicking the Mica Application option on under the “Online Services” as shown on the left hand side of the OneSky Online page.


EUROCONTROL
| Exit OneSky Online |
OneSky Online
The EUROCONTROL extranet: a secure collaborative environment for Stakeholders.
Welcome to OneSky Online
Roshani DHARMASIRI
24 April 2013 11:08
Edit my account
Subscribe for online services
Online Services
Event booking
Mica Application
New to Supplier portal
OneSky Teams
OneSky Teams (new platform)
Welcome
WIFI at Haren
We are pleased to announce that visitors to EUROCONTROL in Haren (Belgium) can now take advantage of a wireless hotspot service covering the lobby and all ground floor conference rooms in the Da Vinci building.
You can use your OneSky Online Login ID and password to access this service.
Wireless Services
available in
HQ Conference Centre
From this page, the EUROCONTROL Extranet portal, and using the various links shown in the left column you can do the following:
EUROCONTROL Web Presence